Version 6.1.0

MessageWay User's Guide and Reference

Progress®

MessageWay®

Document History

Part Number	Product Name	Date
MW420-570	MessageWay User's Guide and Reference	11/2006
MW421-570	same as above	12/2007
MW421-570	same as above	02/2008
MW422-570	same as above	02/2009
MW500-570	same as above	02/2010
MW500-570	same as above	08/2010
MW500-570	same as above	11/2010
MW500-570	same as above	01/2011
MW550-570	same as above	07/2011
MW600-570	same as above	11/2011
MW610-570	same as above	05/2013
MW610-570	same as above	11/2013
MW610-570	same as above	05/2015
MW610-570	same as above	03/2016
MW610-570	same as above	08/2016
MW610-570	same as above	03/2017
MW610-570	same as above	12/2018
MW610-570	same as above	12/2020

Copyright

This document was published on Wednesday, March 24, 2021 at 10:20.

MessageWay User's Guide and Reference

This page intentionally blank.

Contents

Configuring Receipt Monitor 671

Monitoring System Activity 691

Controlling Message Traffic 701

Finding Configurations and Messages 733

Options 893

MessageWay Manager Menus, Tools and Tasks 915

Appendix Licenses 1367

Index 1405

This page intentionally blank.

Introduction

Typographical Conventions

Before you start using this guide, it is important to understand the terms and typographical conventions used in the documentation.

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information
Special Bold	▪ Items you must select, such as menu options, command buttons, or items in a list ▪ Type of note ▪ Values you must type, constants
Emphasis	▪ Titles of books ▪ Important word ▪ Captions for figures ▪ Variable expressions such as parameters
`Monospace`	Code samples
CAPITALS	Names of keys on the keyboard. for example, SHIFT, CTRL or ALT.
KEY+KEY	Key combinations for which the user must press and hold down one key and then press another, for example, CTRL+P or ALT+F4.

The following formatting is used to explain command syntax:

Formatting convention	Type of Information
Special Bold	Values you must type, constants
Emphasis	Variable expressions such as parameters
Monospace	Code samples
[ ]	Brackets enclose optional parameters
{ }	Braces or curly brackets enclose required parameters
|	Bar separates options within brackets or braces
(...)	Indicates options may repeat

Purpose of MessageWay

MessageWay® provides advanced managed file transfer (MFT) to control and secure message traffic. It handles high-performance, high-volume throughput. Base MessageWay includes services to support most business requirements. MessageWay also provides optional services for those whose business needs exceed what is included with the base product.

MessageWay is scalable and portable using modular design and industry standard, multi-threading technology. The modular design for message transport allows us to extend interoperability as industry needs change. Multi-threading allows users to scale the number of processes based on current requirements.

The purpose of this information is to provide users of MessageWay a perspective on what the application does, how it works, and how users control messaging using the MessageWay Manager.

Audience for MessageWay

The audience for this information comprises those who must:

- Manage MessageWay
- Support MessageWay as it interfaces with the operating system
- Support applications that run within MessageWay, such as the translator
- Support MessageWay external applications, such as perimeter servers
- Support the ODBC database used to store MessageWay information
- Configure MessageWay and support the corporate trading partners
- Ensure MessageWay daily operations

Content

The MessageWay Manager user interface includes extensive online help for field-level topics and conceptual practices. The objective of the field-level, *What's This* type of help, is to provide specific information about how a field is used. By design, the field-level help is limited, so complete reference information appears in reference sections. The objective of the conceptual information is to provide a perspective on what the application does, how it works, and how users may control messaging using the Manager.

Information is presented beginning with basics, then concepts and tasks, and finally reference.

When You Need to:	Look Here:
Find out about: ▪ Technical support ▪ Related resources ▪ MessageWay features ▪ Product Platform Support ▪ Ideas for planning, administration and basic security ▪ Basic startup and shutdown procedures	***Getting Started*** (on page 19)
Understand the basics of: ▪ How MessageWay works ▪ The major components ▪ What the MessageWay Manager does ▪ How to set up security for users ▪ How to control messaging	***Understanding MessageWay*** (on page 35)
Configure MessageWay Internal Servers: ▪ Messaging Server ▪ Service Interface ▪ User Server ▪	***Configuring MessageWay Internal Servers*** (on page 79)
Configure MessageWay Perimeter Servers: ▪ AS2 Interface ▪ FTP Perimeter Server ▪ Remote Execution Perimeter Server (RES) ▪ SFTP Perimeter Server ▪ SFTP Proxy Server	***Configuring MessageWay Perimeter Servers*** (on page 113)
Configure users and user and object security to access: ▪ Users ▪ Adapters and services ▪ Locations	***Configuring Users and User and Object Security*** (on page 371)
Configure adapters and services: ▪ Assign threads ▪ Start automatically ▪ Set specific parameters	***Configuring Adapters and Services*** (on page 399)
Configure environment for remote access: ▪ Create single and multi-server environments for MessageWay Managers ▪ Access environments from a MessageWay Manager	***Configuring Remote Access Environments*** (on page 443)

When You Need to:	Look Here:
Configure locations: ▪ Create locations ▪ Associate with an adapter or service ▪ Specify message storage ▪ Specify retry strategy ▪ Specify delivery strategies ▪ Specify notification strategies ▪ View examples for specific types of locations	***Configuring Locations*** (on page 453)
Monitor receipt of critical messages	***Configuring Receipt Monitor*** (on page 671)
Monitor system activity: ▪ Multiple MessageWay environments ▪ Services ▪ Adapters ▪ Locations	***Monitoring System Activity*** (on page 691)
Control message traffic: ▪ Stop and start adapters or services ▪ Hold and release locations and output messages ▪ Cancel messages ▪ Resubmit and redirect messages	***Controlling Message Traffic*** (on page 701)
Find configurations or message information: ▪ Messages ▪ Archive Messages ▪ Locations ▪ Location Schedules ▪ Receipt Schedules ▪ Rules ▪ Users ▪ Sessions	***Finding Configurations and Messages*** (on page 733)
Maintain message information: ▪ To archive or delete messages ▪ To maintain the message archive ▪ To retrieve messages from archive	***Maintaining Message Information*** (on page 783)

When You Need to:	Look Here:
Understand how to use MessageWay utilities: ▪ Administration activities ▪ Import MessageWay configurations ▪ Export MessageWay configurations ▪ Generate shared key files for security when using the Remote Execution Server (RES) ▪ Maintain restart records ▪ Trace communications for adapters, services or internal MessageWay servers	***Using MessageWay Utilities*** (on page 829)
Troubleshooting support: ▪ List of error messages and probable causes ▪ Tracing adapter, service, MessageWay server activity ▪ Restart options for interrupted processing ▪ Recommendations to tune a MessageWay system	***Troubleshooting*** (on page 843)
Configure other options, such as: ▪ Maker/Checker to enhance user security by requiring two users to make changes to user configurations ▪ Translation service for EDI-type message translation and routing	***Options*** (on page 893)
Find general reference information for: ▪ Menus ▪ Tools ▪ Tasks	***MessageWay Manager Menus, Tools and Tasks*** (on page 915)
Find complete reference information for all pages of all windows.	***MessageWay Manager Reference*** (on page 925)

Features

MessageWay uses a common architecture for interfaces to various types of input and output through adapters and services. The architecture provides scalability, so users can add instances of a particular adapter or service to handle increased traffic. The functionality provides user security and traceability of all message processing. Other services provide translation, rules to route messages based on content, compression and monitoring time-critical messages. The features that are part of base MessageWay are called base features. Options that may be purchased separately are called optional features.

The areas of service within MessageWay are:

- MW Director™, which is a centralized management interface that allows users to configure message processing requirements and track and control all messaging activity
- MW Transport™, which controls all file transfers with client and server communications protocols
- MW Integrator™, which provides applications secure access to core MessageWay services
- MW Translator™, which provides any-to-any translation for high-volume, highly complex file information and supports industry standards, such as, XML, X12, EDIFACT, IFX, and SWIFT, among others.

Base Features

MessageWay includes the following base services:

Base Feature	Description
Archive program	Provides archive and delete functions to maintain the SQL database, the Message Store and the Archive Retrieve Message Store
Archive Maintenance program	Provides maintenance of the archive zip files and the archive directory
Archive Retrieve program	Provides ability to retrieve messages that have been archived
Compression service	Compresses (zips) and uncompresses (unzips) message content, supporting both zip and gzip formats
Custom IO adapter	Provides I/O interface between MessageWay and external applications
Custom Processing service	Provides service interface between MessageWay and external applications
Manager	User interface for MessageWay environments that is installed on Windows and/or on one or more remote Windows workstations. Provides secure access for users from the manager, with optional LDAP authentication
Disk Transfer adapter	Provides input from and output to disk locations on the local network
Distribution List service	Delivers messages to multiple recipient locations simultaneously
E-mail adapter	Provides e-mail POP3 and SMTP client services
FTP adapter	Provides File Transfer Protocol (FTP) client services and encryption and decryption services using Transport Layer Security (TLS) and Secure Socket Layer (SSL)
FTP SSL Perimeter Server	Provides secured access to MessageWay using File Transfer Protocol (FTP) with Transport Layer Security (TLS) and Secure Socket Layer (SSL) from an FTP client. The FTP perimeter server includes an FTP SSL Proxy Server for the FTP adapter.
SFTP Adapter	SFTP Adapter provides secured client access using SSH to an external SFTP or SCP capable server
SFTP Proxy Server	SFTP Proxy Server provides secured access for the SFTP adapter outside

Base Feature	Description
	a firewall to an external SFTP or SCP capable server
SFTP Perimeter Server	Provides secured access using SSH to MessageWay from an external SFTP client
Receipt Monitor service	Monitors locations to determine when the required number of messages have been received based on receipt schedules
Rules Processing service	Routes messages based on various properties or content of the message
Scheduling service	Provides control over message input and output using various types of location schedules, and provides monitoring services for Receipt Monitor and the Remote Execution Server option
Service Interface	Controls access to MessageWay from external services, such as AS2, FTP, SFTP and the Web Client, with optional LDAP authentication
User Server	Controls access to MessageWay from the Manager
Web Client	Provides secure access to MessageWay through a Web browser using this client (released separately)

Optional Features

The following options may be purchased separately. For features supported by the Translation Runtime Module (TRM), refer to the *MW Translator Workbench User's Guide and Reference*.

Option	Description
Additional instances of adapters and services	▪ You may have more than one instance of an adapter or service
AS2 Interface	▪ Provides support for the AS2 protocol. Includes both an AS2 adapter to send messages from MessageWay to an external AS2 server and an AS2 server that controls message delivery to and from MessageWay over HTTP or HTTPS
AWS S3 Adapter	▪ Provides support for storing and retrieving any amount of data on Amazon Web Services (AWS) using Simple Storage Service (S3). **NOTE:** This option is documented separately in the document *MessageWay MWAWSS3 User's Guide and Reference*.
Content Validation (anti-virus support)	▪ Provides content validation with anti-virus support using an embedded anti-virus engine
Convert service	▪ Provides character conversion based on character set (code page)
Maker/Checker	▪ Provides additional checking security for additions, changes or deletions

Option	Description
	to user security settings
MQ Adapter	▪ Provides client access using the WebSphere MQ client to exchange messages with an MQ server.
Remote Execution Server	▪ Provides secure remote execution of programs. The Remote Execution Server (RES) will use scripts in a custom service location to execute programs on remote servers, report the status of execution and monitor the status of remote servers
Translation service	▪ Provides translation between different formats, typically between proprietary and EDI standards. ▪ Provides routing with or without translation. ▪ Provides additional logging and reconciliation services to manage acknowledgments

What's New

The core functionality is the same. Many features are now included in the base product and new functionality has been added to both base and optional components.

Beginning with version 5, MessageWay has some new terminology. Additionally, in version 6.0, the MessageWay Dashboard has been renamed to MessageWay Manager.

New Features

The following features are new for MessageWay. The new features are arranged by subversion, newest first, for example, the 6.1 features list precedes earlier features lists.

Base Product Enhancements

MessageWay 6.1 includes the following enhancements to the base product features.

Enhancement	Description
Import/export utilities	▪ Option to export all configurations, including users, rules and schedules ▪ Option to export all location configurations, in both the Locations folder and the File System folder
Seamless upgrades	▪ Users can upgrade directly to MessageWay version 6.1 from versions 5.0, 5.5 or 6.0

Enhancement	Description
Pre-defined security user groups for reporting	▪ Pre-defined user groups added with additional rights to support business requirements for a reporting and analysis tool that will be available separately and later. The new groups include Report Administrators, Report Developers, Report Managers, and Report Users
Disable the resubmit function	▪ Option in User Server configuration file to disable the command to resubmit messages for an entire system
Support Unicode	▪ MessageWay supports Unicode encoded characters and strings from the Basic Multi-Lingual plane.
Hierarchical Message Store view for FTP and SFTP clients	▪ New types of locations, stored in the File System folder, allow MessageWay FTP and SFTP Perimeter servers to present lists of messages to clients in a hierarchical view and allow clients to control their own hierarchies. These locations and messages are maintained separately from the traditional MessageWay locations stored in the Locations folder.
Suppress the *canceled* and *downloaded* directories for FTP and SFTP clients	▪ For messages in the traditional Locations folder, a new parameter *SuppressCanceledAndDownloadDirs* in the configuration files for the FTP and SFTP perimeter servers allows you to hide the *canceled* and *downloaded* directories from view of an FTP or SFTP client. This makes the view from these clients more similar to that of the hierarchical message store and typical FTP servers.
Reference remote file name from the FTP Adapter with a MessageWay token	▪ A new MessageWay token %remotefile% allows you to reference an external file name with pre and post transfer commands. Among other things, this allows you to rename and move files on a remote system.

MessageWay 6.0 includes the following enhancements to the base product features.

Enhancement	Description
Centralized Logging	▪ Provides ability to view MessageWay logs, including the perimeter server logs and all audit and trace logs, from a single place in the user interface. ▪ Consolidates all of these logs in one place, the MessageWay Server database, for easier administration. There is little or no performance impact as a result of this change.
Enhanced Audit Logging	▪ Provides more visibility into data change details (such as who made the change, what change was made, and when was it changed) ▪ Tracks changes by capturing exactly what values were changed and the previous values before being modified.

Enhancement	Description
Tamper-Evident Audit Logs	▪ Ensures all transfer and processing actions and errors are logged to MessageWay's cryptographic tamper-evident database and any changes to the audit logs will be visible and easily detected. ▪ Allows an organization to provide to auditors a provably unaltered history of MessageWay administrative activity.
Interoperability with Tectia SFTP – "Tectia Ready"	▪ Ensures that MessageWay supports transfers between itself and Tectia Client and Tectia Server, a very common SFTP client and server.
FIPS-only Transfer Mode	▪ Ensures that both the sender and recipient are using FIPS compliant cryptography. ▪ Ensures if either the sending or receiving party is not using FIPS compliant algorithms then the transfer fails and an error message will be sent to both parties.
FIPS 140-2 Compliant Cryptography	▪ Federal Information Processing Standards (FIPS) Level 1 compliance for encryption using the HTTPS, FTPS, and SFTP transfer protocols.
Enhanced Role-based Administration and Access	▪ Improvements include adding more granularity to the number of actions that can be granted as roles and also the capability to restrict who has access to what data. ▪ Ensures rules for users overrides those defined for roles (groups). With this approach, the administrator can always tailor profiles that best fit the user and the roles or groups.

MessageWay 5.5 includes the following enhancements to the base product features:

Enhancement	Description
MessageWay Manager able to monitor multi-system environments	▪ Provides ability to monitor up to 4 MessageWay systems from a single environment ▪ Supports find queries for multi-system environments ▪ Integrates silently with single-system environments
Integrity checks for MessageWay FTP Adapter	▪ Provides file integrity, a component of guaranteed delivery. Integrity checking allows MessageWay FTP adapters to confirm that a file they uploaded to or downloaded from a third-party FTP server contains the same data on both source and destination, regardless of format ▪ Currently supports MD5 and SHA1 algorithms, configurable for each listener
Restartable transfer for FTP and SFTP (optional) adapters	▪ Provides checkpoint-restart capability to resume file transfers that were interrupted. Large files can resume a transfer already in progress.

Enhancement	Description
Delete original file on completed transfer	▪ Provides a method to remove content files from Message Store immediately after they have been successfully delivered to their destination, rather than using the archive system ▪ Retains tracking information, because detail records remain
Rescan file information to assure completeness	▪ Provides another mechanism to ensure that MessageWay does not try to transfer files which are incomplete
Password support for zipped and unzipped files	▪ Provides a highly inter-operable mechanism to exchange files with people using Zip desktop software as well as scripted Zip utilities ▪ Does not apply to gzip format
Key management system for client security keys	▪ Provides ability to generate and import SSH client keys using the manager. ▪ Keys are stored in MessageWay database

MessageWay 5.0 includes the following enhancements to the base product features.

Enhancement	Description
Data content storage options	▪ Disk or Database storage now available ▪ Encryption in conjunction with the database storage option ▪ Compression in conjunction with the database storage option
LDAP user authentication	▪ Supports authentication using Open LDAP and Active Directory for all MessageWay interfaces including access from the MessageWay Manager as well as through the MessageWay perimeter servers
Enhanced search capabilities	▪ FIND categories by messages, locations, schedules, rules, and users ▪ Sessions to FIND categories by messages, locations, schedules, rules, and users ▪ Wildcard searching ▪ Retain search criteria (refine search) ▪ Configurable *messages returned* count
Managed file transfer enhancements	▪ Ability to view and identify messages by a file name, which remains consistent throughout the life-cycle of the message
MWFTP Adapter	▪ Enhanced pre and post transfer commands ▪ Restartable feature allows restart from a check-point rather than the beginning of the file
Vista and Windows 7 support for manager	▪ MessageWay Manager is now supported on Microsoft Vista and Windows 7
Custom columns selection and ordering	▪ Ability to select and re-order columns of information displayed on a message list
Rules service	▪ Supports double-byte characters ▪ Enhanced detection of content type

Enhancement	Description
Location scheduling	▪ Daily, weekly, monthly, yearly and absolute schedules ▪ Allow schedule triggers to perform actions: Input or Execute now, Hold Location,Hold Outputs, Release Location, Release Outputs
Receipt Monitor schedules	▪ Daily, weekly, monthly, yearly and absolute schedules ▪ Repeating notifications at configurable intervals
Retry strategy	▪ Multi-level retry strategies ▪ Reroute message after failed delivery
Inbound transfers	▪ View and/or act upon (cancel) inbound transfers (receiving/uploading messages) ▪ Receipt failure notifications
Unique polling intervals by location (mailbox)	▪ Configuration of polling timing by location ▪ Single-threaded processing by location , sender, recipient, classid, filename and more
User management	▪ Enhanced user and password management ▪ Enforcement of complex passwords
Enhanced tracing	▪ Dynamic configuration without stopping adapter/service ▪ Traces are stored in the database for easy access ▪ Utility to filter, output to file and maintain logged information
Multiple recipients	▪ All recipient fields now support multiple entries
Property window change status visible in manager	▪ Most property windows now display the date and time that a configuration was created or modified and by whom

Product Option Enhancements

MessageWay 6.1 includes the following enhancements to product options.

Enhancement	Description
MessageWay SFTP Perimeter Server	▪ Supports traditional SFTP directory view of messages ▪ Supports anonymous login

MessageWay 6.0 includes no enhancements to product options.

MessageWay 5.5 includes the following enhancements to product options.

Enhancement	Description
FTP Perimeter Server supports protocol-level integrity checks	▪ Provides file integrity, a component of guaranteed delivery. Integrity checking allows third-party FTP clients to confirm that a file they uploaded to or downloaded from a MessageWay server contains the same data on both source and destination, regardless of format ▪ Currently supports MD5 and SHA1 algorithms, configurable for each listener
FTP Perimeter Server supports resume in streaming restart mode	▪ Allows external FTP clients to resume transfers of large files without restarting the transfer from the beginning ▪ Includes block mode and streaming restart
FTP Perimeter Server supports anonymous login	▪ Allows external clients to connect to MessageWay using anonymous login
FTP Perimeter Server supports forced binary transfers	▪ Provides ability to force binary mode to avoid mixed-mode transfers that can cause transmission failures

MessageWay 5.0 includes the following enhancements to product options.

Enhancement	Description
MWFTP Perimeter Server	▪ Allow remote users to change passwords

New Product Options

MessageWay 6.1 includes the following new product options:

Enhancement	Description
AWS S3 Adapter	▪ Provides support for storing and retrieving any amount of data on Amazon Web Services (AWS) using Simple Storage Service (S3). **NOTE:** This option is documented separately in the document *MessageWay MWAWSS3 User's Guide and Reference*.
Web Client	▪ Provides access to MessageWay from an internet browser, and includes necessary features to upload and download messages, as well as see related messages and view document reconciliation status for output created by MW Translator. This options is available MessageWay 6.1 HF01. **NOTE:** This option is documented separately in the document *MessageWay Web Client Installation and Configuration, MessageWay Web Client Release Notes* and the Web Client online help.

MessageWay 6.0 as of hotfix 03 includes the following new product option.

Enhancement	Description
Web Client	Provides access to MessageWay from an Internet browser to review information about messages and to upload and download messages. There are two modes available from a browser: one that uses the Web Client Java applet (Java mode) and one that does not (non-Java mode). The Java applet provides more features for uploads and downloads than the mode that does not use Java. Both modes provide the following functionality: ▪ HTTPS transfer method between the browser and the Web Client ▪ Controls user access to information as defined in MessageWay ▪ Allows users to change their passwords ▪ Allows users to access other mailboxes as rights permit ▪ Allows users to search for messages by filename or class ID, with a wild card option ▪ Allows users to upload and download messages NOTE: Non-Java mode is limited to a maximum file size of 250 MB. ▪ Shows results of transfers by category: Available, Downloaded, Canceled, Uploaded ▪ Supports different file formats for uploaded and downloaded messages: ▪ Upload: Binary or Text ▪ Download: Binary, Text or Zip (file is compressed before downloading) ▪ Displays related messages and reconciliation information when appropriate The Java applet provides the following additional file transfer functionality: ▪ Supports transfer of very large files: Maximum file size is controlled by the operating system and available system resources ▪ Multi-file transfers ▪ Supports restart for upload and download: ▪ From a check point (streaming restart) for binary files only ▪ From beginning of file for all other supported file formats ▪ Shows progress of transfer and status information ▪ Automatically updated detail lists ▪ Ability to pause, resume and cancel transfers ▪ Displays additional error information for failed transfers

MessageWay 5.5 includes the following new product options.

Enhancement	Description
Content Validation	▪ Provides integrated anti-virus capabilities against all unencrypted files and messages that pass through the MessageWay system. ▪ Uses real-time data integration with an embedded anti-virus engine. ▪ System-level setting applies to all files that come into or that are generated within MessageWay ▪ Quarantines, and optionally deletes, bad messages
MQ Adapter	▪ Provides an integrated client to exchange files with IBM WebSphere Message Queue (MQ) servers version 6 or 7
SFTP Adapter	▪ Provides an integrated client to exchange files with external SSH servers using SFTP or SCP. ▪ Optionally communicates through SFTP Proxy Server.
SFTP Proxy Server	▪ Provides access to SFTP external servers through this proxy server connection

MessageWay 5.0 includes the following new product options.

Enhancement	Description
MWConvert service	▪ Performs character set conversions ▪ i18n support ▪ Supports most major single and multi-byte character sets
Maker/Checker	▪ Enforces independent approval of additions, changes or deletions made to user configuration records from the MessageWay Manager

New Terminology for MessageWay 5

MessageWay terminology has changed in version 5.0. The interface has remained the same, so users of previous versions of MessageWay will understand the differences quickly. For a bit of help, the following tables relate the new terms to the old terms. New terms for features that do not exist in earlier versions are followed by the word, *new*.

The first table describes some basic terminology.

Terms for Version 5.0	Terms for Pre-5.0 Versions
MessageWay Dashboard	MessageWay Control Console (MCC)
MessageWay Translator, MWTranslator	Edikit

Terms for Version 5.0	Terms for Pre-5.0 Versions
Adapter	I/O Gateway
Service	Processing Gateway
Location	Mailbox

The following terms are labels for the system monitor counts:

Terms for Version 5.0	Terms for Pre-5.0 Versions
Service	Processing
Adapter	I/O
Mailbox	Other

The following terms are folder names visible in the Dashboard (MCC):

NOTE: the **Views** folder has been removed. A more robust Find/Search option is available to locate configurations of various kinds, so you don't have to visually search for locations (mailboxes).

Terms for Version 5.0	Terms for Pre-5.0 Versions
Adapters/Services	Gateways
Locations	Mailboxes
Adapter	I/O Gateway
Service	Processing Gateway
Location	Mailbox
Master Location Schedules (new)	N/A
Receipt Monitor Schedules	Receipt Monitor
Rules Processing	Routing Tables
Servers (new)	N/A

The following terms are specific to locations (mailboxes) and rules processing (routing tables):

Terms for Version 5.0	Terms for Pre-5.0 Versions
Location (generic)	Mailbox
Service location	Processing mailbox
Site	I/O mailbox
Mailbox	Pickup mailbox

Terms for Version 5.0	Terms for Pre-5.0 Versions
Rules processing profile	Routing table
Process rule	Routing definition

The following is a list of services (processing gateways):

Terms for Version 5.0	Terms for Pre-5.0 Versions
Compression (MWCompress)	Compression (MWayCompression)
Conversion (new option) (MWConvert)	N/A
Custom Processing (MWCustomProc)	Custom Processing (MWayProc)
Distribution List (MWDistList)	Distribution List MWayDL
Rules Processing (MWRules)	Routing (MWayRoute)
Translation (MWTranslator)	Edikit (MWayEdikit)

The following is a list of adapters (I/O gateways):

Terms for Version 5.0	Terms for Pre-5.0 Versions
MWAS2 (new)	N/A
Custom IO (MWCustomIO)	Custom IO (MWayIO)
Disk Transfer (MWDisk)	Disk Transfer (MWayDiskTransfer)
E-mail (MWEmail)	E-mail (MWayEmail)
FTP (MWFTP)	FTP (MWayFTP)

New Terminology for MessageWay 6

The following terminology has changed for these versions of MessageWay 6.

The following terms changed for version 6.1.

Terms for Version 6.1	Terms for Pre-6. Versions
MessageWay Web Client	MessageWay Web Interface

The following terms changed for version 6.0.

Terms for Version 6.0	Terms for Pre-6. Versions
MessageWay Manager	MessageWay Dashboard

Getting Started

This section provides the basic information about MessageWay:

- Resources available to you, such as customer support and related documentation
- Product platform support
- Advice on planning and administration
- How to start up and shut down the system

Technical Support

The MessageWay Technical Support hub is an information and diagnostic center available for customers to:

- Obtain advice on proper product installation, configuration, and operation
- Report any product problems and receive timely resolutions
- Request a software enhancement
- Request software updates
- Inquire about software release contents and status
- View publications
- See how to contact Technical Support
- See hours of availability for Technical Support

To visit the MessageWay Technical Support hub, please follow the below link:

https://www.progress.com/support/messageway

The Technical Support Web site is available 24/7, portions of which require a valid Progress ID. If you have not already done so, you can follow the instructions in the following URL to obtain a valid Progress ID:

https://knowledgebase.progress.com/articles/Article/how-to-create-a-progress-id

Related Resources

There are several different types of related and supporting information available in varying formats and locations. Please also review the following:

Title	Level	Description
Progress Support Web site	(Web site for additional technical support) Beginner to advanced	https://www.progress.com/support/messageway This is the Technical Support web site.
MessageWay Knowledgebase	Beginner to advanced	https://knowledgebase.progress.com This web site contains answers to frequently asked questions.
MessageWay Release Notes	Beginner to advanced	https://docs.ipswitch.com/en/messageway.html This web site contains all documentation, including release notes about the new features of MessageWay and problems fixed in maintenance releases.
MessageWay Installation Guide	(For installation and initial testing) Beginner to advanced	Document available as a .pdf file; contains instructions on how to install MessageWay and conduct initial tests.
MessageWay Service Interface API	Advanced	Document available as a pdf file; describes how to write a programmatic interface to access specific MessageWay services.
MessageWay Web Client Installation and Configuration	(For installation and initial testing) Beginner to advanced	Document available as a .pdf file; contains instructions on how to install and configure MessageWay Web Client and conduct initial tests.
MW Translator Workbench User's Guide and Reference	(For EDI testing) Beginner to advanced	Document available as a .pdf and help file; contains instructions to use the Workbench program to configure standards, trade agreements, acknowledgment profiles, document maps, and partners.
MW Translator Workbench Tutorial	(For testing) Beginner to advanced	Document available as a .pdf and help file; contains complete instructions for users to create EDIFACT and X12 translation examples as they familiarize themselves with the Workbench.
MW Translator Operator Guide and Reference	(For production) Beginner to advanced	Document available as a .pdf file; contains instructions to use the Operator program to configure partners, implement and use auditing and reconciliation, and transfer files from a test environment to a MessageWay production environment.

Title	Level	Description
MW Translator User Exits Programming Manual	C or C++ programmer	Document available as a .pdf file on installation medium, contains instructions to write code for one of the seven types of possible user exits.
MW Translator API Reference and Programming Manual	Advanced programmers	Document available as a .pdf file, contains information to allow programmers to integrate the software into an application to provide EDI type validation, translation and acknowledgments.

Product Platform Support

MessageWay version 6.1 supports various operating systems, databases, browsers, distributed architectures and includes some dependencies.

Operating Systems for MessageWay Servers

MessageWay version 6.1 supports the following operating systems for the MessageWay servers and perimeter servers:

- Red Hat Enterprise Linux (RHEL) v6.x and v7.x
- Solaris 10
- SUSE Linux Enterprise Server (SLES) v11 and v12
- Windows Server 2012 Standard R2 64-bit edition
- Windows Server 2016 Standard
- Windows Server 2019 Standard

The following systems are *not* supported for MessageWay 6.1:

- SUSE v10.x
  (If you want to run on SUSE v10.x, please contact MessageWay support.)
- Windows Server 2003

NOTE: No international versions of operating systems are required for MessageWay software.

Operating Systems for MessageWay Manager, MW Translator Workbench and Operator Program

MessageWay version 6.1 supports the following operating systems for the MessageWay Manager and the MW Translator Workbench and Operator Program:

- Windows Server 2019 Standard
- Windows Server 2016 Standard
- Windows Server 2012 Standard R2 64-bit edition
- Windows 10 SP1 32-bit and 64-bit editions (clients run here as legacy 32-bit applications)
- Windows 7 SP1 32-bit and 64-bit editions (clients run here as legacy 32-bit applications)

NOTE: No international versions of operating systems are required for MessageWay software.

Operating Systems for MessageWay Remote Execution Server (RES)

MessageWay version 6.1 supports the following operating systems for the MessageWay Remote Execution Server (RES):

- Windows Server 2019 Standard
- Windows Server 2016 Standard
- Windows Server 2012 Standard R2 64-bit edition
- Windows 10 SP1 32-bit and 64-bit editions (clients run here as legacy 32-bit applications)
- Windows 7 SP1 32-bit and 64-bit editions (clients run here as legacy 32-bit applications)
- Solaris v10
- Red Hat Enterprise Linux v5.6, 6.x and 7.x
- SUSE v11 and v12
- IBM AIX V6 6.1 and V7 7.1

The following systems are *not* supported for MessageWay 6.1:

- SUSE v10.x
  (If you want to run on SUSE v10.x, please contact MessageWay support.)
- Windows Server 2003

NOTE: No international versions of operating systems are required for MessageWay software.

Databases and Database Drivers for the MessageWay Server

MessageWay version 6.1 supports the following databases for the MessageWay Messaging Server.

Microsoft SQL

- Microsoft SQL Server 2012 Enterprise Edition on 64-bit platforms, clustered and standalone
- Microsoft SQL Server 2016 Enterprise Edition on 64-bit platforms, clustered and standalone
- Microsoft SQL Server 2019 Enterprise Edition on 64-bit platforms, clustered and standalone
- MessageWay supports both Windows authentication and SQL authentication

MySQL

- MySQL 5.5.x on 32-bit and 64-bit platforms

- MySQL 5.7.x on 32-bit and 64-bit platforms
- Standalone only (no clusters)
- UNIX/Linux operating systems

Oracle

- Oracle Database 10g Release 2: 10.2.0.1—10.2.0.5, clustered and standalone
- Oracle Database 11g Release 2: 11.2.0.1, clustered and standalone
- Oracle Database 12c Release 2: 12.2.x, clustered and standalone
- Oracle Database 19c Release 3: 19.3.x, clustered and standalone (Linux only)
- UNIX/Linux operating systems

The following table shows the relationship between databases and operating systems.

Database	Solaris 10	RHEL 6.x	RHEL 7.x	Suse 11	Suse 12	Win2012R2 x64	Win2016x64	Win2019 x64
MSSQL_2012_x64						x		
MSSQL_2016_x64							x	
MSSQL_2019_x64								x
MySQL_5.5_x32 & x64	x	x		x				
MySQL_5.7_x32 & x64			x		x			
Oracle 10g & 11g	x	x		x				
Oracle 12c & 19c			x		x			

The following table describes the driver versions for the various databases and platforms that have been tested with Unicode.

IMPORTANT: All drivers must be 32-bit for 64-bit databases.

Database	Platform	Drivers Tested
MSSQL 2012	Windows Server 2012	Native client 11.0
MSSQL 2016	Windows Server 2016	ODBC Driver 13 for SQL Server
MSSQL 2019	Windows Server 2019	ODBC Driver 17 for SQL Server

Database	Platform	Drivers Tested
MySQL	Linux	General release version of MySQLConnector 5.1.8
MySQL	Solaris 10	General release version of MySQLConnector 5.1.8
Oracle 10g & 11g	Linux	DataDirect 8.0 Oracle Wire Protocol
Oracle 12c & 19c	Linux	DataDirect 8.0 Oracle Wire Protocol
Oracle 10g & 11g	Solaris 10	Contact Technical Support

NOTE: Oracle is not supported on Windows.

Distributed Architectures

MessageWay version 6.1 supports the following distributed architectures:

- MessageWay Server (Failover or “Active/Passive”) HA based on Microsoft Cluster Services
- MessageWay Perimeter Servers (Webfarm or “Active/Active”) HA supported on all supported OS platforms

Critical Dependencies

Critical dependencies include versions of software that users must install prior to installing MessageWay software, or it will not install or operate successfully. This software is not packaged with MessageWay installations.

MessageWay version 6.1 has the following critical dependencies:

MessageWay Component	Dependency
AS2 Interface	▪ Java version 8.x ▪ Apache Tomcat version 7.x, 8.x or 9.x
MWMQ Adapter	▪ MQ Client 6, 7 or 9, 32-bit
Remote Execution Server (RES) on IBM AIX	▪ bos.rte.libc 5.3.7.1 libc ▪ bos.rte.security 5.3.7.1 libcrypt, libpam ▪ bos.rte.libpthreads 5.3.7.0 libpthreads ▪ xlC.rte 9.0.0.1 libC (C++ library)
Web Client	Please refer to the "Critical Dependencies" topic in the separate document *MessageWay Web Client Installation and Configuration*
MWSFTPD Server (Windows only)	Cygwin version 3.1.6 or newer

Planning and Administration

The audience for this information has a range of responsibilities, requiring a range of expertise. The expertise available and the current distribution of responsibilities within a company all affect how each will distribute the work associated with MessageWay. These suggestions should help new users to plan their best practices.

Distribution of Work

Consider the following types of users to distribute the responsibilities for MessageWay:

- *MessageWay Administrator* is responsible for the installation of the product and its interface with the operating system and other applications, as well as adapter and service configurations and security.
- *MessageWay Operator* is responsible for the daily operations of message transfer activity, including basic communications issues.
- *MessageWay Configuration Support* is responsible for location configurations for customers and provides customer support.
- *(Optional) MessageWay Translation Support* is responsible for configurations for translation processing and message transfers to and from the MW Translator service.

Security Configurations

MessageWay should be secured with operating system security and ODBC database security. For more information about this type of security, refer to the *MessageWay Installation Guide*. Within the MessageWay database, users may choose to encrypt some or all message content.

Users must log on to the MessageWay Manager. To control user access to MessageWay, configure user and object security. For more information, refer to the topic, ***Configuring User and Object Security*** (on page 371).

Responsibilities of the MessageWay Team

Each area of responsibility will perform certain tasks, as suggested in the following table:

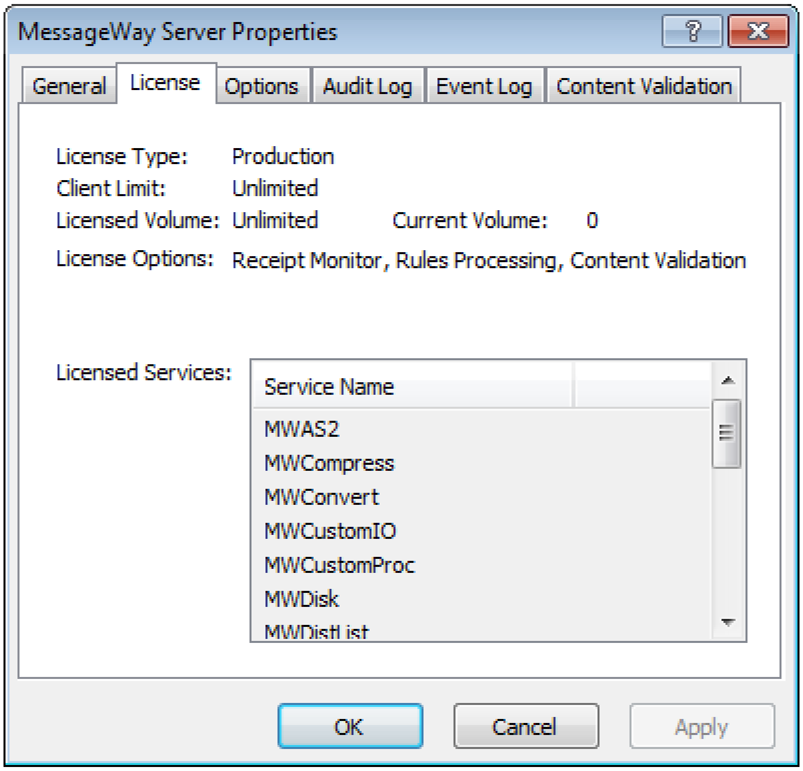
Type of User	Tasks
MessageWay Administrator	▪ Plan and install the product ▪ Support the ODBC/SQL database ▪ Create and maintain user security ▪ Manage initial testing to optimize system settings ▪ Support adapter/service requirements with regard to system communications resources ▪ Manage integration with other applications ▪ Manage critical issues
MessageWay Operator	▪ Monitor the processing of messages using the MessageWay Manager ▪ Control message traffic when necessary ▪ Provide initial diagnostics to troubleshoot messaging problems
MessageWay Configuration Support	▪ Provide the point-of-contact for customers ▪ Create and maintain adapter and service configurations ▪ Create and maintain location configurations ▪ Respond to customer's message delivery issues using the MessageWay query options ▪ Troubleshoot message problems related to configurations, consulting with Translation Support as required
MessageWay Translation Support (Optional)	▪ Provide diagnostic support for operators and Customer Configuration Support when message transfer issues involve Translation Runtime Module (TRM) processing ▪ Help Customer Configuration Support with translation logging and reconciliation issues ▪ Respond to customer's translation reconciliation issues using the MW Translator Operator Query feature

Maintaining Licenses

Part of the installation process includes copying the license file to the appropriate location, which will vary depending on the operating system.

When users log on to the MessageWay Manager, license options will appear on the **Licenses** page of the MessageWay Server Properties window. The type of license and the contracted license volume limit and the current volume in kilobytes appear on the tab as well. To request a license file, contact MessageWay Technical Support.

Note that a few services, such as Receipt Monitor and Rules Processing, appear on the Options list. Most services appear on the Licensed Services list.



License Type: Production
Client Limit: Unlimited
Licensed Volume: Unlimited Current Volume: 0
License Options: Receipt Monitor, Rules Processing, Content Validation

Licensed Services:

Service Name
MWAS2
MWCompress
MWConvert
MWCustomIO
MWCustomProc
MWDisk
MWDistList

TIP: There may be times when increased volume requires additional adapters or services. Users may install additional copies of most adapters or services using the install program. If they do not already have a license that allows them to install a service, they must also receive a new license file from Technical Support. For more information about installing additional adapters or services, refer to the *MessageWay Installation Guide*.

MessageWay Startup and Shutdown for UNIX and Linux

MessageWay should be started and stopped from the operating system. Users may then use the MessageWay Manager to configure the adapters and other services to start automatically or manually.

NOTE: The default installation directory is **/opt/messageway**. That location may vary, so references to it will be in italics as *installation_directory*. The default data directory is **/var/opt/messageway**, which will be referenced as *data_directory*.

The MessageWay Manager runs on Windows and connects to various environments, which point to MessageWay servers. When the MessageWay Server is on the same machine as the Manager, the environment is created automatically. It is called *Default* and the server is named *(local)*.

When the MessageWay Server runs on UNIX or Linux, and because the Manager runs on Windows, any environments to which the Manager connects are considered remote environments, which must be added to the environment list before users log on.

IMPORTANT: The ODBC server must be running before you attempt to start MessageWay. The ODBC database will have to be created separately. For information about how to create the database, DSN and tables for MessageWay, refer to the *MessageWay Installation Guide*.

MessageWay Servers, Adapters and Services for UNIX and Linux

This information is for the System or MessageWay Administrator, who should secure the following services. Users run a script to start, stop or check the status of a service.

The following table lists the base MessageWay servers, adapters and services:

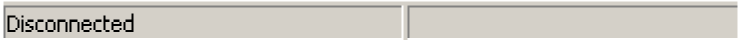
Description	Program Name	Script Name
MessageWay Compression Service	mwcompress	MWCompress
MessageWay Custom IO Adapter	mwcustomio	MWCustomIO
MessageWay Custom Processing Service	mwcustomproc	MWCustomProc
MessageWay Disk Adapter	mwdisk	MWDisk
MessageWay Distribution List Service	mwdistlist	MWDistList
MessageWay E-mail Adapter	mwemail	MWEmail
MessageWay FTP Adapter	mwftp	MWFTP
MessageWay FTP Server	mwftpd	mwftpd
MessageWay Messaging Server	mwmsg	messageway
MessageWay Proxy Server (for SFTP adapter)	mwproxy	MWProxyServer
MessageWay Rules Processing Service	mwrules	MWRules
MessageWay Schedule Server	mwsched	MWSched
MessageWay Service Interface	mwsi	MWSI
MessageWay SFTP Adapter	mwsftp	MWSFTP
MessageWay SFTP Server	mwsftpd	MWSFTPD
MessageWay User Server	mwuser	MWUser

The following table lists the optional MessageWay servers, adapters and services:

Description	Program Name	Script Name
MessageWay AS2 Adapter	mwas2	MWAS2
MessageWay AWSS3 Adapter	mwawss3	MWAWSS3
MessageWay Character Set Conversion Service	mwconvert	MWConvert
MessageWay Logging Server	mwlogging	MWLogging
MessageWay WebSphere MQ Adapter	mwmq	MWMQ
MessageWay Reconciliation Server	mwrecon	MWRecon
MessageWay RES	mwresd	mwresd
MessageWay Translation Service	mwtranslator	MWTranslator

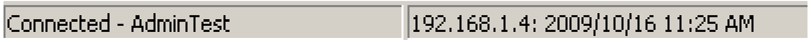
In the lower left corner of the MessageWay Manager, a status, *Connected* or *Disconnected*, indicates whether the Manager is connected to the MessageWay database environment.

The following example shows a system that has not been started, or one that has been started, but no one is logged on to the database environment from this Manager.



Disconnected

The following example shows a system that has been started and that this Manager is now connected to a remote database environment.



Connected - AdminTest | 192.168.1.4: 2009/10/16 11:25 AM

How to Start MessageWay on UNIX or Linux

To start MessageWay, proceed as follows:

1 Log on as the user that owns MessageWay, typically, **mway**.

2 At a command prompt, type the following commands and press **Enter** to:

a) Change the directory to where the script runs, typically **/opt/messageway/init**:

cd /*installation_directory*/init

b) Run the script to start MessageWay

./messageway start

The Messageway Server starts and then starts any other required servers as well as any servers that are configured to start automatically.

3 To check the status of the Messaging Server, type the following command and then press **Enter**:

./messageway status

The system returns a message similar to the following:

```
MessageWay (pid 4436) is running...
```

```
MWSched (pid 4448) is running...
MWSI (pid 4480) is running...
MWUser (pid 4464) is running...
```

- or -

To determine what commands are available, type the following command:

./messageway

NOTE: For Red Hat 7.x, MessageWay supports the systemctl utility, including automatically starting MessageWay when the application server is rebooted, and automatically starting MessageWay perimeter servers when the perimeter server is rebooted. The systemctl files are named *messageway.service*, *mwftpd.service*, *mwproxy.service*, *mwresd.service* and *mwsftpd.service,* and are located in **/usr/lib/systemd/system/**, with symbolic links being added in **/etc/systemd/system/multi-user.target.wants/**. See above systemctl files for more details.

How to Stop MessageWay on UNIX or Linux

Make sure you are logged on as the user that owns MessageWay, typically **mway**. Stop MessageWay as follows:

1 At a command prompt, type the following commands and press **Enter** to:

a) Change the directory to where the script runs:

cd /*installation_directory*/init

b) Run the script to stop MessageWay

./messageway stop

The MessageWay Server stops other servers and then itself.

2 To check the status of the Messaging Server, type the following command and press **Enter**:

./messageway status

MessageWay Startup and Shutdown for Windows

MessageWay must be started and stopped from the operating system. Users may then configure some internal servers and adapters and services to start automatically or manually with MessageWay.

IMPORTANT: The ODBC server must be running before you attempt to start MessageWay. For Windows, the MessageWay database tables should have been created as part of the install process when you use MS SQL Server 2005. For other types of databases, you must create the tables separately. For more information, refer to the *MessageWay Installation Guide*.

MessageWay Servers, Adapters and Services for Windows

Users should not have to access Services to modify settings. This information is for the System or MessageWay Administrator to secure the following Windows Services. These services should only be accessed by MessageWay.

The following table lists the base MessageWay servers, adapters and services:

(Display) Name	Program Name	Service Name
MessageWay Compression Service	mwcompress.exe	MWCompress
MessageWay Custom IO Adapter	mwcustomio.exe	MWCustomIO
MessageWay Custom Processing Service	mwcustomproc.exe	MWCustomProc
MessageWay Disk Adapter	mwdisk.exe	MWDisk
MessageWay Distribution List Service	mwdistlist.exe	MWDistList
MessageWay e-mail Adapter	mwemail.exe	MWEmail
MessageWay FTP Adapter	mwftp.exe	MWFTP
MessageWay FTP Server	mwftpd.exe	MWFTPServer
MessageWay Messaging Server	mwmsg.exe	messageway
MessageWay Proxy Server (for SFTP adapter)	mwproxy.exe	MWProxyServer
MessageWay Rules Processing Service	mwrules.exe	MWRules
MessageWay Schedule Server	mwsched.exe	MWSched
MessageWay Service Interface	mwsi.exe	MWSI
MessageWay SFTP Adapter	mwsftp.exe	MWSFTP
MessageWay SFTP Server	mwsftpd.exe	MWSFTPServer
MessageWay User Server	mwuser.exe	MWUser

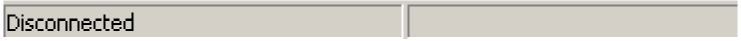
The following table lists the optional MessageWay servers, adapters and services:

(Display) Name	Program Name	Service Name
MessageWay AS2 Adapter	mwas2.exe	MWAS2
MessageWay AWSS3 Adapter	mwawss3.exe	MWAWSS3
MessageWay Character Set Conversion Service	mwconvert.exe	MWConvert
MessageWay Logging Server	mwlogging.exe	MWLogging
MessageWay MQ Adapter	mwmq.exe	MWMQ

(Display) Name	Program Name	Service Name
MessageWay Reconciliation Server	mwrecon.exe	MWRecon
MessageWay RES	mwresd.exe	MWRESServer
MessageWay Translation Service	mwtranslator.exe	MWTranslator

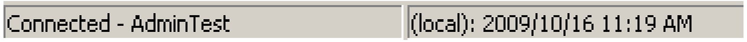
In the lower left corner of the MessageWay Manager, a status, *Connected* or *Disconnected*, indicates whether the Manager is connected to the MessageWay database environment.

The following example shows a system that has not been started, or one that has been started, but no one is logged on to the database environment from this Manager.



Disconnected

The following example shows a system that has been started and that this Manager is now connected to a local database environment.



Connected - AdminTest

(local): 2009/10/16 11:19 AM

How to Start MessageWay on Windows

On Windows, MessageWay runs as a Windows service.

Start MessageWay as follows:

NOTE: Exact instructions vary depending on your operating system.

1 From the **Start** menu or your desktop, right click **My Computer** or **Computer**, and then select **Manage**.

A management window appears.

2 From the left pane, within *Services and Applications* or *Configurations*, click **Services**.

3 From the right pane, right click **MessageWay Messaging Server**.

4 From the pop-up menu, click **Start**.

The MessageWay Messaging Server starts and then starts any dependent services. To view all started services, press **F5**.

How to Stop MessageWay on Windows

On Windows, MessageWay runs as a Windows service. You can stop MessageWay from Windows Services.

IMPORTANT: Closing the MessageWay Manager window does not stop servers or log you off the database.

To stop a MessageWay server on Windows, proceed as follows:

1 Open Windows Services for the machine where the server runs.

2 Right-click the MessageWay Messaging Server, and click **Stop**.

This page intentionally blank.

Understanding MessageWay

This section provides an overview of what tasks MessageWay performs and how it does so. It describes its basic components and the options available to process your data.

System Overview

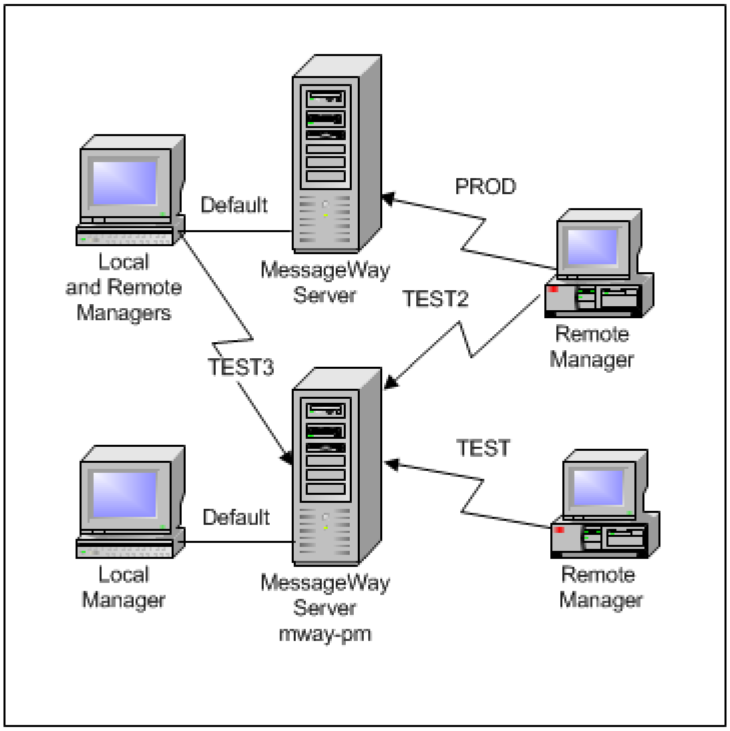
MessageWay is a store-and-forward messaging system. Adapters and services transfer messages to the Message Store and transfer messages from the Message Store for delivery. As an alternative to automated receipt and delivery, users may pick up and send messages using the Internet (Web and AS2), FTP, SFTP and MQ services. Each message is assigned a destination location. For automated delivery, each location has a single adapter or service associated with it. All messages submitted to that location are delivered by the associated adapter or service to a specified address. This model is the basis of operation for the entire MessageWay system.

Understanding How Users Access MessageWay

MessageWay provides options for centralized or distributed processing with centralized or distributed management. Users may access MessageWay servers locally or remotely.

Only one MessageWay Server exists per machine. The server and all of its components and database configurations constitute a MessageWay system. As of MessageWay 5.5, an environment may include one or more MessageWay systems. The MessageWay Manager provides a user interface to MessageWay environments. Each MessageWay Manager accesses one MessageWay environment at a time. Each environment may access one or more MessageWay systems.

Users select the MessageWay environment that they want to access from the MessageWay Manager, which runs on Windows. For more information about using remote access, refer to ***Configuring Remote Access Environments*** (on page 443).



Understanding the Basic Messaging Process

MessageWay sends and receives messages using adapters and services to automate the process. Once messages enter MessageWay, they may be processed by additional services, such as compression, translation, routing by rules based on properties or content of the messages or routing to a distribution list.

Sending and Receiving Messages

MessageWay uses active and passive methods to send and receive messages. Using the active method, MessageWay functions as a client requesting services from external servers. Using the passive method, MessageWay functions as a server, processing requests from outside clients.

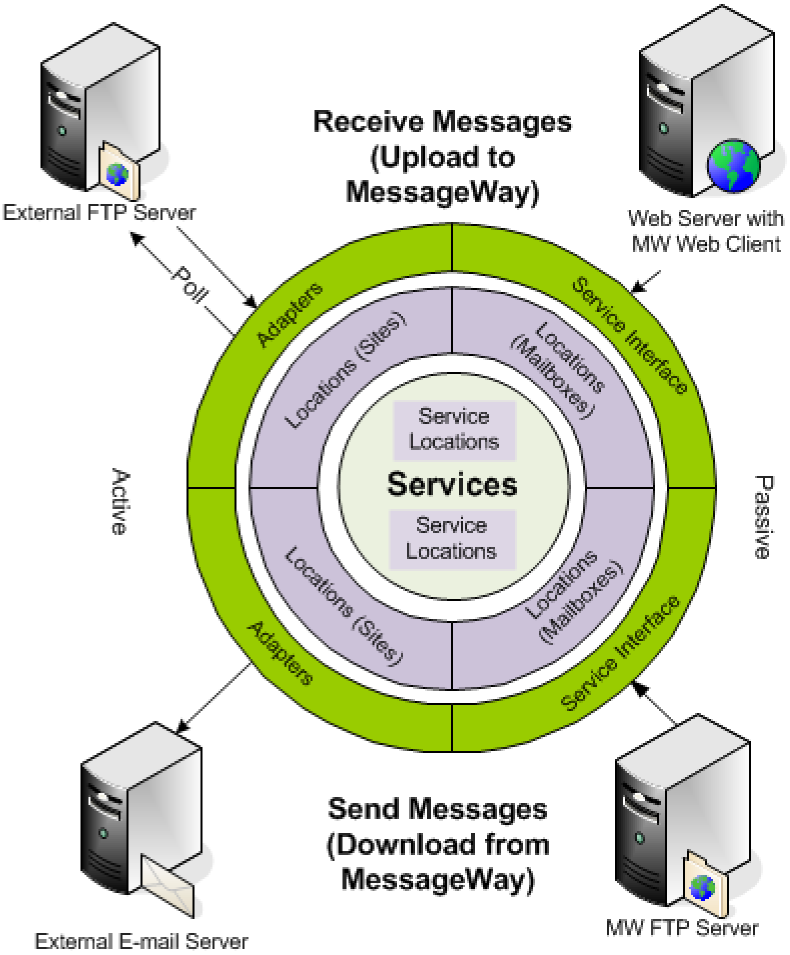
To receive messages from outside entities, the methods are as follows:

- Active: MessageWay polls external servers supported by various adapters that provide Input/Output (I/O) service
- Passive: MessageWay processes upload requests from external services using the Service Interface (Web Client, FTP Server, SFTP Server, AS2 and Custom I/O Adapter)

To deliver messages to outside entities, the methods are as follows:

- Active: MessageWay downloads files to servers supported by various adapters (FTP Server can also work in active mode, as a proxy server)
- Passive: MessageWay processes download requests from the Internet using the Service Interface (Web Client, FTP Server, AS2 and Custom I/O Adapter)

The following diagram shows the basic process MessageWay uses to send and receive messages.



Overview of Basic Sending and Receiving Processes

Using Additional Services

Once messages are stored in MessageWay, users may request additional services. Users may string services together, passing the output of one process to the input of another, before the message is delivered or picked up from the Message Store. Services provide the following processing options:

- Rules processing (route messages based on message attributes or content)
- Distribution List
- Compression (zip and unzip)
- Conversion (convert character set)
- Custom Processing (initiates an external process and optionally returns messages to MessageWay)
- (Optional feature) MessageWay Translator (format conversion and routing)

Routing Messages

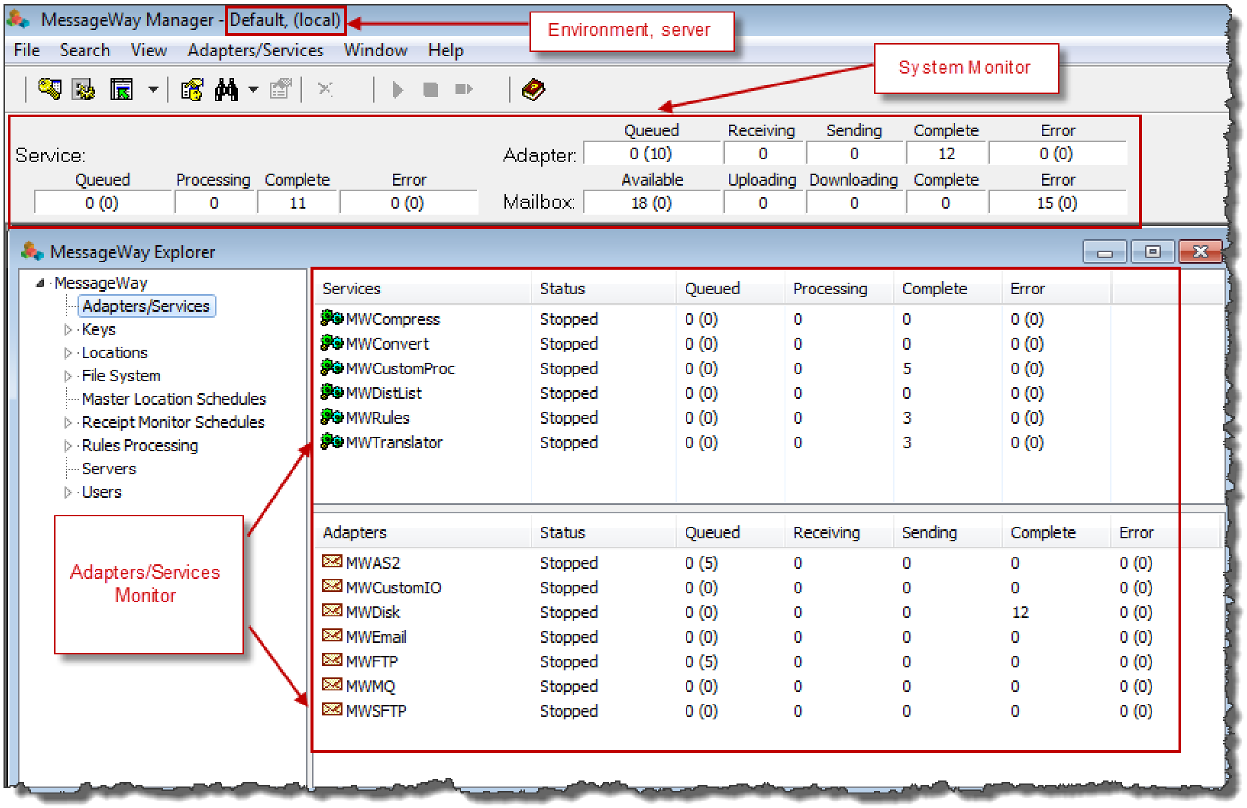
To route messages, MessageWay uses static and dynamic addressing techniques. Users store static addresses with location definitions, but they may also use the Rules Processing service to determine routing addresses dynamically based on message properties or content. The options are as follows:

- Route an inbound message to a site (location associated with an adapter such as Disk Transfer or FTP) or a mailbox (location where users pick up their messages)
- Route an inbound message to one or more services. Some services and their associated service locations have their own means to route messages to delivery locations, such as:
  - Distribution List routes to multiple specified locations
  - Rules processing profiles, which can be nested, use rules applied to the incoming message to route it to a delivery location
  - MWTranslator (optional feature) determines routing based on its own configurations and typically the content of the message headers

Understanding the MessageWay Manager

The MessageWay Manager allows users to configure MessageWay entities and to monitor messaging traffic for a specified MessageWay environment, which is shown in the title bar. In addition, it provides the ability to start and stop its adapters and services, to perform queries on messages and to view message content. The System Monitor shows the overall state of messaging traffic. The Adapters/Services monitor shows the status of messages for individual adapters and services.

Typically, a MessageWay Manager will access a single MessageWay system, and the status and statistics display for that system.



Service:

Queued	Processing	Complete	Error
0 (0)	0	11	0 (0)

Adapter:

Queued	Receiving	Sending	Complete	Error
0 (10)	0	0	12	0 (0)

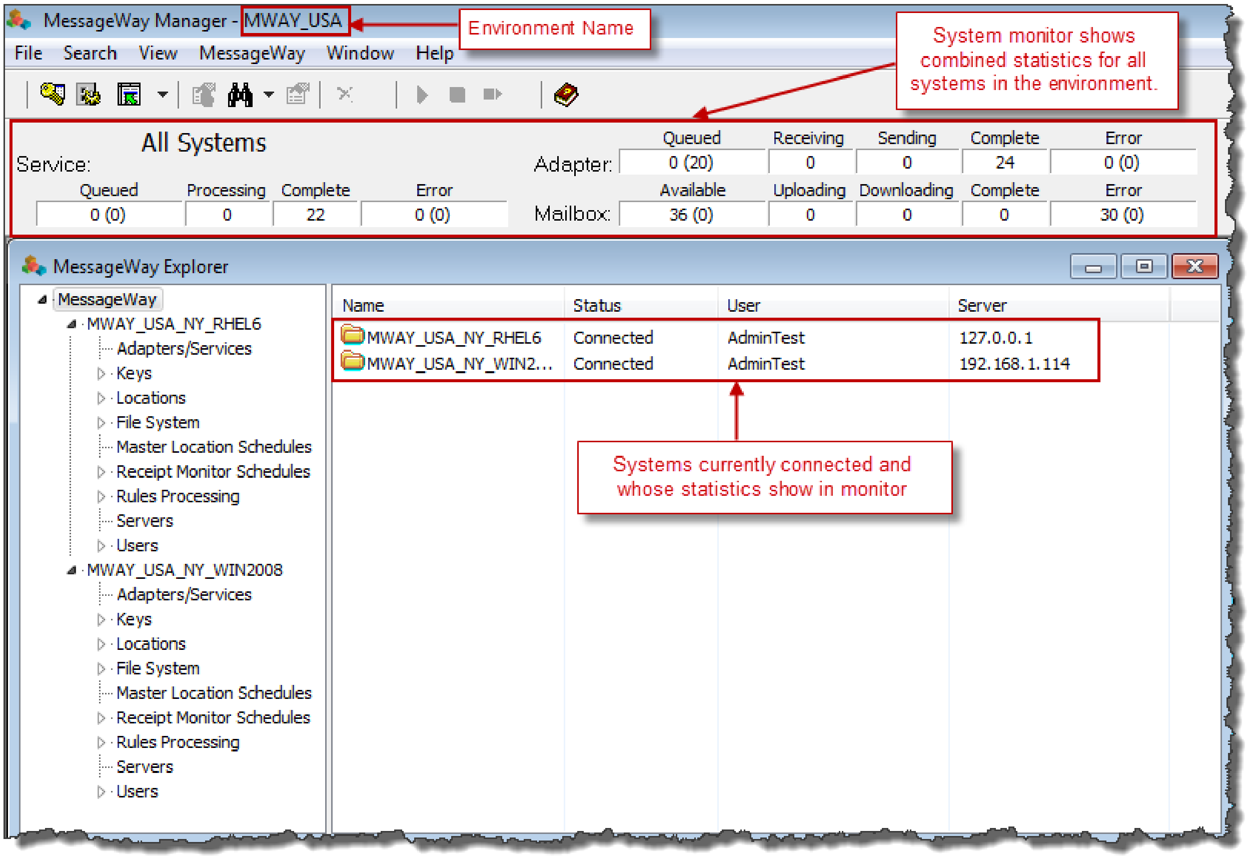
Mailbox:

Available	Uploading	Downloading	Complete	Error
18 (0)	0	0	0	15 (0)

Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0	5	0 (0)
MWDistList	Stopped	0 (0)	0	0	0 (0)
MWRules	Stopped	0 (0)	0	3	0 (0)
MWTranslator	Stopped	0 (0)	0	3	0 (0)

Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWAS2	Stopped	0 (5)	0	0	0	0 (0)
MWCustomIO	Stopped	0 (0)	0	0	0	0 (0)
MWDisk	Stopped	0 (0)	0	0	12	0 (0)
MWEmail	Stopped	0 (0)	0	0	0	0 (0)
MWFTP	Stopped	0 (5)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

However, as of MessageWay 5.5, a MessageWay Manager may point to an environment that monitors multiple systems simultaneously, and the monitor may be configured to show accumulated totals for the combined systems or for individual systems within the environment. You can clearly see when you are monitoring an environment that accesses more than one system, because what the Manager monitors displays prominently above the monitor information. The following shows a Manager monitoring multiple systems in one environment.



Environment Name

System monitor shows combined statistics for all systems in the environment.

All Systems

Service:	Queued	Processing	Complete	Error
	0 (0)	0	22	0 (0)

Adapter:	Queued	Receiving	Sending	Complete	Error
	0 (20)	0	0	24	0 (0)

Mailbox:	Available	Uploading	Downloading	Complete	Error
	36 (0)	0	0	0	30 (0)

Name	Status	User	Server
MWAY_USA_NY_RHEL6	Connected	AdminTest	127.0.0.1
MWAY_USA_NY_WIN2...	Connected	AdminTest	192.168.1.114

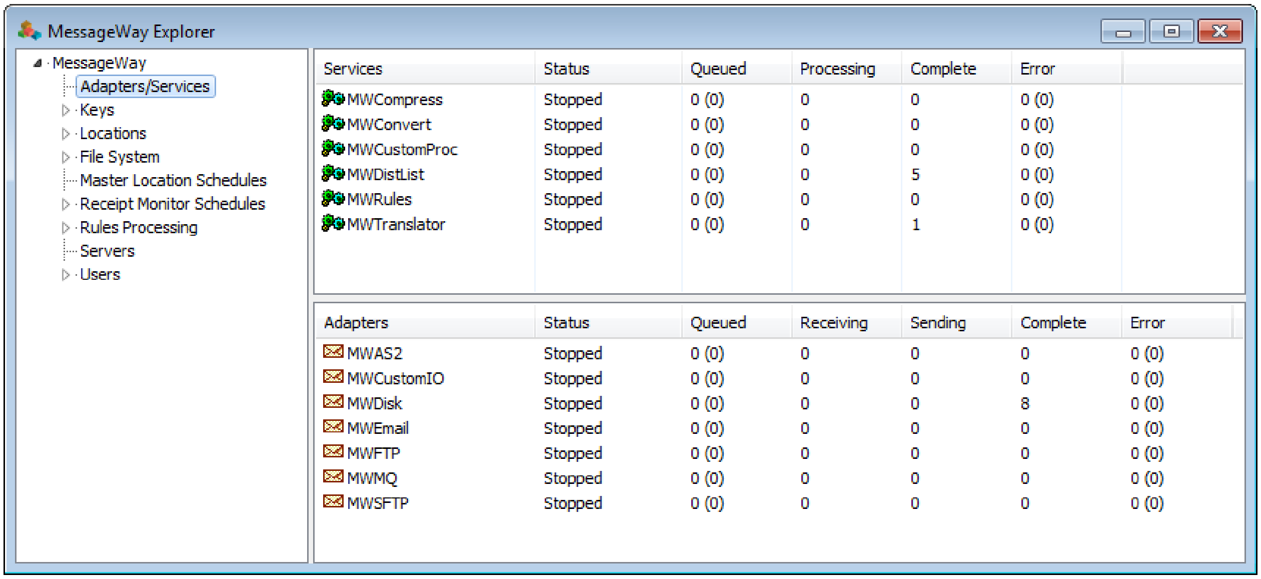
Systems currently connected and whose statistics show in monitor

Understanding Adapters and Services

Adapters and services are created during the install process. They cannot be created from MessageWay, and users may not delete or rename existing ones. With appropriate licenses, users may add copies of existing adapters or services.

Adapters and services automate messaging. Adapters send messages in and out of the MessageWay system. Services process a message and produce zero or more outputs that are resubmitted to the messaging system. They pass the message and information about the message to the Messaging Server. It stores the information in the Message Store associated with a destination location.

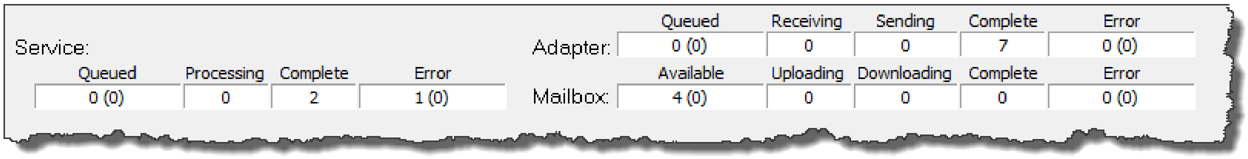
Adapters are typically capable of handling both inbound and outbound traffic, depending on user configurations. The status and statistics of individual adapters appear in the right panes of the MessageWay Explorer window.



Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0	0	0 (0)
MWDistList	Stopped	0 (0)	0	5	0 (0)
MWRules	Stopped	0 (0)	0	0	0 (0)
MWTranslator	Stopped	0 (0)	0	1	0 (0)

Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWAS2	Stopped	0 (0)	0	0	0	0 (0)
MWCustomIO	Stopped	0 (0)	0	0	0	0 (0)
MWDisk	Stopped	0 (0)	0	0	8	0 (0)
MWEmail	Stopped	0 (0)	0	0	0	0 (0)
MWFTP	Stopped	0 (0)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

Users may display consolidated service and adapter statistics in a system monitor, which appears below the MessageWay Manager toolbar. They may toggle the monitor off and on by selecting **System Monitor** ✓ System Monitor from the **View** menu. The System Monitor also displays statistics for a third category of messaging, mailboxes, which includes messages sent to unknown addresses and messages waiting to be picked up by users.



Service:	Queued	Processing	Complete	Error
	0 (0)	0	2	1 (0)

	Queued	Receiving	Sending	Complete	Error
Adapter:	0 (0)	0	0	7	0 (0)
	Available	Uploading	Downloading	Complete	Error
Mailbox:	4 (0)	0	0	0	0 (0)

Consolidated Statistics Displayed in System Monitor

A service performs similar sending and receiving tasks as adapters. Services differ from a pair of I/O adapters in that for a service, MessageWay maintains a link between input and output messages. This provides the user with the ability to find messages related by a process that takes input and produces one or more outputs.

Users may configure adapters or services to start automatically when the MessageWay Server starts. They may also control behavior directly using the toolbar buttons ▶ ■ ■▶ to start and stop them.

Understanding Locations

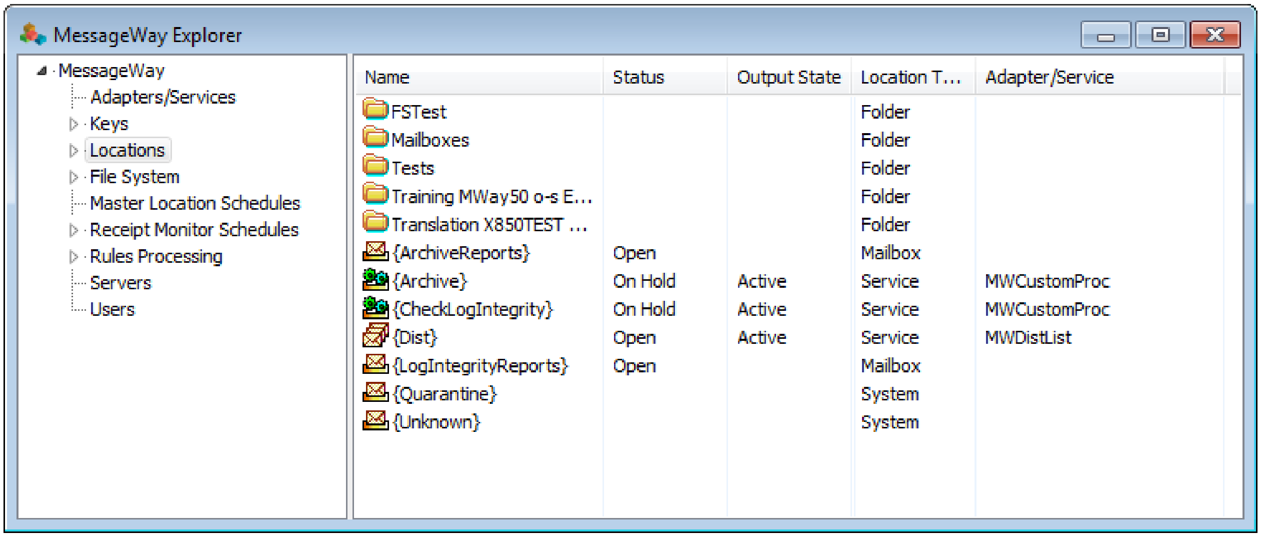
Most messaging behavior is controlled by location configurations. Each location, except a system or pickup mailbox, is associated with a single adapter or service. Users may change this association as required, if the location has no messages currently associated with it. The adapter or service with which a location is associated is listed in the right pane of the MessageWay Explorer window.

When locations are associated with an I/O adapter or service, they assume its type. Locations associated with a service typically send messages to a process. Locations associated with adapters are called *sites* and may be configured to receive messages and to send messages, and may have a type of *Input*, *Output*, or *I/O*.

There are two types of locations, called mailboxes, which are not associated with any adapter or service: system mailbox and pickup mailbox. System mailboxes are created during the installation process and include {Quarantine} and {Unknown}. {Unknown} is used for messages in error when the destination location does not exist. {Quarantine} is used to isolate messages that fail a virus scan, also called content validation. Pickup mailboxes are used with the AS2 Interface, Web Client, FTP Server and SFTP Server options to provide users access to messages on MessageWay. For more information, refer to ***AS2 Interface*** (on page 114), Web Client, ***FTP Server*** (on page 185) and ***SFTP Server*** (on page 298). The location types are listed in the right pane of the MessageWay Explorer window.

There are two systems to create locations. One system is under the *Locations* folder and the other is under the *File System* folder. They are similar in their configuration options and requirements, but they differ in the way information is presented to remote users. The Locations folder provides a view for all remote users that shows messages based on the status of the message. The File System folder is only for remote FTP and SFTP clients whose users prefer a typical hierarchical directory structure that they can view and maintain themselves. These two systems operate independently in MessageWay and the location and messages in the two folders are separate. You can move locations and messages between the Locations and File Systems folders, if the message and location names meet the requirements of the destination folder.

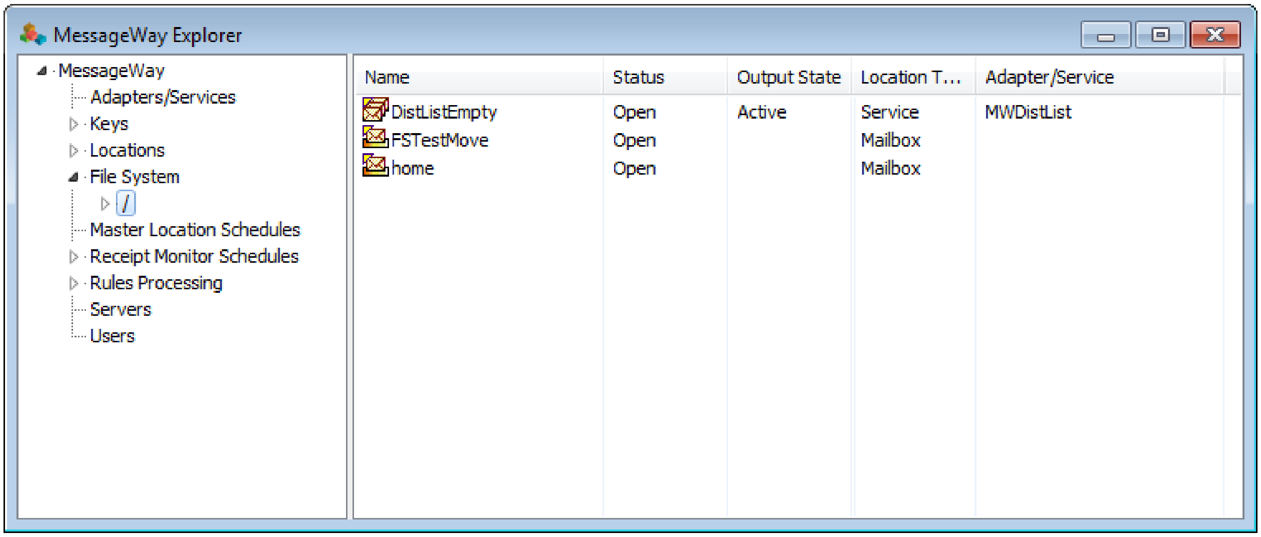
In the Locations folder, users can create folders from Manager to organize their locations, which appear in the right pane. Folders appear as a node under the **Locations** folder, as shown here with the **ABC** folder. The status of the location is calculated based on the state (*Active* or *On Hold*), the schedule (*Open* or *Closed*) and threshold release (*Threshold: nn*).



Name	Status	Output State	Location T…	Adapter/Service
FSTest			Folder	
Mailboxes			Folder	
Tests			Folder	
Training MWay50 o-s E…			Folder	
Translation X850TEST …			Folder	
{ArchiveReports}	Open		Mailbox	
{Archive}	On Hold	Active	Service	MWCustomProc
{CheckLogIntegrity}	On Hold	Active	Service	MWCustomProc
{Dist}	Open	Active	Service	MWDistList
{LogIntegrityReports}	Open		Mailbox	
{Quarantine}			System	
{Unknown}			System	

In the File Systems folder, both client users accessing MessageWay through FTP or SFTP perimeter servers and Manager users can create locations, but not folders such as those in the Locations folder. These locations function as both directory nodes beneath the root node signified by a forward slash / and as locations. This provides clients a more traditional hierarchical view of message storage.

NOTE: Users can only create locations within the File System folder that are pickup mailboxes or service locations. They cannot create input or output locations associated with adapters.

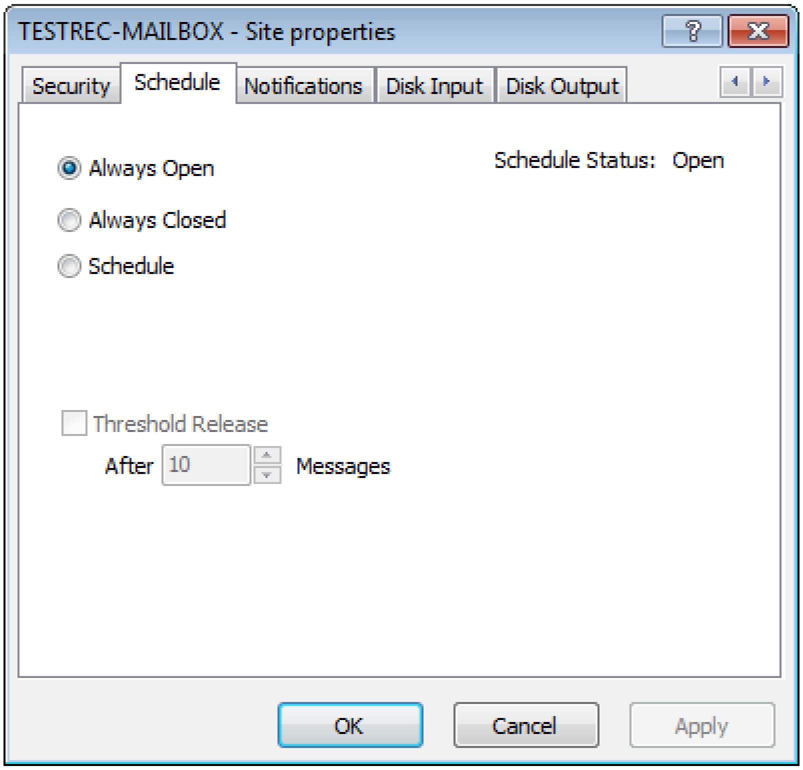


Name	Status	Output State	Location T…	Adapter/Service
DistListEmpty	Open	Active	Service	MWDistList
FSTestMove	Open		Mailbox	
home	Open		Mailbox	

The schedule that is defined for each location and optional threshold release rules control delivery of messages for locations associated with adapters or services. The schedule also controls polling for input locations. The schedule status may be open or closed. Neither message delivery nor polling occurs when the schedule is closed.

NOTE: The names of locations in the Locations folder are simple names, whereas the names of locations in the File Systems folder contain the full path name within the directory, starting with the root, which is a forward slash /.

This schedule is for a location in the Locations folder.



TESTREC-MAILBOX - Site properties

● Always Open

○ Always Closed

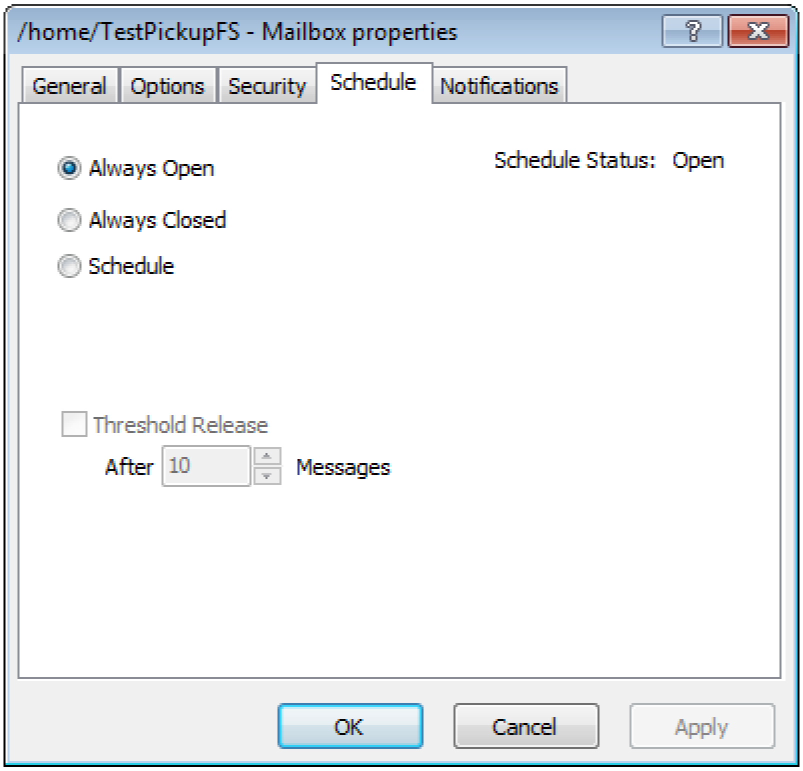
○ Schedule

Schedule Status: Open

□ Threshold Release

After 10 Messages

This schedule is for a location in the File System folder.



● Always Open

○ Always Closed

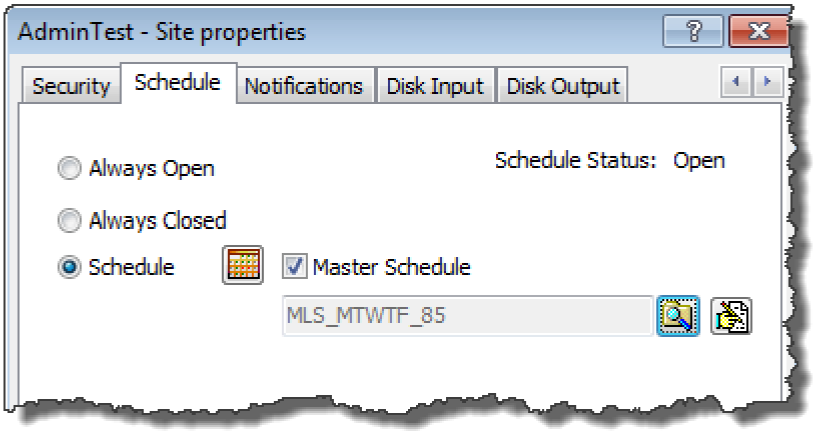
○ Schedule

Schedule Status: Open

☐ Threshold Release

After 10 Messages

Locations may have schedules that are specific to that location or share a schedule with other locations, which is called a Master Location Schedule.



○ Always Open

○ Always Closed

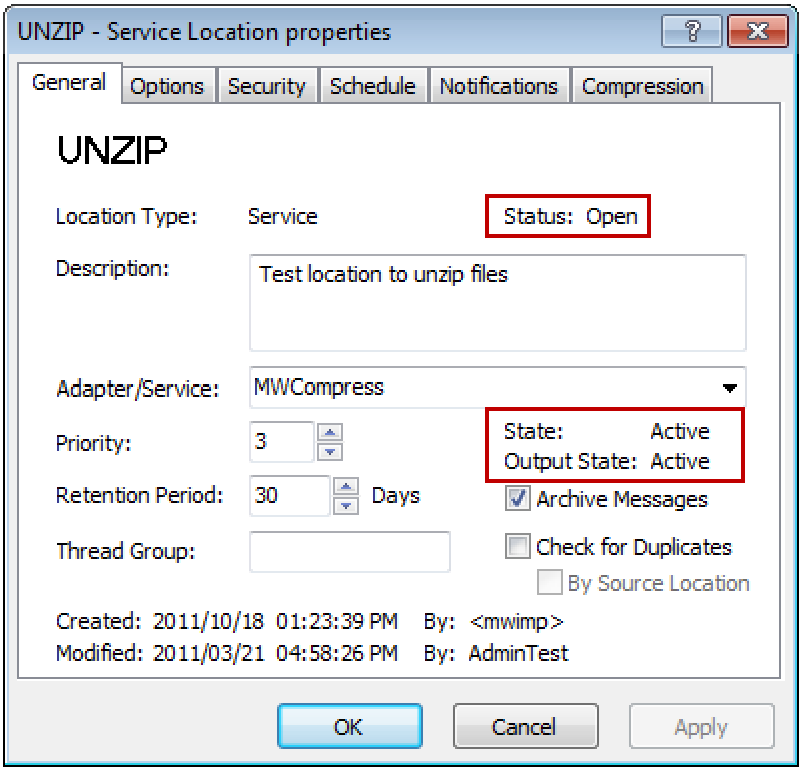
● Schedule

Schedule Status: Open

☑ Master Schedule

MLS_MTWTF_85

On the **General** page, when the location is an output, I/O or service type, a box appears that allows users to check for duplicate messages sent to the location. The status and state values are display-only. They show the state, output state and the calculated status. Output state is only valid for service locations.



UNZIP

Location Type: Service

Status: Open

Description: Test location to unzip files

Adapter/Service: MWCompress

Priority: 3

State: Active
Output State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

☐ By Source Location

Created: 2011/10/18 01:23:39 PM By: <mwimp>
Modified: 2011/03/21 04:58:26 PM By: AdminTest

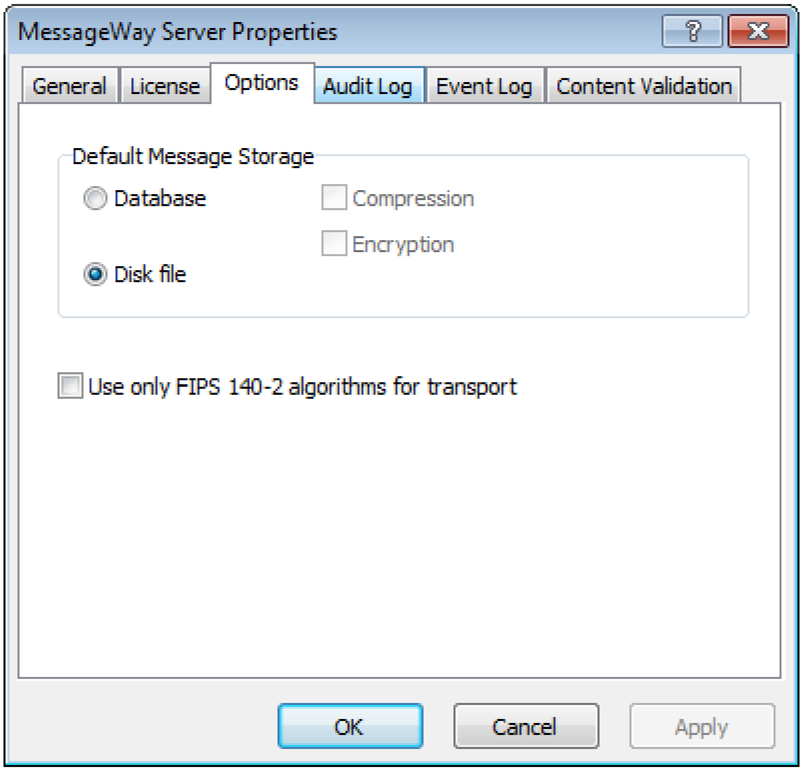
The output state indicates whether output messages, which are results of the service, are allowed to be transferred from the location. A location state can be *Active*, which allows messages to be transferred, or *On Hold*, which transfers output to the appropriate adapter, but the output is then placed on hold in the queue for the adapter.

Understanding the Message Store

There are two parts to a message in the Message Store: information about the message:

- Message detail or header
- Content of the message

Message detail contains information about the message and is always stored in the MessageWay database. Users may configure where the content of messages is stored: in the database, with additional options to compress and encrypt, or on disk. Users specify the type of storage for message content for the MessageWay server, and then may override this system setting for a destination location.



Default Message Storage

○ Database

□ Compression

□ Encryption

● Disk file

□ Use only FIPS 140-2 algorithms for transport

Each message has a unique message identification comprising a message ID and the destination location. The value in **Message Id** is the primary key to the Messages table. The value in **Location** is the name of the destination location where the message typically resides. Users may view the content of the message in a Message window. When users archive messages, MessageWay saves information about the message as well as the message content.

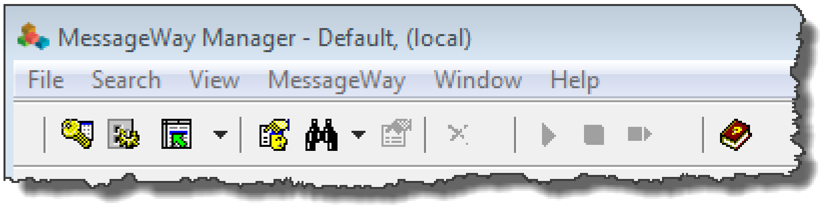
MessageWay Manager

The MessageWay Manager allows users to configure properties and monitor message traffic. The menus and a toolbar provide easy access to commands. The MessageWay Explorer window shows a monitor for individual adapter or service status and activity and a monitor for individual location status. The System Monitor displays consolidated adapter and service activity.

Users may also run more than one instance of the MessageWay Manager on a machine.

Menus and Toolbar

The MessageWay Manager menus and toolbar options change when various options are selected in MessageWay Explorer. The basic set of menus and toolbar options are shown here.

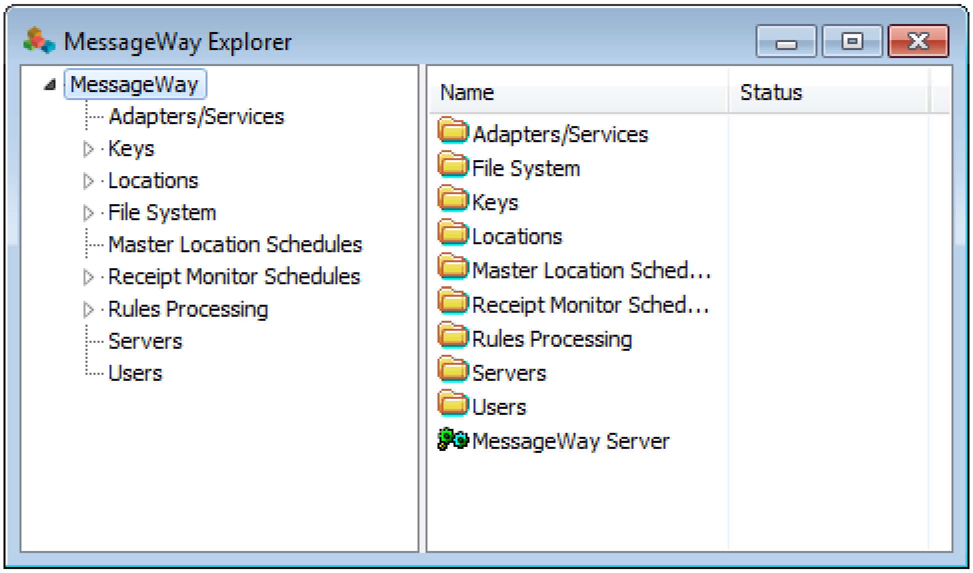


Notice that the header displays the name of the current MessageWay environment.

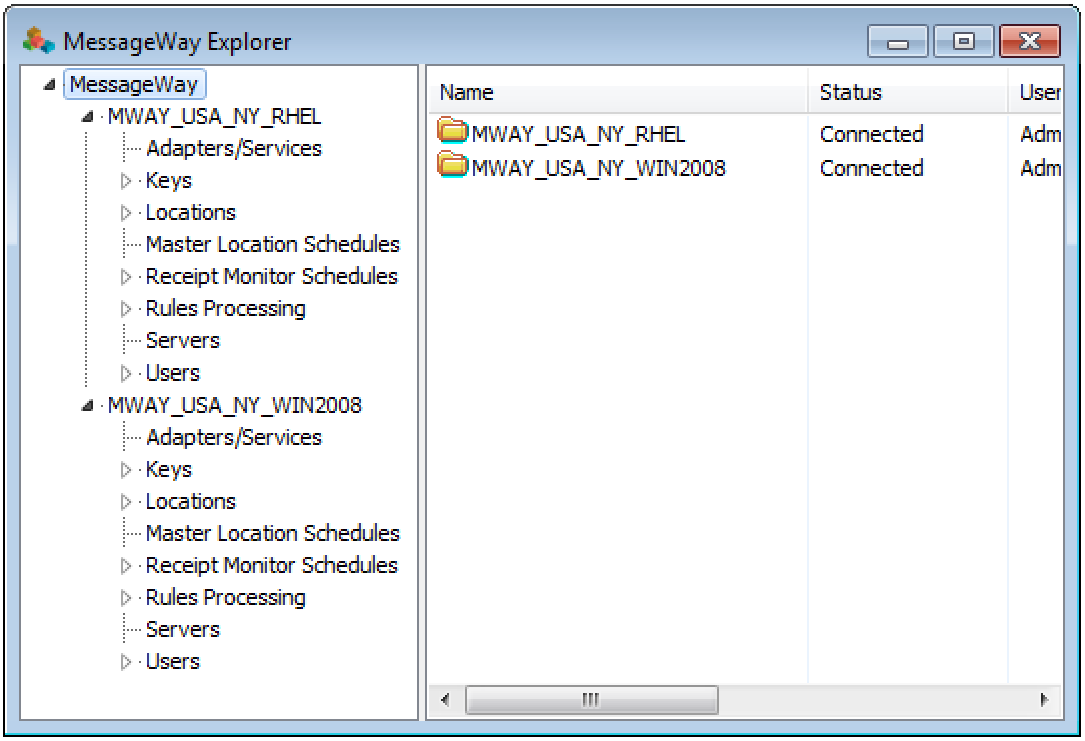
MessageWay Explorer

After starting the MessageWay Manager, an explorer-like window appears. The MessageWay Explorer window provides access to the adapter, service and location monitors and, for local users, access to the MessageWay Server configurations.

You may have only one system in your environment, as shown here.



You may have multiple systems in your environment, a multi-system environment, as shown here.



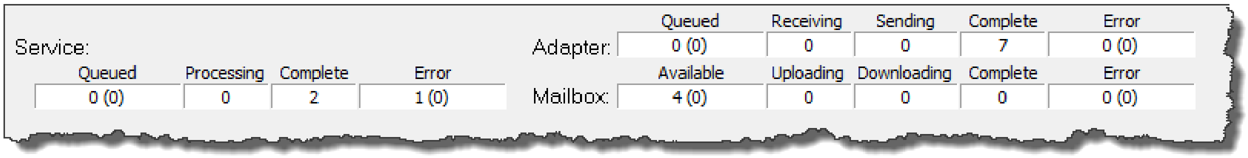
- MessageWay
  - MWAY_USA_NY_RHEL
    - Adapters/Services
    - Keys
    - Locations
    - Master Location Schedules
    - Receipt Monitor Schedules
    - Rules Processing
    - Servers
    - Users
  - MWAY_USA_NY_WIN2008
    - Adapters/Services
    - Keys
    - Locations
    - Master Location Schedules
    - Receipt Monitor Schedules
    - Rules Processing
    - Servers
    - Users

Name	Status	User
MWAY_USA_NY_RHEL	Connected	Adm
MWAY_USA_NY_WIN2008	Connected	Adm

System Monitor

Users display the System Monitor window from the **View** menu. The monitor provides a real-time summary of all adapter and service system activity, which is updated by the MessageWay Server(s). The counts are grouped by services, adapters and mailboxes. Mailboxes includes messages not associated with any adapter or service: those that have been sent to the system mailbox, {Unknown}, and those that have been sent to a pickup mailbox. Pickup mailboxes allow users access to MessageWay from external processes, through services such as the ***AS2 Interface*** (on page 114), the ***FTP Server*** (on page 185) or the ***SFTP Server*** (on page 298).

Users may double-click a count to display a list of messages for that category. If there is an error delivering or processing a message, then the message status is set to *Error*, an exception is generated that can be viewed in the event log, and error code and error text values also appear in the Message Properties window.

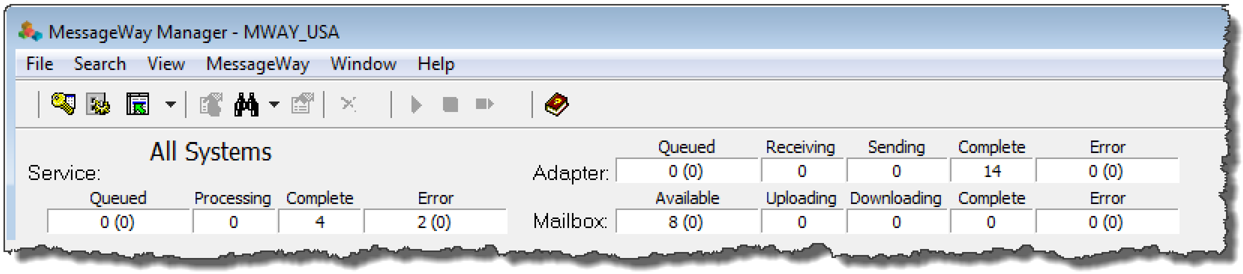


Service:	Queued	Processing	Complete	Error
	0 (0)	0	2	1 (0)

Adapter:	Queued	Receiving	Sending	Complete	Error
	0 (0)	0	0	7	0 (0)

Mailbox:	Available	Uploading	Downloading	Complete	Error
	4 (0)	0	0	0	0 (0)

When monitoring all systems in a multi-system environment, the counts reflect message activity for all systems in that environment to which you are logged on.



All Systems

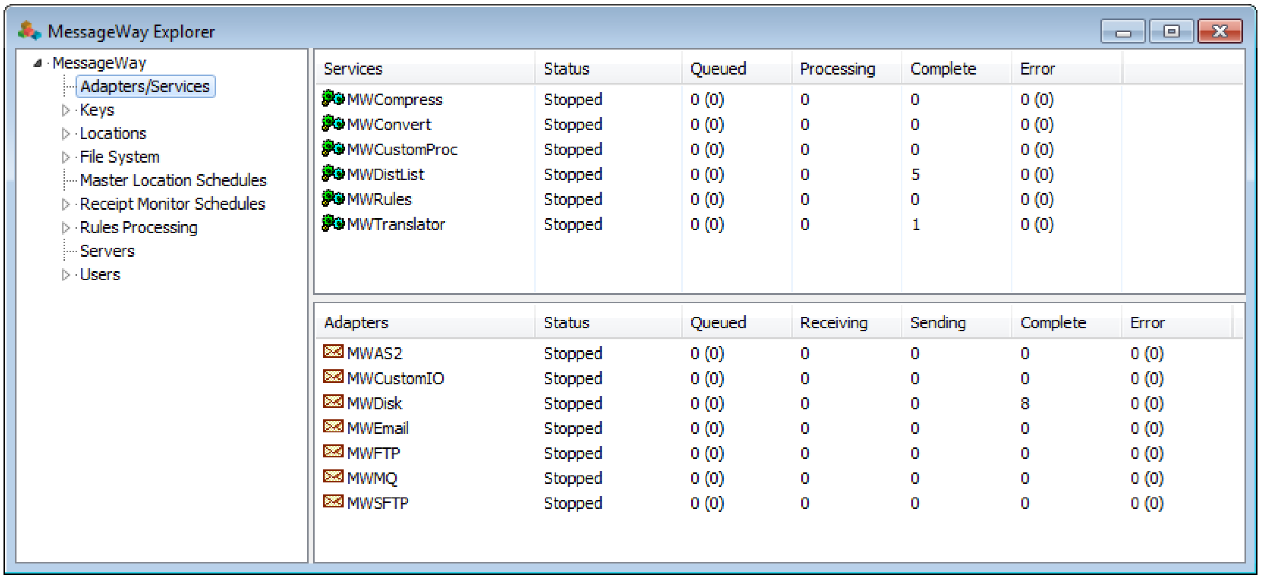
Service:

Queued	Processing	Complete	Error
0 (0)	0	4	2 (0)

	Queued	Receiving	Sending	Complete	Error
Adapter:	0 (0)	0	0	14	0 (0)
	Available	Uploading	Downloading	Complete	Error
Mailbox:	8 (0)	0	0	0	0 (0)

Monitor for Adapters and Services

The monitors provide a real-time summary of message activity for each configured adapter and service. The MessageWay Server provides real-time updates for the monitors.



Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0	0	0 (0)
MWDistList	Stopped	0 (0)	0	5	0 (0)
MWRules	Stopped	0 (0)	0	0	0 (0)
MWTranslator	Stopped	0 (0)	0	1	0 (0)

Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWAS2	Stopped	0 (0)	0	0	0	0 (0)
MWCustomIO	Stopped	0 (0)	0	0	0	0 (0)
MWDisk	Stopped	0 (0)	0	0	8	0 (0)
MWEmail	Stopped	0 (0)	0	0	0	0 (0)
MWFTP	Stopped	0 (0)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

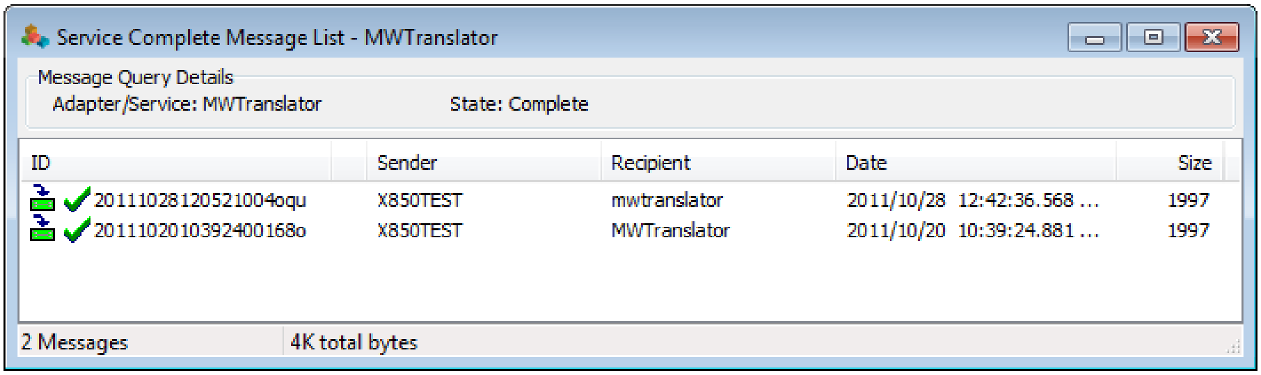
The monitor displays the adapter or service name and status, *Running*, *Stopped* or *Suspended*. For each service, counts are displayed for *Queued (On Hold)*, *Processing*, *Complete* and *Error*. For each adapter, counts are displayed for *Queued (On Hold)*, *Receiving*, *Sending*, *Complete* and *Error*.

To control adapter or service processing, users may select one and then select the appropriate command from the **Adapters/Services** menu, or right-click and select the command from the menu. Users may also select buttons on the toolbar ▶ ■ ■▶ to start, stop and restart an adapter or service. The following table explains the use of the commands:

Command	Shortcut	Icon	Description
Start		▶	Starts an adapter or service.

Command	Shortcut	Icon	Description
Stop		■	Stops an adapter or service.
Restart		■▶	Stops and then starts an adapter or service when it is running. This process rereads the adapter or service configuration files, so use this to make new configurations take effect.
Suspend		menu	When an adapter or service is running, suspends all new activity (sends, receives, polls), allowing current activity to complete processing.
Resume		menu	When an adapter or service is suspended, changes status to running and continues activity. This does not reread configuration files, so use this to continue processing as before.

Users may double click a count to display a message list window with the messages for that category.



Service Complete Message List - MWTranslator

Message Query Details
Adapter/Service: MWTranslator State: Complete

ID	Sender	Recipient	Date	Size
✓ 20111028120521004oqu	X850TEST	mwtranslator	2011/10/28 12:42:36.568 ...	1997
✓ 20111020103924001680	X850TEST	MWTranslator	2011/10/20 10:39:24.881 ...	1997

2 Messages 4K total bytes

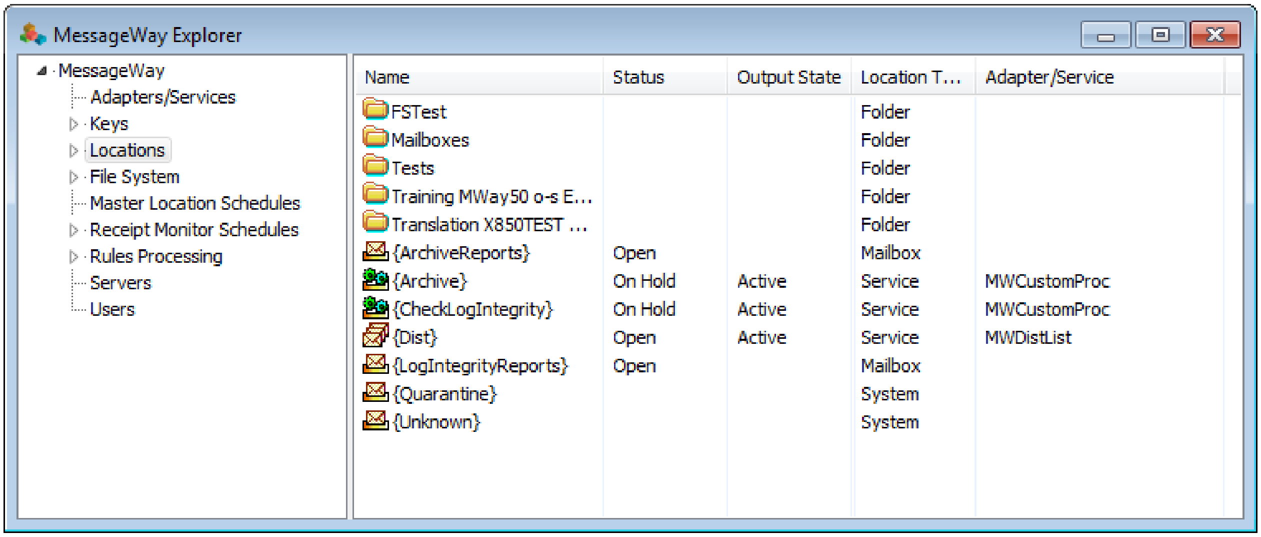
Monitor for Locations

The location monitor provides a summary of the states for each configured location associated with an adapter or service. It also provides counts for locations that are not associated with an adapter or service: the system mailboxes such as {Unknown}, and pickup mailboxes, which are shown in the *Mailboxes* category on the system monitor.

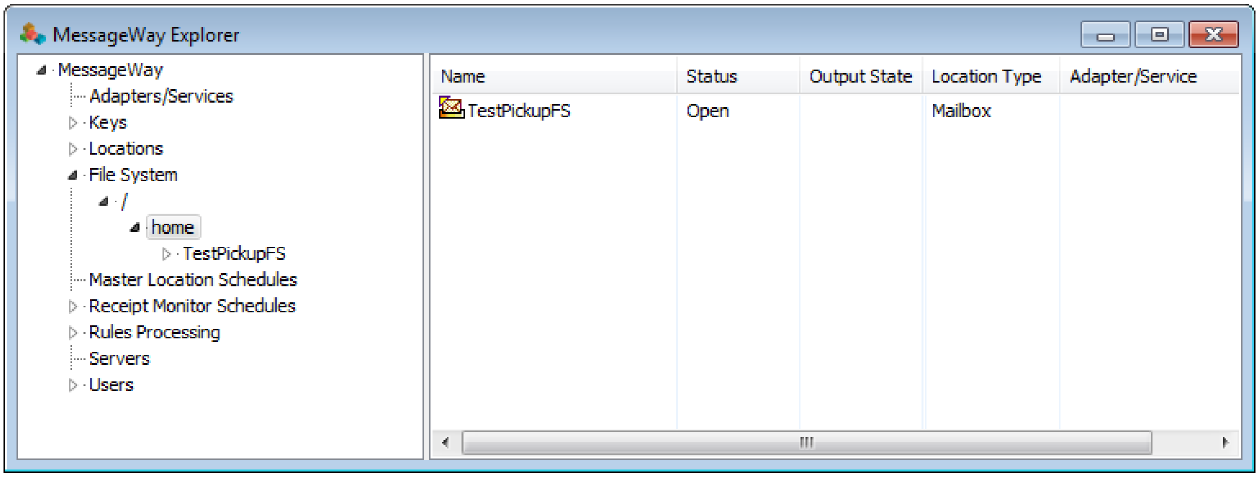
There are two system folders that contain locations: the *Locations* folder and the *File System* folder. The locations in these folders are unique and independent, although once configured, all locations behave the same. The File System folder is for remote users who access MessageWay through FTP and SFTP clients to view their messages in a more familiar directory structure, rather than the structure imposed by the Locations folder.

In the Locations folder from MessageWay Manager, you can add, delete or rename locations and location folders. Locations are defined globally and their names must be unique, even when they are stored within folders. The tree structure of folders for locations allows users to more easily manage large numbers of locations.

In the File System folder from MessageWay Manager, you can add, delete or rename locations only, since there are no folders. The directory structure is simply a view of the relationship of the locations within the folder, because the locations function as locations and as containers or directory nodes. Location names must only be unique within the directory path.



Name	Status	Output State	Location T...	Adapter/Service
FSTest			Folder	
Mailboxes			Folder	
Tests			Folder	
Training MWay50 o-s E...			Folder	
Translation X850TEST ...			Folder	
{ArchiveReports}	Open		Mailbox	
{Archive}	On Hold	Active	Service	MWCustomProc
{CheckLogIntegrity}	On Hold	Active	Service	MWCustomProc
{Dist}	Open	Active	Service	MWDistList
{LogIntegrityReports}	Open		Mailbox	
{Quarantine}			System	
{Unknown}			System	



Name	Status	Output State	Location Type	Adapter/Service
TestPickupFS	Open		Mailbox	

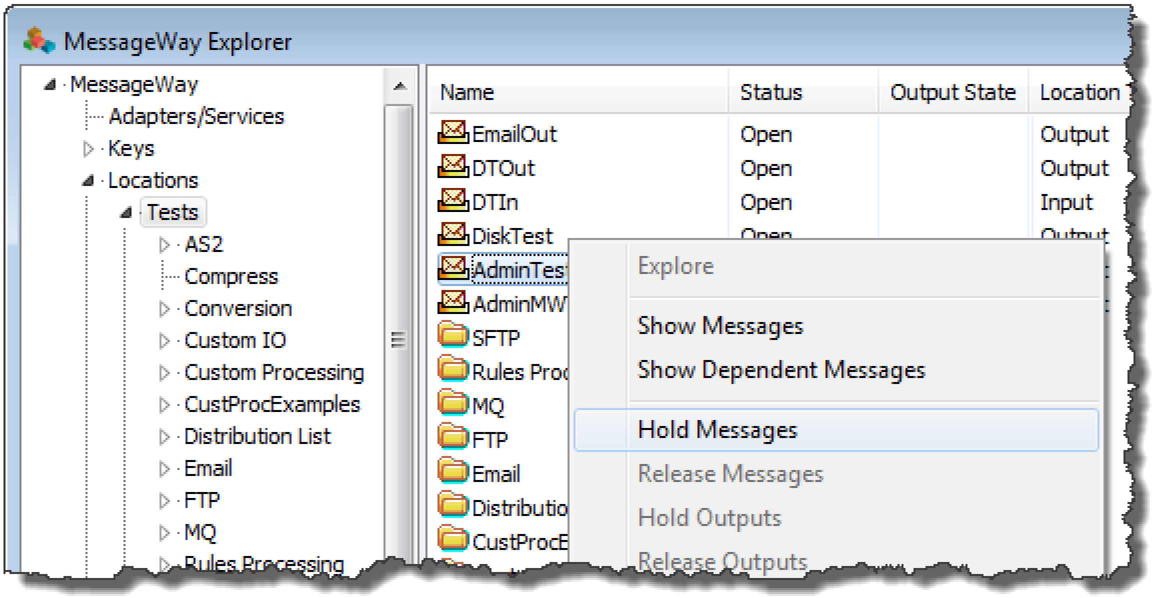
The monitor displays the location name and status for all locations. For each service location, there is an output state. The location type indicates how the location is configured. The monitor also shows the adapter or service associated with the location.

Location information is current at the time of display. Press **F5** to refresh the display. The following table explains the location monitor information:

Column	Description
Status	This is the primary status of all auto-delivery locations, sites and service locations. It is calculated from a combination of the location's state (*Active* or *On Hold*), the schedule state (*Open* or *Closed*) and threshold release. ▪ *Open* means that the schedule will allow the adapter or service to send and receive messages for this location. ▪ *Closed* means that the schedule will not allow the adapter or service to send and receive messages for this location. ▪ *On Hold* means that the location is not available to send or receive data. ▪ *Threshold: nn* means that the schedule is controlled by threshold release rules.
Output State	Valid for service locations only. It is blank for all other types of locations. ▪ *Active* means that the service location will send output for delivery. ▪ *On Hold* means that the service location will send output to the appropriate adapter or service, but the output will be placed on hold in the queue for the service or adapter.
Location Type	▪ *Input* means that the site is configured to send messages into MessageWay. ▪ *Output* means that the site is configured to deliver messages from MessageWay. ▪ *I/O* means that the site is configured to send messages into and deliver messages from MessageWay. ▪ *Mailbox* means that the location waits for users to collect their messages, rather than having them delivered by an adapter. ▪ *Service* means that the location is associated with a service, rather than an adapter. ▪ *System* means that this is the system mailbox, {Unknown}, used for messages that are in error, because the destination location does not exist. This location may not be deleted. ▪ *Folder* means that this item is a folder, which you can use to organize your locations. It has no effect on configurations or processing.
Adapter/Service	The location is currently associated with this adapter or service. This value is blank for group folders, system mailboxes and pickup mailboxes.

Status and output state also appear on the **General** page for quick reference.

Users may right click the location to directly control location status. The menu allows them to select **Properties** to change the schedule or **Hold Messages** to put the location on hold, among other options.



Name	Status	Output State	Location
EmailOut	Open		Output
DTOut	Open		Output
DTIn	Open		Input
DiskTest	Open		Output
AdminTes			
AdminMW			
SFTP			
Rules Proc			
MQ			
FTP			
Email			
Distributio			
CustProcE			

Message Processing Options

These are some basic processing options.

Sending and Receiving Messages

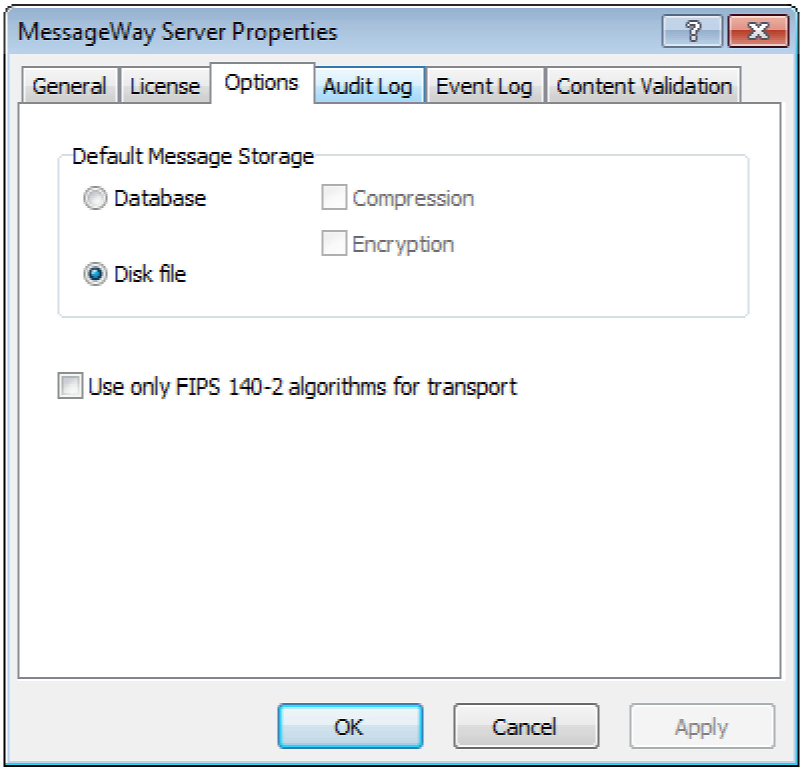
MessageWay offers several methods to send and receive messages, defined by location configurations. When a location is associated with an adapter or service, MessageWay automatically delivers the message to its destination. When a location is *not* associated with an adapter or service, MessageWay holds the messages in a destination mailbox for users to pick up, using some external access, such as the Web, FTP, or SFTP.

Adapters provide services to the Message Store. Services provide access to a processing service. Most adapters and services are part of base MessageWay, and the modular design of the system allows users to easily add other instances of an adapter or service. For a list of basic features and optional features, refer to ***Features*** (on page 5).

Specifying Storage of Message Content

MessageWay always stores information about messages in the MessageWay database. For destination locations, users may decide whether to store the message content on disk, which is the default, or in the database. When the message is stored in the database, users may also choose whether to compress or encrypt it. Data is encrypted using the Advanced Encryption Standard (AES).

Users may specify the setting for an environment on the **Options** page of the MessageWay Server Properties window.



MessageWay Server Properties

Default Message Storage

○ Database

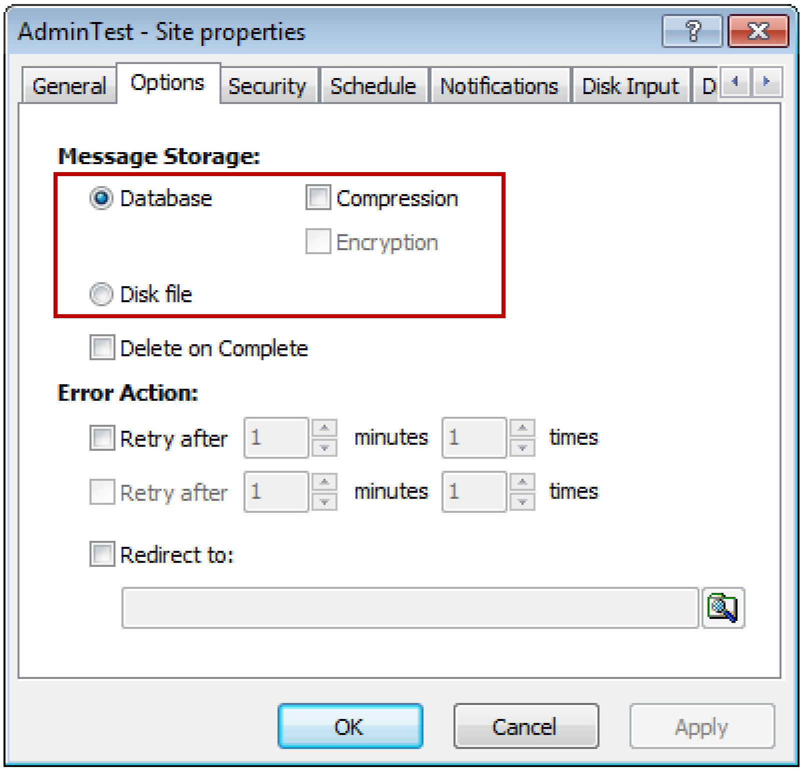
● Disk file

□ Compression

□ Encryption

□ Use only FIPS 140-2 algorithms for transport

Users may override the system setting on the **Options** page for a specific location.



AdminTest - Site properties

Message Storage:

● Database □ Compression

□ Encryption

○ Disk file

□ Delete on Complete

Error Action:

□ Retry after 1 minutes 1 times

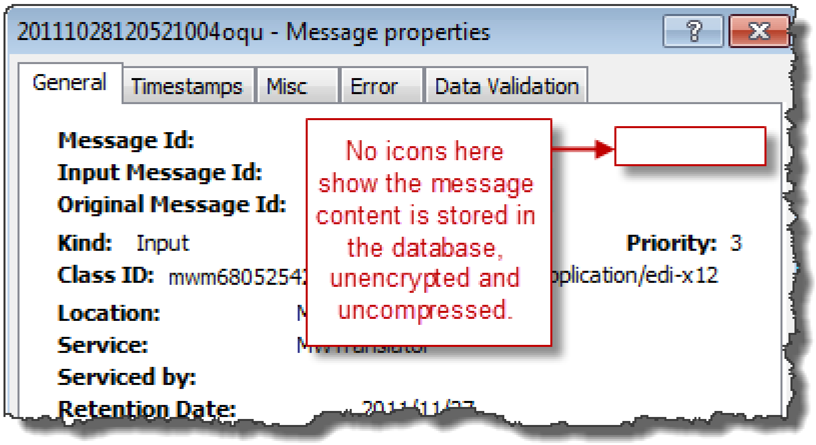
□ Retry after 1 minutes 1 times

□ Redirect to:

Icons on the Message Properties window to the right of the Message ID indicate where and how a message is stored, as follows:

Icon	Storage Option
None	SQL database, no encryption, no compression
🔑	SQL database, Encrypted
🗜	SQL database, Compressed
💾	Disk
❌	Deleted from Message Store after successful delivery

No icons indicate that the message is stored in the database, unencrypted and uncompressed.



Message Id:
Input Message Id:
Original Message Id:
Kind: Input
Priority: 3
Class ID: mwm6805254
pplication/edi-x12
Location: M
Service: MWTranslator
Serviced by:
Retention Date: 2011/11/27

No icons here show the message content is stored in the database, unencrypted and uncompressed.

Specifying Routing

MessageWay determines routing based on location configurations or addresses provided by a MessageWay process, such as MWTranslator. For more information about how MWTranslator determines addresses for messages it generates, refer to the *MW Translator User's Guide and Reference.*

Here, we discuss how MessageWay determines the routing for messages from its own configurations. MessageWay provides several options to route messages:

- To an output location
- To a MessageWay process
- To a sequence of MessageWay processes

The method used to determine the destination address may include any combination of the following:

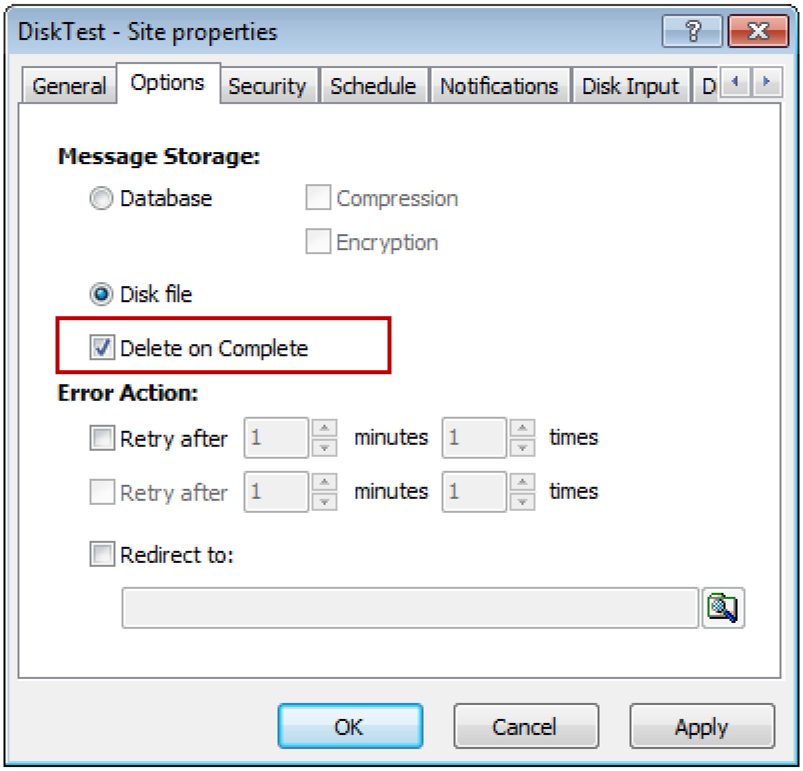
- Addresses specified on sites or service locations
- Address determined by rules applied to the input message that are specified in Rules Processing Profiles
- Addresses received from status files associated with Custom IO or Custom Processing options

The routing addresses on service locations may be simple, compound or a dynamic distribution list. A simple address is a location name, either service or output. A compound address comprises a sequence of service location addresses, typically terminated by an output address. A dynamic distribution list is an ad hoc list of addresses for a single location, the alternative to which is a distribution list service location to be shared by multiple locations when they all need to send to the same destinations.

Adapter, service and user requirements determine which option is used and the specific information users must provide in the location configurations. For more information, refer to the topic, ***Specifying Routing Addresses*** (on page 653).

Deleting Message Content After Successful Delivery

When a message is successfully delivered to its destination, it is marked with a status of *Complete* (for messages in the Locations folder) or *Canceled* (for messages in the File System folder). Users have the option of having MessageWay delete the content of the message when it is marked *Complete* or *Canceled*. The message detail is not deleted. To do this, you check the Delete on Complete box for the location.



Message Storage:

○ Database □ Compression

□ Encryption

● Disk file

☑ Delete on Complete

Error Action:

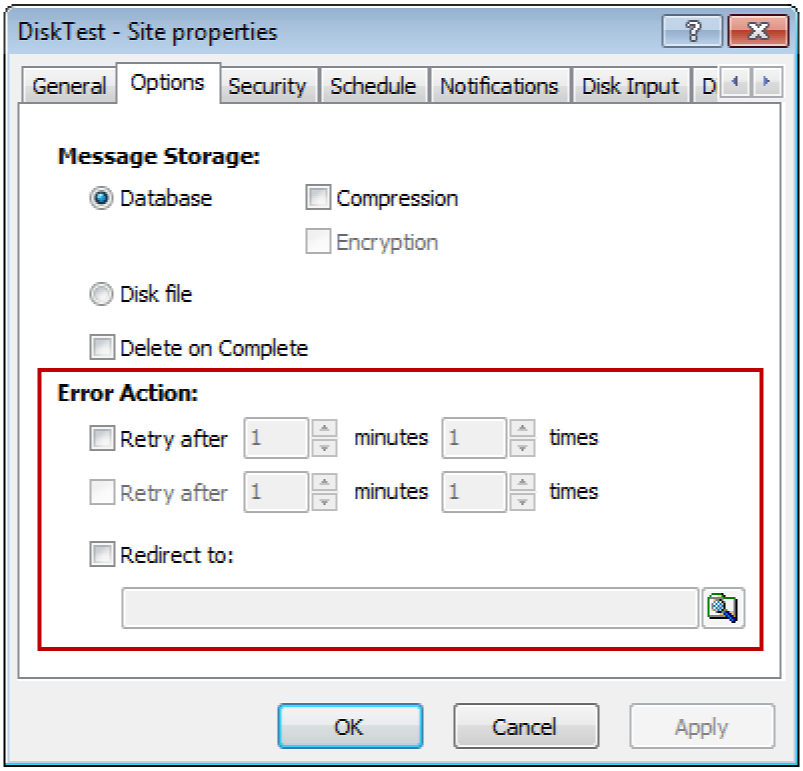
□ Retry after 1 minutes 1 times

□ Retry after 1 minutes 1 times

□ Redirect to:

Specifying Error Actions

Users may configure what happens to a message when MessageWay encounters a delivery error, which is some combination of retry options and redirecting it to another location.



Message Storage:

● Database □ Compression

□ Encryption

○ Disk file

□ Delete on Complete

Error Action:

□ Retry after 1 minutes 1 times

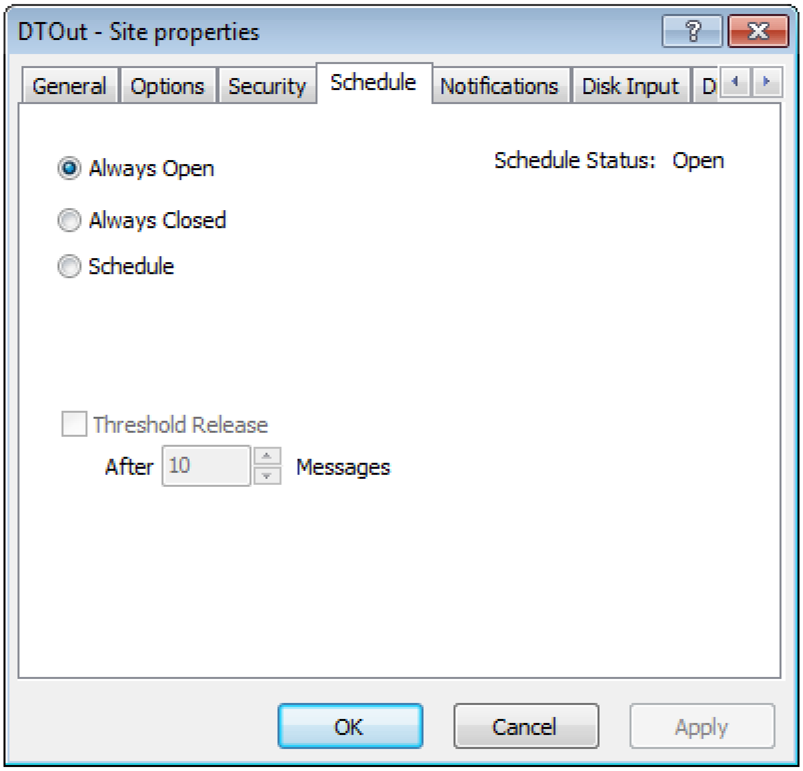
□ Retry after 1 minutes 1 times

□ Redirect to:

Controlling Message Delivery Using Schedules

Schedules defined for each location control automatic delivery of messages and input polling cycles for adapters. Location schedules may be daily, weekly, monthly, annual or absolute. Users may also define Master Location schedules, which can be shared by multiple locations.

The schedule status may be open or closed. Threshold release rules will open a closed schedule, to allow messages to accumulate and be sent in batches. The status of the schedule is used to determine the status of the location, which is displayed in MessageWay Explorer.



● Always Open

○ Always Closed

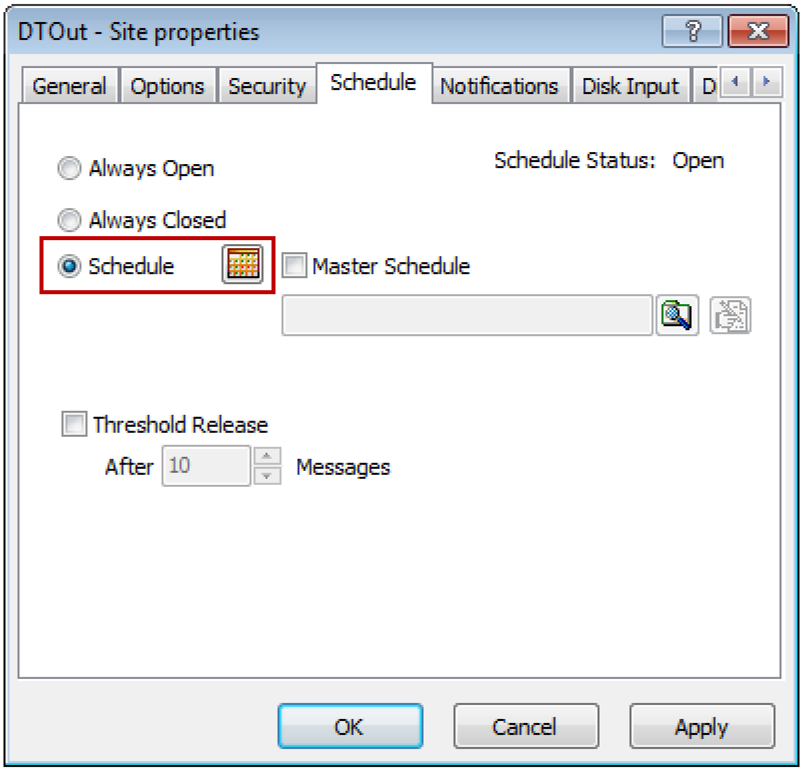
○ Schedule

Schedule Status: Open

□ Threshold Release

After 10 Messages

Users may decide to create a specific schedule that is not always open or closed. They may also create Master Location Schedules, which can be shared among locations, or which can be used as a template that is then modified. If you do not check the Master Schedule box you will create a local schedule.



DTOut - Site properties

○ Always Open

○ Always Closed

● Schedule

□ Master Schedule

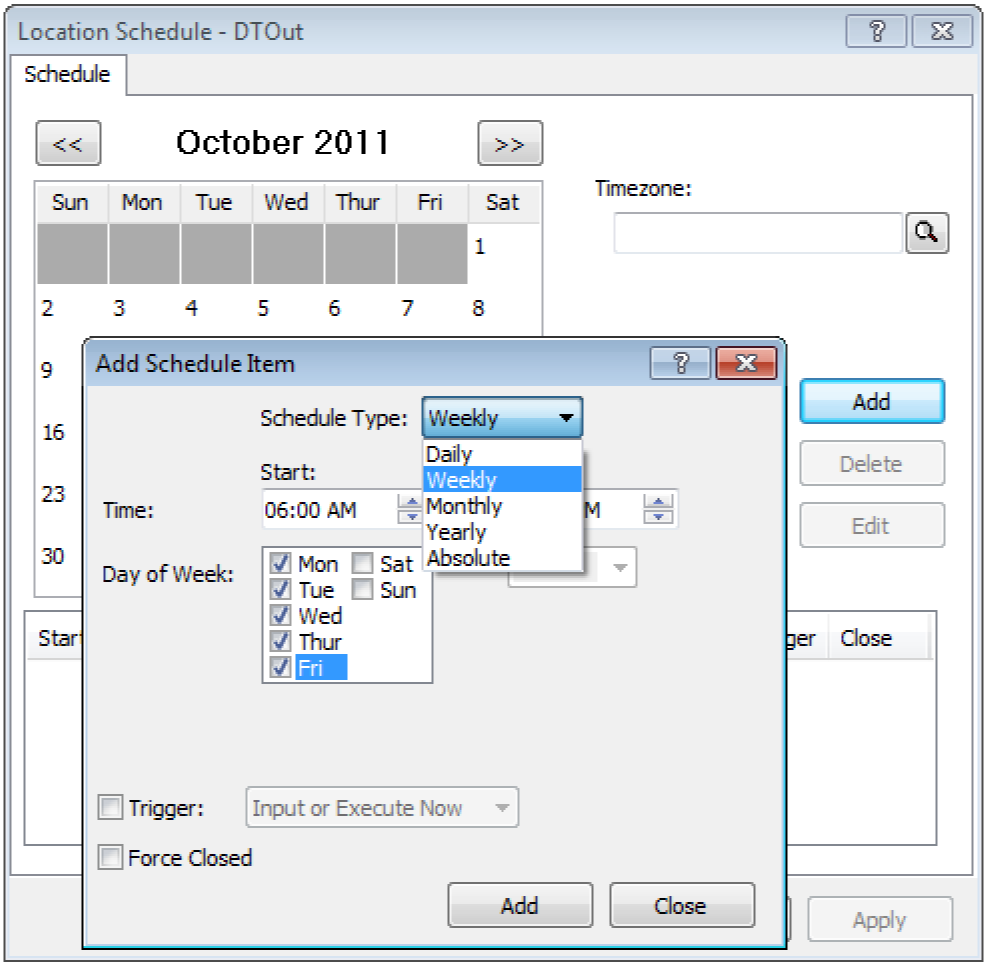
Schedule Status: Open

□ Threshold Release

After 10 Messages

Location Schedules (Schedule Page, Site Properties Window)

When a user creates a location schedule, they have the option to choose a master location schedule or to create a schedule specific to the location.



Schedule Type: Weekly

Start:

Time: 06:00 AM

Day of Week: ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☐ Sat ☐ Sun

Checking for Duplicate Messages

You may configure MessageWay to check for duplicate messages sent to a location that has a type of *Output*, *I/O* or *Service*. When a message sent to a location configured for duplicate checking is determined to be a duplicate of another message, the duplicate message is placed in error status. For more information, refer to ***Identifying Duplicate Messages*** (on page 470).

Controlling Message Flow

MessageWay provides several options to control message flow to and from the Message Store.

To control the flow of inbound messages, users may exercise control as follows:

- At the adapter or service, by stopping and starting the adapter or service
- For the location, holding and releasing messages queued to the location using schedules

To control the flow of outbound messages, users may exercise control as follows:

- At the adapter or service, by starting, suspending and stopping the adapter or service
- For the location, holding and releasing messages queued to the location using schedules (automatic) or putting the location on hold (manual)
- For a message, by holding and releasing the message

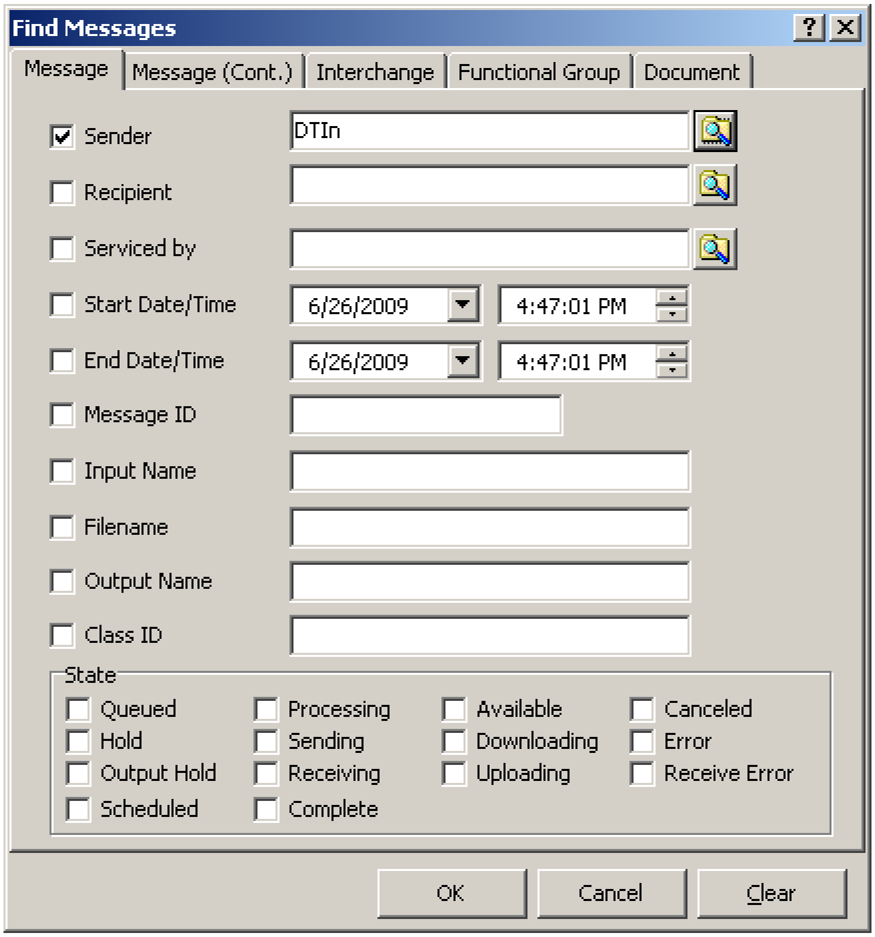
Users can perform other actions on messages that control message delivery:

- Cancel messages on hold or in error status
- Resubmit messages to the same destination that are in error or that have been delivered
- Redirect messages to a different destination that are in error or that have been delivered

Viewing Message Information

MessageWay provides a means to query the Message Store in order to find information about messages, as well as to view the content of messages.

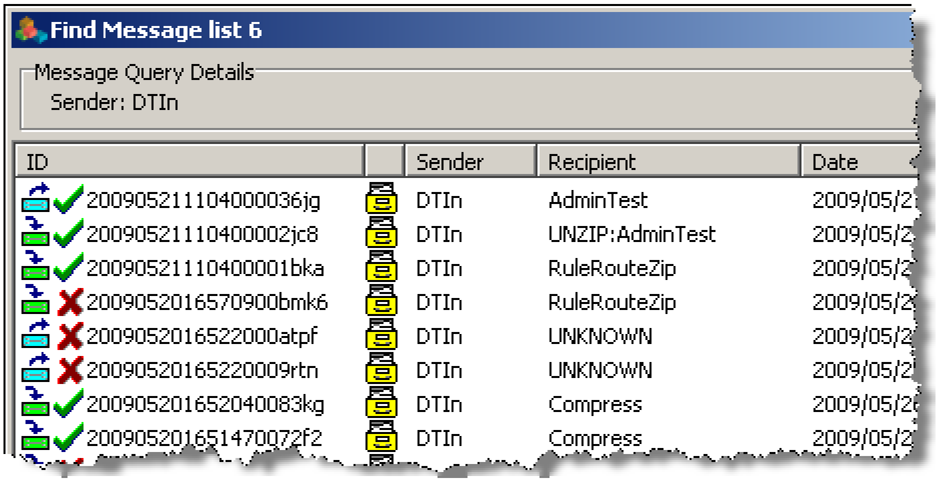
The Find Messages window allows users to perform message queries using various criteria.



☑ Sender DTIn
☐ Recipient
☐ Serviced by
☐ Start Date/Time 6/26/2009 4:47:01 PM
☐ End Date/Time 6/26/2009 4:47:01 PM
☐ Message ID
☐ Input Name
☐ Filename
☐ Output Name
☐ Class ID

State
☐ Queued ☐ Processing ☐ Available ☐ Canceled
☐ Hold ☐ Sending ☐ Downloading ☐ Error
☐ Output Hold ☐ Receiving ☐ Uploading ☐ Receive Error
☐ Scheduled ☐ Complete

When the list of messages that match the criteria displays, you select a message and then right-click, and select **Properties** from the menu.

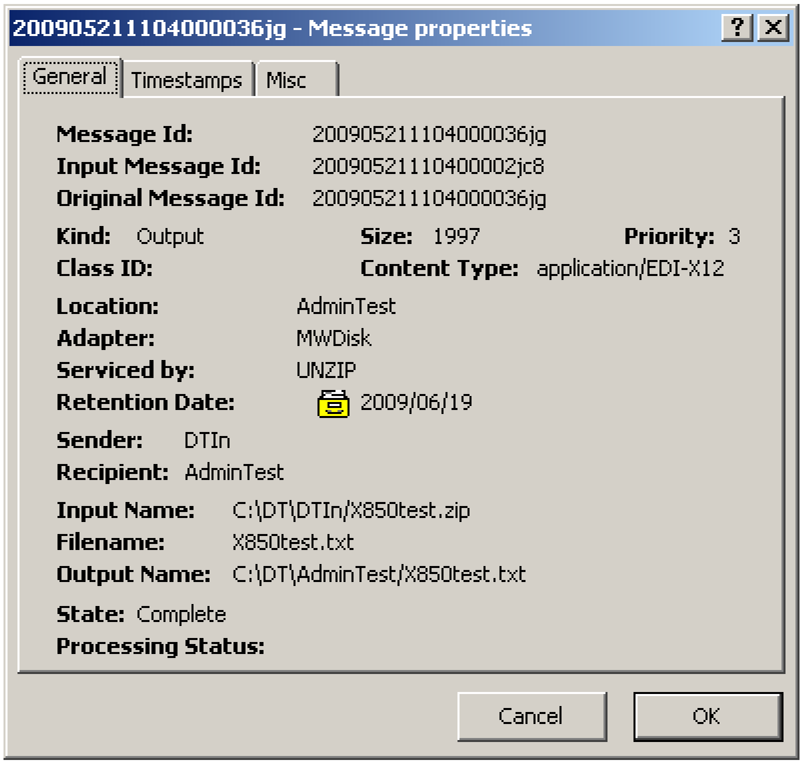


Find Message list 6

Message Query Details
Sender: DTIn

ID		Sender	Recipient	Date
✓ 20090521110400036jg		DTIn	AdminTest	2009/05/2
✓ 2009052111040002jc8		DTIn	UNZIP:AdminTest	2009/05/2
✓ 2009052111040001bka		DTIn	RuleRouteZip	2009/05/2
✗ 200905201657090bmk6		DTIn	RuleRouteZip	2009/05/2
✗ 2009052016522000atpf		DTIn	UNKNOWN	2009/05/2
✗ 20090520165220009rtn		DTIn	UNKNOWN	2009/05/2
✓ 200905201652040083kg		DTIn	Compress	2009/05/2
✓ 200905201651470072f2		DTIn	Compress	2009/05/2

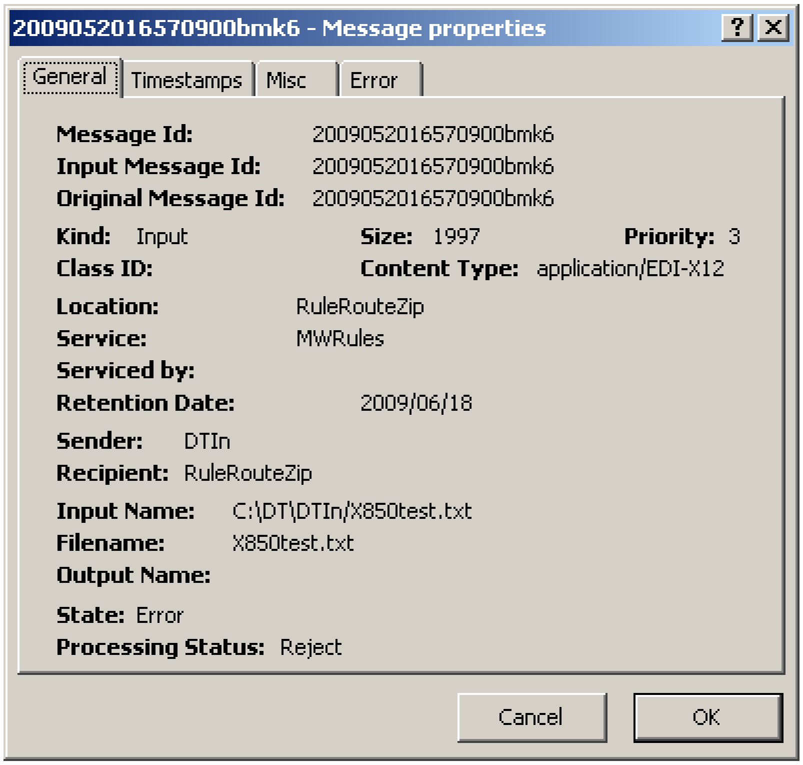
The Message Properties window displays message IDs, date and time stamps, and state, among other things.



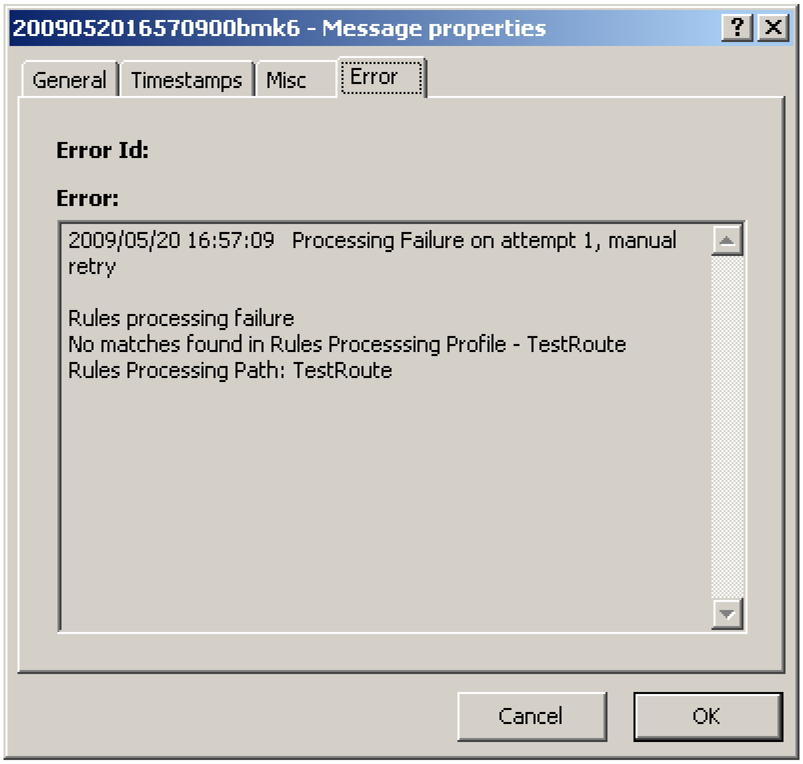
20090521110400036jg - Message properties

Message Id: 20090521110400036jg
Input Message Id: 2009052111040002jc8
Original Message Id: 20090521110400036jg
Kind: Output **Size:** 1997 **Priority:** 3
Class ID: **Content Type:** application/EDI-X12
Location: AdminTest
Adapter: MWDisk
Serviced by: UNZIP
Retention Date: 2009/06/19
Sender: DTIn
Recipient: AdminTest
Input Name: C:\DT\DTIn/X850test.zip
Filename: X850test.txt
Output Name: C:\DT\AdminTest/X850test.txt
State: Complete
Processing Status:

When the message has an error, an **Error** page appears. Additional information might also appear on the **Misc** page.



Message Id: 2009052016570900bmk6
Input Message Id: 2009052016570900bmk6
Original Message Id: 2009052016570900bmk6
Kind: Input **Size:** 1997 **Priority:** 3
Class ID: **Content Type:** application/EDI-X12
Location: RuleRouteZip
Service: MWRules
Serviced by:
Retention Date: 2009/06/18
Sender: DTIn
Recipient: RuleRouteZip
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.txt
Output Name:
State: Error
Processing Status: Reject

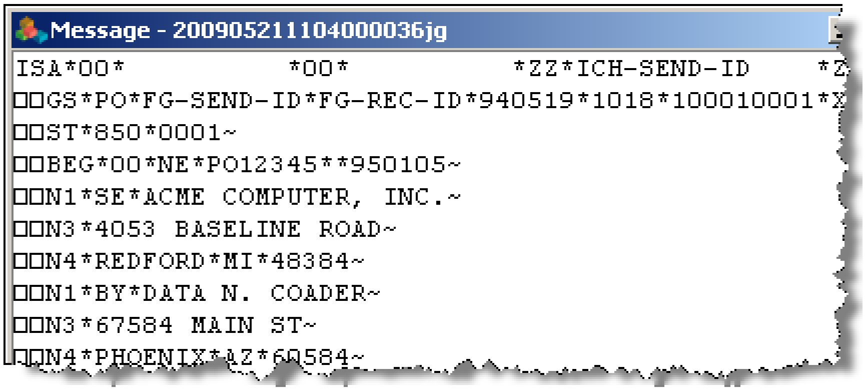


Error Id:

Error:

```
2009/05/20 16:57:09  Processing Failure on attempt 1, manual
retry

Rules processing failure
No matches found in Rules Processsing Profile - TestRoute
Rules Processing Path: TestRoute
```

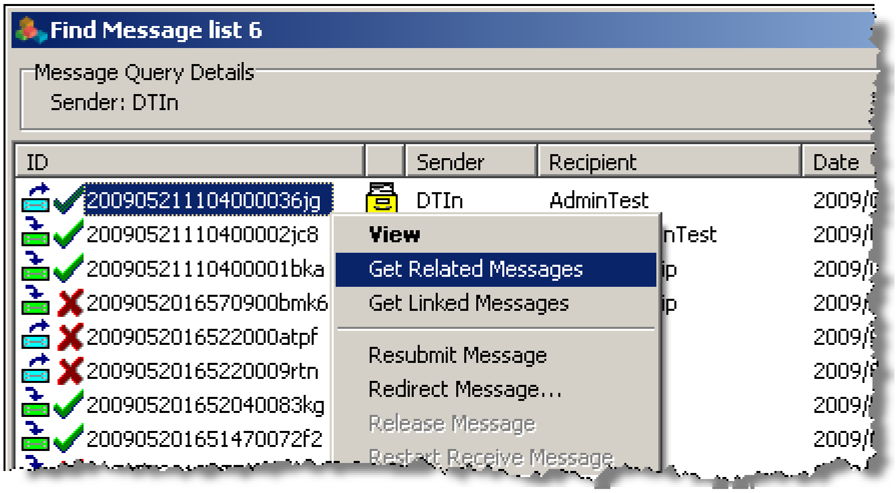
When you select **View** from the menu, the Message window displays the content of the file.



```
ISA*00*          *00*          *ZZ*ICH-SEND-ID     *Z
□□GS*PO*FG-SEND-ID*FG-REC-ID*940519*1018*100010001*X
□□ST*850*0001~
□□BEG*00*NE*PO12345**950105~
□□N1*SE*ACME COMPUTER, INC.~
□□N3*4053 BASELINE ROAD~
□□N4*REDFORD*MI*48384~
□□N1*BY*DATA N. COADER~
□□N3*67584 MAIN ST~
□□N4*PHOENIX*AZ*60584~
```

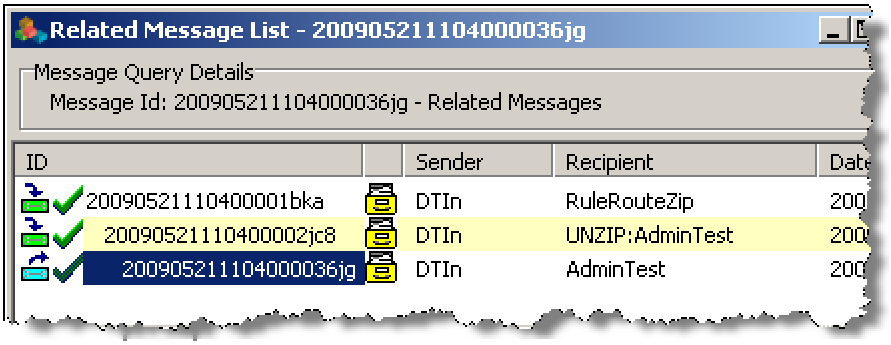
Finding Related and Linked Messages

Each message has a unique message identification comprising a message ID and the destination location. Visible on the **General** page of the Message Properties window, the value in **Message Id** is the primary key to the Messages table. The value in **Location** is the name of the destination location where the message resides. The **Input Message Id** allows the system to display messages related by processing, such as rules or compression processing. The **Get Related Messages** command displays all messages related to the one that is currently selected.



Message Query Details
Sender: DTIn

ID		Sender	Recipient	Date
✓ 200905211104000036jg		DTIn	AdminTest	2009/
✓ 20090521110400002jc8			nTest	2009/
✓ 20090521110400001bka			ip	2009/
✗ 2009052016570900bmk6			ip	2009/
✗ 2009052016522000atpf				2009/
✗ 20090520165220009rtn				2009/
✓ 200905201652040083kg				2009/
✓ 200905201651470072f2				2009/



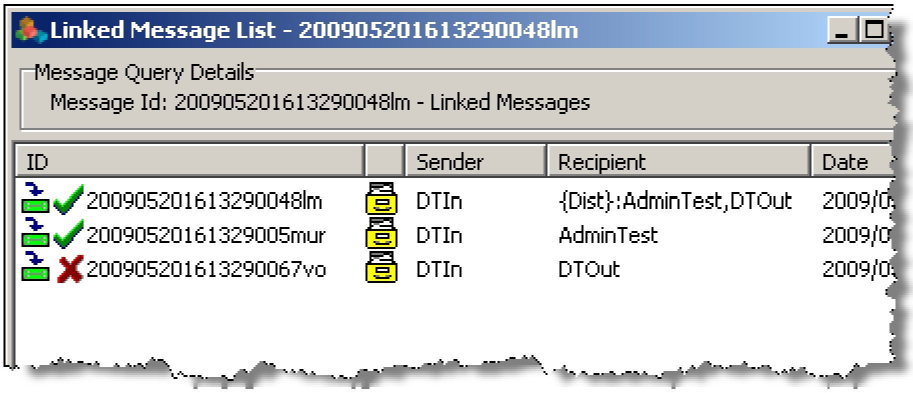
Message Query Details
Message Id: 200905211104000036jg - Related Messages

ID		Sender	Recipient	Date
✓ 20090521110400001bka		DTIn	RuleRouteZip	200
✓ 20090521110400002jc8		DTIn	UNZIP:AdminTest	200
✓ 200905211104000036jg		DTIn	AdminTest	200

Messages are typically linked because they were:

- Copies of reports sent by a service process
- Resent using the **Resubmit** or **Redirect** commands
- Sent to a distribution list service location
- Routed by the Rules Processing service

Such messages all have the same Original Message Id. The **Get Linked Messages** command displays all messages linked to the one selected.



Message Query Details

Message Id: 200905201613290048lm - Linked Messages

ID		Sender	Recipient	Date
✓ 200905201613290048lm		DTIn	{Dist}:AdminTest,DTOut	2009/0
✓ 200905201613290O5mur		DTIn	AdminTest	2009/0
✗ 200905201613290067vo		DTIn	DTOut	2009/0

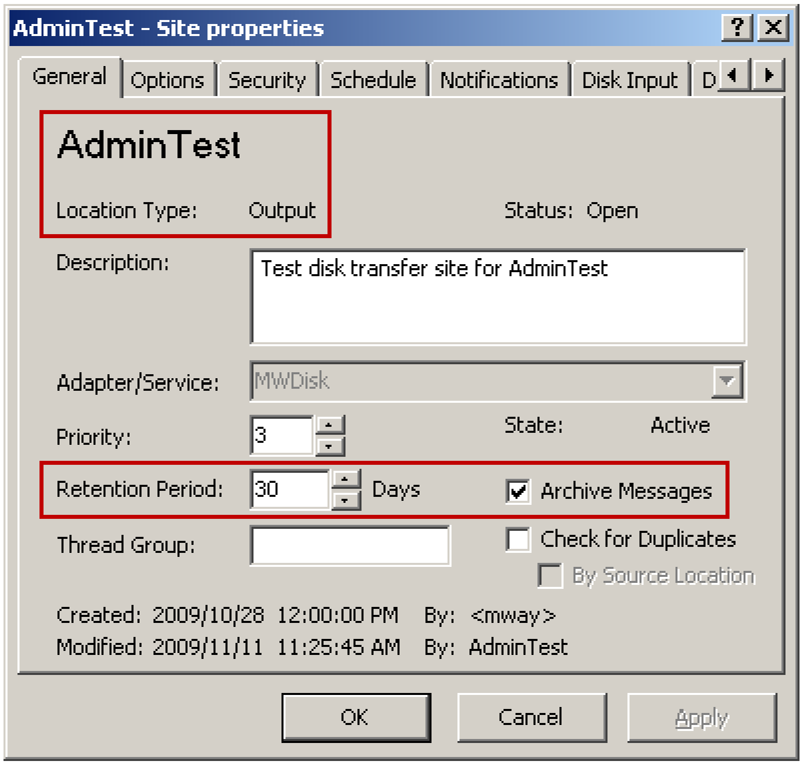
Archiving and Deleting Messages

Users have several options to run the Archive/Delete program:

- From MessageWay, scheduled automatically using the system location, {MWArchive}
- From the operating system, manually
- From the operating system, scheduled to run automatically

When run, the program will query the MessageWay database for messages to archive or delete. Note that archived messages are always deleted when they satisfy the criteria.

Users configure archiving on destination locations. By default, the *Archive Messages* box is checked. Messages delivered to this location are retained in MessageWay for the period specified in *Retention Period*, after which they become eligible for the archive/delete process.



AdminTest

Location Type: Output

Status: Open

Description: Test disk transfer site for AdminTest

Adapter/Service: MWDisk

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

☐ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 11:25:45 AM By: AdminTest

For more information about the archive process, refer to the topic, ***Maintaining Message Information*** (on page 783).

Retrieving Messages from Archive

The Archive Retrieve program retrieves messages from archive. These retrieved archive messages are stored in the Archive Retrieve message store, separate from the message store. The Archive Retrieve message store has two storage options, just like the message store; on disk or in the database. Which storage option is used is based on the storage option of the message before it was archived, and cannot be changed. Messages retrieved into the Archive Retrieve message store do not yet exist as messages in any locations, but can still be viewed using the **Find Archive Messages** function. Messages retrieved from archive only exist as messages in locations after the **Resubmit to MessageWay...** function is performed.

NOTE: Archive zip files that have been moved or renamed in the archive directory cannot be retrieved from. Restoring archive zip files back to their original location or name will restore the ability to retrieve messages from them.

Regarding access rights, all actions performed against messages retrieved from archive are determined by the rights assigned to the location where the message was originally archived from. If the location no longer exists, then only 'Administrator' users can access the retrieved messages. The following access rights are required for the following actions:

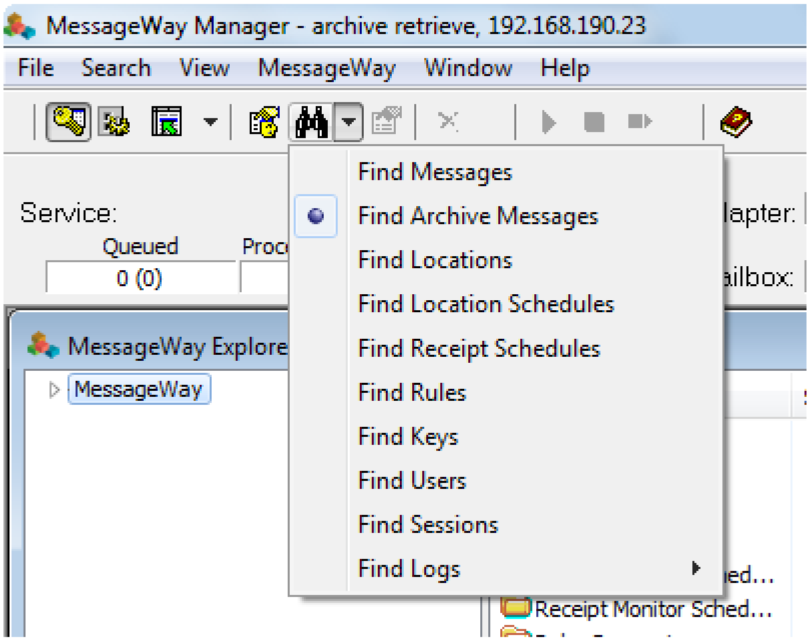
Action	Right
View Retrieved Message(s)	View Messages.
Retrieve from Archive	Retrieve Archive Messages.
Resubmit Retrieved Message(s)	Resubmit Archive Messages (on both the original location and system location {RetrievedMessages}).
Delete Retrieved Message(s)	Delete Archive Message Content.

There are two scenarios related to Archive Retrieve which require different steps to achieve:

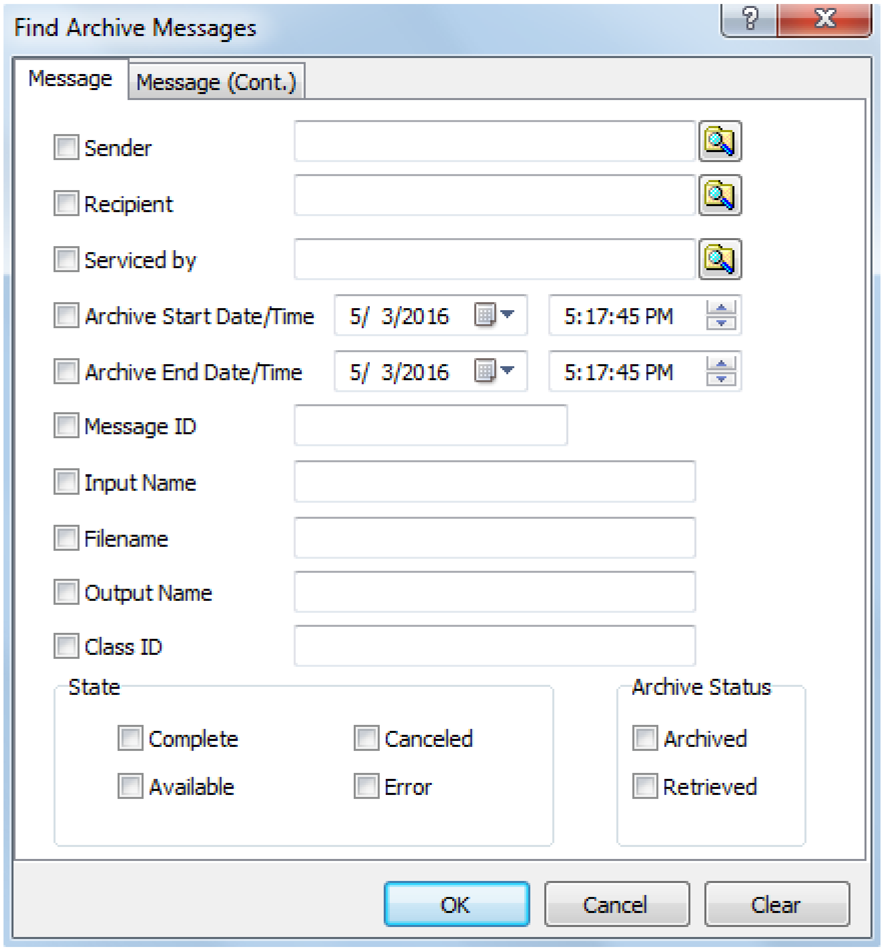
- Retrieve message(s) in order to view message content
- Retrieve message(s) in order to resend to either original recipient or a new recipient

Both scenarios start out the same way:

- Use **Find Archive Messages** to find archived messages that you want to retrieve:



and fill in the appropriate selection criteria:



□ Sender

□ Recipient

□ Serviced by

□ Archive Start Date/Time 5/ 3/2016 5:17:45 PM

□ Archive End Date/Time 5/ 3/2016 5:17:45 PM

□ Message ID

□ Input Name

□ Filename

□ Output Name

□ Class ID

State

□ Complete □ Canceled

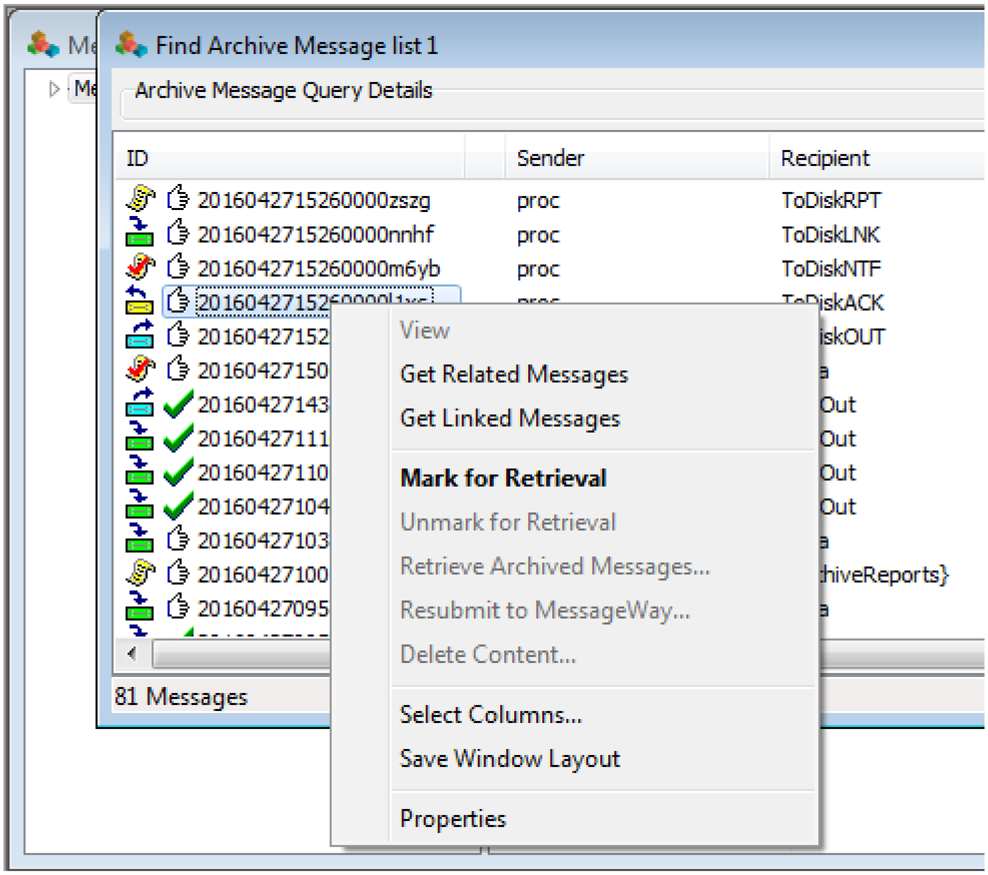
□ Available □ Error

Archive Status

□ Archived

□ Retrieved

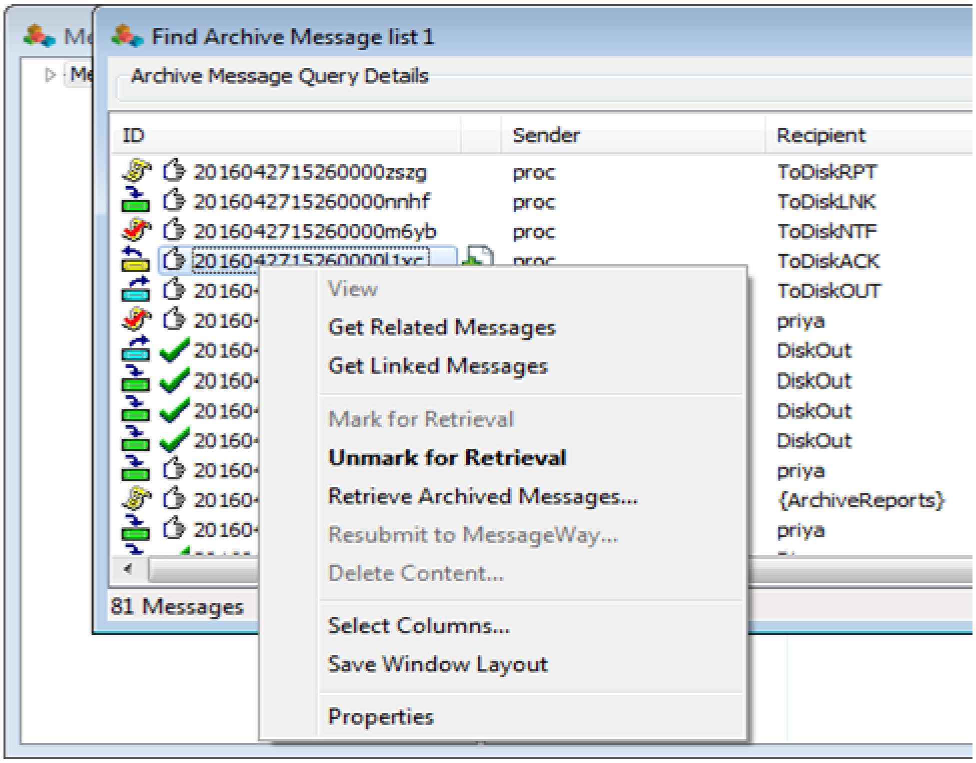
- Next select one or more messages to ‘Mark for Retrieval’:



ID	Sender	Recipient
2016042715260000zszg	proc	ToDiskRPT
2016042715260000nnhf	proc	ToDiskLNK
2016042715260000m6yb	proc	ToDiskNTF
2016042715260000l1xc	proc	ToDiskACK
20160427152		iskOUT
20160427150		a
20160427143		Out
20160427111		Out
20160427110		Out
20160427104		Out
20160427103		a
20160427100		hiveReports}
20160427095		a

81 Messages

If you change your mind, you can select ‘Unmark for Retrieval’:



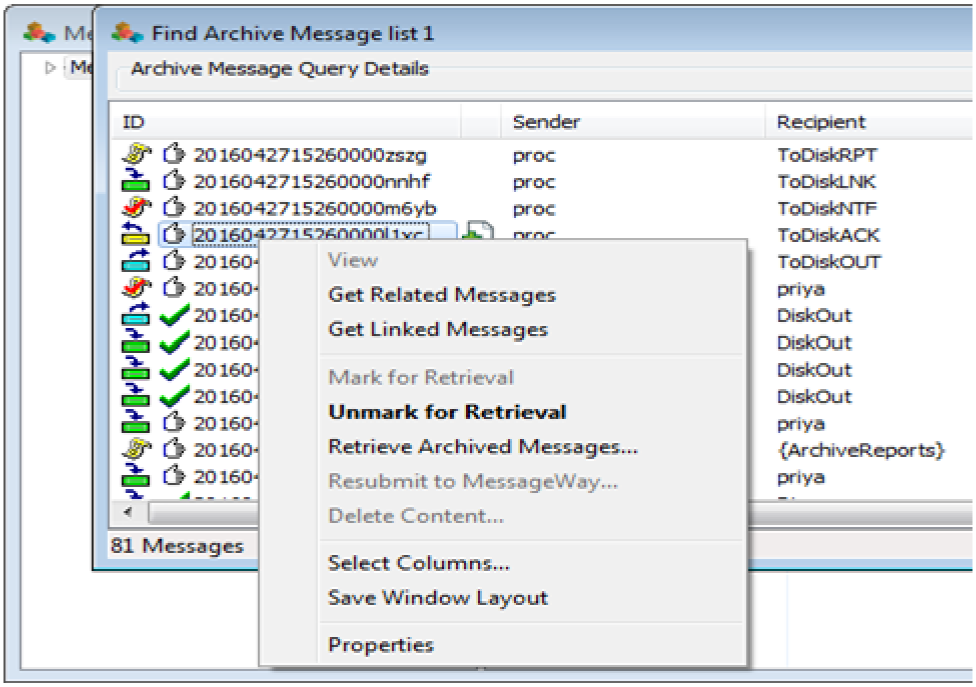
Find Archive Message list 1

Archive Message Query Details

ID	Sender	Recipient
2016042715260000zszg	proc	ToDiskRPT
2016042715260000nnhf	proc	ToDiskLNK
2016042715260000m6yb	proc	ToDiskNTF
2016042715260000l1xc	proc	ToDiskACK
20160		ToDiskOUT
20160		priya
20160		DiskOut
20160		DiskOut
20160		DiskOut
20160		DiskOut
20160		priya
20160		{ArchiveReports}
20160		priya

81 Messages

- Next select ‘Retrieve Archived Messages…’:



Find Archive Message list 1

Archive Message Query Details

ID	Sender	Recipient
2016042715260000zszg	proc	ToDiskRPT
2016042715260000nnhf	proc	ToDiskLNK
2016042715260000m6yb	proc	ToDiskNTF
2016042715260000l1xc	proc	ToDiskACK
20160		ToDiskOUT
20160		priya
20160		DiskOut
20160		DiskOut
20160		DiskOut
20160		DiskOut
20160		priya
20160		{ArchiveReports}
20160		priya

81 Messages

The user can monitor the retrieval process in the Manager, and when complete, view the resulting report file in system location {ArchiveReports}.

NOTE: The Manager will keep track of all messages marked for retrieval within each session even if they occur across multiple archived message lists. As long as the Manager is running, the marked messages will be remembered, even if the session times out. If you re-logon with the same Manager instance under the same system and user Id, then the last session marked messages will be retained. It will be possible to search for all messages that are marked for retrieval by the current session. Note that messages marked for retrieval by one Manager session cannot be retrieved by another Manager session except as described above.

For information about viewing retrieved message content or resending retrieved messages from archive, refer to the topics **Viewing Messages Retrieved from Archive** or **Resending Messages Retrieved from Archive** under, ***Maintaining Message Information*** (on page 783).

MessageWay System Components

The core of the system includes the Messaging Server, the Message Store, the Archive Retrieve Message Store and the adapters and services.

MessageWay consists of several real-time multi-threaded servers that interact to provide store-and-forward messaging. All servers must reside on the same local system. The following table describes the primary functions of each of the base system components:

Component (Name)	**Function**
Messaging Server (MessageWay)	Does the following: ▪ Starts and stops other servers ▪ Maintains the Message Store ▪ Triggers delivery actions ▪ Processes requests from adapters and services ▪ Processes requests from Scheduling server ▪ Processes requests from Service Interface
User Server (MWUser)	Does the following: ▪ Processes logon requests from MessageWay Manager ▪ Provides other user security
Service Interface (MWSI)	Controls access to MessageWay from external servers and interfaces: ▪ (Option) MessageWay AS2 Interface ▪ (Option) MessageWay FTP Server ▪ (Option) MessageWay SFTP Server ▪ (Option) MessageWay Web Client
Scheduling Server (MWSched)	Does the following: ▪ Sends requests to Messaging Server to open and close schedule ▪ Provides monitor service for Remote Execution Server

Component (Name)	Function
Receipt Monitor	Monitors receipt of messages from specific addresses
Archive/Delete program (MWArchive)	Maintains the Message Store and the Archive Retrieve Message Store. Also maintains the archive zip files and the archive directory
Archive Retrieve program (MWArchRetrieve)	Provides ability to retrieve messages that have been archived
Adapters	Provide input/output client services for various communications protocols
Services	Provide internal services to process messages

Messages may be sent to other MessageWay systems on the LAN via direct interaction between two Messaging servers. The sending system makes a request of the receiving system. The receiving adapter accesses the message file to be transferred directly from the sending message store. When the transfer is complete, the sending Messaging server is notified.

For any messaging system, data integrity is of prime importance. Messages must not be lost or duplicated. Since all computer systems can fail at times, the system is designed to recover properly when restarted. Unfinished work in progress may need to be completed or backed out. This responsibility resides mainly with the adapters and services. The Messaging Server will perform services for these adapters and services. If a task, such as inserting a message into the message store, does not complete, then it is the responsibility of the adapter or service to repeat the action after restart. The Messaging server is able to reject duplicate messages based on Message ID and configuration settings.

MessageWay Unicode Support

MessageWay supports Unicode encoded characters and strings from the Basic Multi-Lingual plane. This includes support for characters, symbols, and ideographs from most modern day languages. You can type or paste Unicode strings directly to the MessageWay Manager, and these characters will be successfully stored and retrieved from the MessageWay database.

NOTE: Windows XP SP3 may not display special Unicode characters correctly if you have installed a localized version vs. the Multilingual User Interface (MUI) Pack version of Windows, and you have not installed the appropriate language support packages. To display all supported special characters, download and install the MUI Pack and any appropriate language packages.

Most of our MessageWay utility programs also support Unicode characters and strings and can be executed through Unicode capable terminals. Keep in mind that MessageWay does interface with many different third-party programs through our adapters and services. While most interfaces support the transfer of Unicode encoded data, some may not.

How Unicode Data is Stored in the MessageWay Database

As of version 6.1, MessageWay uses Unicode encoding to store data in the MessageWay database. To support Unicode characters across all database platforms, it uses UCS-2 (a double byte encoding) for variable character columns. For text/blob columns, it uses UTF-8 (a multi-byte encoding) to reduce storage requirements for large amounts of ASCII data. MessageWay handles all Unicode encoded strings as UTF-8, so when we extract UCS-2 data from the database, it is converted to UTF-8 for use throughout the software and utilities. Use the following table and the database schema to identify which columns types use which Unicode encoding.

	MSSQL	**MySQL**	**Oracle**
UCS-2	nvarchar	varchar character set ucs2	nvarchar2
UTF-8	text	text	clob

IMPORTANT: Any scripts or programs you have that pull data directly from the database must anticipate these encodings in the table and interpret them accordingly. Any scripts or programs you have that use data from MessageWay utilities will need to anticipate UTF-8 encoded data.

Please contact MessageWay Technical Support if you need help.

How to Set Up Terminals to Interpret Unicode Data in UNIX/Linux Databases

PuTTY– Use these instructions to enable UTF-8 character interpretation with remote sessions to Linux and Solaris.

1. Open PuTTY.
2. Navigate to *Translation* under the *Window* heading.
3. Set *Remote character set* to **UTF-8**.

Gnome Terminal – Use these instructions to enable UTF-8 character interpretation on Linux and Solaris.

1. Open the user’s .bashrc file (Typically /home/mway/.bashrc).
2. Type the following:

   ```
   export LANG=en_US.UTF8
   ```
3. Save and close .bashrc.
4. Restart your terminal session.
5. In the terminal’s menu bar, select **Terminal** > **Set Character Encoding** > **UTF-8.**

Unicode Issues

Here is a list of issues you may encounter with Unicode characters in MessageWay.

Component Affected	Unicode Issue
MessageWay command-line utilities issues by platform	There may be readability and input issues for Unicode characters when running MessageWay utilities via command line and examining supported databases. ▪ On Windows, by default the cmd.exe and cygwin console are incapable of displaying non-ASCII Unicode characters and MessageWay utilities run through these consoles are unable to interpret non-ASCII Unicode arguments. This includes utilities run through batch scripts or other programs. For additional information about Windows specific utilities, please see the next release note. ▪ On Linux and Solaris, non-ASCII Unicode characters should display correctly, but there are some cases where they are displayed as question-marks. We recommend you set the OS default character-set to UTF-8. ▪ On MySQL shell, non-ASCII Unicode characters in text columns will not be displayed correctly. ▪ On MSSQL Management Studio, non-ASCII Unicode characters in text columns will not be displayed correctly. ▪ On Oracle through ISQL and SQL+, non-ASCII Unicode characters in nvarchar2 and clob columns will not be displayed correctly.

MessageWay command-line utilities on Windows

The following utilities will *not* support Unicode characters for parameters on any Windows platform. Standard output will also be unreadable via a console. If this output is redirected to an ASCII file name, the content will support Unicode characters and can be viewed if it is interpreted from an application that supports UTF-8 (for example, Notepad).

- dbconvert
- dtd2trn
- mwadmin
- mwcfgsrc
- mwchkaudloginteg
- mwexp
- mwimp
- mwkeygen
- mwlogdump
- mwres
- mwrestart
- mwsql
- mwswitch
- mwtrace
- siclient
- wsiclient
- xsdparser

The following components pull a file name from the messageway.conf config file under the "TempFilePath" tag. This file name is used to log server audit information if the project is built with "_TEXT_LOG" defined. The file name will not support Unicode characters on any Windows platform.

- logsrv
- rcnsrv

MessageWay User Policies for Passwords

User password policies treat all non-ASCII Unicode characters as special characters. It is not possible to have MessageWay regard a character as upper-case or lower-case, for instance, unless that character belongs to the ASCII subset of Unicode.

MessageWay Message window

When MessageWay Manager displays the contents of a message, only ASCII characters are recognized. Non-ASCII Unicode characters are treated as if they are unprintable and replaced with periods.

FTP and SFTP clients

To use and/or display non-ASCII Unicode characters in users, locations, and file names through the MessageWay FTP and SFTP perimeter servers, FTP and SFTP clients must support Unicode (specifically UTF-8).

MessageWay Compression Service

The MessageWay Compression Service MWCompress does not support zip files encrypted with Unicode characters in the password.

The Linux/Solaris unzip command line utility cannot decompress zip archives from MWCompress that contain file names with Unicode characters. As an alternative, use MWCompress GZip compression for archives with Unicode character file names that are delivered to Linux systems.

MessageWay Remote Execution Server (RES)

(Windows) The MessageWay Remote Execution Server and the MWRES utility *do not* currently support Unicode characters on Windows systems. They *do* support Unicode on UNIX/Linux systems.

Configuring MessageWay Internal Servers

This section describes how to configure the internal servers for MessageWay.

The following are internal servers whose configurations are discussed here:

- MessageWay Messaging Server
- MessageWay Service Interface (mwsi)
- MessageWay User Server
-

IMPORTANT: Each server has its own configuration file. After you first install MessageWay, you should review the options in the configuration file and set them to suit your needs. Subsequent installs or upgrades will never overlay the configuration file. However, as new parameters are added to provide additional functionality, they will appear in an updated sample configuration file, for example mwsi.conf.samp. To implement a new feature, you should open the sample configuration file and copy the appropriate parameter and its description into your configuration file, for example mwsi.conf.

Setting Server Startup Options

When needed, some servers must be started when MessageWay starts. All except MWArchive, which is not truly a server, can also be started manually within MessageWay.

NOTE: MWArchive provides configurations for the Archive/Delete program and is not a startable server. MessageWay always starts the User Server, so there is no option to start or stop the server from the MessageWay Manager.

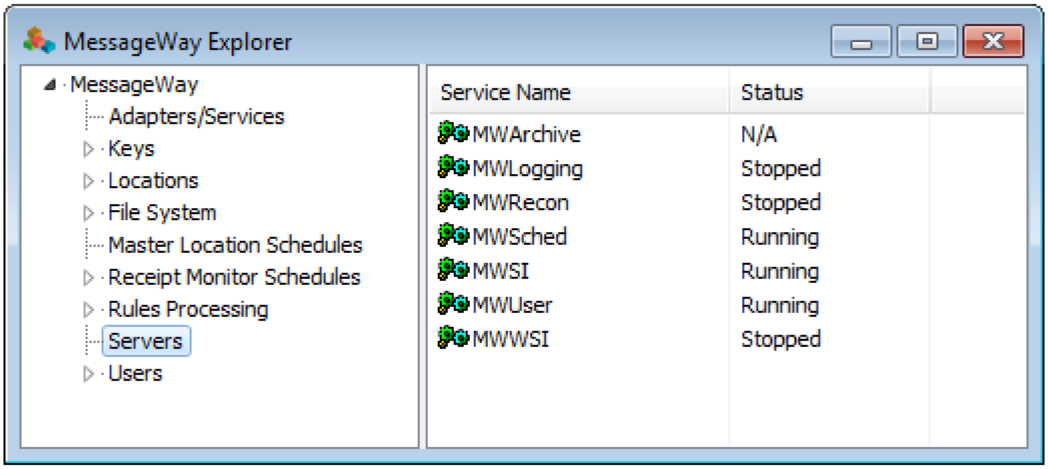
Users may set startup options for the following servers:

Server	Use
Logging (MWLogging)	Only used for the ***MWTranslator*** (on page 902) option.
Reconciliation (MWRecon)	Only used for the ***MWTranslator*** (on page 902) option. The Logging Server must also be running.
Schedule (MWSched)	Supports location schedules, receipt monitor schedules, monitoring for the Remote Execution Server, triggers to retry message delivery and removal

Server	Use
	of inactive sessions.
Service Interface (MWSI)	Used with the ***FTP Perimeter Server*** (on page 186), ***SFTP Perimeter Server*** (on page 298), Web Client and ***AS2 Interface*** (on page 114).
User	Defines the number of messages and/or archive messages returned and then the number displayed at one time when MessageWay displays message lists for this user.

To set startup options for these servers, proceed as follows:

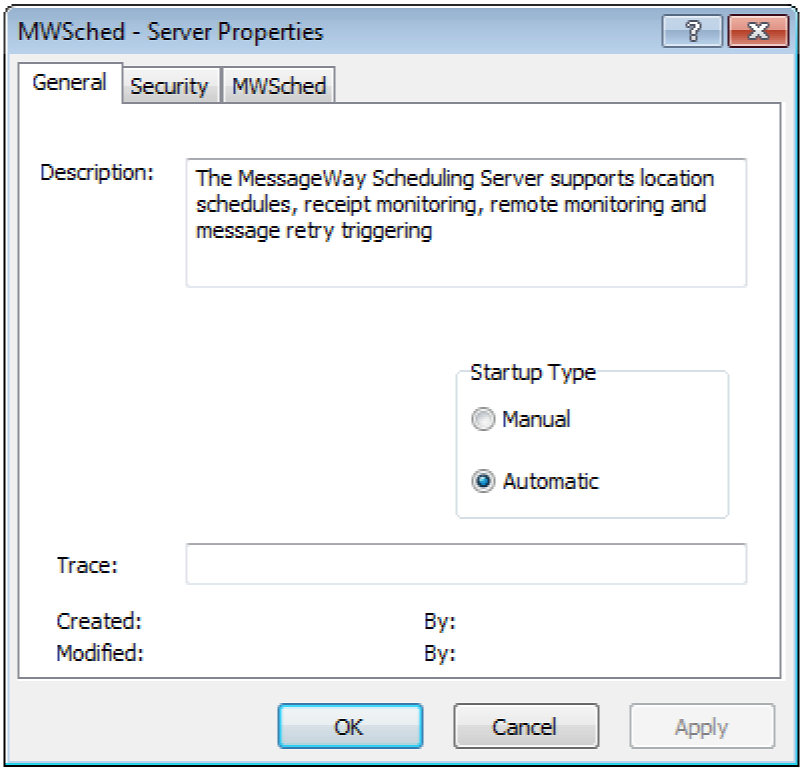
1 From the left pane of MessageWay Explorer, select the **Servers** folder.



Service Name	Status
MWArchive	N/A
MWLogging	Stopped
MWRecon	Stopped
MWSched	Running
MWSI	Running
MWUser	Running
MWWSI	Stopped

2 In the right pane, double-click a server.

The Server Properties window appears.



MWSched - Server Properties

Description: The MessageWay Scheduling Server supports location schedules, receipt monitoring, remote monitoring and message retry triggering

Startup Type

○ Manual

● Automatic

Trace:

Created: By:

Modified: By:

3 On the **General** page, for the Startup type, select one of the following:

- **Manual** to start the server from the Manager

  - or -

- **Automatic** to have MessageWay start the server when it starts

Configuring the MessageWay Messaging Server

The MessageWay Messaging Server, also called the MessageWay Server, is the backbone of MessageWay.

Overview of MessageWay Server Configurations

Only one MessageWay Server runs per machine. The server and all of its components and database configurations constitute environments. The server accesses local and remote databases. The MessageWay configuration file identifies the operating parameters for the MessageWay server, which include:

- Connection options for environments
- MessageWay Server properties
- MessageWay configuration file parameters

Changing the Location of the Message Store Directory

The Message Store directory is where MessageWay writes files when the data content is configured to be stored on disk. To change the location of the Message Store directory, add the following line to the MessageWay Server configuration file before the final </MessageWay> tag:

<MsgStoreDir>*NewLocationOfMessageStore***</MsgStoreDir>**

For an example, refer to the topic, ***MessageWay Messaging Server Configuration File*** (on page 89).

MessageWay Connection Options for Environments

You must tell the MessageWay Manager what MessageWay system or systems you want to access. To do this, you create environments and associate one or more MessageWay systems with an environment.

To monitor multiple MessageWay environments concurrently, users may run multiple copies of the MessageWay Manager on one machine, or they may monitor multiple systems within a single environment, or they may do some combination of these.

To monitor and configure other systems, you can easily add and remove environments. The names that you give to environments and systems within environments are specific to each MessageWay Manager. For more information about remote access, refer to the section ***Overview of Remote Access*** (on page 443).

Users select an environment from the MessageWay Manager. They can then use the Connection Options window to tell MessageWay which system or systems are associated with this environment. When the server is called (local), it is on the same Windows system as the MessageWay Manager. To point to remote systems, users would enter an IP address.

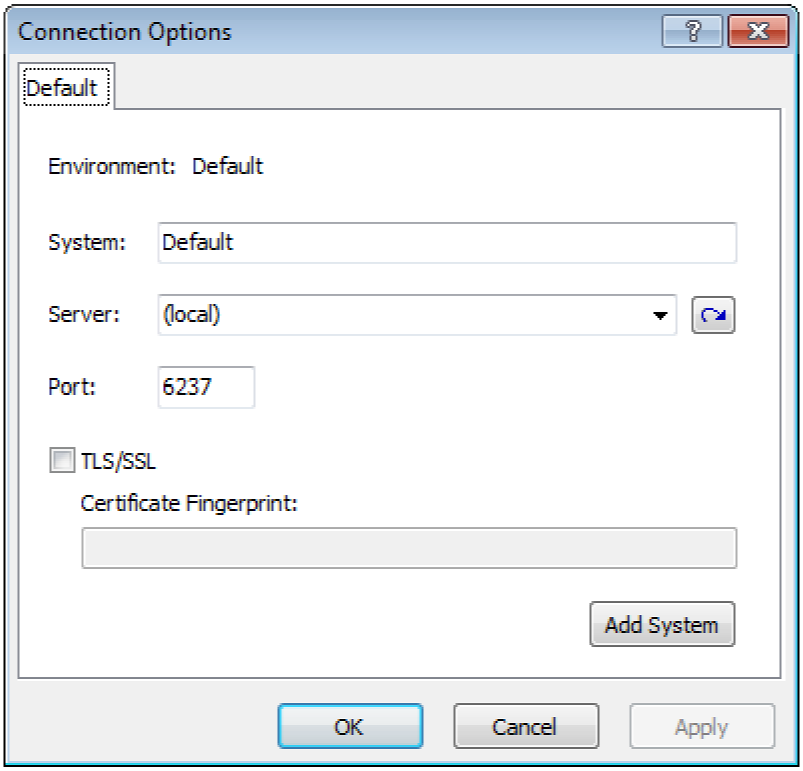
1 First, you must select an environment to monitor.

- To select an existing environment, click the arrow next to the Select Environment button, .
  - or -
- To assign an environment name or to remove an environment, from the Manager click the **Select Environment** button .

2 Then you can change the connection options for the environment.

- To access the Connection Options window, select the **Options** button from the toolbar.

  When an environment includes only one system, typically the environment name is the same as the system name. The name on the tab is the system name.



Connection Options

Default

Environment: Default

System: Default

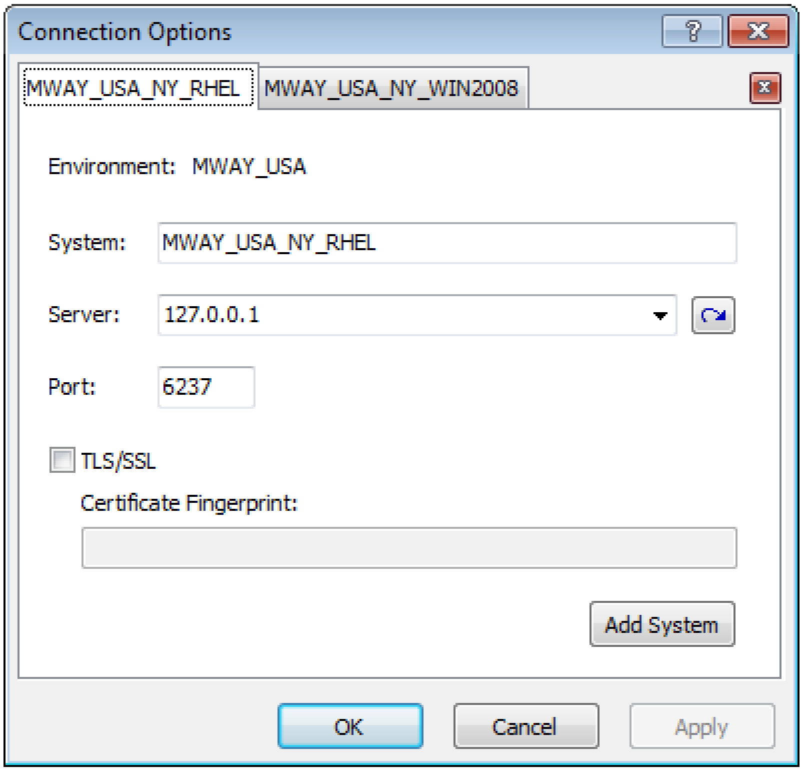
Server: (local)

Port: 6237

□ TLS/SSL

Certificate Fingerprint:

An environment can monitor up to 4 MessageWay systems. Since there is only one server per machine, each system has its own server address. When an environment monitors more than one MessageWay server, typically the environment name is different than any of the system names.



Environment: MWAY_USA

System: MWAY_USA_NY_RHEL

Server: 127.0.0.1

Port: 6237

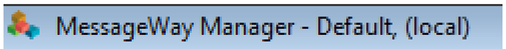
□ TLS/SSL

Certificate Fingerprint:

- To show all environments currently available, click the **Refresh List** button, ↻.
- To use TLS/SSL to connect to MessageWay for more security, check this box, and then enter the fingerprint the Manager uses to authenticate the MessageWay User Server (MWUser).
- To monitor multiple systems, from the Connection Options window click the **Add System** button, which adds a new system tab.
- To delete a system from an environment, select the tab and click the delete button, , to the right of the tabs.

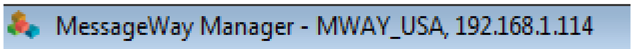
MessageWay Server Properties

The current environment and server appear in the title bar. As a local user, your current environment typically will be *Default* and the server will be listed as *(local)*.



MessageWay Manager - Default, (local)

For users viewing multi-system environments, the title bar shows the name of the environment and its location, when a specific system is selected. When you do not select a specific system, the location is blank.



MessageWay Manager - MWAY_USA, 192.168.1.114

The MessageWay Properties window contains configurations specific to that server.

How to Access the MessageWay Server Properties Window

Open the MessageWay Server Properties window as follows:

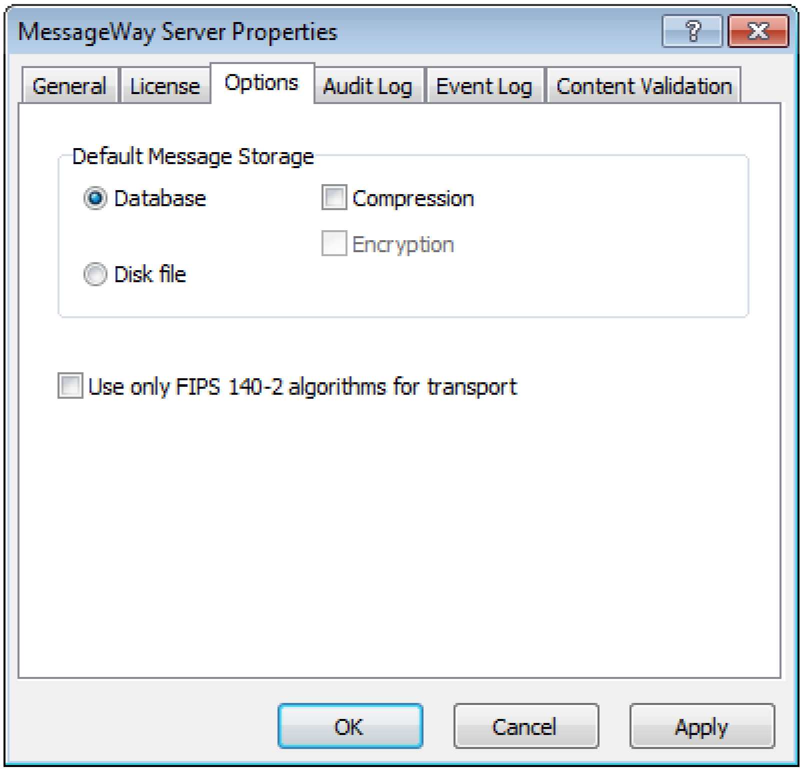
1. From the left pane of MessageWay Explorer, select **MessageWay.**
2. From the right pane, double-click **MessageWay Server**.

Configuring Options to Store Message Content

The **Options** page of the MessageWay Server Properties window allows users to specify where to store the message content: in the MessageWay database or on disk. Disk storage is the default.

For database storage, users may also select whether to compress and/or encrypt the content. This page also provides a system default for file name masks, so that an output file will always have a file name in case one is not assigned otherwise.

The **Encryption** field is dimmed until a user ***adds a master key*** (on page 834).



Default Message Storage

● Database

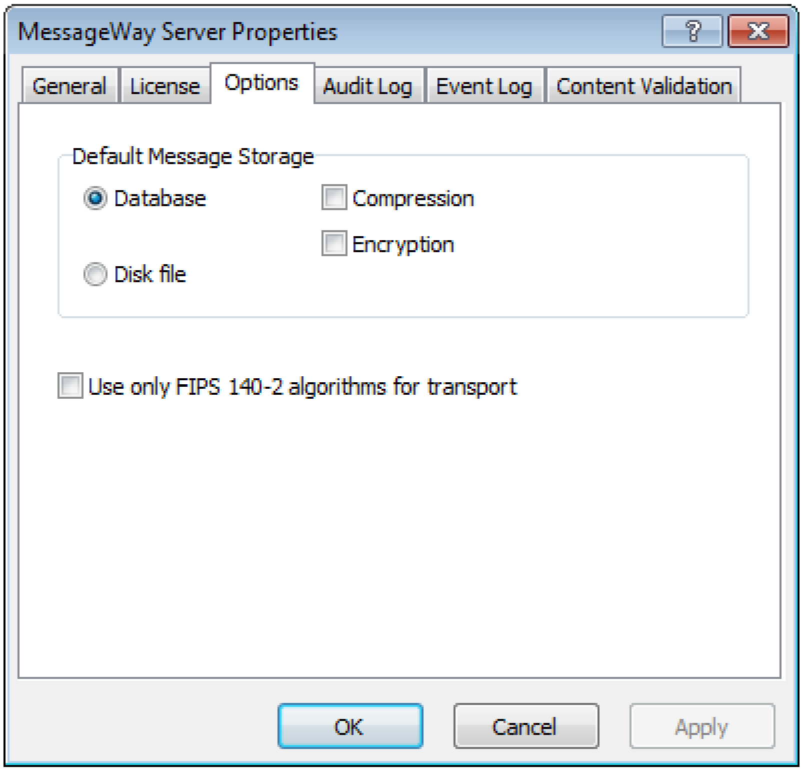
□ Compression

□ Encryption

○ Disk file

□ Use only FIPS 140-2 algorithms for transport

The **Encryption** field is available after a user adds a master key.



Default Message Storage

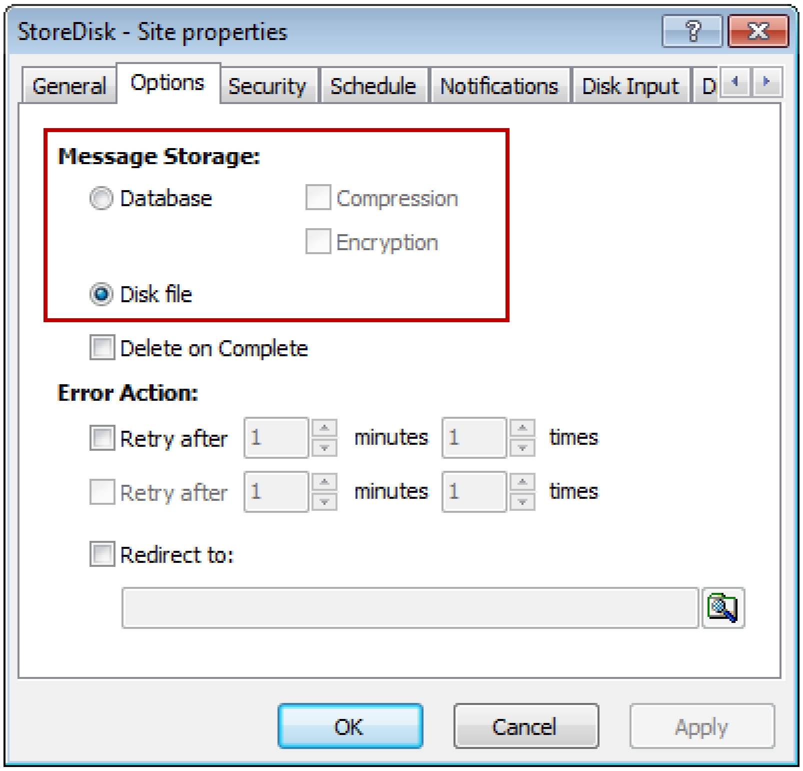
● Database ☐ Compression

☐ Encryption

○ Disk file

☐ Use only FIPS 140-2 algorithms for transport

Users may override this setting on the **Options** page for a location.



Message Storage:

○ Database ☐ Compression

☐ Encryption

● Disk file

☐ Delete on Complete

Error Action:

☐ Retry after 1 minutes 1 times

☐ Retry after 1 minutes 1 times

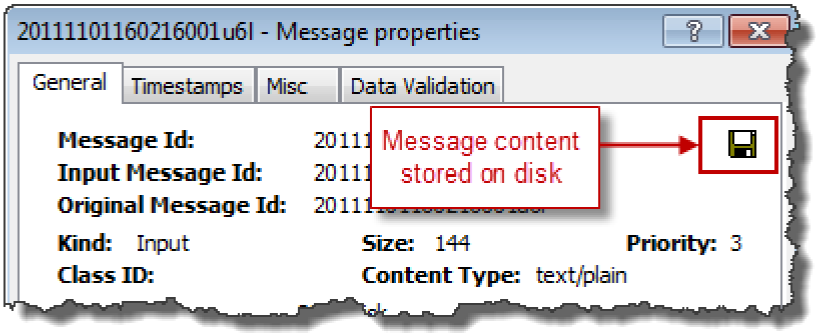
☐ Redirect to:

IMPORTANT: To be able to check the box to encrypt data content in the database, users must first add a master key. A master key is not created during installation. To create and maintain master keys, use the mwadmin utility. For more information, refer to the topic, ***Utility for Database, User, and Master Key Administration*** (on page 830).

The storage options for message content and their representative icons are as follows:

Icon	Storage Option
None	SQL database, no encryption, no compression
🔑	SQL database, Encrypted
🗜	SQL database, Compressed
💾	Disk
❌	Deleted from Message Store after successful delivery

The **General** page of the Message Properties window displays icons to the right of the Message ID to show where and how the message content is stored. No icons indicate that the content is stored in the database, unencrypted and uncompressed. The following figure shows the icon that indicates the message content is stored on disk.



Message Id: 20111
Input Message Id: 20111
Original Message Id: 20111
Kind: Input **Size:** 144 **Priority:** 3
Class ID: **Content Type:** text/plain

Message content stored on disk

Configuring Secure File Transfer

MessageWay provides a system-wide setting to control secure file transfer that determines whether such transfers invoke FIPS (Federal Information Processing Standard) 140-2 encryption algorithms or standard encryption algorithms configured by the user for a particular adapter or server.

FIPS is a standard published by the U. S. National Institute of Standards and Technology (NIST), a non-regulatory agency of the U. S. Department of Commerce. NIST works to establish various standards that the U.S. military and various government agencies must follow. Therefore, vendors, contractors, and any organization working with the government and military must also comply with these standards where they are required. Additionally, despite the fact that FIPS is a U.S.-developed standard, the Canadian government has similar policies requiring FIPS-validated software.

This setting is on the Options tab of the MessageWay Server Properties window and it uses the FIPS option by default for new installs. Users may turn the FIPS option off or on.

To Use Standard Modes (non-FIPS) for Secure File Transfer

When FIPS mode is not enabled, MessageWay encrypts any files sent via SSH, FTP with SSL, or HTTPS using configurations specified for the specific adapter or server.

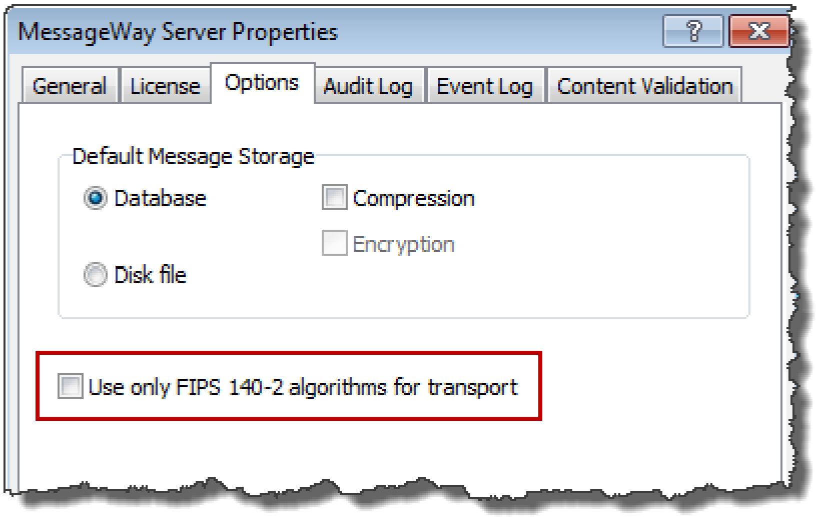
CAUTION: FIPS mode is a system-wide setting that is on by default for new installs only, not upgrades, and overrides any other encryption settings for adapters and MessageWay servers. This is a change to earlier default behavior of MessageWay secure file transfers. To revert to previous behavior, you must disable FIPS mode.

To disable FIPS Mode:

1 In the left pane, click **MessageWay**, and in the right pane double click **MessageWay Server**.

The MessageWay Server Properties window appears.

2 On the **Options** page, clear the box **Use only FIPS 140-2 algorithms for transpor**t.



MessageWay Server Properties

Options tab

Default Message Storage

● Database

○ Disk file

□ Compression

□ Encryption

□ Use only FIPS 140-2 algorithms for transport

3 Restart the MessageWay server.

To Use FIPS Mode for Secure File Transfer

When FIPS mode is enabled, MessageWay encrypts any files sent via SSH, FTP with SSL, or HTTPS with a FIPS 140-2 validated cipher. This system-wide setting is on by default for new installs and overrides any other encryption settings for adapters and MessageWay servers.

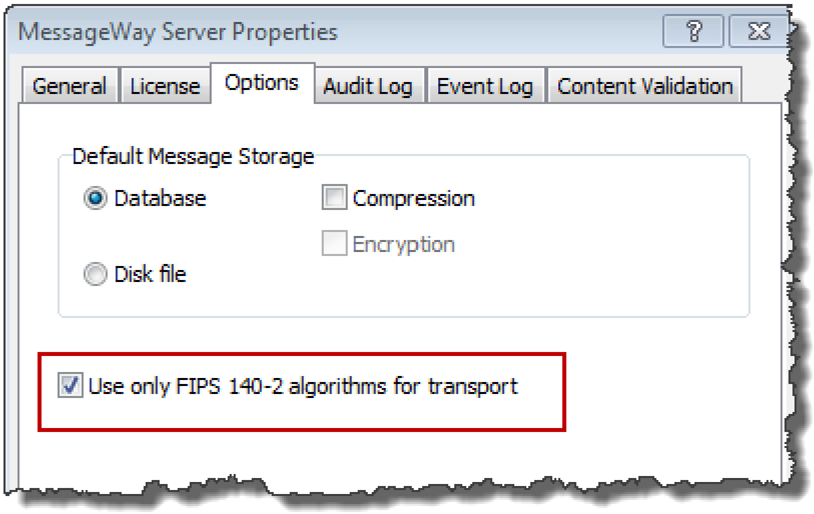
CAUTION: Both MessageWay and the trading partner must use FIPS transfer mode for secure file transfers, or the transfers will fail. Non-secure transfers are still allowed.

To activate FIPS Mode:

1 In the left pane, click **MessageWay**, and in the right pane double click **MessageWay Server**.

The MessageWay Server Properties window appears.

2 On the **Options** page, check the box **Use only FIPS 140-2 algorithms for transpor**t.



☑ Use only FIPS 140-2 algorithms for transport

3 Click **OK**, and restart the MessageWay server.

Any transfers using FTPS (FTP over SSL), SSH, or HTTPS protocols will be sent and received using the FIPS 140-2 validated cryptographic module.

MessageWay Messaging Server Configuration File

Additional configuration information is stored in the MessageWay Messaging Server configuration. The location and name of this file varies, depending on the operating system. The locations are as follows:

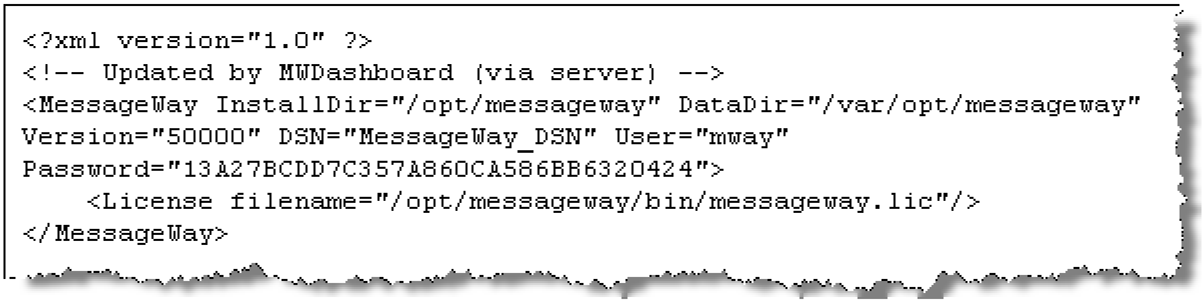
Operating System	Location of the MessageWay Server Configuration File
UNIX or Linux	/etc/messageway/messageway.conf
Windows	\Users\MessageWayUser\AppData\Roaming\messageway\messageway.conf

The configuration file is populated by the installation program with the following information:

- What created or last updated the file:
  - MessageWay installation program
  - MWDashboard (via server)
  - mwadmin utility

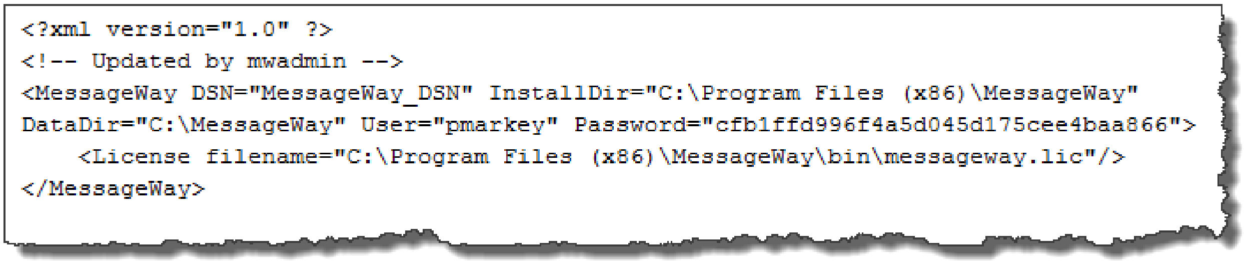
- Location where MessageWay is installed
- Location of data directory
- Data Source Name (DSN) to access the database
- Database logon ID and password when using a database configured to require them, for example, rather than using a trusted connection on Windows
- Location and name of the license file

The following example shows a basic configuration file for Linux:



```
<?xml version="1.0" ?>
<!-- Updated by MWDashboard (via server) -->
<MessageWay InstallDir="/opt/messageway" DataDir="/var/opt/messageway"
Version="50000" DSN="MessageWay_DSN" User="mway"
Password="13A27BCDD7C357A860CA586BB6320424">
    <License filename="/opt/messageway/bin/messageway.lic"/>
</MessageWay>
```

The following example shows a basic configuration file for Windows:

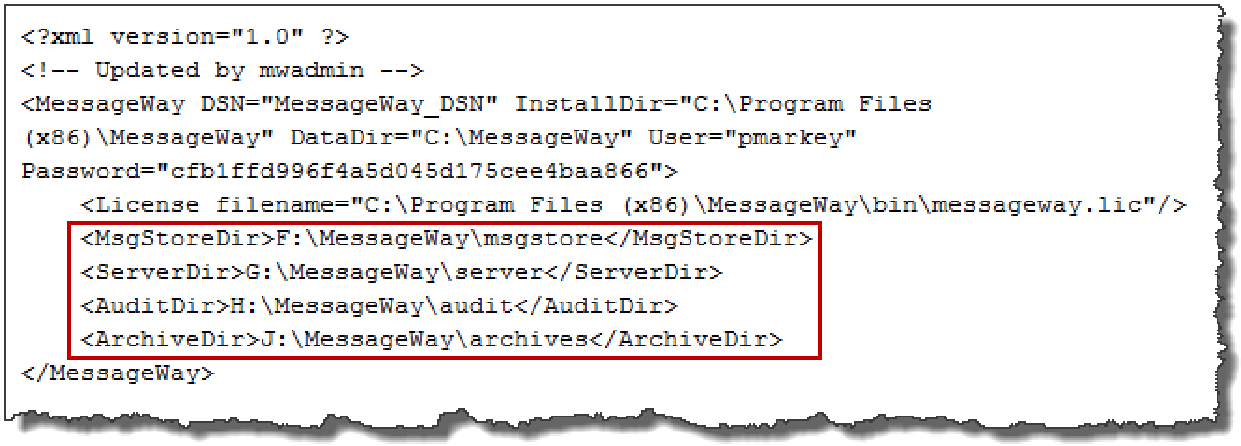


```
<?xml version="1.0" ?>
<!-- Updated by mwadmin -->
<MessageWay DSN="MessageWay_DSN" InstallDir="C:\Program Files (x86)\MessageWay"
DataDir="C:\MessageWay" User="pmarkey" Password="cfb1ffd996f4a5d045d175cee4baa866">
    <License filename="C:\Program Files (x86)\MessageWay\bin\messageway.lic"/>
</MessageWay>
```

Users may change the location of any of the following directories by adding lines to the MessageWay Server configuration file:

- Message store directory
- Server directory
- Audit directory
- Archive directory

The following example shows a configuration file that contains non-default directories:



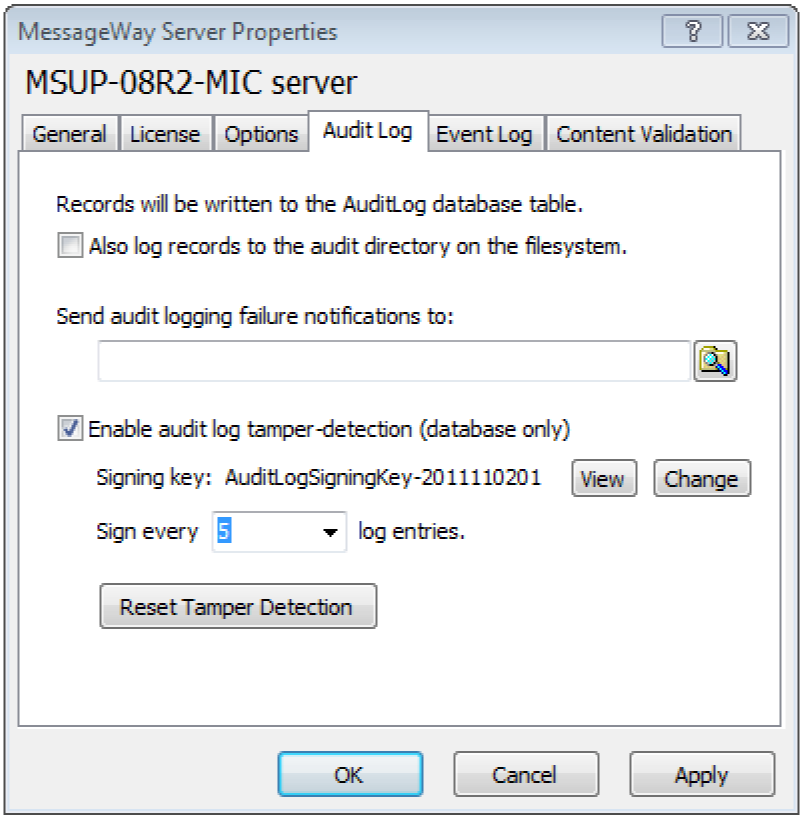
```
<?xml version="1.0" ?>
<!-- Updated by mwadmin -->
<MessageWay DSN="MessageWay_DSN" InstallDir="C:\Program Files
(x86)\MessageWay" DataDir="C:\MessageWay" User="pmarkey"
Password="cfb1ffd996f4a5d045d175cee4baa866">
    <License filename="C:\Program Files (x86)\MessageWay\bin\messageway.lic"/>
    <MsgStoreDir>F:\MessageWay\msgstore</MsgStoreDir>
    <ServerDir>G:\MessageWay\server</ServerDir>
    <AuditDir>H:\MessageWay\audit</AuditDir>
    <ArchiveDir>J:\MessageWay\archives</ArchiveDir>
</MessageWay>
```

Configuring Audit Logging

To support the centralized logging function (new in v6.0), audit records are written to the AuditLog table in the MessageWay database. The Audit Log contains the following types of entries: MWUser logs important MessageWay Manager transactions; MWSI logs important perimeter server transactions.

Database storage allows the addition of tamper detection (security), and makes the log entries available using the Search Logs features.

To configure options for also logging to a file, sending a logging failure notification, or enabling tamper detection on the AuditLog records in the database, open the ***MessageWay Server Properties, Audit Log*** (on page 1231) page, then configure the settings.



MessageWay Server Properties

MSUP-08R2-MIC server

Records will be written to the AuditLog database table.

☐ Also log records to the audit directory on the filesystem.

Send audit logging failure notifications to:

☑ Enable audit log tamper-detection (database only)

Signing key: AuditLogSigningKey-2011110201

Sign every 5 log entries.

1 Optionally, enable tamper detection for the audit records. This allows for detection of attempts to alter log records in the database.

If you enable tamper detection, each server that writes to the AuditLog database table will use the signing key to open a hash chain, and sign log entries. The audit log signing key that is generated is added to the Keys list in the MessageWay Explorer. You can select the key from this view to configure properties, such as permissions.

The {CheckLogIntegrity} custom process (in **MessageWay, Locations** in the MessageWay Explorer) executes the command line program "mwchkaudloginteg" to periodically verify the Audit Log database entries. By default, the location is set to run once a week on Saturday at 2:00 AM local time.

This custom process writes a report to the {LogIntegrityReports} location. To view reports, right-click on the location, then select **Show Messages**.

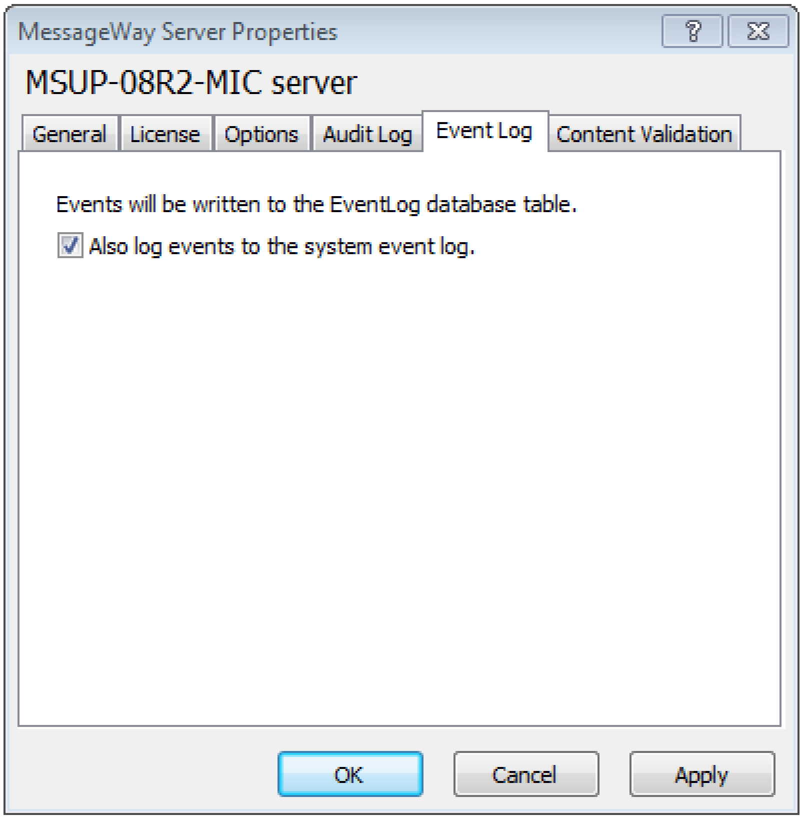
2 You can search for and view Audit log entries using the **Search, Find Logs, Find Audit Logs** (on page 774) page.

3 Log tables will be periodically pruned, and old entries optionally archived via the {Archive} custom process and reports written to the {ArchiveReports} location.

Configuring Event Logging

To support the centralized logging feature (new with v6.0), events reported to the operating system, such as server startup and shutdown, are logged to the MessageWay database, in the EventLog Table.

The **Event Log** page of the MessageWay Server Properties window allows users to configure logging settings.



Events will be written to the EventLog database table.

☑ Also log events to the system event log.

In addition to the database table, by default, events are also logged to the system log (syslog on UNIX, Event Log on Windows), which is the pre-v.6.0 method. We recommend this default setting so that events continue to be written to the system log, particularly in the event of a MessageWay database failure.

Log tables will be periodically pruned, and old entries optionally archived via the {Archive} custom process and reports written to the {ArchiveReports} location.

You can search for and view log entries using the ***Search, Find Logs, Find Event Logs*** (on page 777) features.

Configuring Content Validation (AntiVirus)

Content Validation is an optional feature that requires a license. Content Validation:

- Provides integrated antivirus capabilities against all unencrypted files and messages that pass through the MessageWay system.
- Uses real-time data integration with third-party anti-virus scanning software.

NOTE: Please contact MessageWay Technical Support for information about obtaining the public anti-virus engine.

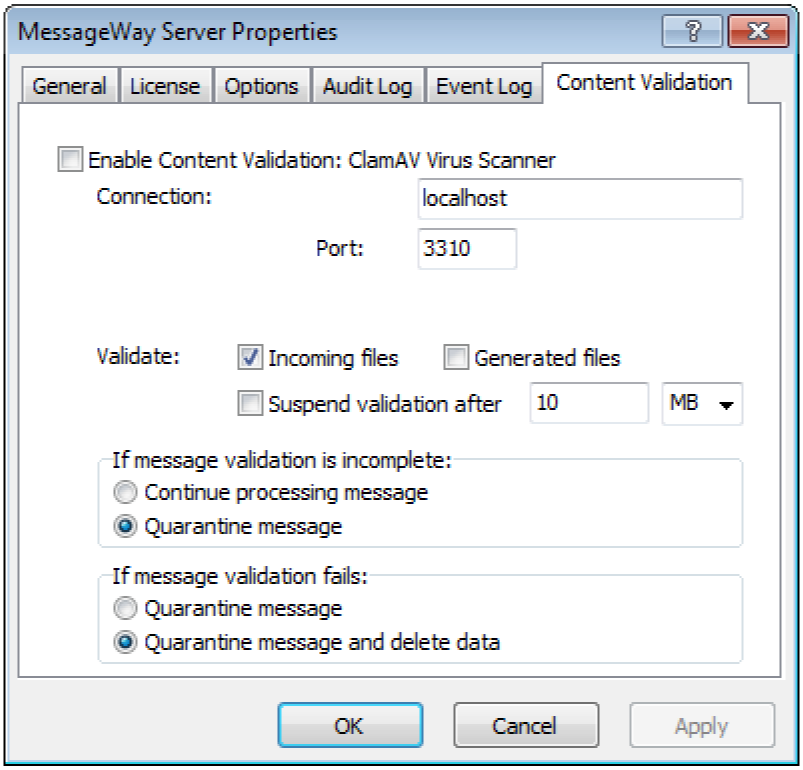
- Is a system-level setting that applies to all files that come in to or that are generated within MessageWay.
- Quarantines, and optionally deletes, bad messages. Creates a new system level mailbox named {Quarantine}.

To use Content Validation, you need to:

1 Install the anti-virus engine, or have an existing version of the engine, either on the same system with MessageWay, or on a system that can be accessed by the MessageWay system.

The public anti-virus engine is an open source (GPL) antivirus toolkit available in Linux and Windows versions.

2 Open the ***MessageWay Server Properties, Content Validation*** (on page 1234) page, then configure the settings.



☐ Enable Content Validation: ClamAV Virus Scanner

Connection: localhost

Port: 3310

Validate: ☑ Incoming files ☐ Generated files

☐ Suspend validation after 10 MB

If message validation is incomplete:

○ Continue processing message

● Quarantine message

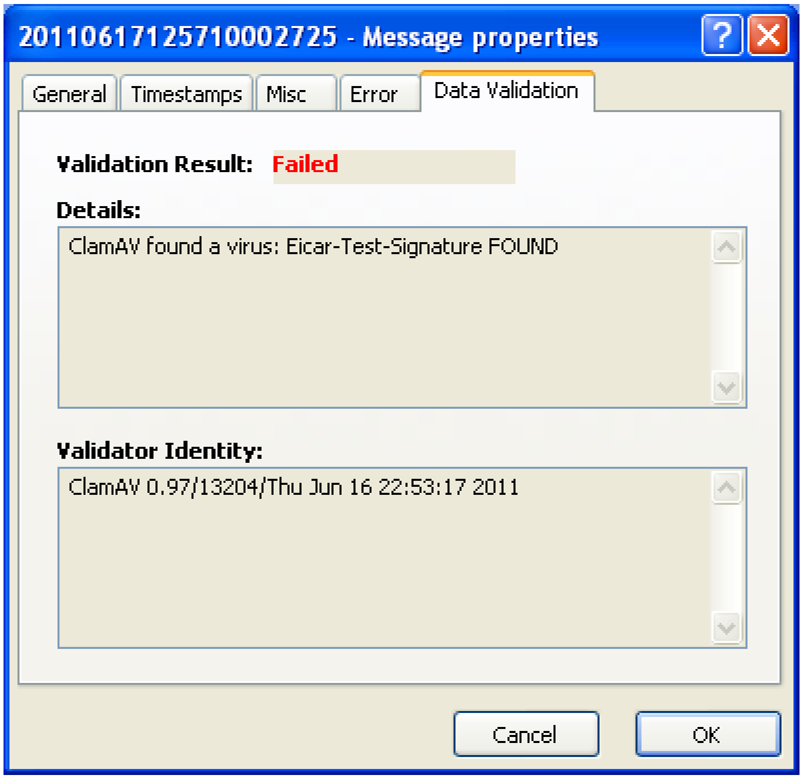
If message validation fails:

○ Quarantine message

● Quarantine message and delete data

NOTE: If you select **Continue processing message** when message validation is incomplete, possibly because the anti-virus server is not running, the message will be delivered and marked *Complete*. An error event, 3007 "Data validation incomplete", appears in the system log, but *not* on the **Error** tab

3 You can view the results of the anti-virus scan by opening the ***Message Properties, Data Validation*** (on page 1210) page.



Validation Result: Failed

Details:

ClamAV found a virus: Eicar-Test-Signature FOUND

Validator Identity:

ClamAV 0.97/13204/Thu Jun 16 22:53:17 2011

Results are also written to the log file. By default, when a message fails the anti-virus scan, the data associated with the message is deleted. The message header information can be found in the {Quarantine} mailbox.

Configuring the Service Interface (MWSI)

The MessageWay Service Interface (MWSI) provides access to MessageWay for external users through MessageWay interfaces and servers, such as the Web Client, the SFTP Server, AS2 and the FTP Server. The MWSI is installed with the MessageWay Server.

Typically, the MessageWay User Server authenticates users using a MessageWay user ID and password. Alternatively, to authenticate external users with LDAP (Lightweight Directory Access Protocol), you must also do the following:

1 Configure the MessageWay Service Interface to support LDAP.

2 ***Configure individual users for LDAP authentication*** (on page 387).

Configurations for the Service Interface

The MessageWay Service Interface (SI) controls outside connections to MessageWay. It resides on the same system as the MessageWay Messaging Server.

The following table shows the default location for the Service Interface configuration file, which depends on the operating system where the MessageWay Messaging and User Servers reside:

Operating System	**Location of the MW Service Interface Configuration File**
UNIX or Linux	/etc/messageway/mwsi.conf
Windows	\Users\MessageWayUser\AppData\Roaming\messageway\mwsi.conf

There are seven sections in the configuration file, mwsi.conf. The following table describes the purpose of each section.

Section	**Purpose**
Global	▪ Sets the maximum number of simultaneous connections
Listeners	▪ List of HTTP connections, configured in HTTP Listener configurations section
Allowed Hosts	▪ IP addresses allowed to connect
Denied Hosts	▪ IP addresses *not* allowed to connect
HTTP Listener Configurations	▪ IP address of host running the Service Interface ▪ Port ▪ Security type ▪ Reference to Security context configuration ▪ Reference to LDAP section ▪ Full path name of the agents file that contains the list of trusted authentication agents for SI ▪ Deny ability to upload files to a location with a closed schedule ▪ Option to change the sender of messages to the user name, rather than the default location of the user
Security Context Configurations	▪ Public and private key information
LDAP Authentication	▪ Allows authentication of external users by LDAP server rather than the Service Interface, which uses MessageWay user configurations

Global Section

This table explains the parameters used in the Global section of mwsi.conf.

Parameter	Description
MaxConnections	The maximum number of simultaneous connections permitted by the server. Additional connections will be rejected.

HTTP Listeners Section

This table explains the parameters used in the HTTP Listeners section of mwsi.conf.

Parameter	Description
No keyword used	List of listeners, one per line. The configurations for each listener are specified in the HTTP Listener Configurations section.

Allowed Hosts Section

This table explains the parameters used in the Allowed Hosts section of mwsi.conf.

Parameter	Description
No keyword used	List IP addresses, one per line, of clients that are allowed to connect to the Service Interface. You may enter a range of addresses on a line, using the syntax typically used to denote sub-networks: 192.168.1.0/255.255.255.0 or 192.168.1.0/24, which both allow connections from 192.168.1.0 to 192.168.1.255. When a specific IP address allowed here also falls within a range of denied addresses, the connection will be allowed. When there are no entries in the Allowed Hosts section, all IP addresses are allowed.

Denied Hosts Section

This table explains the parameters used in the Denied Hosts section of mwsi.conf.

Parameter	Description
No keyword used	List of IP addresses, one per line, of clients that are not allowed to connect to the Service Interface. You may enter a range of addresses on a line, using the syntax typically used to denote sub-networks: 192.168.2.0/255.255.255.0 or 192.168.2.0/24, which both allow connections from 192.168.2.0 to 192.168.2.255. When a specific IP address denied here falls within a range of allowed addresses, the connection will be denied. When there are no entries in the Denied Hosts section, no IP address is denied.

HTTP Listener Configurations Section

This table explains the parameters used in the HTTP Listener Configurations section of mwsi.conf. There should be a configuration for each port on which the SI listens.

CAUTION: Every listener configured here MUST be referenced by a listener in the HTTP Listeners section. If a configuration exists in this section but is not referenced, the Service Interface will not start.

Parameter	Description
IP=	IP address of the host that is running the MessageWay Service Interface. When the host has multiple Network Interface Cards (NICs), use an asterisk, *****, to listen on all IP addresses on the server.
Port=	Port number on which the SI listens.
Security=	Enter a security type. Valid values: ▪ **None** (for non-secure connection) ▪ **SSL** ▪ **TLS**
SecurityContext=	Pointer to one of the security context configurations specified in this file.
LDAP=	Pointer to an LDAP section defined in section 6. **NOTE:** Add this pointer to the listener and add the LDAP configuration in section 6 when an external MessageWay user will be ***authenticated using LDAP*** (on page 387).
AgentFile=	Supports public key authentication. Name of the file that contains the list of trusted authentication agents for SI. The name of an agent must be the same as the Common Name (CN) on the client certificate.
DenyClosedScheduleUpload=	Controls whether user is allowed to upload messages to a location with a closed schedule. When the parameter is not set or it is set to *false*, the user will be allowed to upload messages to a location whose schedule is closed. When set to *true*, the user will receive an error.

Parameter	Description
SenderIsUser=	This overrides the default behavior where the sender of the message is the default location for the user. When set to *true*, the sender of messages using this listener will be the User ID. The options are: ▪ **True** ▪ **False** or blank (default)

Security Context Configuration Section

This table explains the parameters used in the Security Context Configurations section of mwsi.conf. This information is used to connect the FTP Server, the SFTP Server, the AS2 interface or the Web Client to MessageWay through the Service Interface.

Default security files are installed with SI, which is installed with the MessageWay Server. These security files work with the default security files installed with the FTP Server and the Web Client. Together with the default settings in the configuration files, users are able to test a secure connection between the FTP Server, the SFTP Server, the AS2 interface or the Web Client.

CAUTION: Every Security Context configured here MUST be referenced by a **SecurityContext=** value in HTTP Listeners Configuration section. If a configuration exists in this section but is not referenced, the Service Interface will not start.

Parameter	Description
CertificateFile=	Fully qualified file name (path and file name) of the Public Key file.
PrivateKeyFile=	Fully qualified file name (path and file name) of the Private Key file.
PrivateKeyPassPhrase=	Pass phrase to use when the PrivateKeyFile is encrypted.
CipherList=	Identifies the encrypted algorithm, such as RC4, AES and Triple DES. For more information refer to OpenSSL documentation.
RequestClientCert=	Supports public key authentication. Options are **True** or **False**. When this is set to **True**, SI will request a client certificate and verify it when provided. **IMPORTANT:** You may use either RequireClientCert *or* RequestClientCert. The other should be commented.
RequireClientCert=	Supports public key authentication. Options are **True** or **False**. When this is set to **True**, SI will require and validate a client certificate. If no certificate is presented, the connection will fail. **IMPORTANT:** You may use either RequireClientCert *or* RequestClientCert. The other should be commented.
CertVerifyFile=	Supports public key authentication. This file contains the certificates from the client trading partner.

LDAP Authentication

This table explains the parameters used in the LDAP Authentication section of mwsi.conf. This information is used to connect to a MessageWay entity that is also capable functioning as a client, such as FTP and SFTP and Web Client.

Each LDAP Authentication section contains these parameters:

Parameter	Description
URI=	URL of the LDAP server. The default is **ldap://localhost:389** It supports both LDAP and LDAPS (LDAP with SSL).
BindDN=	Distinguished Name for making the initial connection to the server. This authenticates the client to the server. For example, **cn=Manager,dc=messageway,dc=com**
BindPassword=	Password for BindDN.
LookupDN=	DN of User container used for User lookup. Some examples: **OpenLDAP= "ou=employees,dc=messageway,dc=com"** **OpenLDAP="ou=people,dc=messageway,dc=com"** **AD="cn=Users,dc=Domain,dc=Root"** **AD="ou=Users,dc=Domain,dc=Root"**
LookupFilter=	LDAP filter used for User lookup. Some examples: **OpenLDAP=(&(objectClass=posixAccount)(uid=%s))** **OpenLDAP=(&(objectClass=*)(uid=%s))** **AD=(&(objectClass=User)(sAMAccountName=%s))** **AD=(&(objectClass=User)(sAMAccountName=%s)(userAccountControl=512))** **NOTE:** Some control numbers: 512- Account ready for logon; 514- Account disabled
LookupScope=	Scope for User lookup. The default is **sub**. Options are as follows: ▪ **base** Search is limited to only the object ▪ **one** Search object and its immediate children ▪ **sub** Search object, its immediate children and all descendants

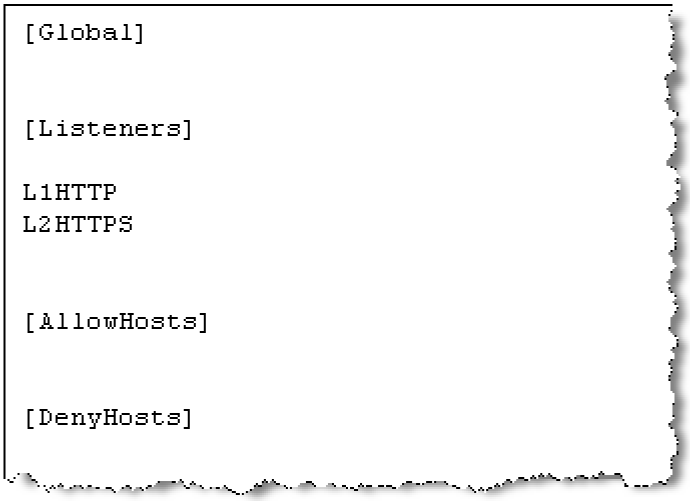
Parameter	Description
LookupTimeout=	User lookup Query Timeout (in seconds). The default is 5 seconds.
LookupSize=	Maximum lookup query result size (in bytes). The default is 4096 bytes.
StartTLS=	Use the LDAPv3 Transport Layer Security (TLS) extension for a secure connection. The default is **false**. The options are: ▪ Blank or **false** ▪ **true** **NOTE:** Set this to *true* if SSL is required with "ldap://" scheme; It has no effect if LDAP server URL uses "ldaps://" scheme.
CertVerifyFile=	Fully qualified file name of the issuer (CA) certificate file.
ClientCertFile=	Fully qualified file name of the client certificate file.
ClientKeyFile=	Fully qualified file name of the client certificate private key file.

NOTE: Client certificate and private key files are required only when the LDAP server requires it.

Examples of Configurations for the Service Interface

This example shows the configurations that permit the Service Interface running on the same system as the MessageWay Messaging Server to negotiate external connection and data transfer requests to and from MessageWay. These configurations are for initial testing only.

The following part of the file shows the first four sections: Global, Listeners, Allowed Hosts and Denied Hosts. The Global section is used to limit concurrent connections. Notice that there are no entries in the latter two, which means that anyone can connect to the Service Interface.



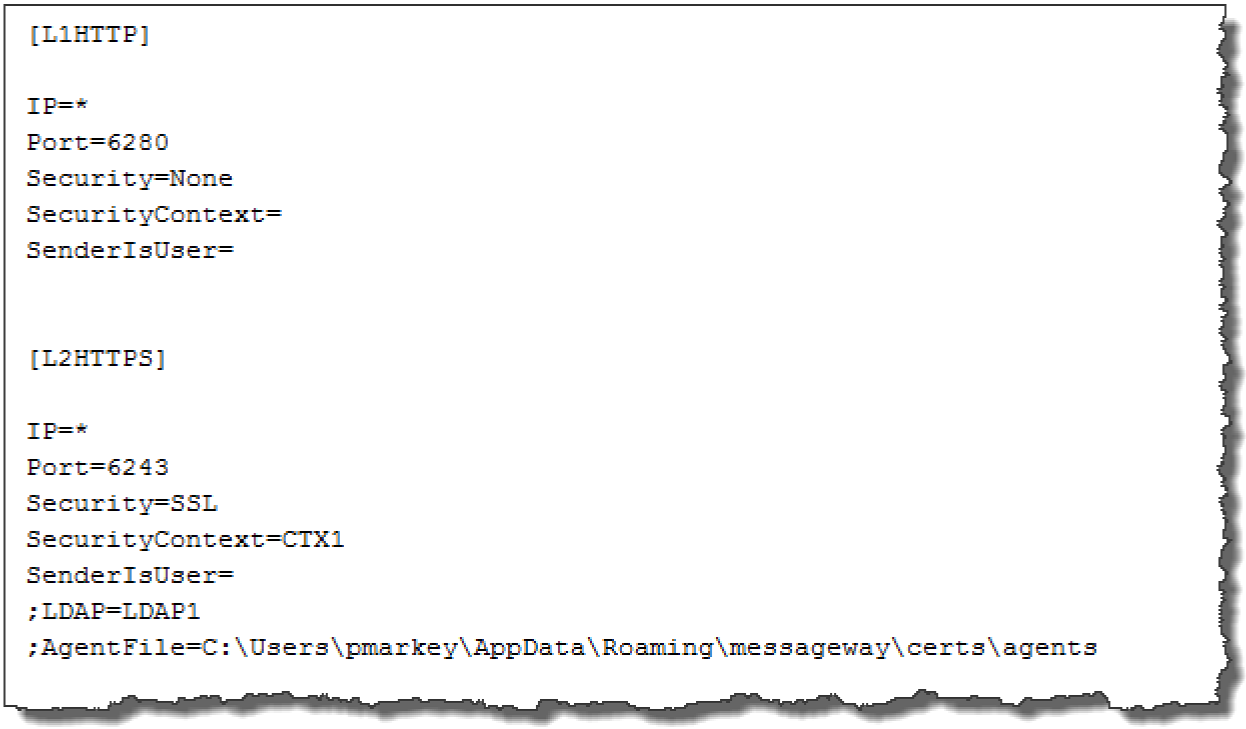
```
[Global]


[Listeners]

L1HTTP
L2HTTPS


[AllowHosts]


[DenyHosts]
```

The HTTP Listener Configurations section configures the listeners, L1HTTP and L2HTTP, listed previously in the Listeners section. L1HTTP is the default, non-secure listener that listens on port 6280.

L2HTTP is the secure listener, HTTPS. It points to a configuration for the SSL security context, CTX1, which appears later in this file. The asterisk, (*), means that it will listen on all IP addresses available on this system.

When a user is authenticated using LDAP, this section must also contain the parameter, **LDAP=** that points to a configuration in the LDAP section.

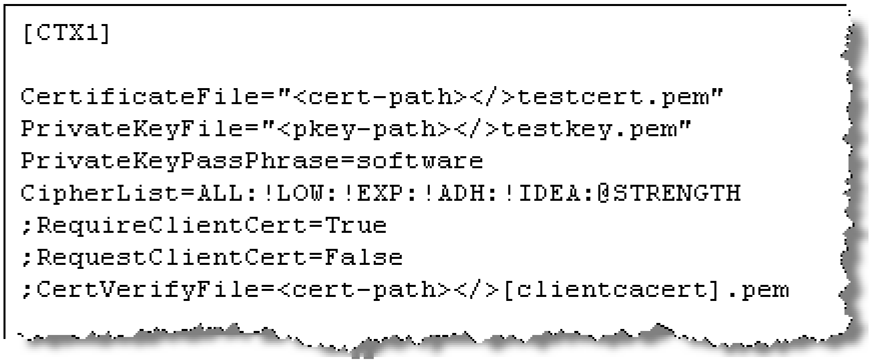
NOTE: The AgentFile parameter supports public key authentication of the user.



```
[L1HTTP]

IP=*
Port=6280
Security=None
SecurityContext=
SenderIsUser=


[L2HTTPS]

IP=*
Port=6243
Security=SSL
SecurityContext=CTX1
SenderIsUser=
;LDAP=LDAP1
;AgentFile=C:\Users\pmarkey\AppData\Roaming\messageway\certs\agents
```

The Security Context Configurations section specifies the security context, specifying the public and private key information.

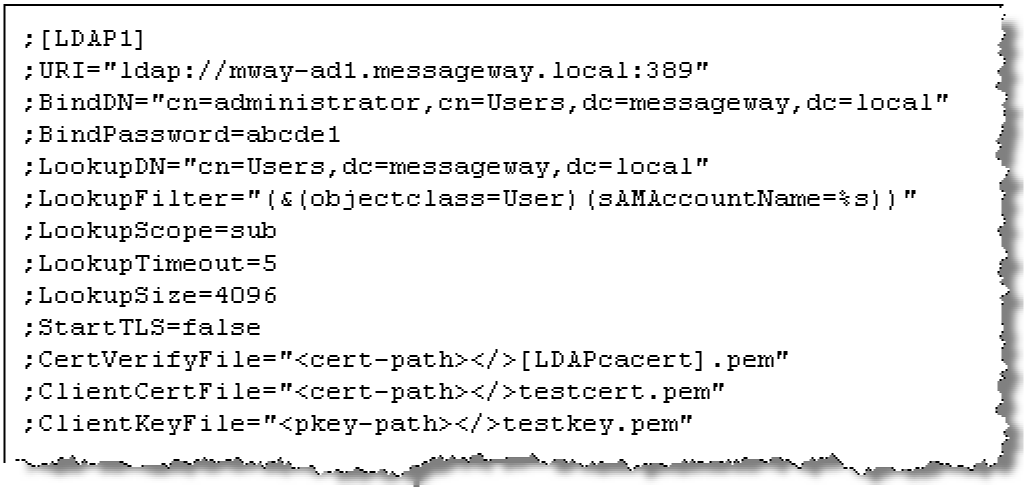
NOTE: The parameters, RequireClientCert, RequestClientCert and CertVerifyFile, support public key authentication of the user.



```
[CTX1]

CertificateFile="<cert-path></>testcert.pem"
PrivateKeyFile="<pkey-path></>testkey.pem"
PrivateKeyPassPhrase=software
CipherList=ALL:!LOW:!EXP:!ADH:!IDEA:@STRENGTH
;RequireClientCert=True
;RequestClientCert=False
;CertVerifyFile=<cert-path></>[clientcacert].pem
```

When a ***user is authenticated with LDAP*** (on page 387), the Service Interface must communicate with an LDAP server. You configure the parameters in the LDAP Authentication section.

NOTE: The Client Certificate and Key files are required only when the LDAP server requires it.



```
;[LDAP1]
;URI="ldap://mway-ad1.messageway.local:389"
;BindDN="cn=administrator,cn=Users,dc=messageway,dc=local"
;BindPassword=abcde1
;LookupDN="cn=Users,dc=messageway,dc=local"
;LookupFilter="(&(objectclass=User)(sAMAccountName=%s))"
;LookupScope=sub
;LookupTimeout=5
;LookupSize=4096
;StartTLS=false
;CertVerifyFile="<cert-path></>[LDAPcacert].pem"
;ClientCertFile="<cert-path></>testcert.pem"
;ClientKeyFile="<pkey-path></>testkey.pem"
```

Testing the Service Interface

You should test the service interface before you test the FTP Server, the SFTP Server, the AS2 interface or the Web Client.

Start the Service Interface

You can have MessageWay start the Service Interface automatically.

How you start the Service Interface manually depends on the operating system where the server resides: UNIX/Linux or Windows.

To Start the Service Interface Automatically When MessageWay Starts

You may start the Service Interface (SI) automatically when MessageWay starts. For more information, refer to the topic, ***Setting Server Startup Options*** (on page 79).

To Start the Service Interface Manually on Windows

To start the MessageWay Service Interface manually on Windows, proceed as follows:

1 From the **Start** menu, select **Programs|Administrative Tools|Computer Management**.

The Computer Manager window appears.

2 In the left pane, expand the folder **Services and Applications**, and click **Services**.

The Services window appears.

3 In the right pane, scroll to the service, **MessageWay Service Interface**.

4 Right-click **MessageWay Service Interface**, and select **Start** from the menu.

The Status column should display **Started**.

To Start the Service Interface Manually on UNIX or Linux

On UNIX or Linux, you start the Service Interface (MWSI) with a startup script, MWSI. The MessageWay Server must be running. For more information about starting the MessageWay server, refer to the topic, ***MessageWay Startup and Shutdown for UNIX and Linux*** (on page 27).

To start the SI, proceed as follows:

1 Make sure you are logged on as the owner of MessageWay, which is typically **mway**.

2 Go to the subdirectory where the script resides by typing:

cd /opt/messageway/init

3 To start the server daemon process, type:

./MWSI start

4 To review all options available in the startup script, type:

./MWSI statusall

Test the Secure Connection to the Service Interface

You test the connection to the Service Interface to verify that the secure connection works. A successful test assures you that shared keys and IP address are correct and that the encryption is working properly.

You can test the secure connection to the Service Interface from a browser.

1 Make sure the Service Interface is started.

For more information, refer to the topic, ***Start the Service Interface*** (on page 103).

2 Make sure the Service Interface configuration file has a secure listener at port 6243.

For more information, refer to the topics, ***Configurations for the Service Interface*** (on page 96) and ***Examples of Configurations for the Service Interface*** (on page 101).

3 In the browser, type **https://localhost:6243**, and press **ENTER**.

A message from your browser should appear stating that the Web site is certified by an unknown authority.

4 Select the option to accept this certificate temporarily for the session.

If successful, a message appears from the Service Interface, "You have reached the MessageWay Service Interface."

5 View the audit or event logs for the MWSI Started entry:

- Use the ***Find Logs*** (on page 733) menu to view Audit or Event log information.

- or -

- If you have the audit log also written to disk, you can check the audit log file for the Service Interface. The location of the audit log is as follows, depending on the operating system:

Windows	**\MessageWay\audit\siaudit***yyyymmdd***.csv**

UNIX or Linux **/var/opt/messageway/audit/siaudit***yyyymmdd***.csv**

Configuring the User Server

The MessageWay User Server provides access to MessageWay for internal users through the MessageWay Manager, and also presents security credentials to MessageWay from an LDAP server.

Configurations for the User Server

The MessageWay User Server controls internal connections to MessageWay. It resides on the same system as the MessageWay Messaging Server.

The following table shows the default location for the User Server configuration file, which depends on the operating system where the MessageWay Messaging and User Servers reside:

Operating System	Location of the User Server Configuration File
UNIX or Linux	/etc/messageway/mwuser.conf
Windows	\Users*MessageWayUser*\AppData\Roaming\messageway\mwuser.conf

There are seven sections in the configuration file, mwuser.conf. The following table describes the purpose of each section.

Section	Purpose
Global	▪ Sets the maximum number of simultaneous connections ▪ Disable the message Resubmit function for all users
Listeners	▪ List of connections, configured in Listener configurations section
Allowed Hosts	▪ IP addresses allowed to connect
Denied Hosts	▪ IP addresses *not* allowed to connect
Listener Configurations	▪ IP address of host running the User Server ▪ Port ▪ Security type ▪ Reference to Security context configuration
Security Context Configurations	▪ Public and private key information
LDAP Authentication	▪ Allows authentication of internal users by LDAP server rather than the User Server, which uses MessageWay user configurations

Global Section

This table explains the parameters used in the Global section of mwuser.conf.

Parameter	Description
MaxConnections=	The maximum number of simultaneous connections permitted by the server. Additional connections will be rejected. If not set, there is no limit to the number of simultaneous connections.
DisableResend=	Users can typically resubmit messages that have certain statuses. This parameter disables that function for all users. Valid values are: ▪ **True** ▪ **False** (default)

Listeners Section

This table explains the parameters used in the Listeners section of mwuser.conf.

Parameter	Description
No keyword used	List of listeners, one per line. The configurations for each listener are specified in the Listener Configurations section.

Allowed Hosts Section

This table explains the parameters used in the Allowed Hosts section of mwuser.conf.

Parameter	Description
No keyword used	List IP addresses, one per line, of clients that are allowed to connect to the User Server. You may enter a range of addresses on a line, using the syntax typically used to denote sub-networks: 192.168.1.0/255.255.255.0 or 192.168.1.0/24, which both allow connections from 192.168.1.0 to 192.168.1.255. When a specific IP address allowed here also falls within a range of denied addresses, the connection will be allowed. When there are no entries in the Allowed Hosts section, all IP addresses are allowed.

Denied Hosts Section

This table explains the parameters used in the Denied Hosts section of mwuser.conf.

Parameter	Description
No keyword used	List of IP addresses, one per line, of clients that are not allowed to connect to the User Server. You may enter a range of addresses on a line, using the syntax typically used to denote sub-networks: 192.168.2.0/255.255.255.0 or 192.168.2.0/24, which both allow connections from 192.168.2.0 to 192.168.2.255. When a specific IP address denied here falls within a range of allowed addresses, the connection will be denied. When there are no entries in the Denied Hosts section, no IP address is denied.

Listener Configurations Section

This table explains the parameters used in the Listener Configurations section of mwuser.conf. There should be a configuration for each port on which the User Server listens.

CAUTION: Every listener configured here MUST be referenced by a listener in the Listeners section. If a configuration exists in this section but is not referenced, the User Server will not start.

Parameter	Description
IP=	IP address of the host that is running the MessageWay User Server. When the host has multiple Network Interface Cards (NICs), use an asterisk, *****, to listen on all IP addresses on the server.
Port=	Port number on which the User Server listens.
Security=	Enter a security type. Valid values: ▪ **None** (for non-secure connection) ▪ **SSL** ▪ **TLS**
SecurityContext=	Pointer to one of the security context configurations specified in this file.
AccessClass=	Restricts access to MessageWay via this listener to only those users whose configuration does not include an access class list or includes this value in their access class list. This value should be alphanumeric and is case-sensitive. It must match exactly what is specified for the user. Optional, but if used, only one access class value is allowed.

Parameter	Description
LDAP=	Pointer to an LDAP connection defined in the LDAP Authentication section. **NOTE:** Add this pointer to the listener and add the LDAP configuration in the LDAP Authentication section when an internal MessageWay user will be ***authenticated using LDAP*** (on page 387).

Security Context Configuration Section

This table explains the parameters used in the Security Context Configurations section of mwuser.conf.

Default security files are installed with the User Server, which is installed with the MessageWay Server. These security files work with the sample fingerprint provided for the MessageWay Manager. For more information regarding this sample fingerprint and how to configure it, refer to the topic, ***Connection Options Window*** (on page 976).

CAUTION: Every Security Context configured here MUST be referenced by a **SecurityContext=** value in Listeners Configuration section. If a configuration exists in this section but is not referenced, the User Server will not start.

Parameter	Description
CertificateFile=	Fully qualified file name (path and file name) of the Public Key file.
PrivateKeyFile=	Fully qualified file name (path and file name) of the Private Key file.
PrivateKeyPassPhrase=	Pass phrase to use when the PrivateKeyFile is encrypted.
CipherList=	Identifies the encrypted algorithm, such as RC4, AES and Triple DES. For more information refer to OpenSSL documentation.
RequireClientCert=	Supports public key authentication. Options are **True** or **False** (default). When this is set to **True**, User Server will require and validate a client certificate. If no certificate is presented, the connection will fail. **IMPORTANT:** You may use either RequireClientCert *or* RequestClientCert. The other should be commented.
RequestClientCert=	Supports public key authentication. Options are **True** or **False** (default). When this is set to **True**, User Server will request a client certificate and verify it when provided. **IMPORTANT:** You may use either RequireClientCert *or* RequestClientCert. The other should be commented.
CertVerifyFile=	Supports public key authentication. This file contains the certificates from the connecting Manager.

LDAP Authentication

This table explains the parameters used in the LDAP Authentication section of mwuser.conf. This information is used to connect to a MessageWay entity that is also capable functioning as a client.

Each LDAP Authentication section contains these parameters:

Parameter	Description
URI=	URL of the LDAP server. The default is **ldap://localhost:389** It supports both LDAP and LDAPS (LDAP with SSL).
BindDN=	Distinguished Name for making the initial connection to the server. This authenticates the client to the server. For example, **cn=Manager,dc=messageway,dc=com**
BindPassword=	Password for BindDN.
LookupDN=	DN of User container used for User lookup. Some examples: **OpenLDAP= "ou=employees,dc=messageway,dc=com"** **OpenLDAP="ou=people,dc=messageway,dc=com"** **AD="cn=Users,dc=Domain,dc=Root"** **AD="ou=Users,dc=Domain,dc=Root"**
LookupFilter=	LDAP filter used for User lookup. Some examples: **OpenLDAP=(&(objectClass=posixAccount)(uid=%s))** **OpenLDAP=(&(objectClass=*)(uid=%s))** **AD=(&(objectClass=User)(sAMAccountName=%s))** **AD=(&(objectClass=User)(sAMAccountName=%s)(userAccountControl=512))** **NOTE:** Some control numbers: 512- Account ready for logon; 514- Account disabled
LookupScope=	Scope for User lookup. The default is **sub**. Options are as follows: ▪ **base** Search is limited to only the object ▪ **one** Search object and its immediate children ▪ **sub** Search object its immediate children and all descendants

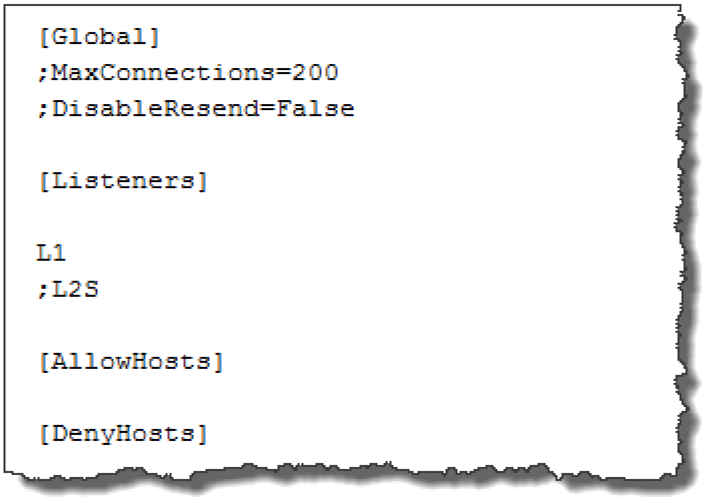
Parameter	Description
LookupTimeout=	User lookup Query Timeout (in seconds). The default is 5 seconds.
LookupSize=	Maximum lookup query result size (in bytes). The default is 4096 bytes.
StartTLS=	Use the LDAPv3 Transport Layer Security (TLS) extension for a secure connection. The default is **false**. The options are: ▪ Blank or **false** ▪ **true** **NOTE:** Set this to true if SSL is required with "ldap://" scheme; It has no effect if LDAP server URL uses "ldaps://" scheme.
CertVerifyFile=	Fully qualified file name of the issuer (CA) certificate file.
ClientCertFile=	Fully qualified file name of the client certificate file.
ClientKeyFile=	Fully qualified file name of the client certificate private key file.

NOTE: Client certificate and private key files are required only when the LDAP server requires it.

Examples of Configurations for the User Server

This example shows the configurations that permit the User Server to negotiate internal connection and data transfer requests to and from MessageWay. It also supports authentication using an LDAP server. These configurations are for initial testing only.

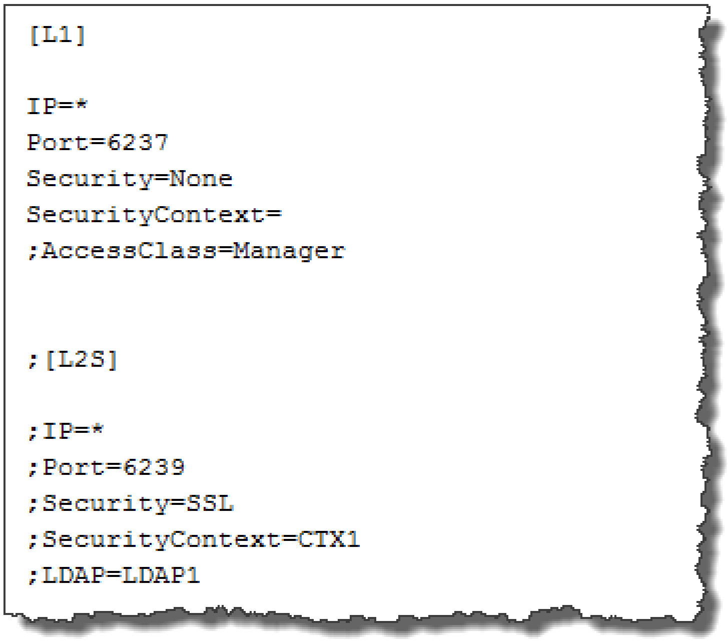
The following part of the file shows the first four sections: Global, Listeners, Allowed Hosts and Denied Hosts.



```
[Global]
;MaxConnections=200
;DisableResend=False

[Listeners]

L1
;L2S

[AllowHosts]

[DenyHosts]
```

The Listener Configurations section configures the listeners, L1 and L2S, listed previously in the Listeners section. L1 is the default, non-secure listener that listens on port 6237. L2S is the secure listener. It points to a configuration for the SSL security context, CTX1, which appears later in this file. The asterisk, (*), means that it will listen on all IP addresses available on this system.

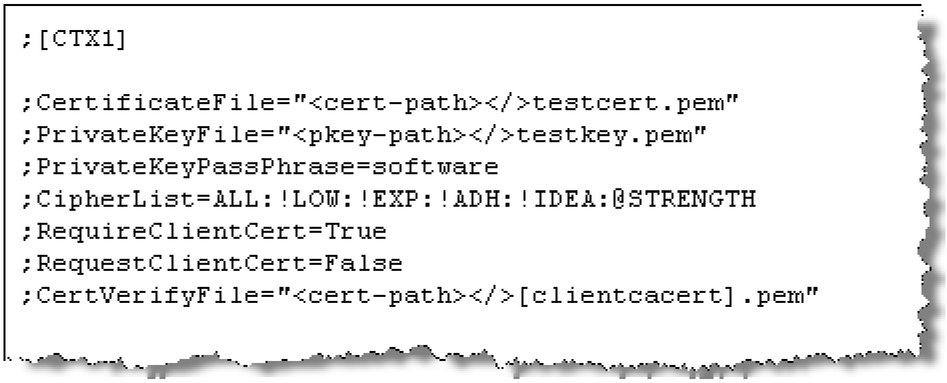
When a user is authenticated using LDAP, this section must also contain the parameter, **LDAP=** that points to a configuration in the LDAP section.



```
[L1]

IP=*
Port=6237
Security=None
SecurityContext=
;AccessClass=Manager


;[L2S]

;IP=*
;Port=6239
;Security=SSL
;SecurityContext=CTX1
;LDAP=LDAP1
```

The Security Context Configurations section specifies the security context, specifying the public and private key information.

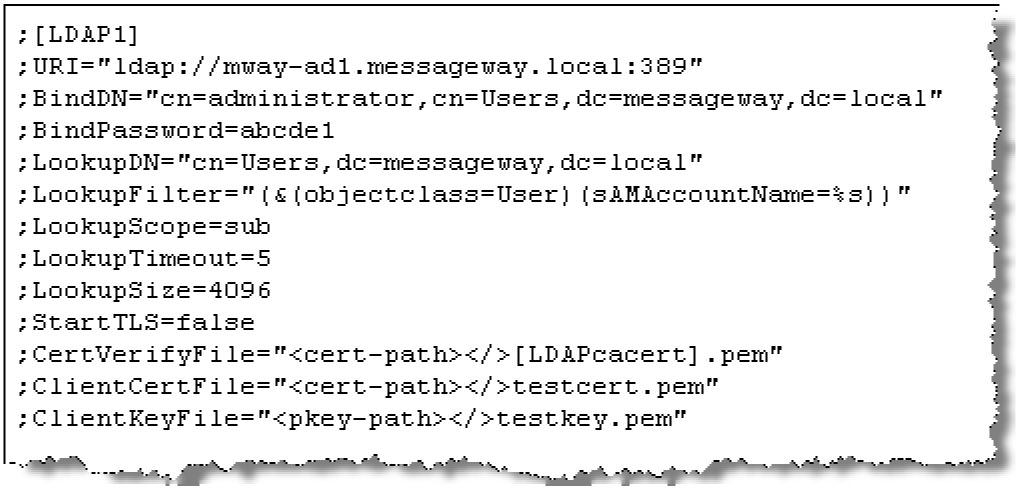
NOTE: The parameters, RequireClientCert, RequestClientCert and CertVerifyFile, support public key authentication of the user.



```
;[CTX1]

;CertificateFile="<cert-path></>testcert.pem"
;PrivateKeyFile="<pkey-path></>testkey.pem"
;PrivateKeyPassPhrase=software
;CipherList=ALL:!LOW:!EXP:!ADH:!IDEA:@STRENGTH
;RequireClientCert=True
;RequestClientCert=False
;CertVerifyFile="<cert-path></>[clientcacert].pem"
```

When a ***user is authenticated with LDAP*** (on page 387), the User Server must communicate with an LDAP server. You configure the parameters in the LDAP Authentication section.

NOTE: The Client Certificate and Key files are required only when the LDAP server requires it.



```
;[LDAP1]
;URI="ldap://mway-ad1.messageway.local:389"
;BindDN="cn=administrator,cn=Users,dc=messageway,dc=local"
;BindPassword=abcde1
;LookupDN="cn=Users,dc=messageway,dc=local"
;LookupFilter="(&(objectclass=User)(sAMAccountName=%s))"
;LookupScope=sub
;LookupTimeout=5
;LookupSize=4096
;StartTLS=false
;CertVerifyFile="<cert-path></>[LDAPcacert].pem"
;ClientCertFile="<cert-path></>testcert.pem"
;ClientKeyFile="<pkey-path></>testkey.pem"
```

Configuring MessageWay Perimeter Servers

This section describes how to configure MessageWay perimeter servers or processes that may run outside the firewall.

The following are perimeter servers and interfaces whose configurations are discussed here:

- MessageWay AS2 Interface
- MessageWay FTP Perimeter Server
- MessageWay Remote Execution Perimeter Server (RES)
- MessageWay SFTP Proxy Server
- MessageWay SFTP Perimeter Server

Information is available separately for the following perimeter servers:

-
- MessageWay Web Client information is in the document *MessageWay Web Client Installation and Configuration*.

Users who access MessageWay from somewhere other than the MessageWay Manager are called external users. To authenticate external users with LDAP (Lightweight Directory Access Protocol), you must also do the following:

1. Configure the ***MessageWay Service Interface*** (on page 95) to support LDAP.
2. ***Configure individual users for LDAP authentication*** (on page 387).

Updating Configuration Files for Perimeter Servers

The perimeter servers use configuration files. New installs will create this configuration file, which you will need to configure. When you update a perimeter server, you may need to update your current configuration file, if new configuration parameters have been added for the release. The update programs do not replace your configuration files, so you must do this manually. You will find the new parameters in one or more of the following places:

- Sample configuration file that contains the new parameters in the same location where you install the perimeter server
- *MessageWay Release Notes* document for the release
- *MessageWay User's Guide and Reference*, in the section "Configuring MessageWay Perimeter Servers."

To add new parameters to your configuration file:

1. If there is a sample configuration file, follow the instructions to copy the parameter(s) to the specified location(s) in your current configuration file.
2. Alternatively, use the release notes and the user's guide:
   a) From the release notes, find the list of new parameters.
   b) In the configuration section for the appropriate server within *MessageWay User's Guide and Reference*, find the location of the new parameter(s) in the examples, and type the parameter(s) in the appropriate location(s) in your current configuration file.

Configuring the AS2 Interface

The AS2 Interface provides both server and client functionality. As a server, it provides secure communications between an AS2 client and MessageWay. As a client, it uses the MessageWay AS2 Adapter to initiate the delivery of messages to an AS2 server.

The AS2 Interface includes the following configurable entities:

- AS2 server for inbound and outbound messages
- MessageWay Service Interface (SI), installed with the MessageWay Server, for inbound messages
- AS2 adapter and AS2 outbound sites for outbound messages
- AS2 remote users

These components typically have the following physical relationships:

- AS2 server may reside on any server where the Web container runs that supports Java servlet specification 2.4, such as Apache Tomcat
- MessageWay Service Interface and AS2 adapter reside on the same system as the MessageWay Server

IMPORTANT: By protocol design, AS2 processes much of its data in memory. Therefore, it is not well suited to exchanging extremely large files.

Licensing Requirements for the AS2 Interface

The MessageWay AS2 server and the AS2 adapter require a license from Progress. For more information, contact MessageWay Technical Support.

Overview of the AS2 Interface

Applicability Statement 2 (AS2) is a specification to transfer structured business data between computers using the Internet Web page protocol, the Hypertext Transfer Protocol (HTTP). Although any structured data format may be used, the prevalent formats are XML or Electronic Data Interchange (EDI), such as ANSI X12 or UN/EDIFACT.

The AS2 standard uses both Multi-Purpose Internet Mail Extensions (MIME) and Secure Multi-Purpose Internet Mail Extensions (S/MIME) to package data. It uses HTTP or a more secure version, HTTPS, to transmit data over the Internet. It supports data integrity and authenticity through the optional use of X.509 (***RFC2459*** (***http://www.ietf.org/rfc/rfc2459.txt***)) certificates, an international standard (Recommendation) for public key infrastructure (PKI) certificates.

The MessageWay AS2 interface provides the AS2 protocol interface between MessageWay and a remote host.

The AS2 Interface is based on the following reference:

- Applicability Statement 2 (AS2) ***RFC 4130*** (***http://www.ietf.org/rfc/rfc4130.txt***)

Prerequisites for the MessageWay AS2 Interface

The MessageWay AS2 Interface has been developed with and requires at a minimum specific versions of MessageWay software as well as third-party software. These are the prerequisites:

Software Component	Minimum Requirement
Java Runtime Environment (JRE) (***http://www.java.com***)	Java version 8.x
Web container that supports Java Servlet specification 2.4, such as ***Apache Tomcat*** (***http://tomcat.apache.org/***)	Apache Tomcat version 7.x, 8.x or 9.x

IMPORTANT: Tomcat must be installed as a service. Not all versions of Tomcat do this automatically. Refer to the installation instructions provided with Tomcat, since the instructions may vary between versions.

Components and Processes of the AS2 Interface

The interface allows a remote host to deliver files to MessageWay via AS2, called an inbound transfer, and allows MessageWay to auto-deliver files via AS2 to a remote host, called an outbound transfer.

The MessageWay AS2 Interface uses the following components to provide inbound and outbound services, many of which are optional:

Component	Service
AS2 Inbound Servlet	▪ Verifies signatures to authenticate remote AS2 clients when messages are signed ▪ Optionally verifies that remote AS2 clients were authenticated by HTTP when messages are not signed ▪ Decompresses messages when compressed ▪ Decrypts messages when encrypted ▪ Sends parsed messages to MessageWay SI ▪ Creates and sends requested synchronous or asynchronous MDNs back to remote host using HTTP or HTTPS protocols ▪ Optionally creates AS2 processing log files, used primarily for debugging
Service Interface (SI)	▪ Ensures secure access to MessageWay through the AS2 Inbound Servlet
AS2 Adapter	▪ Delivers messages from MessageWay to the AS2 Outbound Servlet ▪ Maintains statuses of messages, based on information from AS2 Outbound Servlet ▪ Records inbound MDN information for non-repudiation
AS2 Outbound Servlet	▪ Receives messages from AS2 Adapter ▪ Optionally signs messages ▪ Optionally compresses messages ▪ Optionally encrypts messages ▪ Optionally requests synchronous MDNs ▪ Sends generated AS2 packages to remote AS2 servers ▪ Parses returned MDNs, extracts and sends non-repudiation information to adapter ▪ Optionally creates AS2 processing log files, used primarily for debugging

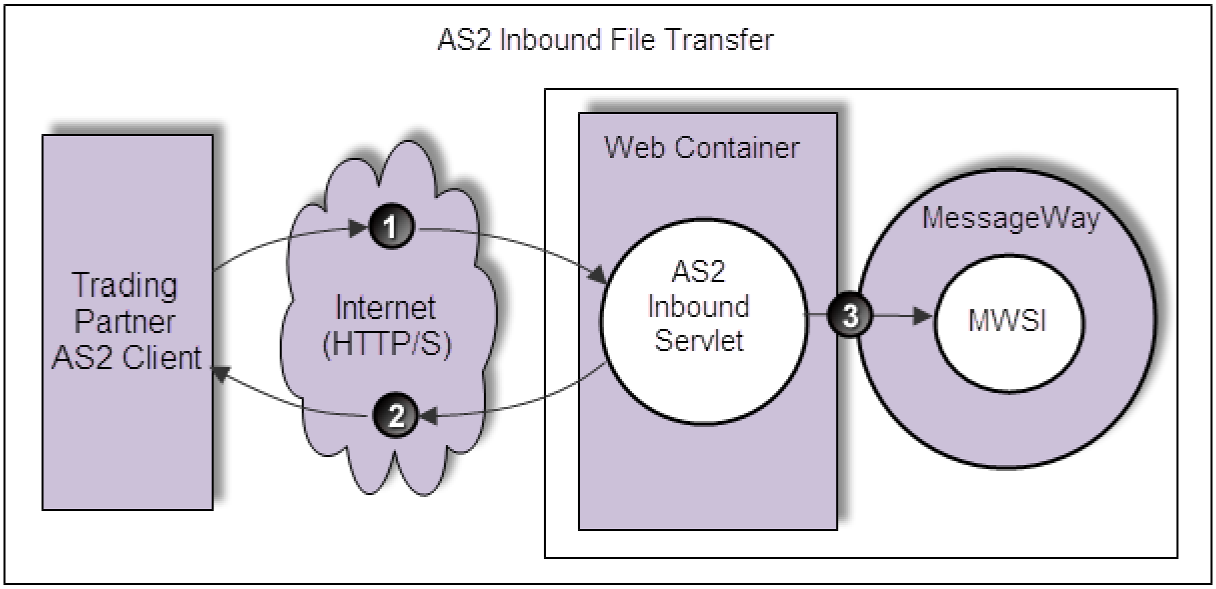
Overview of AS2 Inbound Transfer

For inbound AS2 communications, an AS2 client sends a message to MessageWay. The diagram shows the process. The steps listed in the diagram are as follows:

1. A remote AS2 client connects to the MessageWay AS2 Inbound Servlet over the Internet using HTTP or HTTPS protocols.
2. The AS2 Inbound Servlet parses the message and sends it to the MessageWay Service Interface (MWSI) over HTTPS connections to load the file into MessageWay.
3. When MessageWay has successfully received the message, the servlet:

   a) Creates and sends a requested synchronous or asynchronous MDN to the remote client using HTTP or HTTPS protocols

b) Optionally logs all AS2 processing information in a log file



Overview of AS2 Outbound Transfer

For outbound AS2 communications, the AS2 adapter initiates delivery of messages that are queued to AS2 sites to an AS2 remote host. The diagram shows the process. The steps listed in the diagram are as follows:

1 The MessageWay AS2 adapter sends messages queued to AS2 sites to the AS2 Outbound Servlet over an HTTP connection.

2 The AS2 Outbound Servlet:

a) Creates the AS2 package

b) Sends the AS2 package to the remote host over the Internet using an HTTP or HTTPS connection

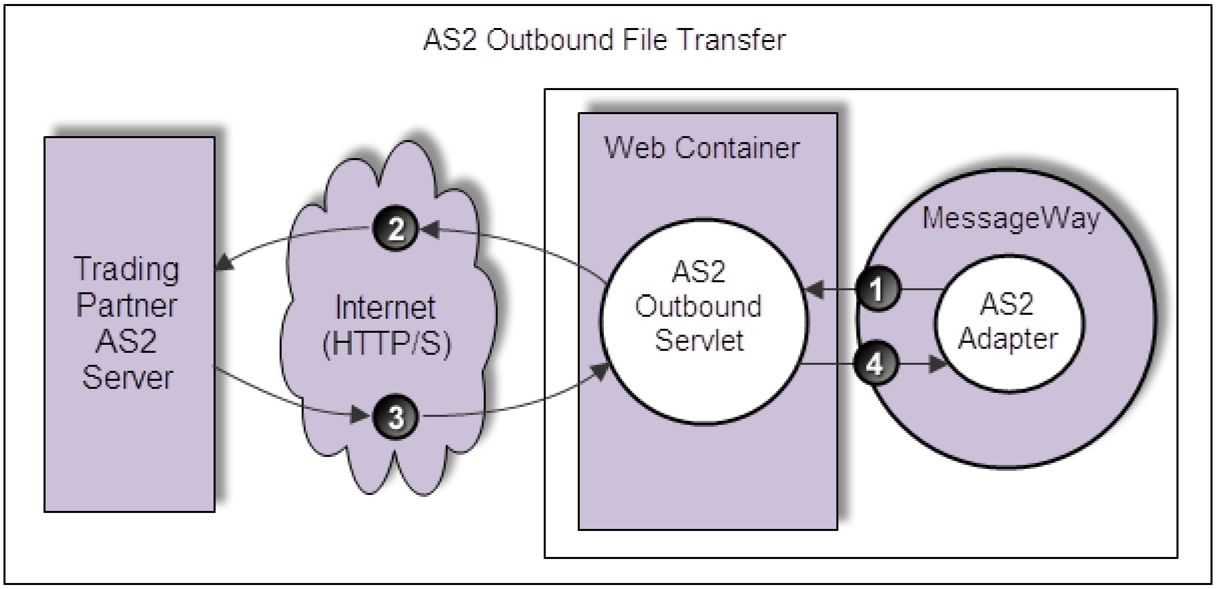
c) Optionally requests a synchronous MDN

3 The AS2 remote host returns an MDN to the AS2 Outbound Servlet.

4 The AS2 Outbound Servlet parses the MDN and:

a) Sends pertinent MDN information to the AS2 adapter , viewable as properties of the original outbound message

b) Optionally logs all AS2 processing information in a log file



Basic Installation Tasks

The installation process installs the components of the AS2 Interface. The installation process also requires a Java Runtime Environment and a Web container, such as Apache Tomcat. For specific MessageWay and third-party requirements, refer to the topic, ***Prerequisites for the MessageWay AS2 Interface*** (on page 115).

These tasks assume that you have already installed MessageWay, which includes the following components of interest here:

- MessageWay Messaging Server, which processes messaging requests
- MessageWay User Server, which controls access to MessageWay
- MessageWay Service Interface, which provides access to MessageWay from MessageWay servers and the Internet
- MessageWay Manager, which provides the user interface to configure MessageWay

These are the basic tasks to install the MessageWay AS2 Interface:

- Install the MessageWay AS2 inbound and outbound servlets on any system within a Web container in the LAN or WAN
- Install the MessageWay AS2 adapter on the system where the MessageWay Server runs

IMPORTANT: You must have a license for the AS2 Interface before you can start the AS2 adapter.

After you have installed the AS2 Interface, you must perform the following tasks to configure and test the system:

- Modify the configuration file for the Service Interface on the MessageWay system
- Modify the configuration files for the AS2 Interface
- Configure MessageWay users and locations
- Create and populate Java Key Store (.jks) file to manage X.509 certificates
- Start the Service Interface
- Start the Web container, such as Apache Tomcat, which starts the AS2 servlets
- Test the connection from a browser to the AS2 Interface
- Test inbound AS2 transmissions
- Start the AS2 adapter
- Test outbound AS2 transmissions

For the actual installation information, refer to the *MessageWay Installation Guide*.

Basic Configuration Tasks

There are various things you must do and configure to use the AS2 Interface. Tasks vary depending on whether you are sending AS2 messages, receiving AS2 messages, and how you perform authentication and authorization. Although AS2 allows users to send unencrypted and unsigned data, it is recommended that users exchange encrypted and signed messages using X.509 certificates.

Everyone should perform the following general tasks, but ignore the ones marked (Inbound only) if you do not accept inbound AS2 messages:

- ***Create and manage your AS2 certificates*** (on page 120)
  - Create a Java keystore (.jks) file, and populate it with your private key and public certificate pair
  - Create a .pem file containing your public certificate, and place it in MessageWay's certificates directory. A .pem file is a BASE64 encoded DER certificate, enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"
  - Exchange X.509 public certificates with your trading partner
    - Supply your trading partner with your public certificate
    - Receive and verify your trading partner's public certificate, and store it in the keystore
- ***Configure the Web application deployment descriptor file*** (on page 134), web.xml, to specify:
  - Location of the servlets
  - Level of logging
- ***Configure the AS2 Interface configuration file*** (on page 136), mwas2.conf, to set the operating parameters for the AS2 servlets
- (Inbound only) Configure entities to allow client authentication of the AS2 Inbound Servlet and authorization of the remote user by the MessageWay Service Interface (SI):
  - ***Service Interface configuration file*** (on page 145), mwsi.conf, to support client authentication between the AS2 Inbound Servlet and SI
  - ***Agents file*** (on page 148) to specify valid MessageWay users or user groups that access MessageWay through the AS2 Inbound Servlet

To receive AS2 messages using the AS2 Inbound Servlet, perform these tasks from the MessageWay Manager:

- ***Configure a trading partner*** (on page 152), a MessageWay user, with appropriate access to MessageWay
- ***Configure locations with appropriate access*** (on page 160) to which a trading partner sends AS2 messages

To send AS2 messages using the AS2 Outbound Servlet, perform these tasks from the MessageWay Manager:

- ***Configure the AS2 Adapter*** (on page 408)
- Configure an AS2 output location

Certificates for AS2 Security

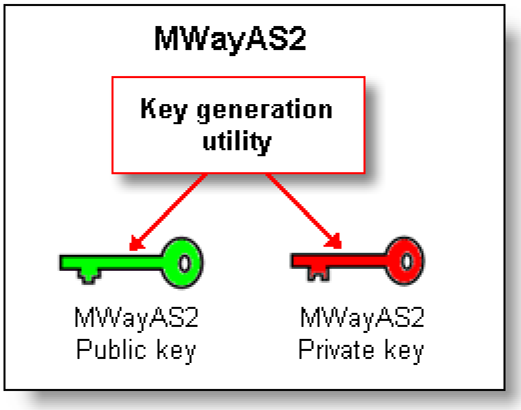
Although it is optional, the AS2 standard recommends using public-key cryptography. To support public-key cryptography, the AS2 standard requires X.509 certificates. Public-key cryptography, also called asymmetric cryptography, supports:

- Public-key encryption to ensure confidentiality
- Digital signatures to ensure authenticity

Public-key cryptography requires that a trading partner maintain a public and private key pair that uniquely represents them, and public keys for each of their other trading partners. The private key must be a closely guarded secret. Partners must exchange and verify certificates before they begin a secure exchange of data.

The process to create and exchange X.509 certificates between AS2 trading partners is as follows:

- Trading partner, for example MWayAS2, creates a public and private key pair, a self-signed certificate



- (Optional in AS2) Trading partner uses an accepted X.509 validation method to validate its public certificate, such as sending it to a certificate authority (CA), which signs the certificate and returns it to the trading partner to ensure its authenticity
- Trading partners exchange public certificates and, if not using a CA to sign the certificate, they must certify their validity to one another in a mutually agreed way

Using AS2 Certificates in MessageWay

AS2 processing uses certificates as required by the AS2 specification to encrypt/decrypt and sign/authenticate data. The AS2 software component that performs this work, and on which the MessageWay AS2 Interface is built, has been certified by the Drummond Group.

In general, one should understand how certificates are used:

- To encrypt and digitally sign data
- To allow mutual authentication between the AS2 Inbound Servlet and MessageWay, through the MessageWay Service Interface (MWSI)

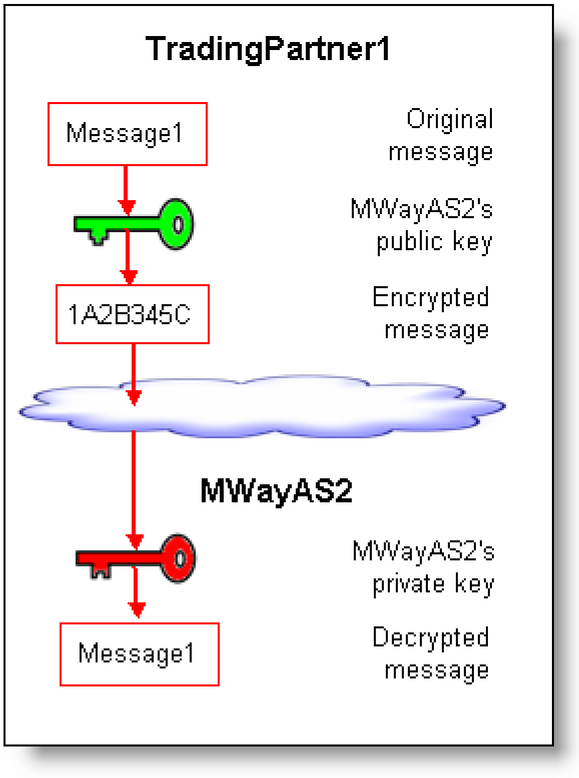
Assume that we have two trading partners: MWayAS2, which is our company, and TradingPartner1. Each trading partner has one or more stores where it keeps its certificates. The contents of our example key stores would contain at minimum the following:

Trading Partner	Contents of Certificate Store
MWayAS2	▪ Public certificate and private key for each of its identities ▪ Public certificate for TradingPartner1 ▪ Public certificate for MWSI
TradingPartner1	▪ Public certificate and private key for itself ▪ Public certificate for MWayAS2

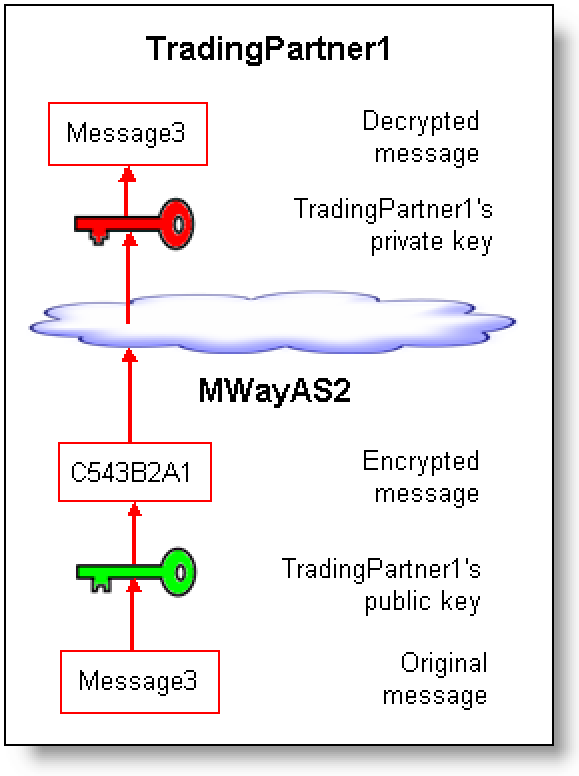
MWayAS2 uses its keys as follows:

MWayAS2 public key	▪ Provided to trading partner to encrypt outbound data and authenticate signatures on inbound data ▪ Send to MWSI for client authentication
MWayAS2 private key	▪ Decrypt inbound data ▪ Sign outbound data
TradingPartner1 public key	▪ Encrypt outbound data for TradingPartner1 ▪ Authenticate signatures on data from TradingPartner1
MWSI public key	▪ Authenticate MWSI as a trusted agent

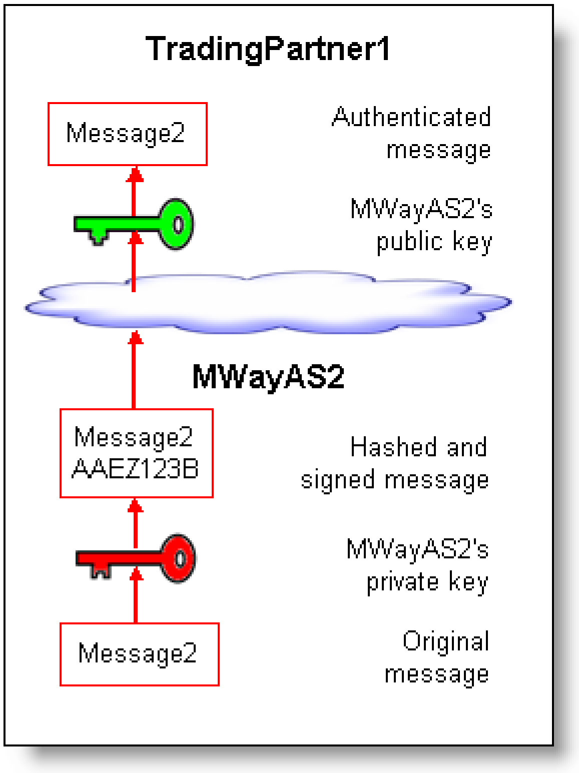
In this example, TradingPartner1 encrypts a message with MWayAS2's public key and sends it to MWayAS2. MWayAS2 decrypts the message with its own private key. Only the person with the corresponding private key can decrypt a message encrypted with its public key. Therefore, private keys must be carefully safeguarded.



The following example is the reverse of the previous example. MWayAS2 encrypts a message with TradingPartner1's public key and sends it to TradingPartner1. TradingPartner1 decrypts the message with its own private key.



The next example shows a digitally signed message, such as an MDN, that is sent from MWayAS2 to TradingPartner1. MWayAS2 calculates a hash value of Message2, called a document fingerprint, which it then signs, that is, it encrypts the fingerprint with its private key, and then sends the encrypted fingerprint with the message. When TradingPartner1 receives the message, it calculates a fingerprint for Message2 using the agreed-upon algorithm and then decrypts the fingerprint sent with the message using MWayAS2's public key. If the hash values match, the signature has been authenticated. Anyone with a user's public key can verify a signature from that user. Note that the message itself is not encrypted.



Once it has performed its AS2 duties, the AS2 Inbound servlet logs on to MessageWay over a TLS/SSL connection. The two entities perform mutual verification using certificates. The inbound servlet sends its certificate to MWSI for client authentication and MWSI sends its certificate to the inbound servlet for server authentication.

Storing AS2 Certificates in MessageWay

We use a java keystore to store the certificates. For the sake of simplicity in our examples, all parameters, except those specified in mwsi.conf, use the same java keystore (.jks) file.

The locations of the files that store the certificates are specified in the following configurations files:

MessageWay AS2 Interface configuration file (on page 136)	mwas2.conf
MessageWay Service Interface configuration file (on page 145)	mwsi.conf

The following table describes the options in the ***Global section*** (on page 137) of the mwas2.conf, which the AS2 Interface uses to communicate with its AS2 trading partners:

Process	Parameters	Purpose
AS2 Outbound Servlet (as AS2 client)	AS2SignKeyStore	▪ Sign AS2 messages ▪ Authenticate signatures on MDNs
	AS2KeyStore	▪ Encrypt AS2 messages When AS2SignKeyStore is not used ▪ Sign AS2 messages ▪ Authenticate signatures on MDNs
AS2 Inbound Servlet (as AS2 server)	AS2SignKeyStore	▪ Authenticate signatures on AS2 messages ▪ Sign MDNs
	AS2KeyStore	▪ Decrypt AS2 messages When AS2SignKeyStore is not used ▪ Authenticate signatures on AS2 messages ▪ Sign MDNs

The next table describes the options in the ***Msi section*** (on page 142) of the mwas2.conf, that specify parameters used to securely connect to MessageWay during inbound transmissions:

Process	Parameter	Purpose
AS2 Inbound Servlet (As MessageWay client)	CertVerifyStore	▪ Verify the certificate sent by MessageWay Service Interface
	ClientKeyStore	▪ Send certificate to the MessageWay Service Interface When CertVerifyStore is not used: ▪ Verify the certificate sent by MessageWay Service Interface

The next table describes the options in the ***Security Context Configurations section*** (on page 145) of the mwsi.conf, which the MessageWay Service Interface uses when an inbound client makes a secure connection:

Process	Parameter	Purpose
MessageWay Service Interface (As MessageWay server)	CertificateFile	▪ Send certificate to AS2 Inbound Servlet
	CertVerifyFile	▪ Verify the inbound servlet's certificate

Creating and Managing AS2 Certificates

It helps to have a system to manage your certificates in the Java key stores, .jks files. Here, we use keytool, a command-line key and certificate management utility, which was developed by Sun Microsystems. For more information about keytool, visit their ***Web site*** (***http://java.sun.com/***) and search the documentation. Additionally, we use the command line OpenSSL product, which is an open source SSL and TLS toolkit that includes a cryptography library, to manipulate some of the file formats. For more information, visit the ***Web site*** (***http://www.openssl.org/docs/***) and review the documentation.

For testing, we have chosen to create a Java keystore and a new test certificate. However, if you prefer to use existing certificates for testing, read the following information, and then skip to the topic, ***To Import Existing Certificates*** (on page 128). For importing, we use the pkcs12import utility, pkcs12import. For more information, visit the ***Java Web site*** (***http://java.sun.com/webservices/docs/1.5/tutorial/doc/XWS-Security8.html#wp526882***) and review the documentation.

For our examples, we will create the following:

- Self-signed certificates and Java keystore for the inbound servlet, MWayAS2
- Self-signed certificates and Java keystore for our trading partner, TradingPartner1
- Key file for MWayAS2 public certificate for MWSI to authenticate MWayAS2 as a trusted agent

Creating and storing keys is a multi-step process, because different applications require different key formats. For our example, we require the following formats:

File format	Description	Where used in Example
.jks	Java keystore file contains private and public key pairs and trusted public certificates from external users	MessageWay AS2 Interface
.pem	Base64-encoded file; for MessageWay, contains one key, public or private	MessageWay Service Interface and AS2 Connector
.cer (DER)	Binary-encoded file; for MessageWay, contains one key, typically public	AS2 Connector and to import key into .jks file
.p12	Personal Information Exchange format contains private and public key pairs	OpenSSL as intermediate file to combine separate public and private .pem key files
.pfx	Personal Information Exchange format contains private and public key pairs	AS2 Connector, which is a Microsoft .NET application, developed by /n software

On Windows, in order to use some of these commands without having to type full path names, you should add the following locations to the system variable, Path:

- Location of OpenSSL \bin directory, for example,
  c:\Program Files\OpenSSL\bin
- Location of the Java \bin directory, for example,
  c:\Program Files\Java\jre6\bin

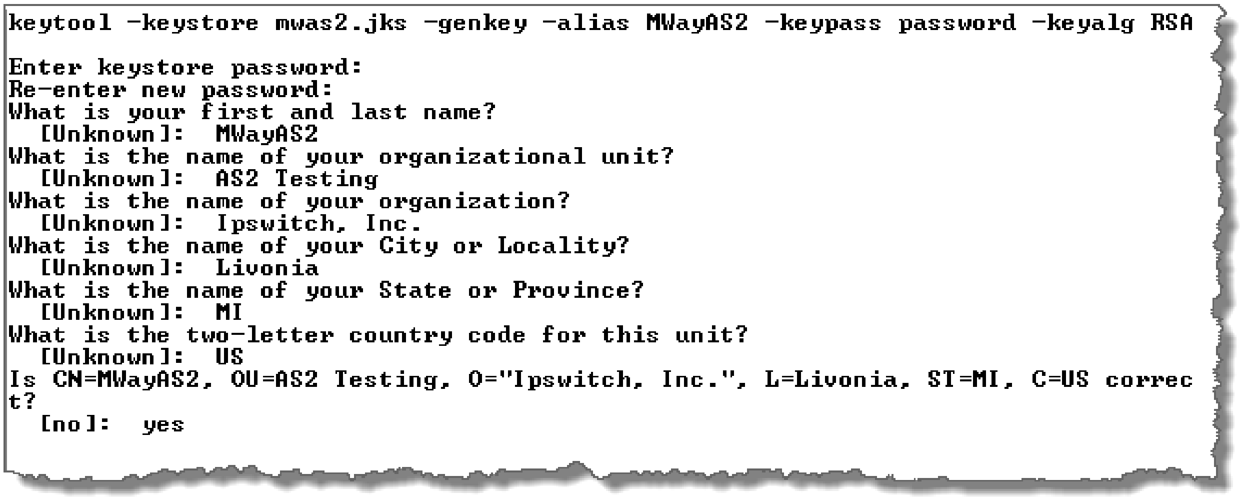
To Create a Java Keystore and New Test Certificates for Trading Partner MWayAS2

First we have to create the public and private key pair and a keystore for Trading Partner MWayAS2. To do this, we create a self-signed certificate using keytool.

1 Change your directory to where you store the certificates for the AS2 Interface. The default locations are as follows:

Linux/UNIX	/etc/messageway/certs
Windows	\Users*MessageWayUser*\AppData\Roaming\messageway\certs

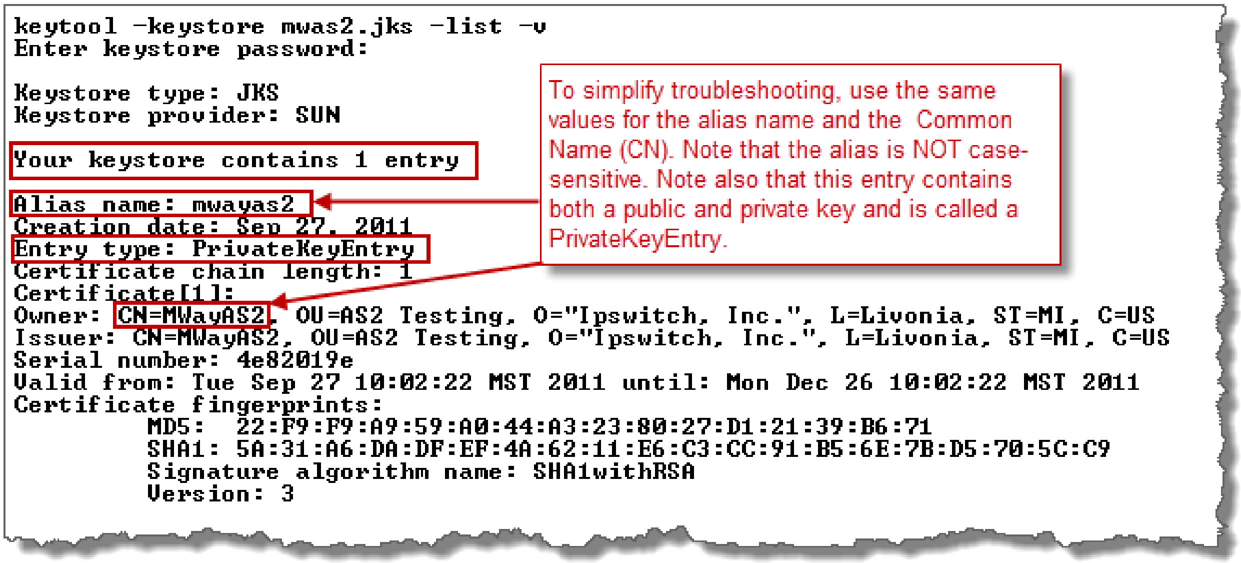
2 At a command line, type the keytool command and respond to the questions, as in the following example:



```
keytool -keystore mwas2.jks -genkey -alias MWayAS2 -keypass password -keyalg RSA

Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  MWayAS2
What is the name of your organizational unit?
  [Unknown]:  AS2 Testing
What is the name of your organization?
  [Unknown]:  Ipswitch, Inc.
What is the name of your City or Locality?
  [Unknown]:  Livonia
What is the name of your State or Province?
  [Unknown]:  MI
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=MWayAS2, OU=AS2 Testing, O="Ipswitch, Inc.", L=Livonia, ST=MI, C=US correc
t?
  [no]:  yes
```

NOTE: By default, these self-signed certificates are valid for 90 days. To use them longer than 90 days, include the following parameter in the command line: **-validity 9999**, and they will be valid for about 27 years.

3 To review the entry in your new keystore, type the following command and respond to the password question, as in the following example:



```
keytool -keystore mwas2.jks -list -v
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: mwayas2
Creation date: Sep 27, 2011
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=MWayAS2, OU=AS2 Testing, O="Ipswitch, Inc.", L=Livonia, ST=MI, C=US
Issuer: CN=MWayAS2, OU=AS2 Testing, O="Ipswitch, Inc.", L=Livonia, ST=MI, C=US
Serial number: 4e82019e
Valid from: Tue Sep 27 10:02:22 MST 2011 until: Mon Dec 26 10:02:22 MST 2011
Certificate fingerprints:
         MD5:  22:F9:F9:A9:59:A0:44:A3:23:80:27:D1:21:39:B6:71
         SHA1: 5A:31:A6:DA:DF:EF:4A:62:11:E6:C3:CC:91:B5:6E:7B:D5:70:5C:C9
         Signature algorithm name: SHA1withRSA
         Version: 3
```

To simplify troubleshooting, use the same values for the alias name and the Common Name (CN). Note that the alias is NOT case-sensitive. Note also that this entry contains both a public and private key and is called a PrivateKeyEntry.

IMPORTANT: The name and location of this file should match the values in the AS2 Interface. Specifically, the file should match the location specified in the AS2KeyStore parameter in the ***Global section*** (on page 137) and the ClientKeyStore in the ***Msi section*** (on page 142) of the mwas2.conf file.

To Import Existing Certificates

When you have an existing key pair that you want to use for testing, you should proceed as follows:

- Create a test Java keystore with dummy certificates, and then delete the test certificates you just created to create an empty keystore
- (Optional) If your public and private keys are in separate files, you must copy them to a single .p12 file
- Import your existing certificates into the empty Java Keystore

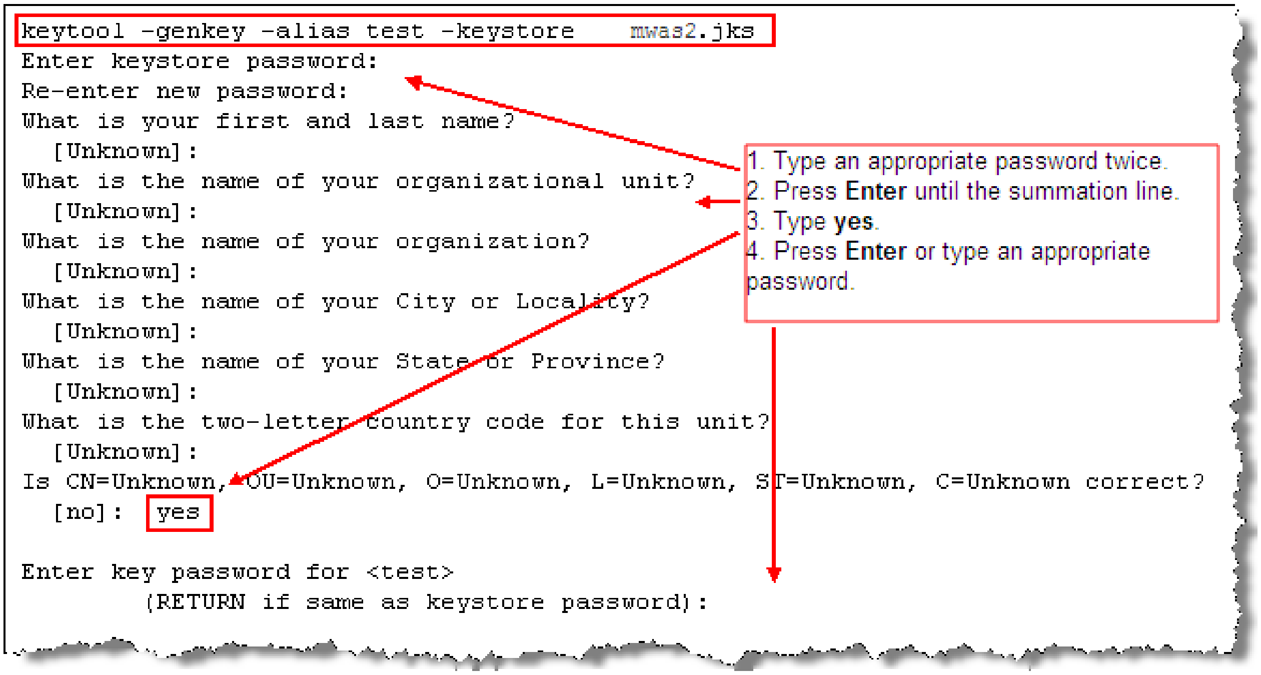
NOTE: In this example, we will use the MessageWay certificates available for SI, but you would substitute your own certificates. To import existing certificates we use the pkcs12import utility. The utility is available with the Java Web Services Developer Pack 2.0.

First, use keytool to create a keystore for MWayAS2 that will contain a dummy certificate, and then empty the keystore. To do this, we create a self-signed certificate using keytool.

1 Change your directory to where you store the certificates for the AS2 Interface. The default locations are as follows:

Linux/UNIX	/etc/messageway/certs
Windows	\Users\MessageWayUser\AppData\Roaming\messageway\certs

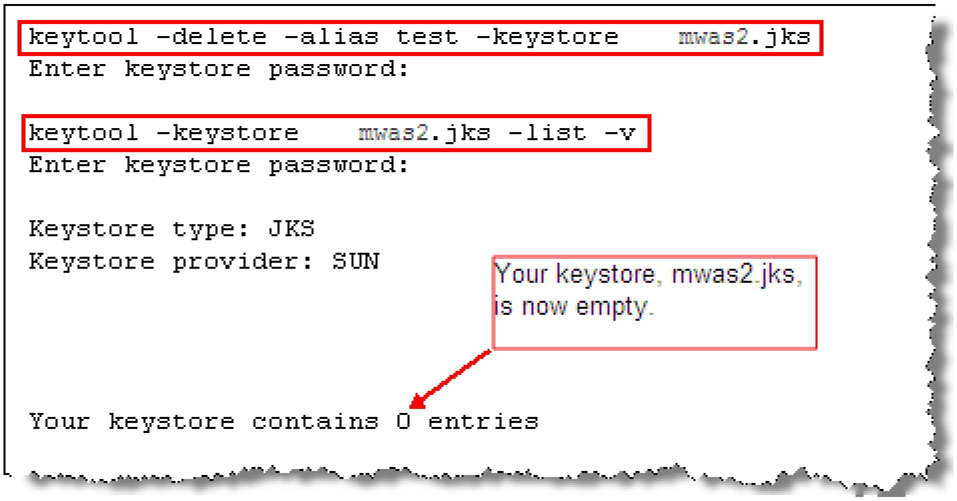
2 To create the keystore, at a command line, type the keytool command and respond to questions, as in the following example:



```
keytool -genkey -alias test -keystore    mwas2.jks
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
  [no]:  yes

Enter key password for <test>
        (RETURN if same as keystore password):
```

1. Type an appropriate password twice.
2. Press **Enter** until the summation line.
3. Type **yes**.
4. Press **Enter** or type an appropriate password.

3 To delete the contents of the keystore and then verify that it is empty, type the keytool commands and respond to the questions, as in the following example:



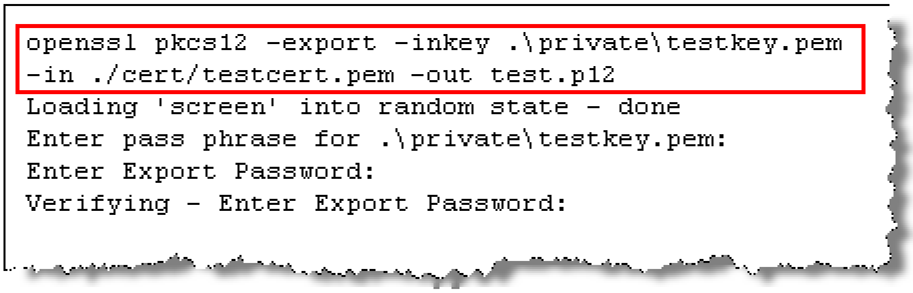
```
keytool -delete -alias test -keystore    mwas2.jks
Enter keystore password:

keytool -keystore    mwas2.jks -list -v
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN



Your keystore contains 0 entries
```

Your keystore, mwas2.jks, is now empty.

IMPORTANT: The name and location of this file should match the values in the AS2 Interface. Specifically, the file should match the location specified in the AS2KeyStore parameter in the ***Global section*** (on page 137) and the ClientKeyStore in the ***Msi section*** (on page 142) of the mwas2.conf file.

The next step is optional, depending on whether you have your certificates in a .p12 file or not. In this example, we are using existing MessageWay test certificates, whose public and private keys are in separate files. Therefore, we will use openssl to combine the two keys in one .p12 file.

4 To combine the public and private keys in one .p12 file, type the openssl command and respond to the questions, as in the following example:



```
openssl pkcs12 -export -inkey .\private\testkey.pem
-in ./cert/testcert.pem -out test.p12
Loading 'screen' into random state - done
Enter pass phrase for .\private\testkey.pem:
Enter Export Password:
Verifying - Enter Export Password:
```

The final step is to import the key pair into MessageWay JKS using pkcs12import utility.

5 Type the following, using your own locations:

pkcs12import -file "C:\Projects\Internal\MWay Service Interface and AS2\Certificates\test.p12" -keystore "C:\Projects\Internal\MWay Service Interface and AS2\Certificates\MessageWay.jks" -alias MessageWay

pkcs12-password: **password**
keystore-password: **password**
key-password: **password**

To Export the Trading Partner MWayAS2 Certificate File

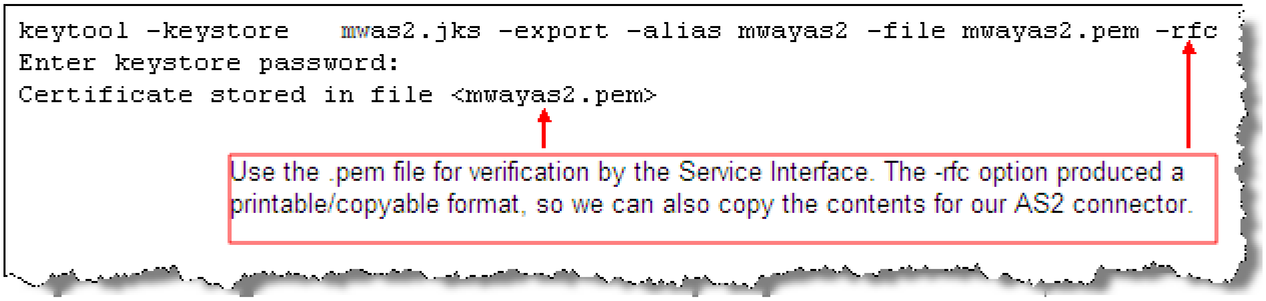
The MessageWay Service Interface (mwsi) must authenticate its client, so it needs to compare what it receives from MWayAS2, its client, with the public certificate provided by MWayAS2. Similarly, the AS2 Connector must also authenticate its client. We will export the public certificate as a .pem file from the mwas2.jks file we just created and provide it to both mwsi and AS2 Connector.

NOTE: You will copy the contents of the .pem file you create to the TradingPartner1 configurations before you ***test*** (on page 172).

1 If necessary, change your directory to where you store the certificates for the AS2 Interface. The default locations are as follows:

Linux/UNIX	/etc/messageway/certs
Windows	\ProgramData\messageway\certs

2 At a command line, type the following keytool command and respond to the question, as in the following example:



```
keytool -keystore   mwas2.jks -export -alias mwayas2 -file mwayas2.pem -rfc
Enter keystore password:
Certificate stored in file <mwayas2.pem>
```

Use the .pem file for verification by the Service Interface. The -rfc option produced a printable/copyable format, so we can also copy the contents for our AS2 connector.

IMPORTANT: The location and name of this file should match what you have put in the configuration file for the MessageWay Service Interface, ***mwsi.conf*** (on page 145). Specifically, its complete path and file name should match the value in the CertVerifyFile parameter in the Security Context Configuration section, CTX2.

To Create Certificate Files for TradingPartner1

The ***AS2 connector*** (***http://www.freeas2.com/***) we use for this example, is able to create its own certificates, which must be in .pfx format, because it is a Microsoft .NET application.

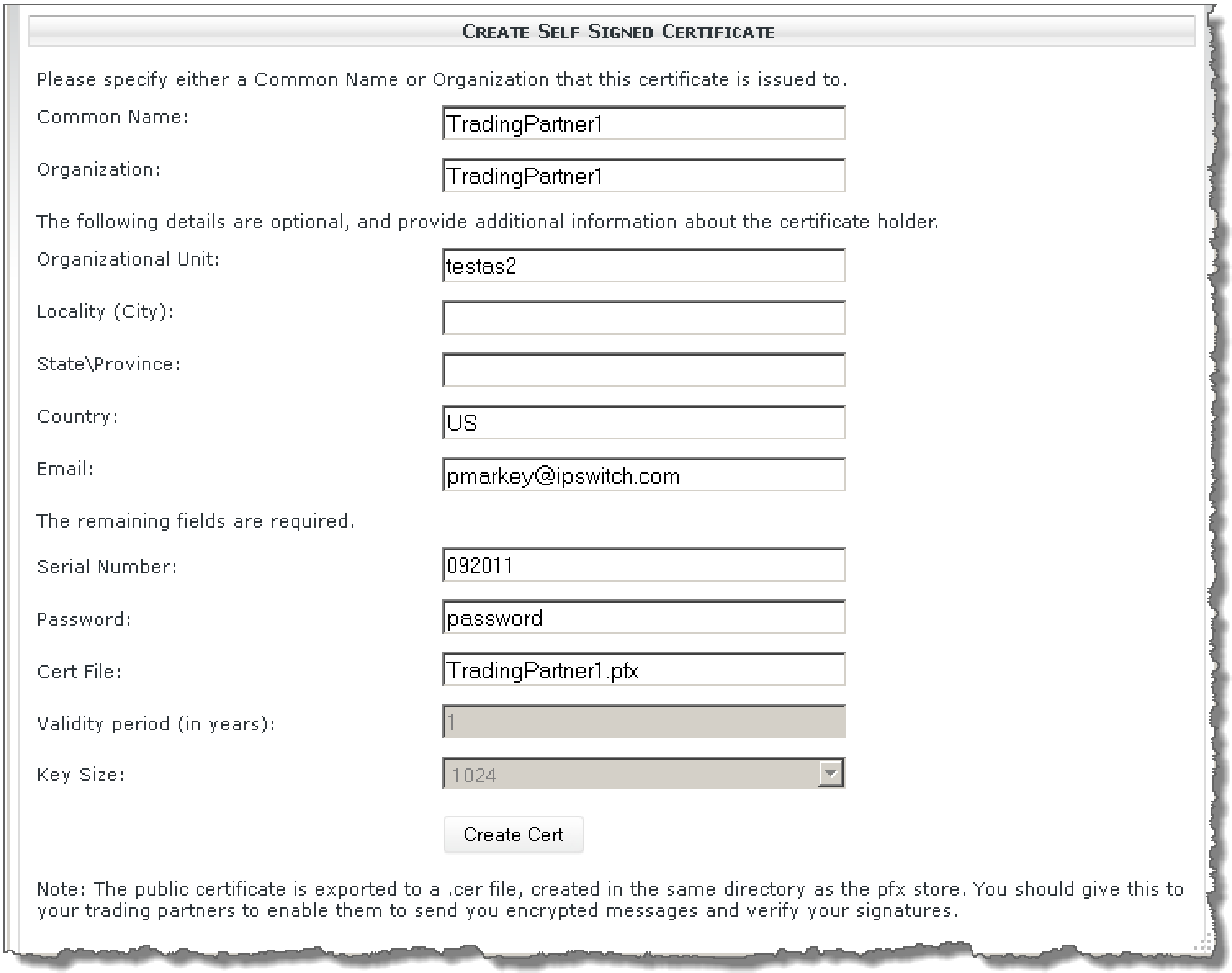
1 Start the AS2 connector.

The Administration Console Web application appears in your browser.

2 On the **Setup** tab, click **Create Certificate**.

A dialog box appears.

3 Type the following information in the dialog box (you can enter more than just the CN value if you wish):



CREATE SELF SIGNED CERTIFICATE

Please specify either a Common Name or Organization that this certificate is issued to.

Common Name:	TradingPartner1
Organization:	TradingPartner1

The following details are optional, and provide additional information about the certificate holder.

Organizational Unit:	testas2
Locality (City):	
State\Province:	
Country:	US
Email:	pmarkey@ipswitch.com

The remaining fields are required.

Serial Number:	092011
Password:	password
Cert File:	TradingPartner1.pfx
Validity period (in years):	1
Key Size:	1024

Note: The public certificate is exported to a .cer file, created in the same directory as the pfx store. You should give this to your trading partners to enable them to send you encrypted messages and verify your signatures.

You will specify the full path of the .pfx file and the password when you ***test*** (on page 172).

NOTE: TradingPartner1.pfx, which contains the public and private key pair, as well as TradingPartner1.cer, which contains the distributable public certificate, will both be created within the AS2 Connector as2data directory, typically ..\Program Files\nsoftware\AS2 Connector V2\as2data.

To Import Certificates for SI and TradingPartner1

Now you must import the public key certificates for the Service Interface (SI) and TradingPartner1 into the MWAS2 keystore, mwas2.jks. The certificate for SI will allow MWAS2 to authenticate SI as a trusted server. The certificate for TradingPartner1 will allow MWAS2 to encrypt messages destined for TradingPartner1 and authenticate signed messages and MDNs received from Trading Partner 1.

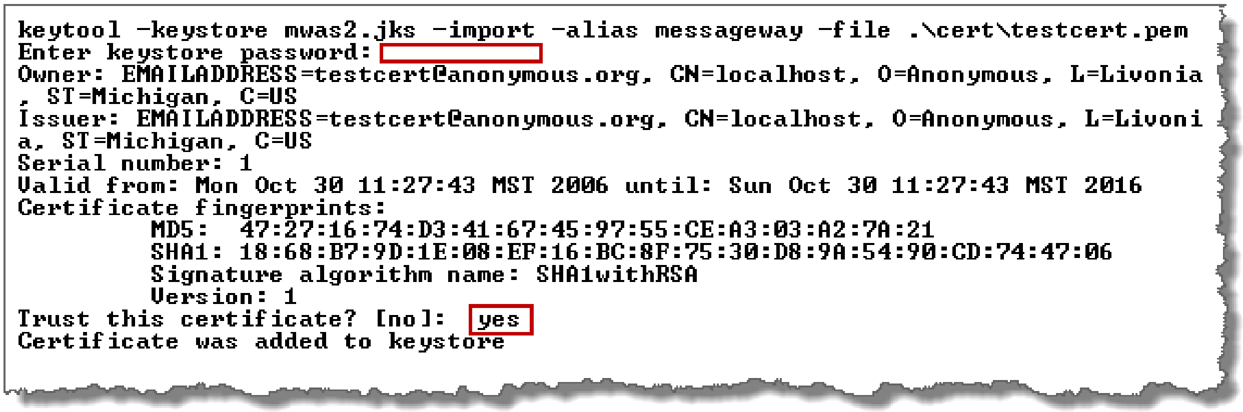
1 If necessary, change your directory to where you store the certificates for the AS2 Interface. The default locations are as follows:

Linux/UNIX	/etc/messageway/certs
Windows	\Users\MessageWayUser\AppData\Roaming\messageway\certs

2 At a command line, type the following keytool command and respond to the question to import the SI public certificate, testcert.pem, to mwas2.jks as in the following example:

Note the following for the file testcert.pem:

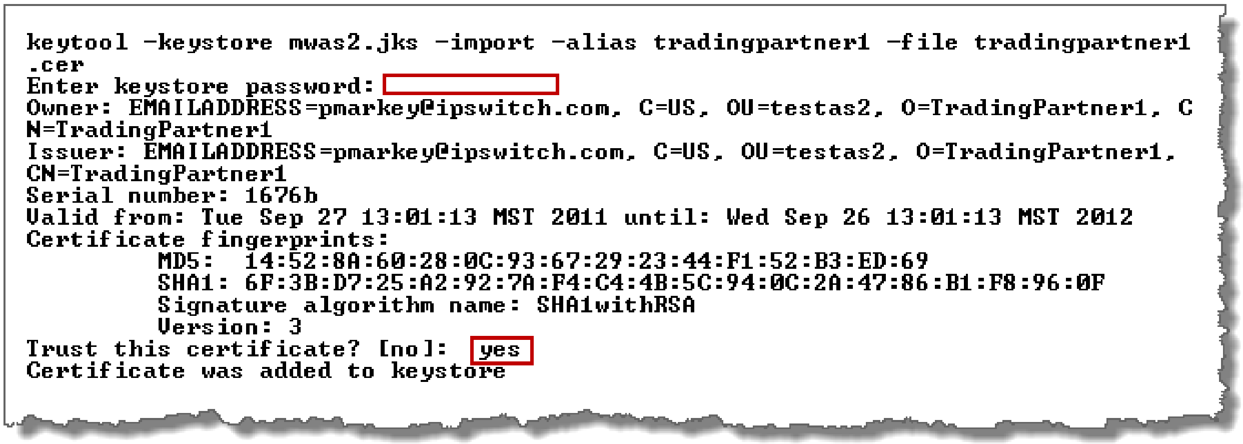
Alias	messageway
Location	One level lower than the certs directory, /certs/cert: (Windows) **.\cert\testcert.pem** (Linux/UNIX) **./cert/testcert.pem**



```
keytool -keystore mwas2.jks -import -alias messageway -file .\cert\testcert.pem
Enter keystore password:
Owner: EMAILADDRESS=testcert@anonymous.org, CN=localhost, O=Anonymous, L=Livonia
, ST=Michigan, C=US
Issuer: EMAILADDRESS=testcert@anonymous.org, CN=localhost, O=Anonymous, L=Livoni
a, ST=Michigan, C=US
Serial number: 1
Valid from: Mon Oct 30 11:27:43 MST 2006 until: Sun Oct 30 11:27:43 MST 2016
Certificate fingerprints:
         MD5:  47:27:16:74:D3:41:67:45:97:55:CE:A3:03:A2:7A:21
         SHA1: 18:68:B7:9D:1E:08:EF:16:BC:8F:75:30:D8:9A:54:90:CD:74:47:06
         Signature algorithm name: SHA1withRSA
         Version: 1
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

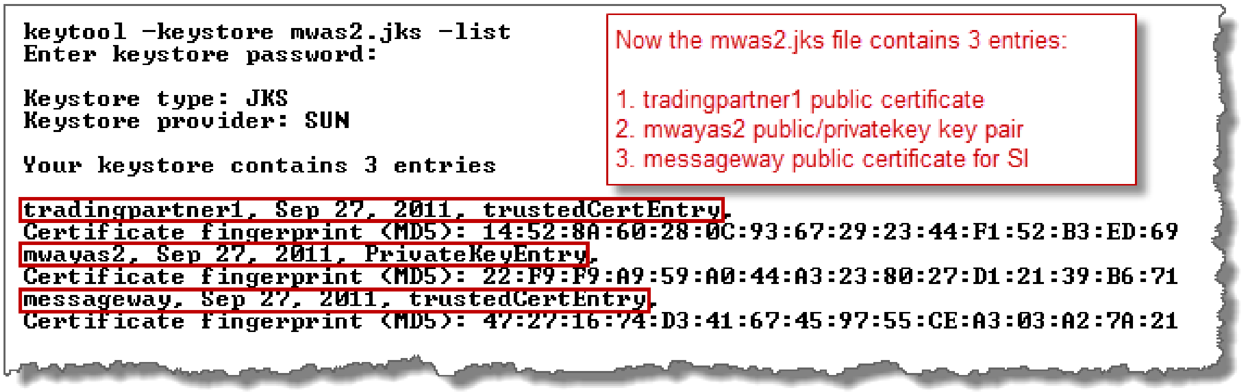
3 Copy TradingPartner1.cer, which you created previously, to the directory specified in step 1.

4 At a command line, type the following keytool command and respond to the question to import the TradingPartner1 public certificate, tradingpartner1.cer, to mwas2.jks as in the following example:



```
keytool -keystore mwas2.jks -import -alias tradingpartner1 -file tradingpartner1
.cer
Enter keystore password:
Owner: EMAILADDRESS=pmarkey@ipswitch.com, C=US, OU=testas2, O=TradingPartner1, C
N=TradingPartner1
Issuer: EMAILADDRESS=pmarkey@ipswitch.com, C=US, OU=testas2, O=TradingPartner1,
CN=TradingPartner1
Serial number: 1676b
Valid from: Tue Sep 27 13:01:13 MST 2011 until: Wed Sep 26 13:01:13 MST 2012
Certificate fingerprints:
         MD5:  14:52:8A:60:28:0C:93:67:29:23:44:F1:52:B3:ED:69
         SHA1: 6F:3B:D7:25:A2:92:7A:F4:C4:4B:5C:94:0C:2A:47:86:B1:F8:96:0F
         Signature algorithm name: SHA1withRSA
         Version: 3
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

5 To review the entry in your new keystore, type the following command and respond to the password question, as in the following example:



```
keytool -keystore mwas2.jks -list
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 3 entries

tradingpartner1, Sep 27, 2011, trustedCertEntry,
Certificate fingerprint (MD5): 14:52:8A:60:28:0C:93:67:29:23:44:F1:52:B3:ED:69
mwayas2, Sep 27, 2011, PrivateKeyEntry,
Certificate fingerprint (MD5): 22:F9:F9:A9:59:A0:44:A3:23:80:27:D1:21:39:B6:71
messageway, Sep 27, 2011, trustedCertEntry,
Certificate fingerprint (MD5): 47:27:16:74:D3:41:67:45:97:55:CE:A3:03:A2:7A:21
```

Now the mwas2.jks file contains 3 entries:

1. tradingpartner1 public certificate
2. mwayas2 public/privatekey key pair
3. messageway public certificate for SI

Configuration Files for AS2 Interface Components

You set the parameters for the AS2 Interface system in the following files:

- **web.xml** is the deployment descriptor file for the Web container
- **mwas2.conf** is the configuration file for the AS2 servlets
- **mwsi.conf** is the configuration file for the Service Interface

For more information about configuring the Service Interface file, refer to the topic, ***Service Interface*** (on page 95).

The following table shows the default location for the AS2 configuration file, mwas2.conf, and the deployment descriptor file, web.xml, using the directory structure for Apache Tomcat as the Web container:

Operating System	Location of the AS2 Configuration Files
UNIX or Linux	/*Web container installation directory*/**webapps/mwas2/WEB-INF/**
Windows, Explorer	\Web container installation directory\webapps\\mwas2\\WEB-INF\

Web Application Deployment Descriptor File

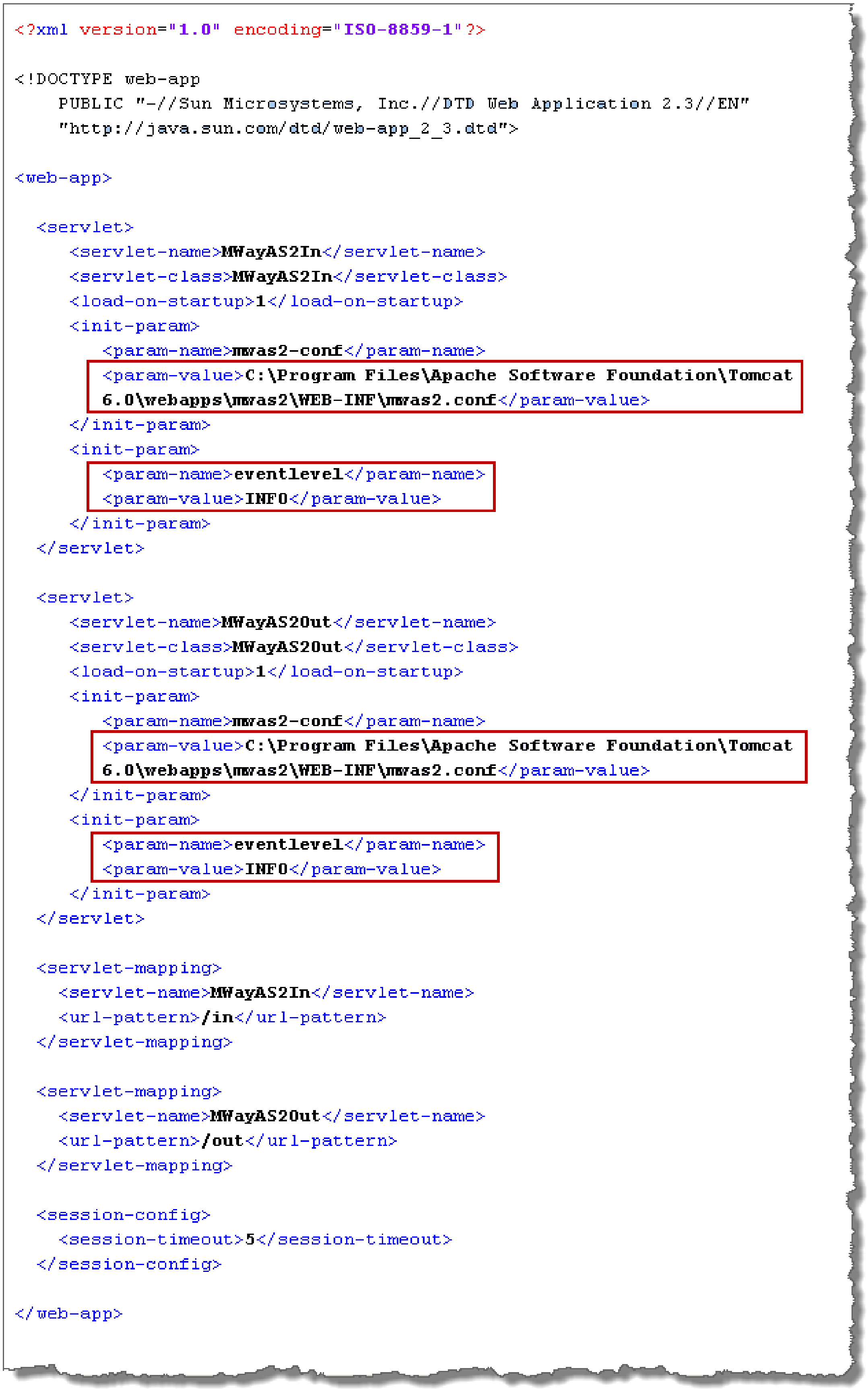
The deployment descriptor file, web.xml, is located within the mwas2 Web application's WEB-INF directory. It defines parameters that are used when the AS2 servlets are deployed in the servlet container. Deployment occurs when the Web container, such as Apache Tomcat, is started.

CAUTION: Make sure you restart the Web container, such as Apache Tomcat, after you make changes to web.xml.

You may need to change some of the param values. The following table describes two of interest:

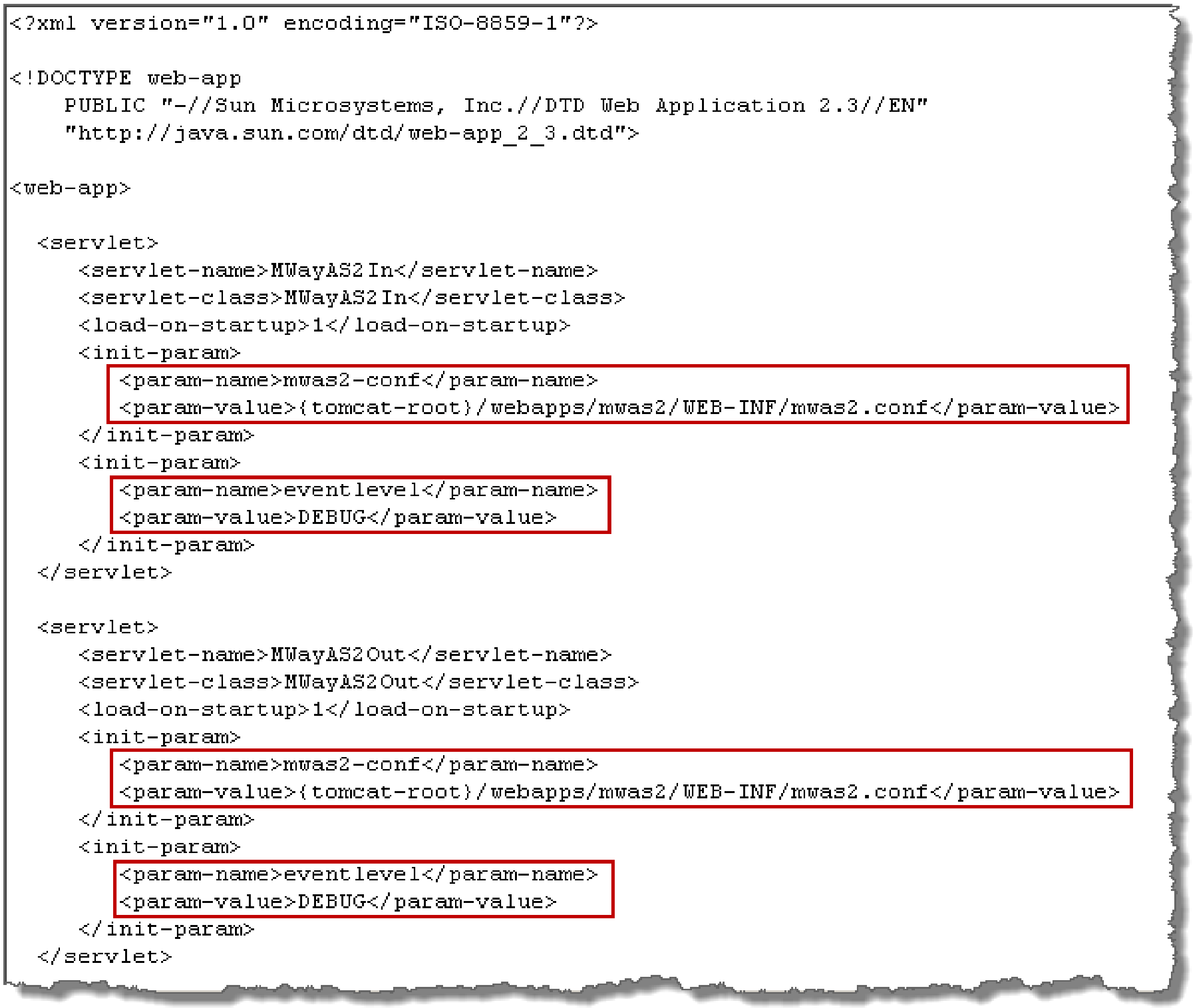
Param-name	Description of param-value
mwas2-conf	Fully qualified name of the AS2 configuration file, mwas2.conf. This value must match the location of the mwas2.conf file on your system.
eventlevel	Defines the lowest level of event messages that the AS2 servlets will write to the system event log. If not present or not configured, INFO will be used as the event level. Set the value to DEBUG for each servlet to trace processing.

Here are examples of these settings in a web.xml file:



```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE web-app
    PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
    "http://java.sun.com/dtd/web-app_2_3.dtd">

<web-app>

  <servlet>
     <servlet-name>MWayAS2In</servlet-name>
     <servlet-class>MWayAS2In</servlet-class>
     <load-on-startup>1</load-on-startup>
     <init-param>
        <param-name>mwas2-conf</param-name>
        <param-value>C:\Program Files\Apache Software Foundation\Tomcat
        6.0\webapps\mwas2\WEB-INF\mwas2.conf</param-value>
     </init-param>
     <init-param>
        <param-name>eventlevel</param-name>
        <param-value>INFO</param-value>
     </init-param>
  </servlet>

  <servlet>
     <servlet-name>MWayAS2Out</servlet-name>
     <servlet-class>MWayAS2Out</servlet-class>
     <load-on-startup>1</load-on-startup>
     <init-param>
        <param-name>mwas2-conf</param-name>
        <param-value>C:\Program Files\Apache Software Foundation\Tomcat
        6.0\webapps\mwas2\WEB-INF\mwas2.conf</param-value>
     </init-param>
     <init-param>
        <param-name>eventlevel</param-name>
        <param-value>INFO</param-value>
     </init-param>
  </servlet>

  <servlet-mapping>
    <servlet-name>MWayAS2In</servlet-name>
    <url-pattern>/in</url-pattern>
  </servlet-mapping>

  <servlet-mapping>
    <servlet-name>MWayAS2Out</servlet-name>
    <url-pattern>/out</url-pattern>
  </servlet-mapping>

  <session-config>
    <session-timeout>5</session-timeout>
  </session-config>

</web-app>
```

AS2 Web.xml file configurations for Windows



```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE web-app
    PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
    "http://java.sun.com/dtd/web-app_2_3.dtd">

<web-app>

  <servlet>
     <servlet-name>MWayAS2In</servlet-name>
     <servlet-class>MWayAS2In</servlet-class>
     <load-on-startup>1</load-on-startup>
     <init-param>
        <param-name>mwas2-conf</param-name>
        <param-value>{tomcat-root}/webapps/mwas2/WEB-INF/mwas2.conf</param-value>
     </init-param>
     <init-param>
        <param-name>eventlevel</param-name>
        <param-value>DEBUG</param-value>
     </init-param>
  </servlet>

  <servlet>
     <servlet-name>MWayAS2Out</servlet-name>
     <servlet-class>MWayAS2Out</servlet-class>
     <load-on-startup>1</load-on-startup>
     <init-param>
        <param-name>mwas2-conf</param-name>
        <param-value>{tomcat-root}/webapps/mwas2/WEB-INF/mwas2.conf</param-value>
     </init-param>
     <init-param>
        <param-name>eventlevel</param-name>
        <param-value>DEBUG</param-value>
     </init-param>
  </servlet>
```

AS2 web.xml file configurations for Linux

AS2 Interface Configuration File

The MessageWay AS2 Interface comprises an inbound servlet, which functions as a server to the outside world, and an outbound servlet, which functions as a client to the outside world. These servlets may reside anywhere in the LAN or WAN. The servlets provide secure and unsecure communications with remote locations using HTTPS and HTTP, respectively.

The inbound servlet, acting as a server, receives files from an AS2 client, which is typically outside the network. The inbound servlet also acts as a client when it forwards messages to the MessageWay Service Interface (SI). A secure HTTP connection (HTTPS) is mandatory between the AS2 Inbound Servlet and SI.

The outbound servlet, acting as a client, sends files that it receives from the AS2 adapter to a remote AS2 server.

CAUTION: Make sure you restart the Web container, such as Apache Tomcat, after you make changes to mwas2.conf.

There are two sections, Global and Msi, in the configuration file, mwas2.conf. The following table describes the purpose of each section.

Section	Purpose
Global	▪ Access class to authenticate MessageWay users ▪ Settings to support Java key store for keys and certificates for AS2 inbound and outbound encryption/decryption and signing ▪ Settings to support Java key store for keys and certificates used only for signing ▪ Toggle to allow signed/unsigned inbound messages ▪ Toggle to allow authenticated/unauthenticated inbound messages ▪ Toggle to store inbound AS2 file name or AS2 message id on MessageWay message. ▪ Optional directory to log inbound message processing ▪ Optional directory to log outbound message processing
Msi	▪ IP address and port on which Service Interface listens ▪ Security certificate information ▪ Client certificate information for public key authentication ▪ Timeouts

Global Section

The global section specifies the attributes required by the AS2 servlets. The following table explains the parameters used in the global section of mwas2.conf.

Parameter	Description
AccessClass	Restricts access to MessageWay via this listener to only those users whose configuration does not include an access class list or includes this value in their access class list. This value should be alphanumeric and is case-sensitive. It must match exactly what is specified for the user. Optional, but if used, only one access class value is allowed.

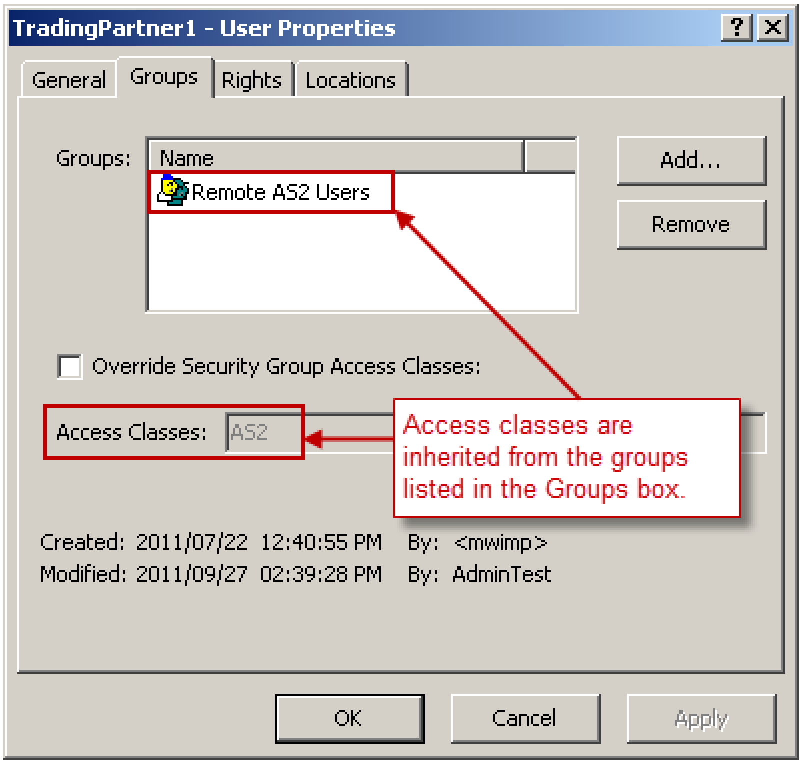
Parameter	**Description**
AS2KeyStore	Fully qualified file name of the Java key store (jks), which contains the keys and certificates used for AS2 message encryption/decryption. The keys might also be used for AS2 message and MDN signing and signature authentication. Conditional; Not needed if encryption/decryption and signing never used.
AS2KeyStorePW	AS2KeyStore password. All private keys within the jks MUST have the same password as the key store when the separate AS2KeyPW is not used. Mandatory if AS2KeyStore configured.
AS2KeyPW	Key password for private key(s) within AS2KeyStore. Valid values are: ▪ **AS2ID** ▪ *hard coded value* ▪ *blank* Use **AS2ID** when *AS2-To* or *AS2-From* value is the password. For inbound, **AS2ID** will cause the *AS2-To* value to be used, since the recipient's private key is needed to decrypt the message. For outbound, **AS2ID** will cause the *AS2-From* value to be used, since the sender's private key is needed to sign the message. If blank, defaults to AS2KeyStorePW.
AS2KeySubject	Unique, partial key subject used to locate the proper private key within AS2KeyStore. Valid values are: ▪ **AS2ID** ▪ *hard coded value* Use **AS2ID** when *AS2-To* or *AS2-From* value on transmission is uniquely contained within the respective private key's subject. For inbound, **AS2ID** will cause the *AS2-To* value to be used. For outbound, **AS2ID** will cause the *AS2-From* value to be used. An example key subject follows: `CN=MWayAS2, OU=AS2 Testing, O="Progress" L=Livonia, ST=MI, C=US` The qualifier tags, such as CN=, OU=, and O=, should not be used, only one of their values. **IMPORTANT:** When MessageWay functions as a VAN, it may impersonate multiple sending/receiving identities. In this case, AS2KeySubject must be set to **AS2ID** and each respective private key subject must contain the appropriate and unique *AS2-To* or *AS2-From* value. Optional; Default is **AS2ID**.

Parameter	Description
AS2SignKeyStore	Fully qualified Java key store (jks) file name, which contains the keys and certificates used for AS2 message and MDN signing and signature authentication when different from those used for encryption/decryption. Optional.
AS2SignKeyStorePW	AS2SignKeyStore password. Mandatory if AS2SignKeyStore configured.
AS2SignKeyPW	Key password for private key(s) within AS2SignKeyStore. Valid values are: ▪ **AS2ID** ▪ *hard coded value* ▪ *blank* Use **AS2ID** when *AS2-To* or *AS2-From* value is the password. For inbound, **AS2ID** will cause the *AS2-To* value to be used, since the recipient's private key is needed to sign the returned MDN, if requested. For outbound, **AS2ID** will cause the *AS2-From* value to be used, since the sender's private key is needed to sign the message. If blank, defaults to AS2SignKeyStorePW.
AS2SignKeySubject	Unique, partial key subject used to locate the proper private key within AS2SignKeyStore. Valid values are: ▪ **AS2ID** ▪ *hard coded value* Use **AS2ID** when A*S2-To* or *AS2-From* value on transmission is uniquely contained within the respective private key's subject. For inbound, **AS2ID** will cause the *AS2-To* value to be used. For outbound, **AS2ID** will cause the *AS2-From* value to be used. An example key subject follows: `CN=MWayAS2, OU=AS2 Testing, O="Progress" L=Livonia, ST=MI, C=US` The qualifier tags, such as CN=, OU=, and O=, should not be used, only one of their values. **IMPORTANT:** When MessageWay functions as a VAN, it may impersonate multiple sending/receiving identities. In this case AS2SignKeySubject must be set to **AS2ID** and each respective private key subject must contain the appropriate and unique *AS2-To* or *AS2-From* value. Optional; Default is **AS2ID**.
AllowUnsigned	Allow unsigned inbound AS2 messages to be received. Valid values are: ▪ **yes** ▪ **no** Optional; Default is **no**.

Parameter	**Description**
AllowUnauthenticated	Allow unauthenticated inbound AS2 messages to be received. An unauthenticated message is one that was not signed and was not authenticated by HTTP. Valid values are: ▪ **yes** ▪ **no** Optional; Default is **no**.
InboundLogDir	Location used to store AS2 logs for inbound processing. Configured directory will be created if it does not exist. Two files will be created for each inbound transmission. The log file will have a .log extension and the data file will have a .dat extension. Both file names will be of the format *yyyy-mm-dd-hh-mm-ss-mmmm.ext*. A file with a .err extension will be generated if an AS2 processing error occurs. Best used for debugging. Optional.
OutboundLogDir	Location used to store AS2 logs for outbound processing. Configured directory will be created if it does not exist. A log file will be created for each outbound transmission. The log file name will be of the format *yyyy-mm-dd-hh-mm-ss-mmmm-sent.log*. A file with a .err extension will be generated if an AS2 processing error occurs. Best used for debugging. Optional.

Here is an example of a Global section in the mwas2.conf file. Note the following:

- **AccessClass** value requires that AS2 users who have access classes defined must have the ***AS2 access class*** (on page 152) defined on their access list to be able to send messages into MessageWay



Groups: Remote AS2 Users

□ Override Security Group Access Classes:

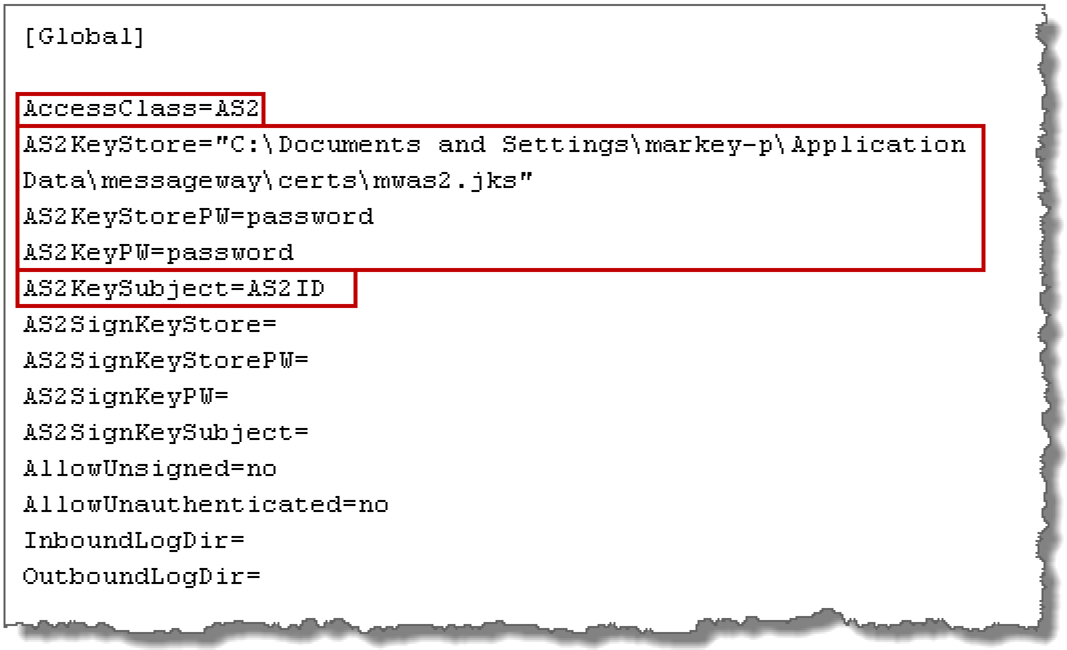
Access Classes: AS2

Access classes are inherited from the groups listed in the Groups box.

Created: 2011/07/22 12:40:55 PM By: <mwimp>
Modified: 2011/09/27 02:39:28 PM By: AdminTest

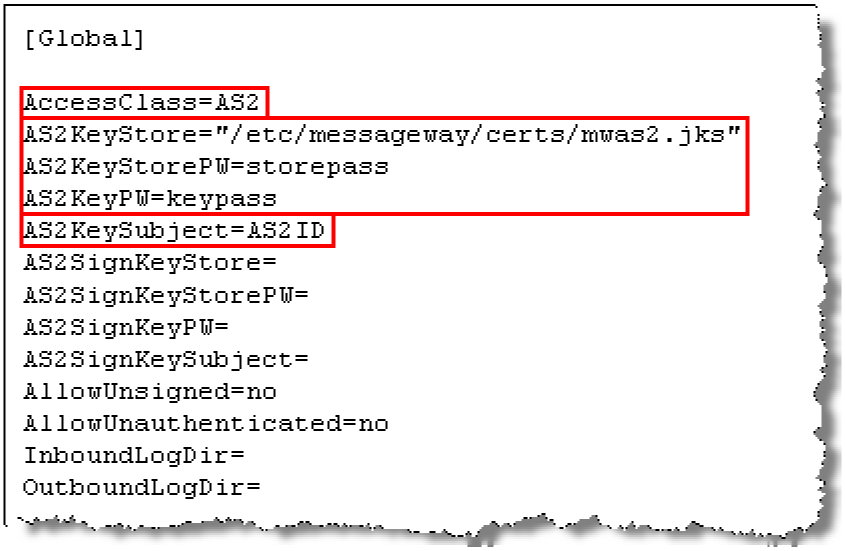
- **AS2KeyStore** must match the location of the ***certificate keystore*** (on page 127)

- **AS2ID** allows MessageWay to impersonate multiple trading partners, instead of just one (MWayAS2) as in our example.



```
[Global]

AccessClass=AS2
AS2KeyStore="C:\Documents and Settings\markey-p\Application
Data\messageway\certs\mwas2.jks"
AS2KeyStorePW=password
AS2KeyPW=password
AS2KeySubject=AS2ID
AS2SignKeyStore=
AS2SignKeyStorePW=
AS2SignKeyPW=
AS2SignKeySubject=
AllowUnsigned=no
AllowUnauthenticated=no
InboundLogDir=
OutboundLogDir=
```

mwas2.conf, Global Section Example for Windows



```
[Global]

AccessClass=AS2
AS2KeyStore="/etc/messageway/certs/mwas2.jks"
AS2KeyStorePW=storepass
AS2KeyPW=keypass
AS2KeySubject=AS2ID
AS2SignKeyStore=
AS2SignKeyStorePW=
AS2SignKeyPW=
AS2SignKeySubject=
AllowUnsigned=no
AllowUnauthenticated=no
InboundLogDir=
OutboundLogDir=
```

mwas2.conf, Global Section Example for UNIX/Linux

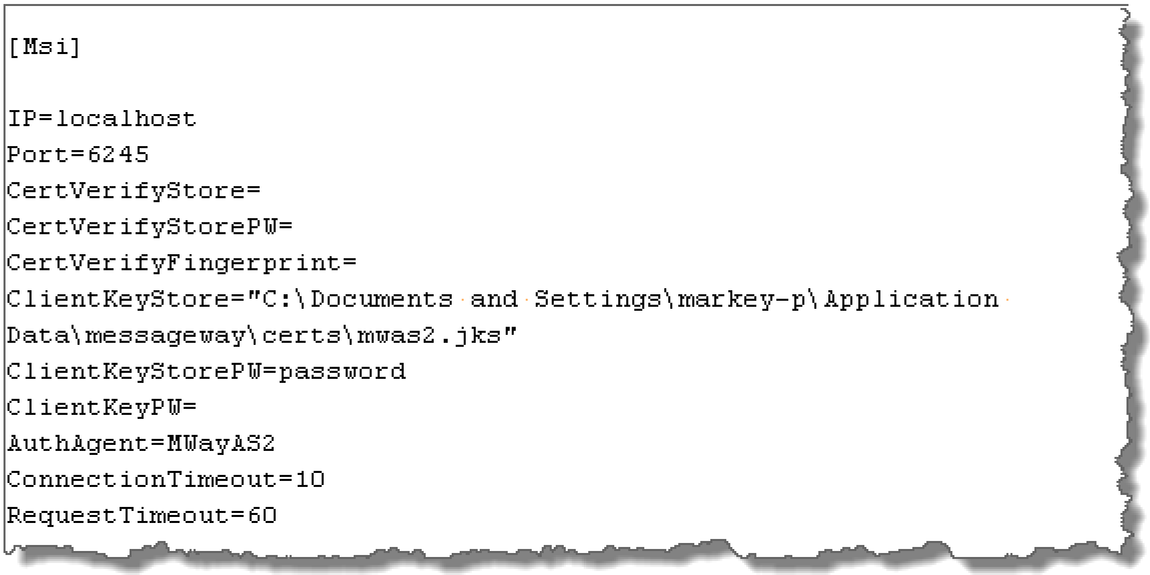
MSI Section

This section specifies how the AS2 inbound servlet communicates with the MessageWay Service Interface (SI). The following table explains the parameters used in the MSI section of mwas2.conf.

Parameter	Description
IP	Remote IP address of the server that is running the MessageWay Service Interface. The AS2 Inbound Servlet will connect to this IP address. Mandatory.
Port	Secure remote Port number where the MessageWay Service Interface is listening. The AS2 Inbound Servlet will connect to this port. A secure port MUST be used, since Client Authentication is performed. **IMPORTANT:** This must match a port configured in the Listeners section of the SI configuration file, mwsi.conf. Mandatory.
CertVerifyStore	Fully qualified file name of the Java key store (jks) on the AS2 Servlet box that is used to verify the certificate file sent to the AS2 Inbound Servlet from SI when establishing a secure connection (SSL). Not needed if the mandatory ClientKeyStore contains the SI certificate. Only one of CertVerifyStore or CertVerifyFingerprint should be configured. Conditional.
CertVerifyStorePW	CertVerifyStore password. Mandatory if CertVerifyStore configured.
CertVerifyFingerprint	SHA1 or MD5 digest of the SI certificate. Not needed if the mandatory ClientKeyStore contains the SI certificate. Only one of CertVerifyStore or CertVerifyFingerprint should be configured. Conditional.
ClientKeyStore	Fully qualified file name of the Java key store (jks) on the AS2 Servlet box that is used for client authentication between the AS2 Inbound Servlet and SI. This jks contains the AS2 server box client private key and certificate. This jks can be the same jks configured in the Global section (AS2KeyStore) provided only one private key exists and it is used for both AS2 processing and client authentication. Mandatory.
ClientKeyStorePW	ClientKeyStore password. Mandatory.
ClientKeyPW	Key password for private key within ClientKeyStore. Default is value in ClientKeyStorePW. Optional.

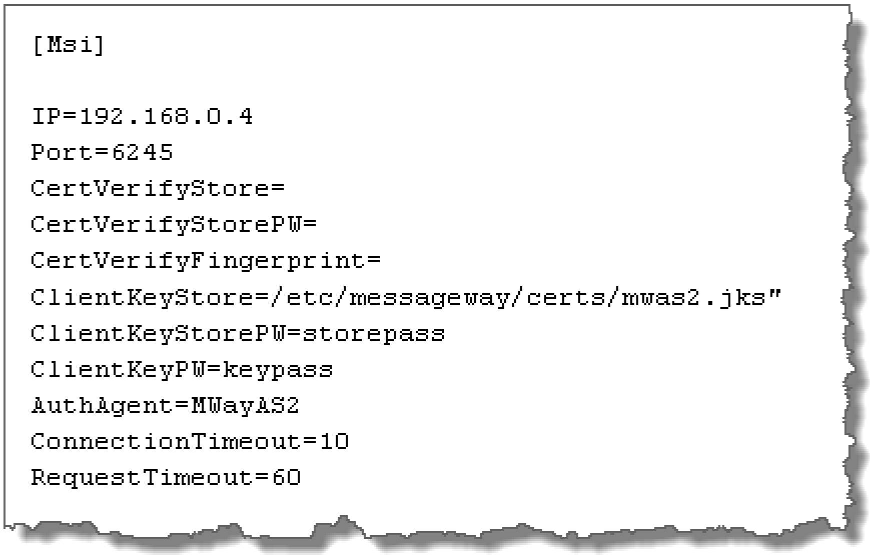
Parameter	Description
AuthAgent	Name of the trusted authentication agent as identified by the Common Name on the client certificate. This case-sensitive name must match the Common Name (CN) on the client certificate that is stored in the ClientKeyStore and must be included in the SI agents file (i.e. trusted by SI). Mandatory.
ConnectionTimeout	Time (in seconds) that the AS2 Inbound Servlet will wait for a connection to the MessageWay Service Interface to complete. Optional; Default is 10 seconds.
RequestTimeout	Time (in seconds) that the AS2 Inbound Servlet will wait for a response from the MessageWay Service Interface. Optional; Default is 60 seconds.

Here are examples of an Msi section in the mwas2.conf file.



```
[Msi]

IP=localhost
Port=6245
CertVerifyStore=
CertVerifyStorePW=
CertVerifyFingerprint=
ClientKeyStore="C:\Documents and Settings\markey-p\Application
Data\messageway\certs\mwas2.jks"
ClientKeyStorePW=password
ClientKeyPW=
AuthAgent=MWayAS2
ConnectionTimeout=10
RequestTimeout=60
```

mwas2.conf, Msi Section Example for Windows



```
[Msi]

IP=192.168.0.4
Port=6245
CertVerifyStore=
CertVerifyStorePW=
CertVerifyFingerprint=
ClientKeyStore=/etc/messageway/certs/mwas2.jks"
ClientKeyStorePW=storepass
ClientKeyPW=keypass
AuthAgent=MWayAS2
ConnectionTimeout=10
RequestTimeout=60
```

mwas2.conf, Msi Section Example for UNIX/Linux

Service Interface Configuration File

For AS2 messages sent to MessageWay, the AS2 Inbound Servlet must communicate with the Service Interface (SI) over a secure, HTTPS, connection. The ports specified on the AS2 configuration file, mwas2.conf, and the ***SI configuration*** (on page 95) file, mwsi.conf, must match. This port may be different from other secure ports that SI monitors, because the security context configuration sections may require different information.

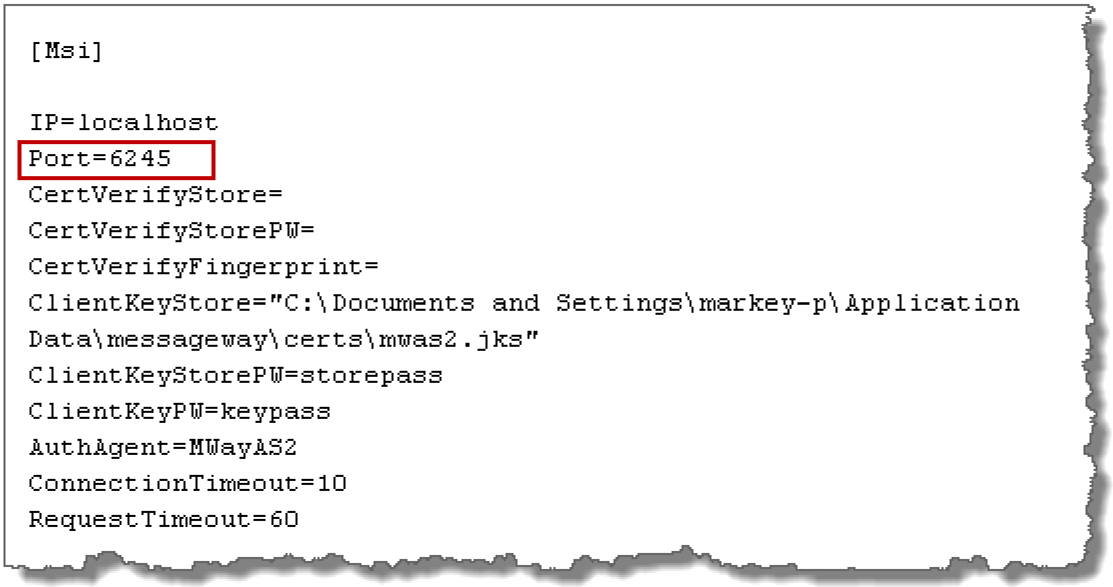
CAUTION: Make sure you restart the MessageWay Service Interface after you make changes to mwsi.conf.

Also, the SI must authenticate the AS2 Inbound Servlet from the servlet's client certificate and authorize the user it represents to access MessageWay. To do this, it uses public key authentication, which requires a secure connection.

These are the default locations for the mwsi.conf file:

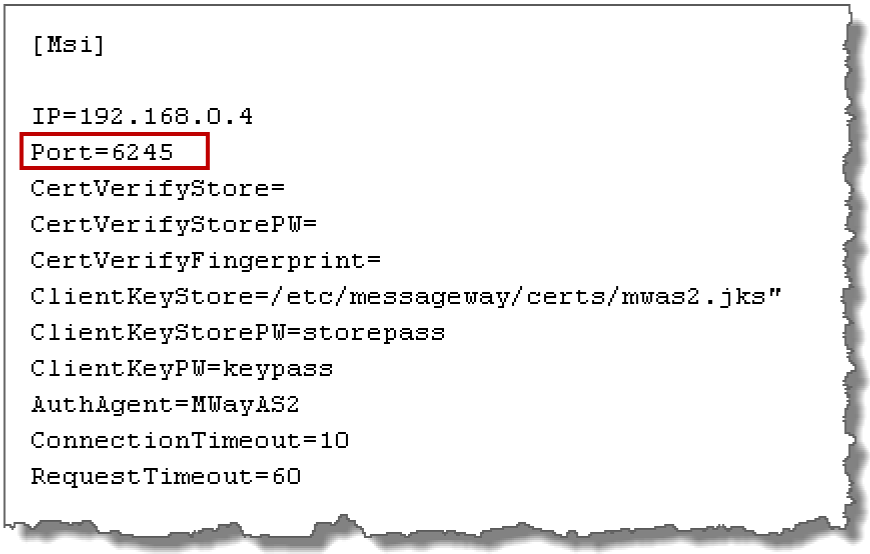
Operating System	Location of the MW Service Interface Configuration File
UNIX or Linux	/etc/messageway/mwsi.conf
Windows	\Users\MessageWayUser\AppData\Roaming\messageway\mwsi.conf

For example, here is the configuration in the MessageWay Service Interface Configuration Section of the mwas2.conf file. Notice that the port listed must match an HTTPS port configured for SI.



```
[Msi]

IP=localhost
Port=6245
CertVerifyStore=
CertVerifyStorePW=
CertVerifyFingerprint=
ClientKeyStore="C:\Documents and Settings\markey-p\Application
Data\messageway\certs\mwas2.jks"
ClientKeyStorePW=storepass
ClientKeyPW=keypass
AuthAgent=MWayAS2
ConnectionTimeout=10
RequestTimeout=60
```

mwas2.conf, Msi Section, Port, Windows

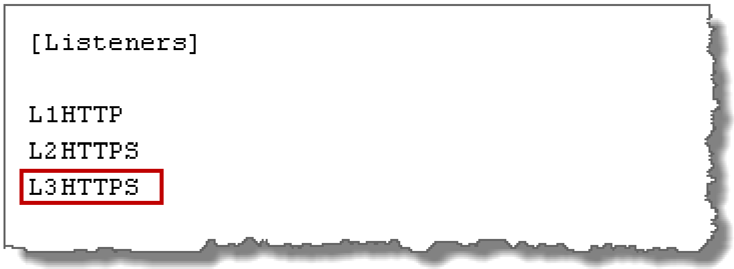


```
[Msi]

IP=192.168.0.4
Port=6245
CertVerifyStore=
CertVerifyStorePW=
CertVerifyFingerprint=
ClientKeyStore=/etc/messageway/certs/mwas2.jks"
ClientKeyStorePW=storepass
ClientKeyPW=keypass
AuthAgent=MWayAS2
ConnectionTimeout=10
RequestTimeout=60
```

mwas2.conf, Msi Section, Port, Linux

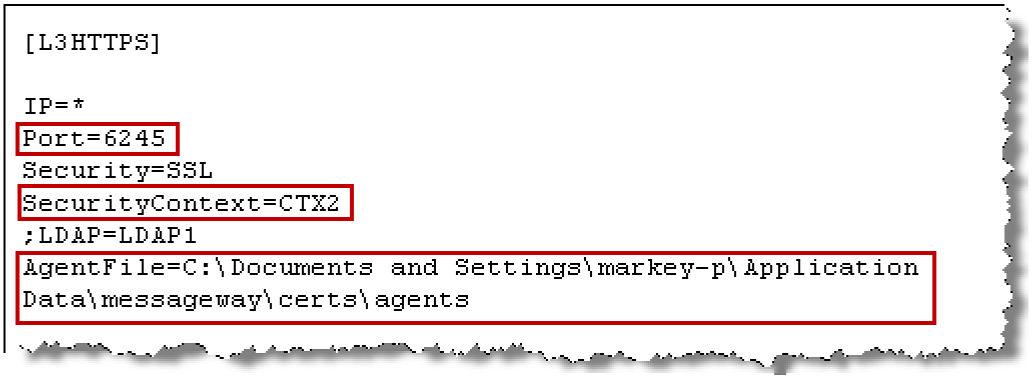
The related configuration in the HTTP Listeners Configuration section of the ***mwsi.conf file*** (on page 96), must have the following configurations:

NOTE: The Listeners section must also have a secure listener that you can use for AS2:



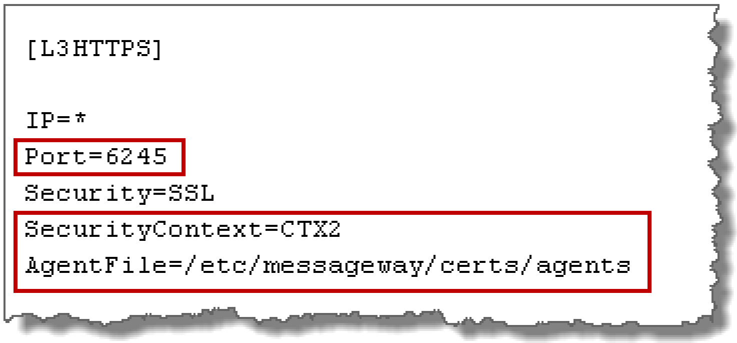
```
[Listeners]

L1HTTP
L2HTTPS
L3HTTPS
```

- **Port** must be the same as the port configured in the mwas2.conf file
- **SecurityContext** must point to the appropriate configuration that supports public key authentication for AS2
- **AgentFile** must specify the fully qualified name of the agents file, used to authenticate the Inbound AS2 Servlet and the AS2 user to MessageWay



```
[L3HTTPS]

IP=*
Port=6245
Security=SSL
SecurityContext=CTX2
;LDAP=LDAP1
AgentFile=C:\Documents and Settings\markey-p\Application
Data\messageway\certs\agents
```

mwsi.conf, Listeners Section, L3HTTPS, Windows



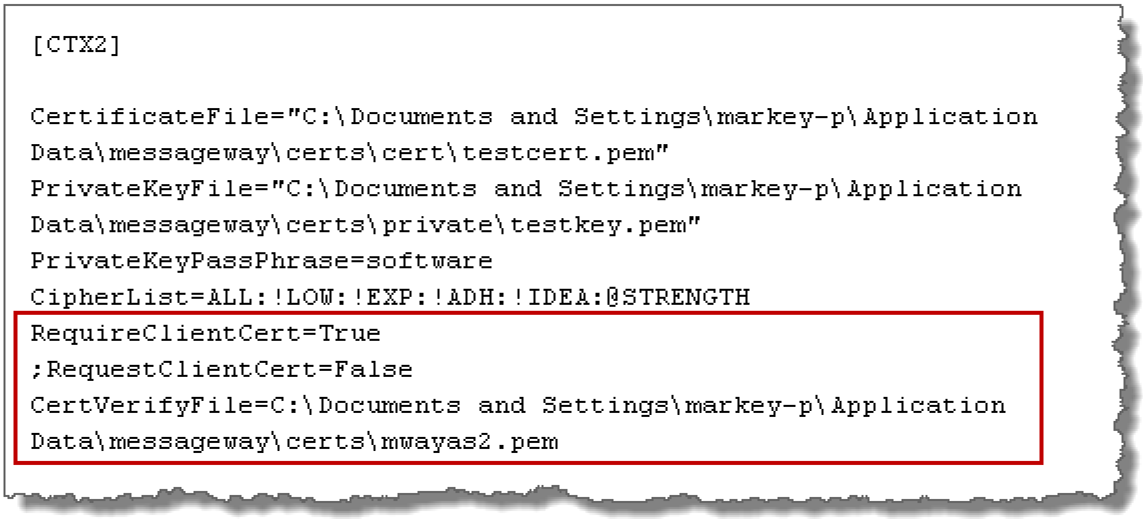
```
[L3HTTPS]

IP=*
Port=6245
Security=SSL
SecurityContext=CTX2
AgentFile=/etc/messageway/certs/agents
```

mwsi.conf, Listeners Section, L3HTTPS, Linux

IMPORTANT: The port in this example is different than the standard L2HTTPS port, 6243, which comes preconfigured in the mwsi.conf installed with MessageWay, because the security context configurations are different.

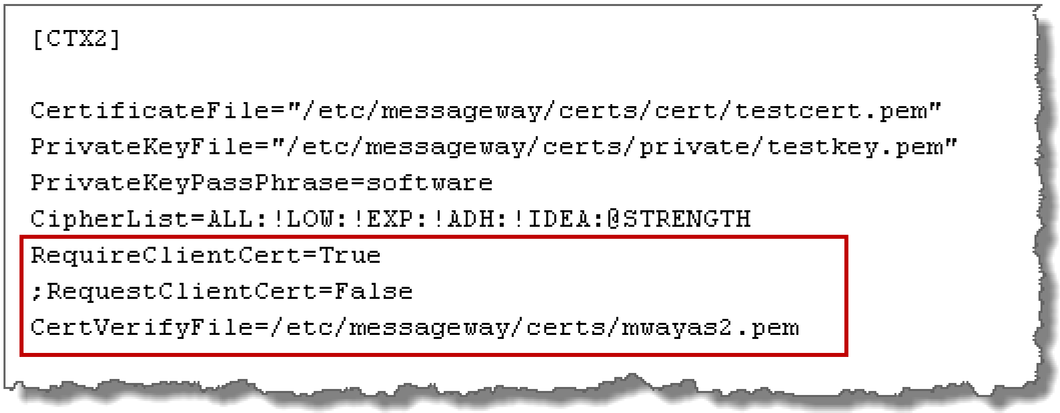
The configuration, CTX2, specifies public key client authentication that is required to support communications between the AS2 Inbound Servlet and SI. These parameters must be configured as follows:

- **RequireClientCert=True**
- **RequestClientCert** must be commented or removed
- **CertVerifyFile** must identify the fully qualified certificate file, which here is used to verify the AS2 Inbound Servlet and the user to MessageWay



```
[CTX2]

CertificateFile="C:\Documents and Settings\markey-p\Application
Data\messageway\certs\cert\testcert.pem"
PrivateKeyFile="C:\Documents and Settings\markey-p\Application
Data\messageway\certs\private\testkey.pem"
PrivateKeyPassPhrase=software
CipherList=ALL:!LOW:!EXP:!ADH:!IDEA:@STRENGTH
RequireClientCert=True
;RequestClientCert=False
CertVerifyFile=C:\Documents and Settings\markey-p\Application
Data\messageway\certs\mwayas2.pem
```

mwsi.conf, Security Context Section, CTX2, Windows



```
[CTX2]

CertificateFile="/etc/messageway/certs/cert/testcert.pem"
PrivateKeyFile="/etc/messageway/certs/private/testkey.pem"
PrivateKeyPassPhrase=software
CipherList=ALL:!LOW:!EXP:!ADH:!IDEA:@STRENGTH
RequireClientCert=True
;RequestClientCert=False
CertVerifyFile=/etc/messageway/certs/mwayas2.pem
```

mwsi.conf, Security Context Section, CTX2, UNIX/Linux

Agents File

To enable public key client authentication, the MessageWay Service Interface (SI) uses the agents file to authenticate MessageWay servers that present themselves as clients to SI and to authenticate the users they represent.

Syntax for the Agents File

You must create the agents file in the location specified in the parameter, AgentFile, in the mwsi.conf file.

By default, a sample file called agents.sample is installed in the following locations, depending on the operating system:

Operating System	**Location of the Agents Sample File**
UNIX or Linux	/etc/messageway/certs/agents.sample
Windows	\Users*MessageWayUser*\AppData\Roaming\messageway\certs\agents.sample

The general rules for the agents file are as follows:

- Must list the AuthAgent value in the appropriate configuration file, such as mwas2.conf or mwsftpd.conf or mwftpd.conf if you are configuring anonymous user access
- Must list all groups and users allowed or denied connection for a given agent

The syntax rules for the agents file are as follows:

- Use Semi-colon (;) to comment a line
- Use separate lines for each AuthAgent and its users and groups list
    - AuthAgent must be first item on the line separated from list of users by at least one space or tab character
        - AuthAgent must match the common name (CN) used in the client certificate
        - Users and groups must be users or groups configured in MessageWay
    - Users and groups follow AuthAgent on the same line
        - Items in this list are separated by commas
        - Items may be in any order
        - Allowed or denied status of user overrides status of group
        - Allowed or denied status of group or user overrides asterisk (*)
        - Use an exclamation mark (!) to deny access to a user or group
        - Enclose group names in greater than (<) and less than (>) signs
        - Optionally use quotation marks (" ") around user names

The following table provides some examples for the user list:

User List Syntax	**Description**
!*user* - or - **!"***user***"**	Deny access to this user. This access overrides any access for a group to which the user belongs.
user - or - **"***user***"**	Allow access to this user. This access overrides any access for a group to which the user belongs.
!<*group***>**	Deny access to this group. Individual user access overrides group access.

User List Syntax	Description
<*group*>	Allow access to this group. Individual user access overrides group access.
*	Allow all users. Individual user or group access overrides this access.

How to Create an Agents File

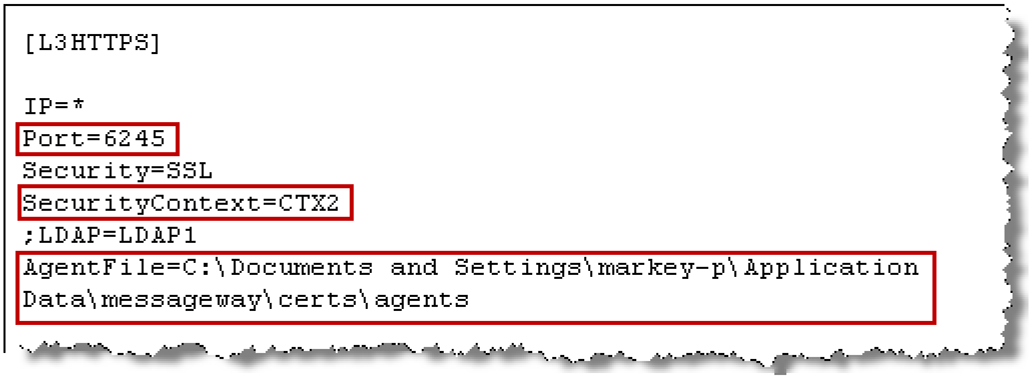
Other processes, such as the MessageWay SFTP Server, also use the agents file, so it may already exist. If it already exists, start with step 2.

The default location of the agents file is as follows:

Operating System	Location of the Agents Sample File
UNIX or Linux	/etc/messageway/certs/agents.sample
Windows	\Users\MessageWayUser\AppData\Roaming\messageway\certs\agents.sample

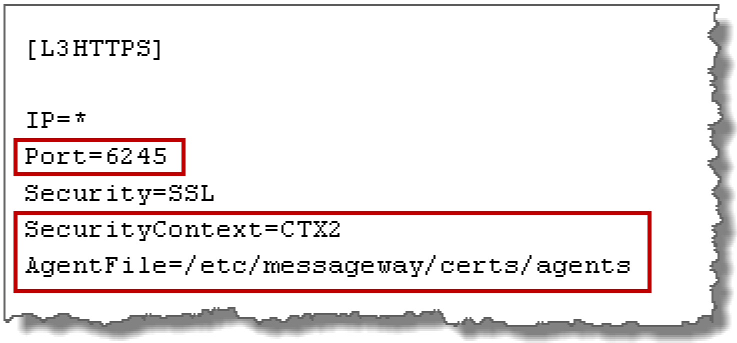
Otherwise, if it doesn't exist or you want to create a new one, start with step 1.

1 Using a text editor, create an empty file called **agents** (no extension) in the same location specified in the AgentFile parameter of the HTTP Listeners Configuration section in the MessageWay Service Interface configuration file, ***mwsi.conf*** (on page 145).



```
[L3HTTPS]

IP=*
Port=6245
Security=SSL
SecurityContext=CTX2
;LDAP=LDAP1
AgentFile=C:\Documents and Settings\markey-p\Application
Data\messageway\certs\agents
```

Service Interface Configuration File, Location of Agents file, Windows



```
[L3HTTPS]

IP=*
Port=6245
Security=SSL
SecurityContext=CTX2
AgentFile=/etc/messageway/certs/agents
```

Service Interface Configuration File, Location of Agents file, UNIX/Linux

2 On a new line in the agents file, type the following:

a) The case-sensitive name that matches the common name (CN) on the AS2 client certificate.

This name is also the AuthAgent value in the mwas2.conf file.

b) At least one space or tab character.

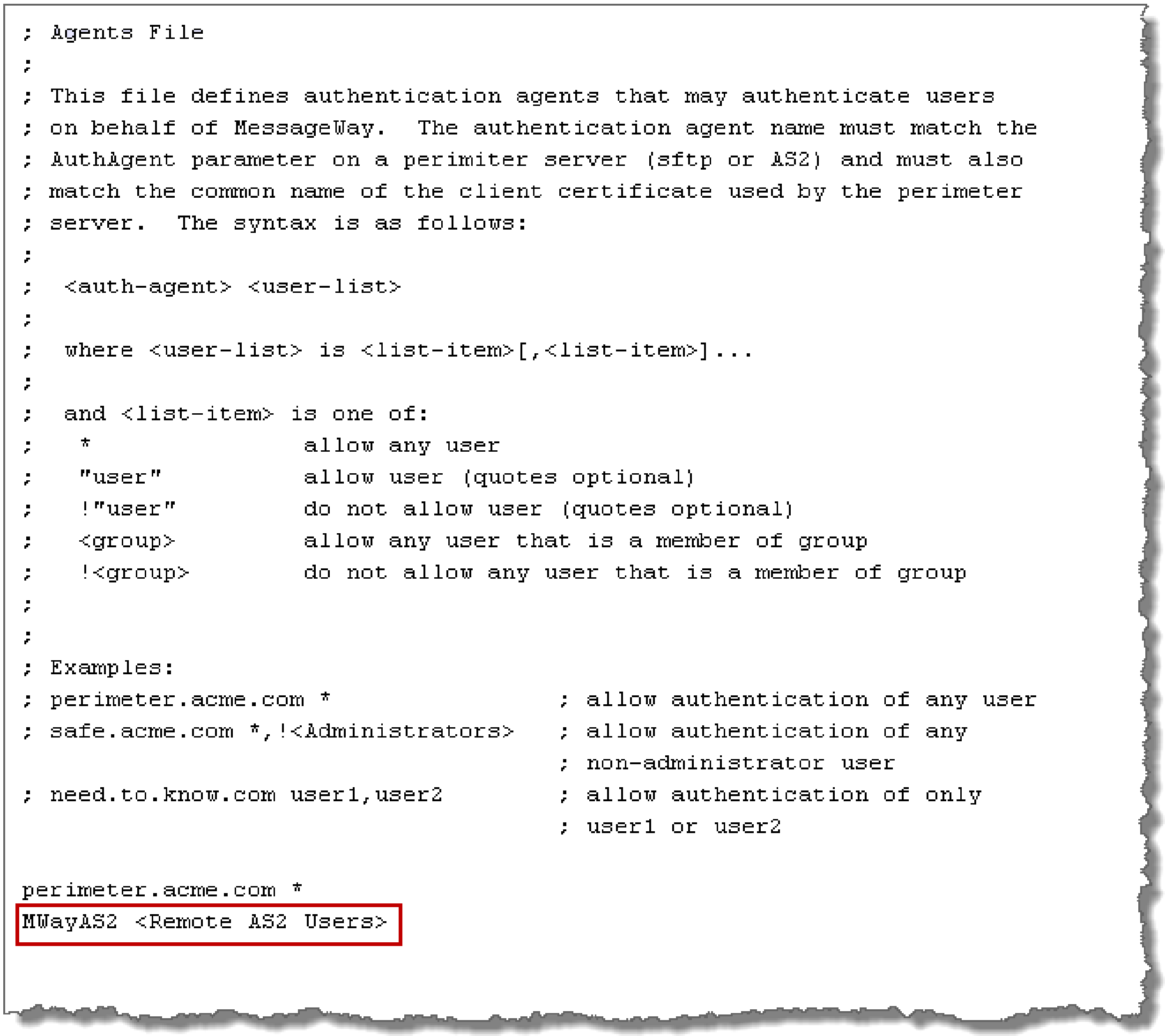
c) MessageWay groups and users that will be allowed to send messages to MessageWay, via the AS2 Interface, with names separated by commas.

The users are typically the *AS2-From* values on the incoming AS2 messages.

TIP: Since we have added our user, TradingPartner1, to the group, Remote AS2 Users, we will add the group name to the agents file so when we add other trading partners to the group, we won't have to change the agents file:

Following our example, type:

MWayAS2 <Remote AS2 Users>



```
; Agents File
;
; This file defines authentication agents that may authenticate users
; on behalf of MessageWay.  The authentication agent name must match the
; AuthAgent parameter on a perimiter server (sftp or AS2) and must also
; match the common name of the client certificate used by the perimeter
; server.  The syntax is as follows:
;
;  <auth-agent> <user-list>
;
;  where <user-list> is <list-item>[,<list-item>]...
;
;  and <list-item> is one of:
;   *               allow any user
;   "user"          allow user (quotes optional)
;   !"user"         do not allow user (quotes optional)
;   <group>         allow any user that is a member of group
;   !<group>        do not allow any user that is a member of group
;
;
; Examples:
; perimeter.acme.com *                ; allow authentication of any user
; safe.acme.com *,!<Administrators>   ; allow authentication of any
                                      ; non-administrator user
; need.to.know.com user1,user2        ; allow authentication of only
                                      ; user1 or user2

perimeter.acme.com *
MWayAS2 <Remote AS2 Users>
```

NOTE: There may be other lines for agents and users in the file. Any MessageWay servers, such as ***SFTP*** (on page 298), or interfaces that use public key authentication for input to MessageWay must be listed as an agent.

Configuring AS2 Trading Partners and MessageWay Locations

In order to add configurations to support AS2 message exchange, you need to do the following:

- Configure an AS2 trading partner as a remote user
- Create a default location for an AS2 trading partner
- Configure sites for inbound AS2 messages
- Configure the AS2 adapter
- Configure locations for outbound AS2 messages

Configuring an AS2 Trading Partner in MessageWay

The MessageWay user ID that represents the remote user must match data passed from the AS2 Inbound Servlet, as shown in the following table:

Source of User ID	**When**
AS2-From	▪ AS2 message is signed ▪ No form of authentication was performed, and the **AllowUnauthenticated** parameter in mwas2.conf is set to **yes**.
HTTP authenticated user	▪ AS2 message is not signed and HTTP authentication occurred. **IMPORTANT:** A user authenticated by HTTP might not be the same as the user specified in *AS2-From*. In this case, the HTTP authenticated user must be configured as a valid MessageWay user, and not the *AS2-From* value.

To access MessageWay, remote users must have the following configured in MessageWay:

- User ID and password for AS2 trading partner, with rights to upload messages. The password is not used for AS2, but is required to create a MessageWay user.
- Appropriate rights to access locations to which messages will be sent or uploaded. Each message is uploaded to the location defined by the *AS2-To* value.
- Default location required for remote users to log on to MessageWay

To configure remote AS2 users, we will take advantage of a user group, which allows us to configure the rights for the user at the group level, because users in a group inherit the rights of the group. Then, whenever we add AS2 users for other trading partners, we will add the users to the user group rather than set the rights individually for each user. For more information about creating users and user groups, refer to the topic, ***Configuring User Security*** (on page 375).

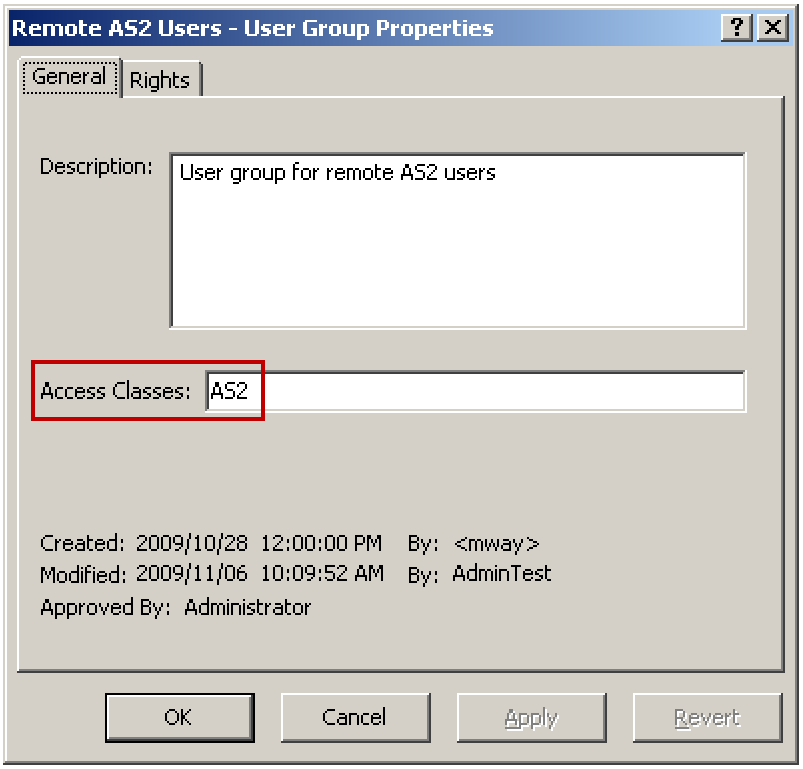
TIP: You could also use the predefined user group, Remote Users, but it has more rights in its default configuration than AS2 users need.

To configure a remote user for testing purposes, proceed as follows:

1 From MessageWay Explorer, ***create a user group*** (on page 378) called **Remote AS2 Users**.

a) On the **General** tab, type a description and the access class, **AS2**.

Remember that the access class AS2 is not strictly required, but it is required for our example, because we configured it in the ***Global section*** (on page 137) of the AS2 Interface configuration file, mwas2.conf.



Description: User group for remote AS2 users

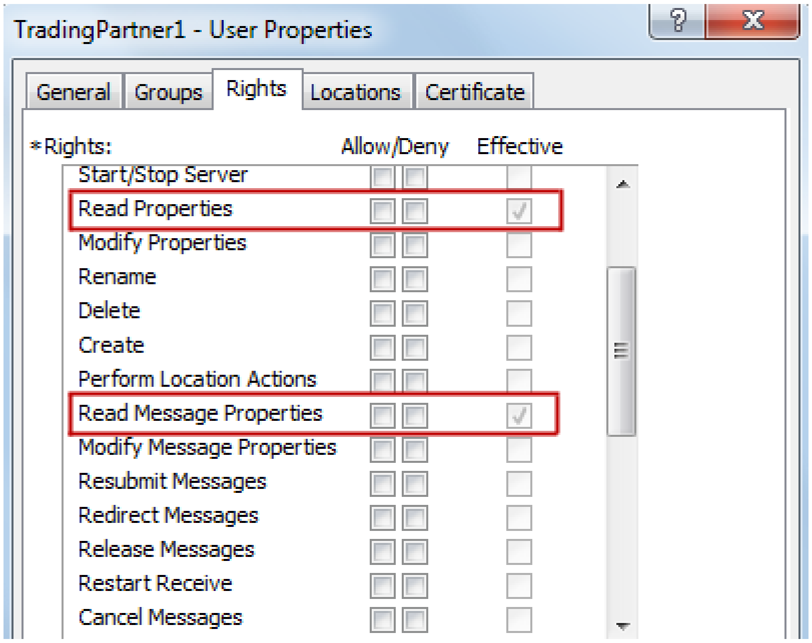
Access Classes: AS2

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/06 10:09:52 AM By: AdminTest
Approved By: Administrator

b) Click the **Rights** tab, and in the **Rights** box, check **Upload Messages**.

When you check the **Upload Messages** in the **Rights** box for the user group, the other related boxes are automatically checked.

The following boxes should be checked, at minimum.



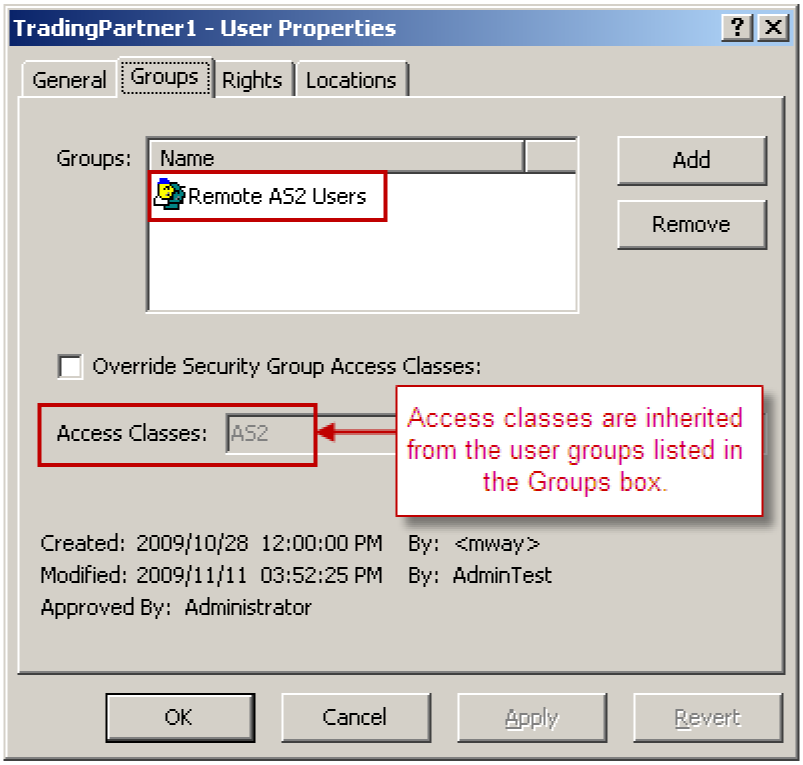
TradingPartner1 - User Properties

*Rights:	Allow/Deny		Effective
Start/Stop Server	□	□	□
Read Properties	□	□	☑
Modify Properties	□	□	□
Rename	□	□	□
Delete	□	□	□
Create	□	□	□
Perform Location Actions	□	□	□
Read Message Properties	□	□	☑
Modify Message Properties	□	□	□
Resubmit Messages	□	□	□
Redirect Messages	□	□	□
Release Messages	□	□	□
Restart Receive	□	□	□
Cancel Messages	□	□	□

2 ***Create a user*** (on page 381) with the following information:

- User ID of **TradingPartner1**
- Password of **password**
- Group of **Remote AS2 Users**

This is an efficient way to consistently set the rights for users who have common needs. The access class, AS2, is inherited from the user group and limits user access to the AS2 Interface.



TradingPartner1 - User Properties

Groups:

Name
Remote AS2 Users

□ Override Security Group Access Classes:

Access Classes: AS2

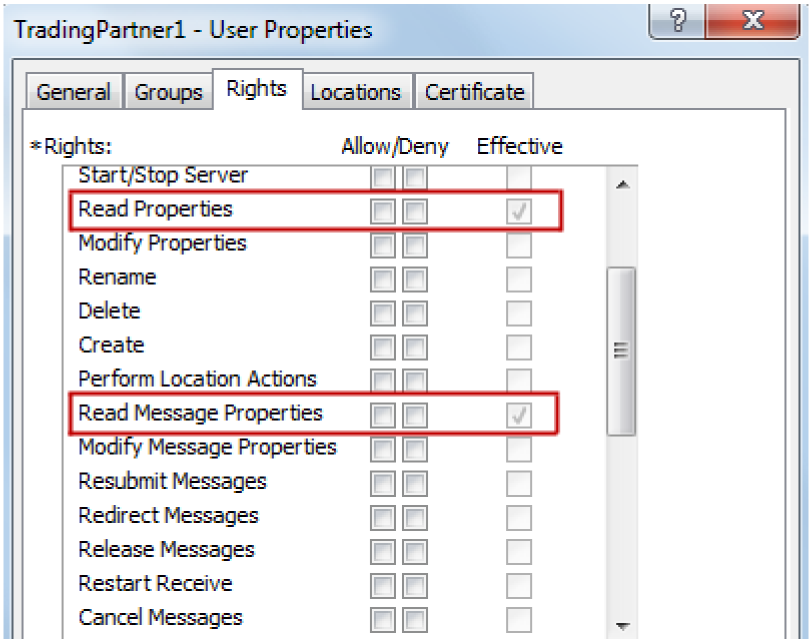
Access classes are inherited from the user groups listed in the Groups box.

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/11 03:52:25 PM By: AdminTest
Approved By: Administrator

3 Make sure that at least the user rights shown here are checked:

- Read Properties
- Read Message Properties
- Upload Messages (when you check this option, the other two are automatically checked)

The user's rights are the combined rights of all groups to which the user belongs. In this case, the user only belongs to the Remote AS2 Users group, whose rights appear in the Effective column on the **Rights** page of the User Properties window.



*Rights:	Allow/Deny		Effective
Start/Stop Server	□	□	□
Read Properties	□	□	☑
Modify Properties	□	□	□
Rename	□	□	□
Delete	□	□	□
Create	□	□	□
Perform Location Actions	□	□	□
Read Message Properties	□	□	☑
Modify Message Properties	□	□	□
Resubmit Messages	□	□	□
Redirect Messages	□	□	□
Release Messages	□	□	□
Restart Receive	□	□	□
Cancel Messages	□	□	□

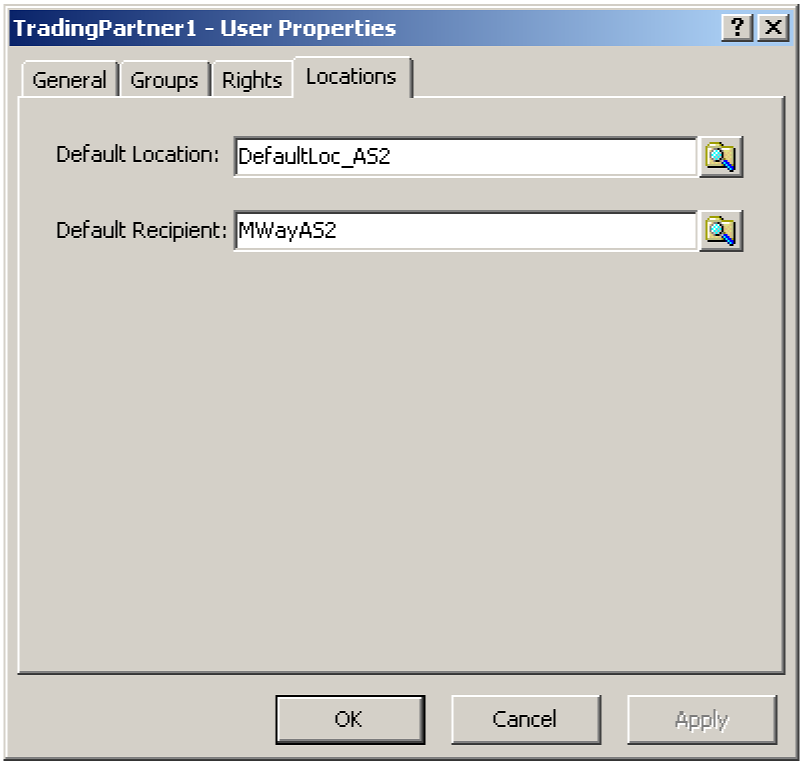
4 On the **Locations** tab, enter at least a default location, and optionally a default recipient.

- Enter a default location of **DefaultLoc_AS2**. You will create this location in the ***next task*** (on page 158).

  Each user accessing MessageWay through the Service Interface must be assigned a default location.

- For AS2, you can leave the Default Recipient value blank, because the destination location for an AS2 message always comes from the AS2-To value in the AS2 message.

  Optionally, enter a default recipient of **MWayAS2**. If a location is not provided in the inbound message, messages are uploaded to the Default Recipient, or the Default Location if the Default Recipient is blank. You will create this site in a ***separate task*** (on page 160).



Default Location: DefaultLoc_AS2

Default Recipient: MWayAS2

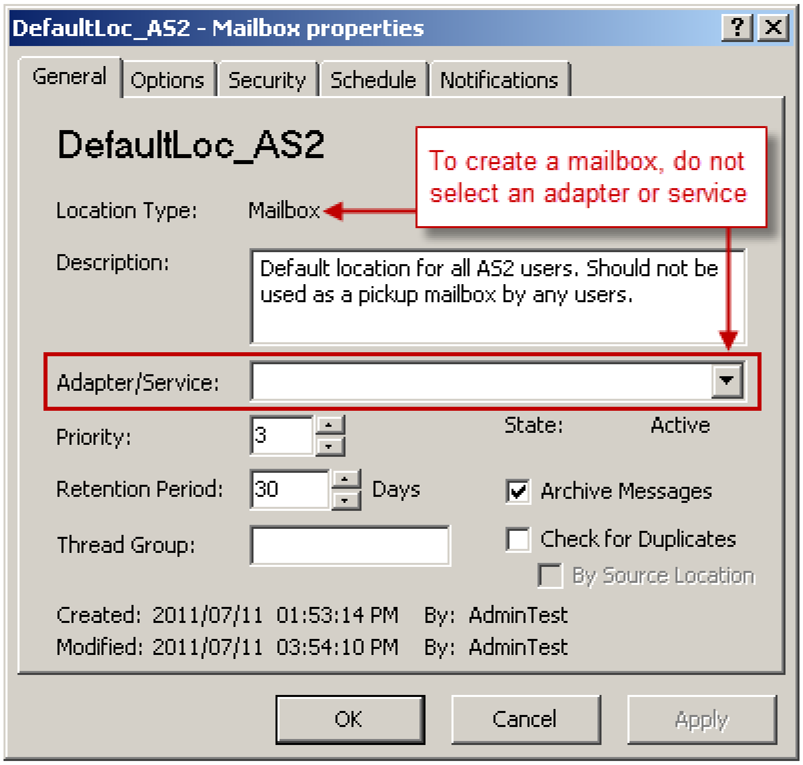
Creating a Default Location for an AS2 Trading Partner

You must assign a default location to each AS2 trading partner configured in MessageWay.

Default locations must be configured as pickup mailboxes.

1 Create a mailbox type location called DefaultLoc_AS2. Do not select an adapter or service. For more information about creating locations, refer to the topic, ***Configuring Locations*** (on page 453).

Notice on the **General** page of the Mailbox Properties window, when you do not select an adapter or service, after you save your changes, the location type is *Mailbox*. Notice also that there is no special adapter or service tab.



DefaultLoc_AS2 - Mailbox properties

DefaultLoc_AS2

Location Type: Mailbox

To create a mailbox, do not select an adapter or service

Description: Default location for all AS2 users. Should not be used as a pickup mailbox by any users.

Adapter/Service:

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

□ Check for Duplicates

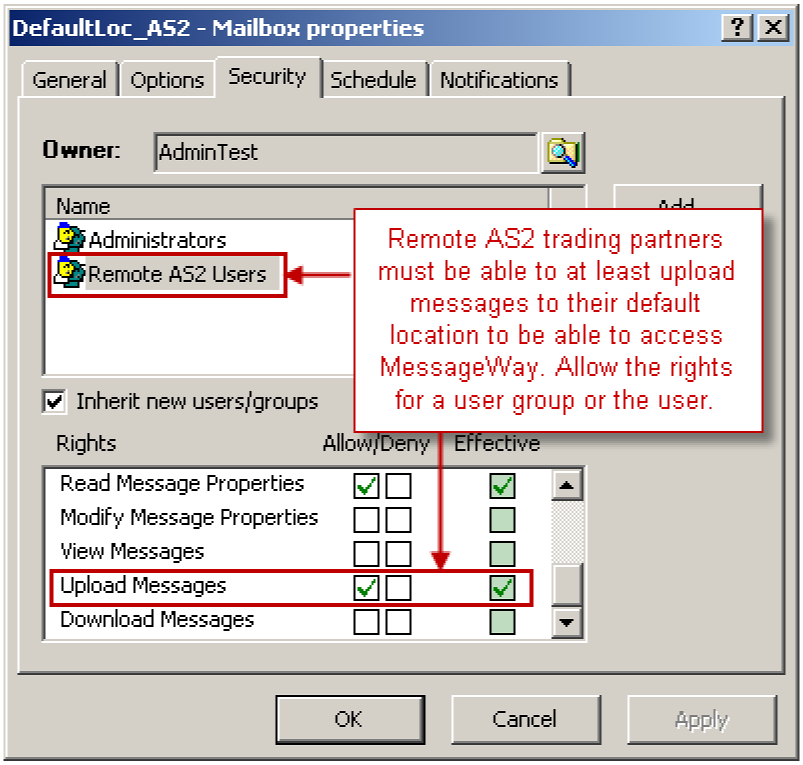
□ By Source Location

Created: 2011/07/11 01:53:14 PM By: AdminTest

Modified: 2011/07/11 03:54:10 PM By: AdminTest

2 On the **Security** page, click **Add**, select the Remote AS2 Users group, and click **Select**.

The Remote AS2 Users group appears on the list.



Owner: AdminTest

Name
Administrators
Remote AS2 Users

☑ Inherit new users/groups

Rights	Allow/Deny		Effective
Read Message Properties	☑	☐	☑
Modify Message Properties	☐	☐	☐
View Messages	☐	☐	☐
Upload Messages	☑	☐	☑
Download Messages	☐	☐	☐

Remote AS2 trading partners must be able to at least upload messages to their default location to be able to access MessageWay. Allow the rights for a user group or the user.

3 From the list, click **Remote AS2 Users**.

4 In the Rights box, check **Allow** for the Upload Messages right.

This also checks the dependent rights, Read Message Properties and Read Properties, which is for location properties.

5 Click **Apply** or **OK** to save your changes.

Configuring locations for Inbound AS2 Messages

To allow AS2 clients to send messages to MessageWay through the AS2 Interface, you create locations in MessageWay to receive the messages. They can be auto-delivery locations or pickup mailboxes.

When you create auto-delivery locations, they must be an output site associated with an adapter or a service location associated with a service. To create locations where the user will collect the messages, they must be pickup mailboxes.

Creating a Location to Receive AS2 Messages

We want to create a location that will receive the AS2 messages destined for the specified trading partner. We could create one of several types of locations:

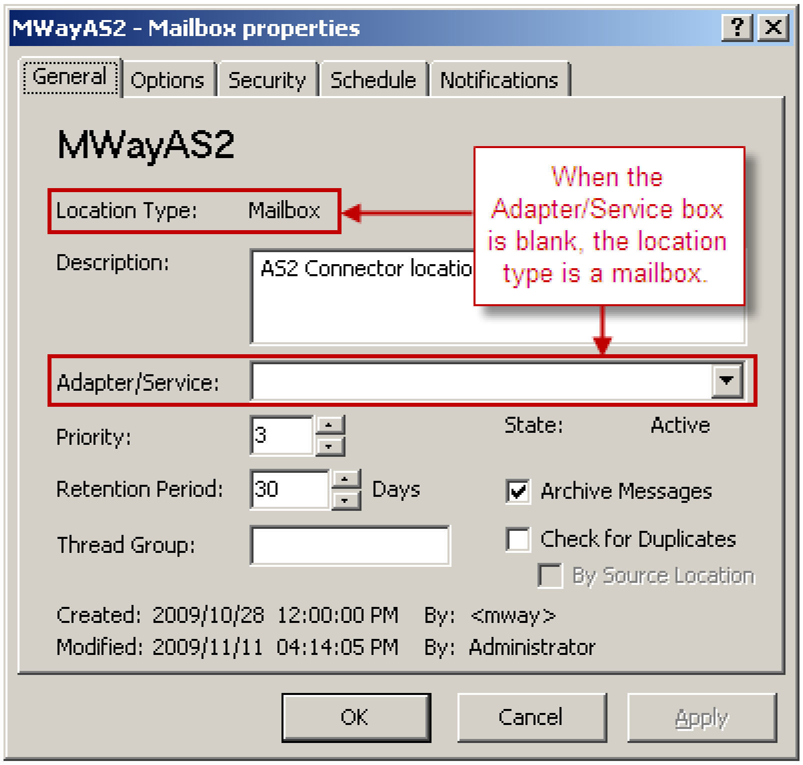
- Output site associated with an adapter, such as Disk Transfer or FTP, so MessageWay would automatically deliver the message to the trading partner
- Service location that would forward the message to a process, such as routing or the translator
- Mailbox, that would hold messages for the trading partner to collect

For this example, we will create a pickup mailbox.

To create a pickup mailbox to collect AS2 messages, proceed as follows:

1. Create a location with the following properties:
   - Location name of **MWayAS2**
   - **Adapter/Service** box should be blank
2. Click **OK** to save your changes.
3. Double-click **MWayAS2** to reopen the properties window.

   The **General** page of the **MWayAS2** mailbox should look similar to the following:



MWayAS2

Location Type: Mailbox

Description: AS2 Connector locatio

Adapter/Service:

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

☐ Check for Duplicates

☐ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 04:14:05 PM By: Administrator

When the Adapter/Service box is blank, the location type is a mailbox.

Assigning Rights for Locations

Your remote user must be able to access the necessary locations. To do so, you assign appropriate rights to the locations to which they need access, including:

- All destination locations (*AS2-To* value on the AS2 message)
- ***Default location assigned to this user*** (on page 152)

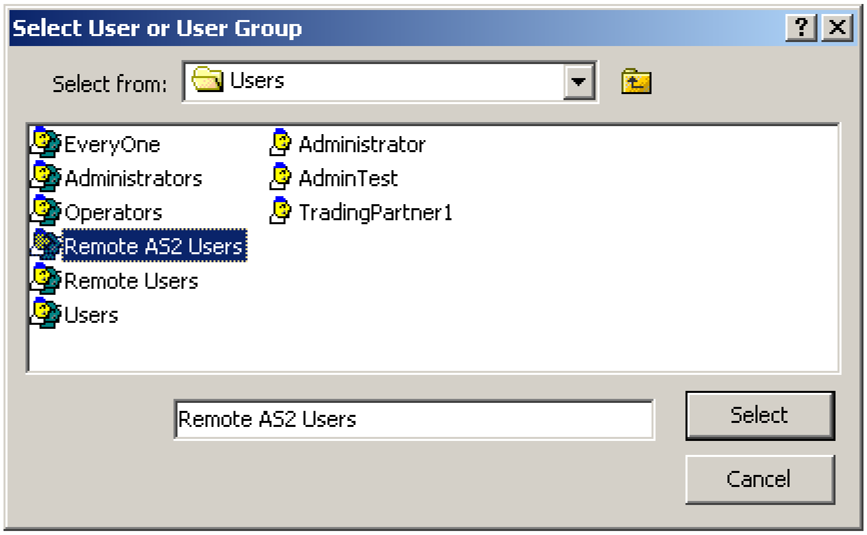
Access lists determine who can do what to locations. To create an access list, you add user groups or users to the **Names** box and specify the rights in the **Rights** box. You set these rights separately from the rights set for the user. When a user attempts to access a location, the rights of the location are compared with the rights of the user, and only those rights that match are allowed. The user must be a member of one of the listed groups or must be listed separately. For more information, refer to the topic ***Configuring User Security*** (on page 375).

For our example, add the Remote AS2 Users group to the **Security** page of the destination location, MWayAS2, and set the same rights for the mailbox as those we set for the Remote AS2 Users user group. Proceed as follows:

1. For the MWayAS2 mailbox, from the **Security** tab, click **Add**.

   The **Select User or User Group** dialog box appears with a list of all users and groups you have configured.

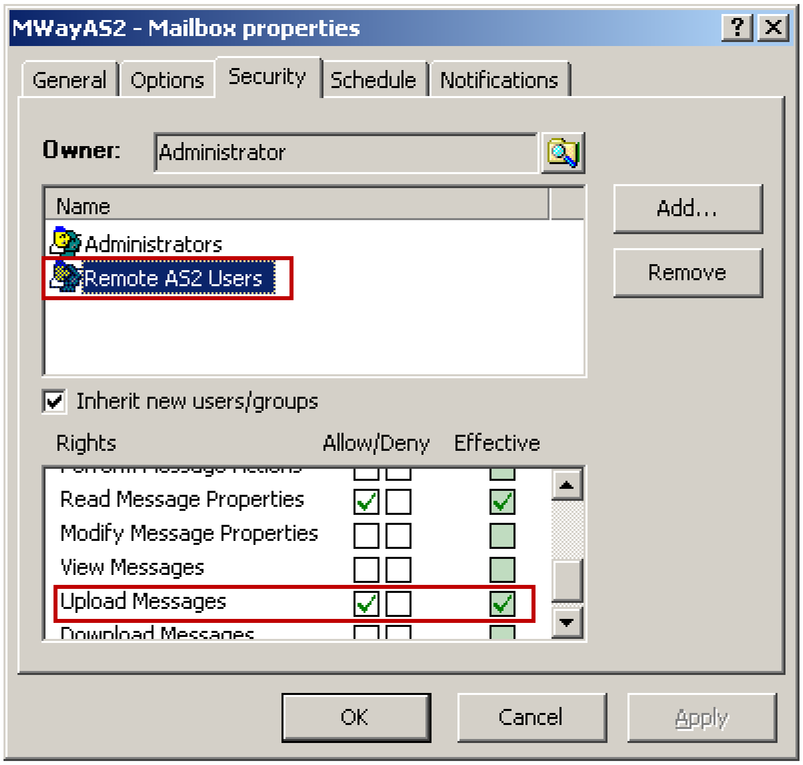
2. Select the group, **Remote AS2 Users**, and click **Select**.



3. On the **Security** tab, in the **Name** box, select **Remote AS2 Users**.
4. In the **Rights** box, check **Upload Messages**.

   Other dependent boxes will also appear checked.

NOTE: We had to check **Allow** for the Upload Messages right, because the Remote AS2 Users group was added to this specific location rather than being inherited from its folder. That is, the Remote AS2 Users group is not listed on the **Security** tab of the Folder Properties window for the **Locations** folder, so its rights could not be inherited. Had Remote AS2 Users group been inherited from the **Locations** folder, this mailbox would have inherited the rights set at the folder level. Since they weren't inherited, we had to specifically set the rights for the user group for this location.



Owner: Administrator

Name
Administrators
Remote AS2 Users

☑ Inherit new users/groups

Rights	Allow/Deny		Effective
Read Message Properties	☑	□	☑
Modify Message Properties	□	□	□
View Messages	□	□	□
Upload Messages	☑	□	☑
Download Messages	□	□	□

Since the rights for our user will match the rights for the location, the user will be able to send messages to this location.

IMPORTANT: For users to be able to access messages in locations other than their default location, they must have access rights to those other locations.

Configuring the AS2 Adapter

To allow MessageWay to send messages to an AS2 server through the AS2 Interface, you must configure the properties of the AS2 adapter.

1 From the MessageWay Manager, in the left pane of MessageWay Explorer, click **Adapters/Services**.

2 In the right pane, double click **MWAS2**.

The Adapter Properties window appears.

3 Type or select the information as follows:

Servlet URL	This required field identifies the location of the outbound servlet. The values are case-sensitive. Type the Web address of the AS2 outbound servlet. For example, if the servlet is on the same system as the AS2 adapter, you might type, http://localhost:8080/mwas2/out. If the servlet is on a different machine than the AS2 adapter, you might type, http://192.168.0.4:8080/mwas2/out.

Request Timeout

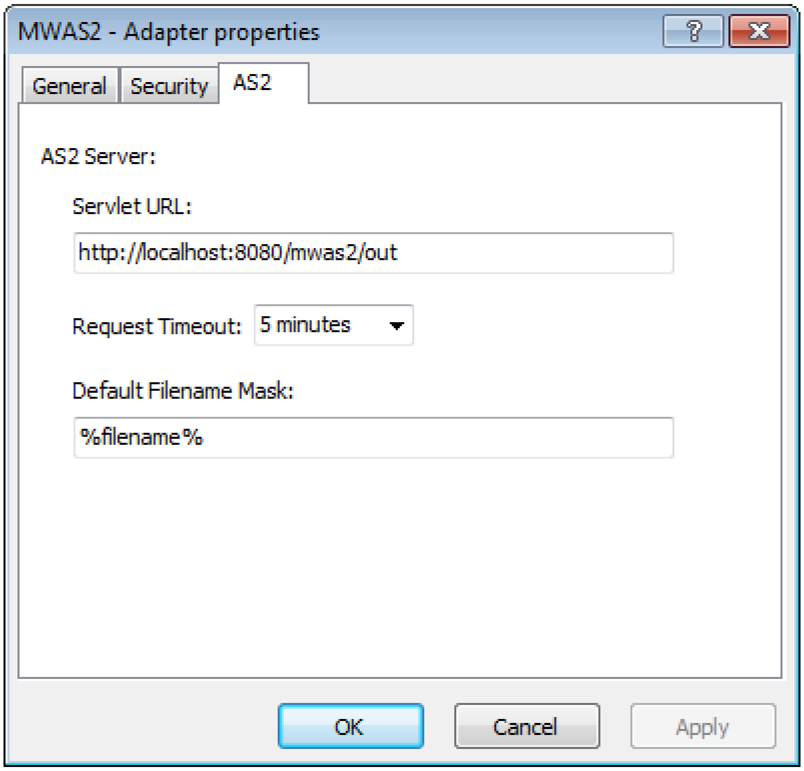
Select or type the amount of time in seconds, minutes or hours to allow the AS2 outbound processing cycle to complete. This is a default value for AS2 sites, which users can override by selecting a Request Timeout value for a site.

Default FilenameMask

This is a template to create a file name for the output file. For new installations, the default mask is **%filebase%[%msgid%].%fileext%**. This mask generates unique names using the MessageWay message ID, which is enclosed in square brackets, [ ]. This avoids sending files that might be rejected because the file name already exists at the remote location. To change this default mask, use any combination of constants and MessageWay tokens. You may override this default for a specific location. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name.

4 Click **Apply** or **OK** to save your changes.

Here is an example of the configurations on an **AS2** page for a connection to an AS2 outbound servlet that is on the same Windows system as the AS2 adapter:



MWAS2 - Adapter properties

AS2 Server:

Servlet URL: http://localhost:8080/mwas2/out

Request Timeout: 5 minutes

Default Filename Mask: %filename%

NOTE: The MessageWay AS2 server and the AS2 adapter require a license from Progress. For more information, contact MessageWay Technical Support.

Configuring Locations for Outbound AS2 Messages

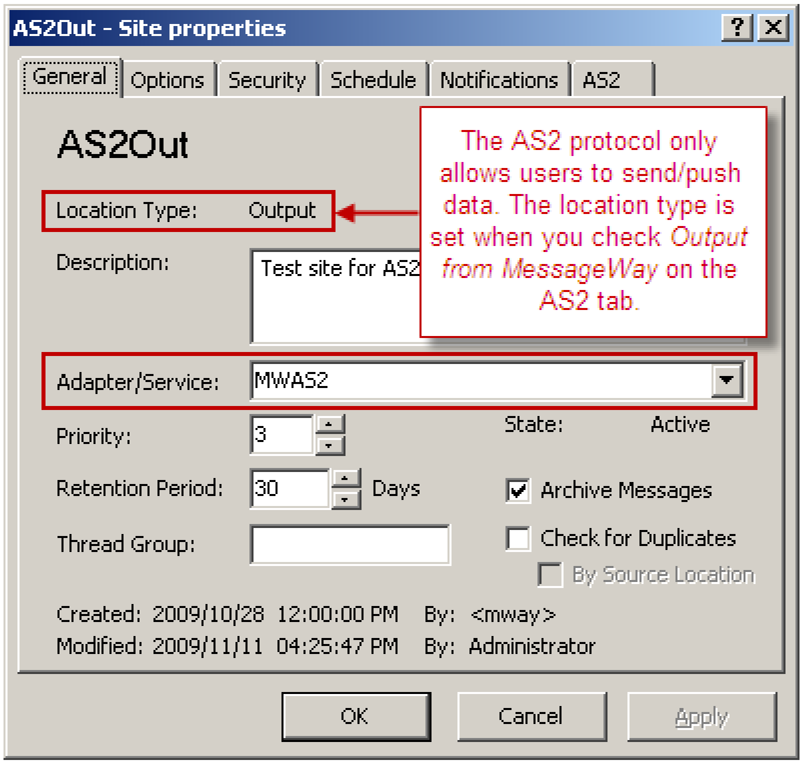
To allow MessageWay to send messages to an AS2 server through the AS2 Interface, you create an AS2 site in MessageWay.

To create an output site to send AS2 messages to your trading partner, proceed as follows:

1 Create a location with the following properties:

- Site name of **AS2Out**
- Adapter/Service should be **MWAS2**

The **General** page of the **MWAS2** site should look similar to the following:



AS2Out - Site properties

AS2Out

Location Type: Output

Description: Test site for AS2

Adapter/Service: MWAS2

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

□ Check for Duplicates

□ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 04:25:47 PM By: Administrator

The AS2 protocol only allows users to send/push data. The location type is set when you check *Output from MessageWay* on the AS2 tab.

2 On the AS2 tab, configure the following:

Output from MessageWay	Check this box.
Remote URL	This address is required to connect to the remote AS2 server where MessageWay will send messages to an AS2 trading partner. Type the remote URL. The default port for AS2 servers is 8080.
To	Type the name for the recipient, upon which both parties agree, such as a DUNS number or company name. This value will appear as the AS2-To address on the AS2 message.

From MessageWay Sender
Do not select this unless you want MessageWay to specify the sender of the message.

From
This field identifies the sender. Select this radio button, and type a value that identifies the sender to the remote AS2 server. This value will be the AS2-From address on the AS2 message.

For messages that will be signed, this value must uniquely match part of the sender's private key subject within the Java keystore (.jks). A private key subject includes the common name (CN), organizational unit (OU), organization (O), location (L), state (ST), and country (C), for example:

CN=MWayAS2, OU=AS2 Testing, O=Progress, L=Livonia, ST=MI, C=US

Filename
You may specify tokens to create a file name. Use any combination of constants and MessageWay tokens. This value overrides the one for the AS2 Adapter, mwas2, visible on the AS2 page of the AS2 Adapter Properties window. For new installations, the default mask is **%filebase%<[msgid]>.%fileext%**. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name, for example, **MW%msgid%.txt**.

Request Timeout
Select the amount of time in seconds or minutes to allow the AS2 outbound processing cycle to complete. Initially, this default value comes from the value defined on the AS2 adapter, which users can override here.

Compress Data
Check this box to compress the data.

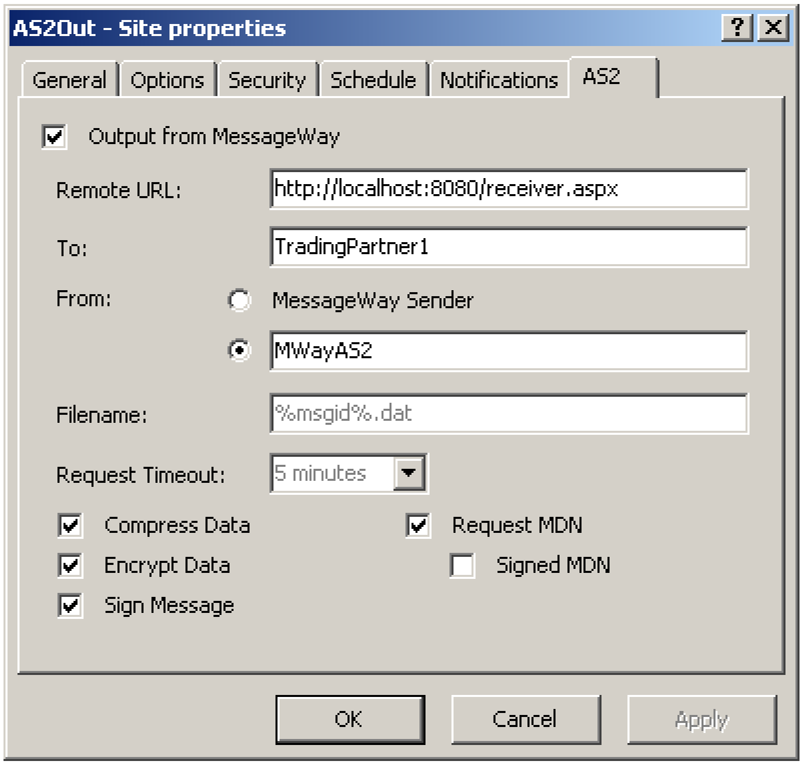
Encrypt Data
Check this box to encrypt the data.

Sign Message
Check this box to sign the message.

Request MDN
Check this box to request a return synchronous MDN.

Sign MDN
Do not check this box, unless you want your partner to sign the returned MDN.

The **AS2** page of the **AS2Out** site should look similar to the following:



AS2Out - Site properties

☑ Output from MessageWay

Remote URL: http://localhost:8080/receiver.aspx

To: TradingPartner1

From: ○ MessageWay Sender

● MWayAS2

Filename: %msgid%.dat

Request Timeout: 5 minutes

☑ Compress Data

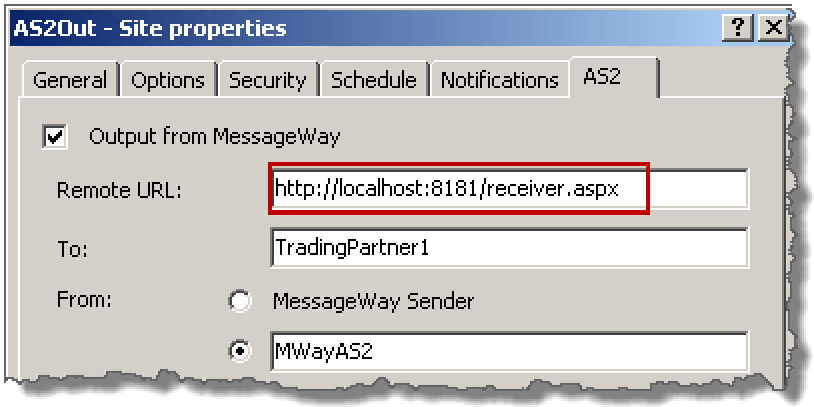
☑ Encrypt Data

☑ Sign Message

☑ Request MDN

☐ Signed MDN

NOTE: The default port for AS2 servers is 8080. If the AS2 server identified in Remote URL is on the same machine as the MessageWay AS2 Interface, which also functions as an AS2 server, they cannot both use the same port. In this case, we change the port in the remote URL to 8181. The remote, i.e. not MessageWay, ***AS2 server must be listening on this port*** (on page 172). In this case, the configuration would look as follows:



AS2Out - Site properties

☑ Output from MessageWay

Remote URL: http://localhost:8181/receiver.aspx

To: TradingPartner1

From: ○ MessageWay Sender

● MWayAS2

3 Click **Apply** or **OK** to save your changes.

Testing the AS2 Interface

To test the AS2 Interface, we must have another AS2 process with which we can exchange messages. In our example, we will use ***AS2 Connector*** (***http://www.freeas2.com/***), which allows us to test with one trading partner without a license. This application runs on Windows. If you have your own process, you can use that and adjust the instructions.

Make sure you have configured the entities described in the topic, ***Basic Configuration Tasks (AS2 Interface)*** (on page 119).

If you have not already done so, start the following:

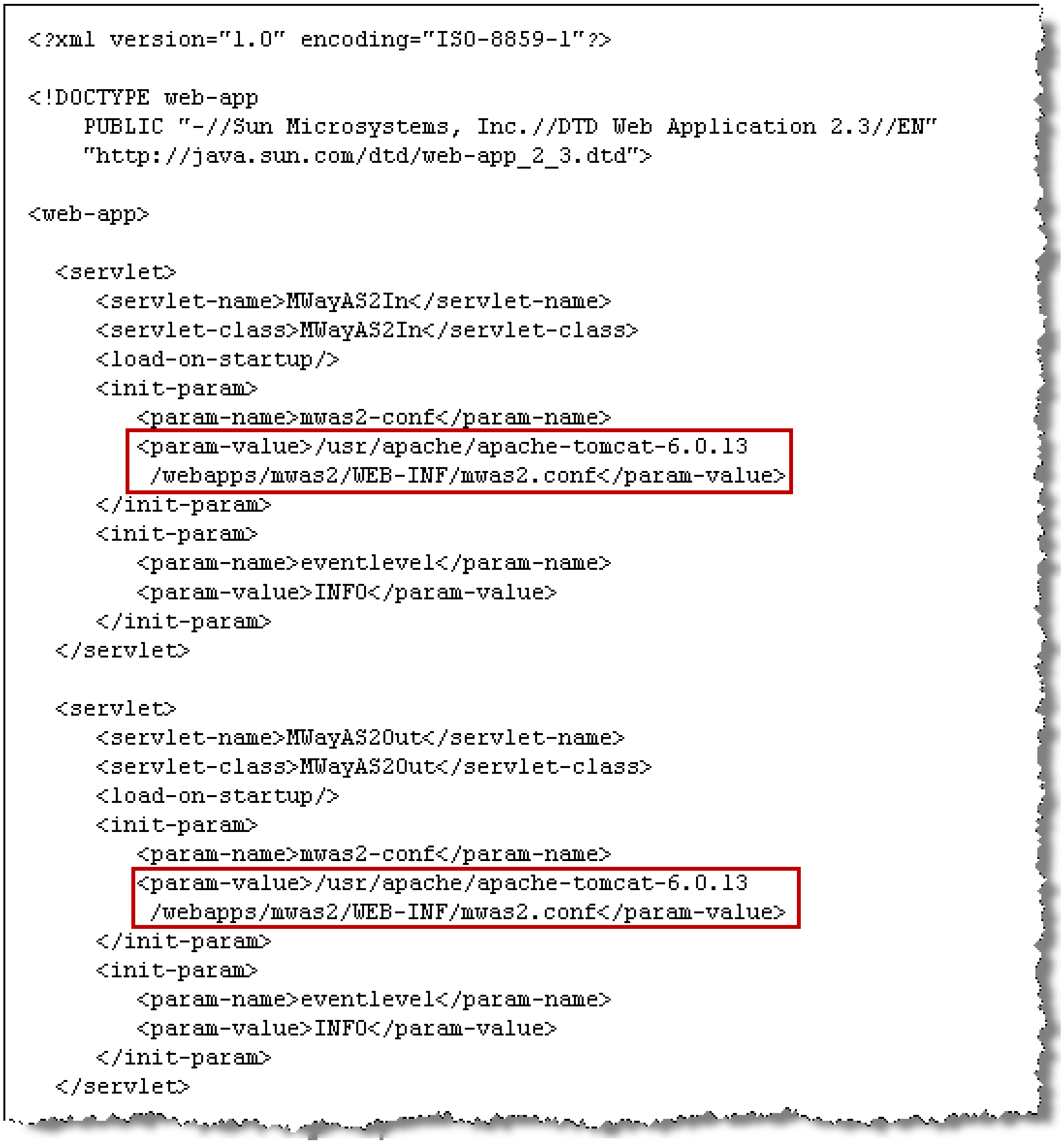
- MessageWay Server (starts the Messaging Server, the Service Interface and the User Server)
- MessageWay Manager
- Web container, such as Apache Tomcat, which should also start the MessageWay AS2 Interface
- AS2 connector for your trading partner, such as AS2 Connector
- AS2 Adapter

To Start the AS2 Interface on UNIX or Linux

Before you start the AS2 servlets, you must configure the file that identifies the location of the servlet configuration file. Then you start the Web container, Apache Tomcat, which starts the AS2 servlets.

IMPORTANT: These instructions allow you to start the servlets. To complete the configurations, refer to the topic, "Configuring the AS2 Interface" within the *MessageWay User's Guide and Reference* or in the Manager online help.

1 Edit the file, web.xml, within the /webapps/mwas2/WEB-INF directory, to specify the current location of the servlet configuration file for both the inbound and outbound parameters, and save your changes. Typically, you would only replace the values **{Tomcat root}** with your install location, but be sure to check the entire path.



```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE web-app
    PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
    "http://java.sun.com/dtd/web-app_2_3.dtd">

<web-app>

  <servlet>
     <servlet-name>MWayAS2In</servlet-name>
     <servlet-class>MWayAS2In</servlet-class>
     <load-on-startup/>
     <init-param>
        <param-name>mwas2-conf</param-name>
        <param-value>/usr/apache/apache-tomcat-6.0.13
         /webapps/mwas2/WEB-INF/mwas2.conf</param-value>
     </init-param>
     <init-param>
        <param-name>eventlevel</param-name>
        <param-value>INFO</param-value>
     </init-param>
  </servlet>

  <servlet>
     <servlet-name>MWayAS2Out</servlet-name>
     <servlet-class>MWayAS2Out</servlet-class>
     <load-on-startup/>
     <init-param>
        <param-name>mwas2-conf</param-name>
        <param-value>/usr/apache/apache-tomcat-6.0.13
         /webapps/mwas2/WEB-INF/mwas2.conf</param-value>
     </init-param>
     <init-param>
        <param-name>eventlevel</param-name>
        <param-value>INFO</param-value>
     </init-param>
  </servlet>
```

2 To start the Apache Tomcat Web container, which in turn starts the servlets, from the /bin directory of Apache Tomcat, type:

./startup.sh.

3 Test to make sure the servlets are running and you can access them:

a) To test access to the inbound servlet, from your Web browser, type:

http://localhost:8080/mwas2/in

b) To test access to the outbound servlet, from your Web browser, type:
http://localhost:8080/mwas2/out

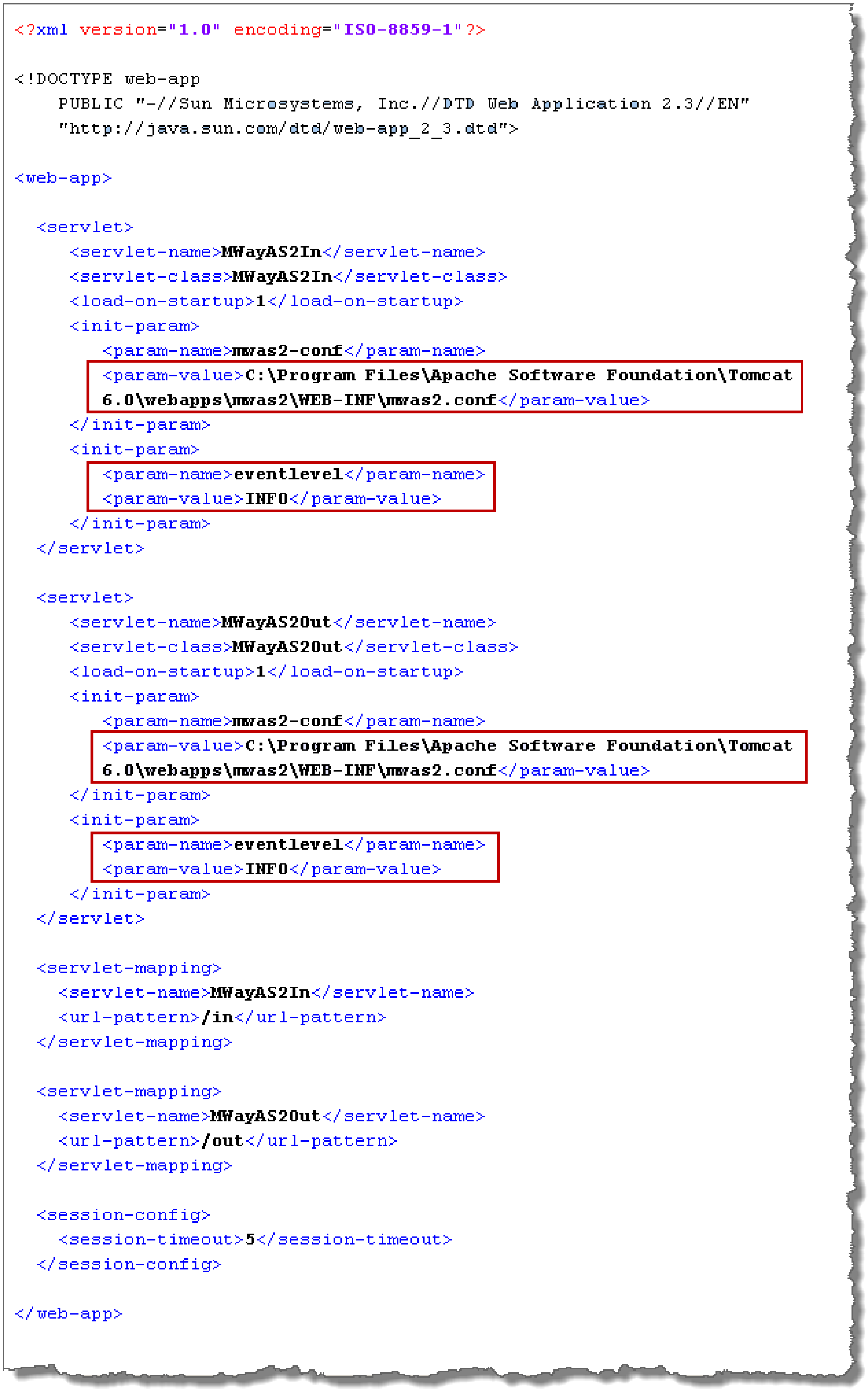
NOTE: If you do not receive messages, "You have reached the MessageWay AS2 ... Interface", test to see if you can access the Web container. Type, **http://localhost:8080**. If the Web browser is on a different machine, replace **localhost** with the IP Address of the machine hosting the servlets.

To Start the AS2 Interface on Windows

Before you start the AS2 servlets, you must configure the file that identifies the location of the servlet configuration file. Then you start the Web container, Apache Tomcat, which starts the AS2 servlets.

IMPORTANT: These instructions allow you to start the servlets. To complete the configurations, refer to the topic, "Configuring the AS2 Interface" within the *MessageWay User's Guide and Reference* or in the Manager online help.

1 In the file, web.xml, within the \webapps\mwas2\WEB-INF directory, specify the current location of the servlet configuration file for both the inbound and outbound parameters, and save your changes.



```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE web-app
    PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
    "http://java.sun.com/dtd/web-app_2_3.dtd">

<web-app>

  <servlet>
     <servlet-name>MWayAS2In</servlet-name>
     <servlet-class>MWayAS2In</servlet-class>
     <load-on-startup>1</load-on-startup>
     <init-param>
        <param-name>mwas2-conf</param-name>
        <param-value>C:\Program Files\Apache Software Foundation\Tomcat
        6.0\webapps\mwas2\WEB-INF\mwas2.conf</param-value>
     </init-param>
     <init-param>
        <param-name>eventlevel</param-name>
        <param-value>INFO</param-value>
     </init-param>
  </servlet>

  <servlet>
     <servlet-name>MWayAS2Out</servlet-name>
     <servlet-class>MWayAS2Out</servlet-class>
     <load-on-startup>1</load-on-startup>
     <init-param>
        <param-name>mwas2-conf</param-name>
        <param-value>C:\Program Files\Apache Software Foundation\Tomcat
        6.0\webapps\mwas2\WEB-INF\mwas2.conf</param-value>
     </init-param>
     <init-param>
        <param-name>eventlevel</param-name>
        <param-value>INFO</param-value>
     </init-param>
  </servlet>

  <servlet-mapping>
    <servlet-name>MWayAS2In</servlet-name>
    <url-pattern>/in</url-pattern>
  </servlet-mapping>

  <servlet-mapping>
    <servlet-name>MWayAS2Out</servlet-name>
    <url-pattern>/out</url-pattern>
  </servlet-mapping>

  <session-config>
    <session-timeout>5</session-timeout>
  </session-config>

</web-app>
```

2 Start the Apache Tomcat Web container, which also starts the servlets. The task varies depending on how you installed the software:

- From the Microsoft Management Console (MMC) Services window, start it as a Windows service.

  - or -

- Right-click the icon in the system tray, and click **Start service**.

3 Test to make sure the servlets are running and you can access them:

a) To test access to the inbound servlet, from your Web browser, type:

http://localhost:8080/mwas2/in

b) To test access to the outbound servlet, from your Web browser, type:

http://localhost:8080/mwas2/out

NOTE: If you do not receive messages, "You have reached the MessageWay AS2 ... Interface", test to see if you can access the Web container. Type, **http://localhost:8080**. If the Web browser is on a different machine, replace **localhost** with the IP Address of the machine hosting the servlets.

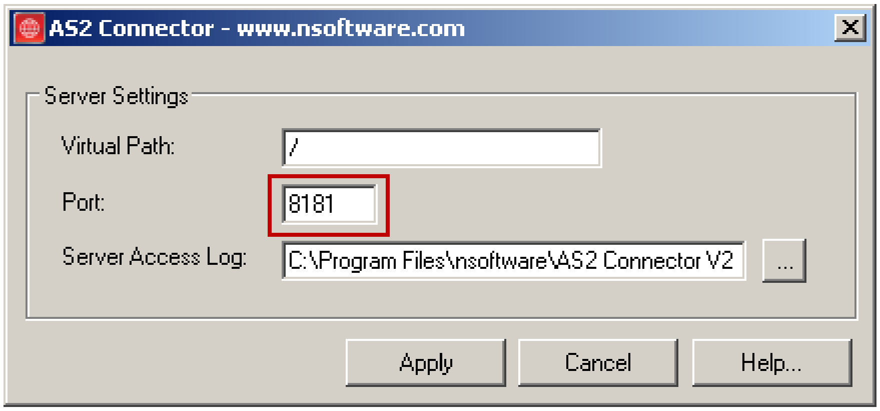
To Configure Trading Partners in the AS2 Connector

If you do not have an existing trading partner with whom to test or another AS2 testing environment, you can create your own trading partner with ***AS2 Connector*** (***http://www.freeas2.com/***).

1 Before you start the connector, you may want to change the port, which by default is 8080, the same port you are using for mwas2 running under Tomcat. You must do this if you are running these two applications on the same system.

a) For the AS2 Connector in this example, right click the icon in the system tray/notification area, and click **Server Options**.

b) In Port, type **8181** and click **Apply**.



AS2 Connector - www.nsoftware.com

Server Settings

Virtual Path: /

Port: 8181

Server Access Log: C:\Program Files\nsoftware\AS2 Connector V2

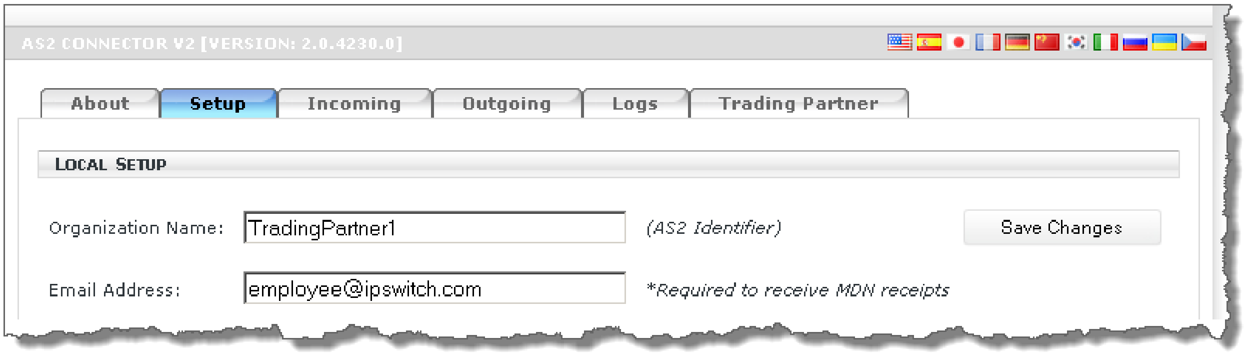
2 Start the AS2 connector.

The Administration Console Web application appears in your browser.

3 On the **Setup** tab, enter the following information:

- Local Setup
  - Organization Name: **TradingPartner1**

- Email Address: valid e-mail address, *my.email@myco.com*



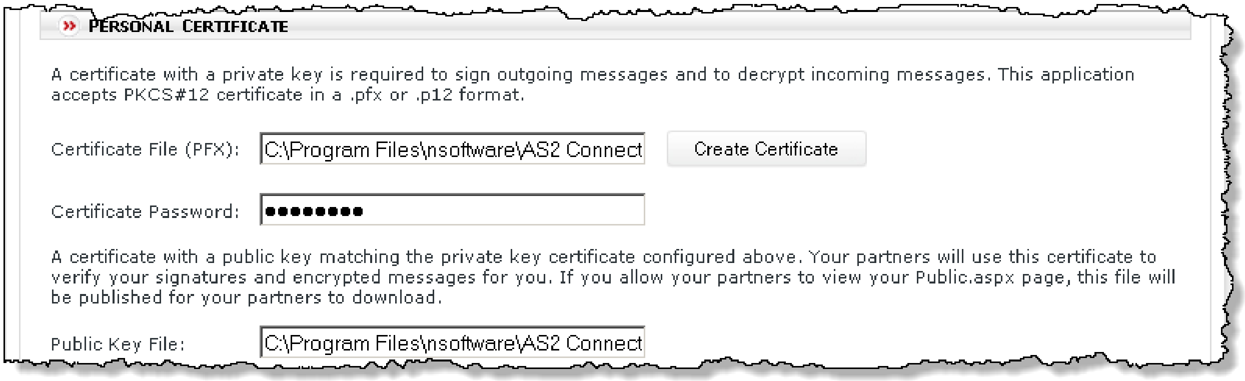
LOCAL SETUP

Organization Name: TradingPartner1 *(AS2 Identifier)*

Email Address: employee@ipswitch.com **Required to receive MDN receipts*

- Personal Certificate (Provide location and password used when we created the self-signed certificate, refer to the topic, ***To Create Certificate Files for TradingPartner1*** (on page 131))
  - Certificate File:

    *C:\Program Files\nsoftware\AS2 Connector V2\as2data\***TradingPartner1.pfx**
  - Certificate Password: **password**



» PERSONAL CERTIFICATE

A certificate with a private key is required to sign outgoing messages and to decrypt incoming messages. This application accepts PKCS#12 certificate in a .pfx or .p12 format.

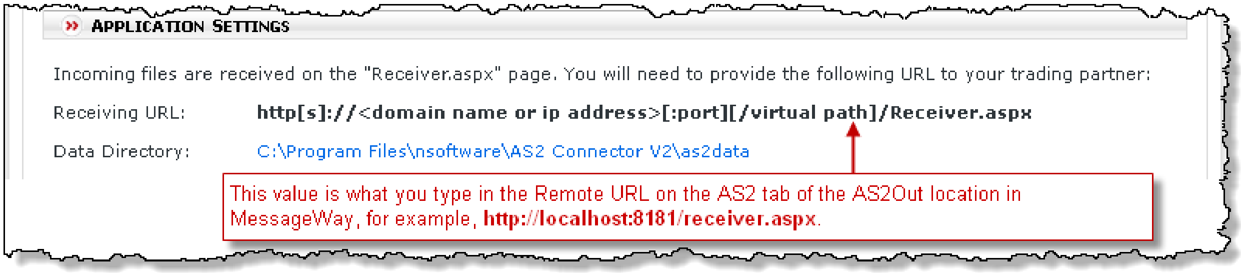
Certificate File (PFX): C:\Program Files\nsoftware\AS2 Connect

Certificate Password: ●●●●●●●●●

A certificate with a public key matching the private key certificate configured above. Your partners will use this certificate to verify your signatures and encrypted messages for you. If you allow your partners to view your Public.aspx page, this file will be published for your partners to download.

Public Key File: C:\Program Files\nsoftware\AS2 Connect

- Application Settings (information only) - this value is what is used to tell the MessageWay outbound AS2 site where to send messages.



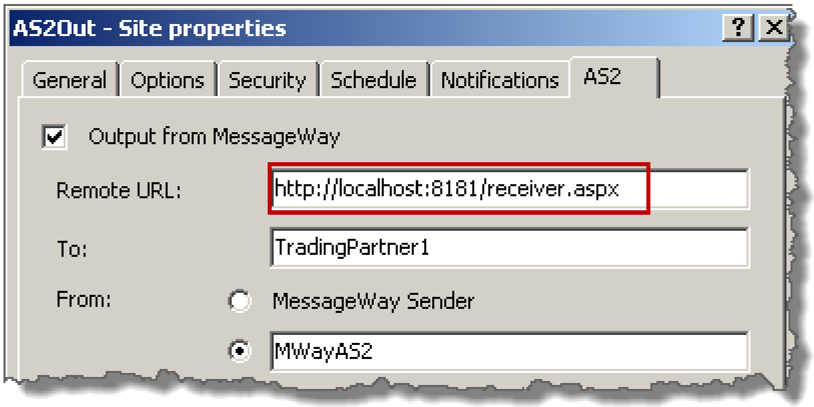
» APPLICATION SETTINGS

Incoming files are received on the "Receiver.aspx" page. You will need to provide the following URL to your trading partner:

Receiving URL: **http[s]://<domain name or ip address>[:port][/virtual path]/Receiver.aspx**

Data Directory: C:\Program Files\nsoftware\AS2 Connector V2\as2data

This value is what you type in the Remote URL on the AS2 tab of the AS2Out location in MessageWay, for example, **http://localhost:8181/receiver.aspx**.



☑ Output from MessageWay

Remote URL: http://localhost:8181/receiver.aspx

To: TradingPartner1

From: ○ MessageWay Sender

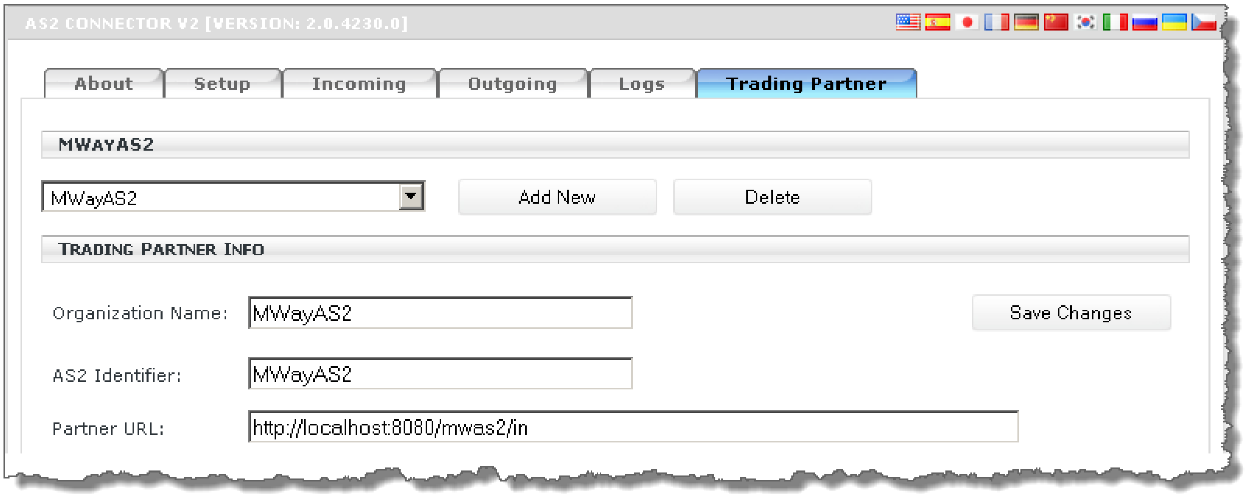
● MWayAS2

4 On the **Setup** tab, click **Save Changes**.

5 On the **Trading Partner** tab, click **Delete** to delete the default trading partner, and then click **Add New** to add your own trading partner, since you can only have one defined at a time.

6 On the **Trading Partner** tab, enter the following information:

- Trading Partner Info
  - Organization Name: **MWayAS2** (AS2-To)
  - Partner URL: **http://localhost:8080/mwas2/in**
  - Automate Send: make sure this is unchecked



MWAYAS2

MWayAS2 ▾ | Add New | Delete

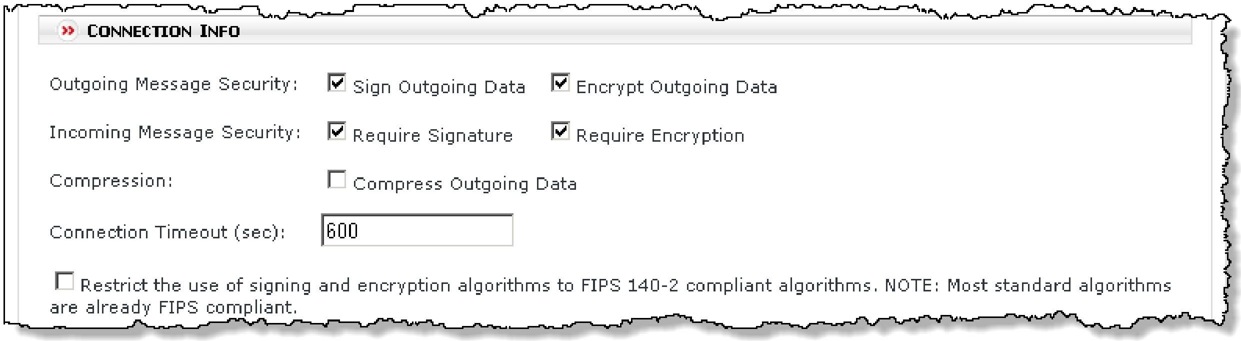
TRADING PARTNER INFO

Organization Name: MWayAS2

AS2 Identifier: MWayAS2

Partner URL: http://localhost:8080/mwas2/in

- Connection Info: select the following parameters for your test.



CONNECTION INFO

Outgoing Message Security: ☑ Sign Outgoing Data ☑ Encrypt Outgoing Data

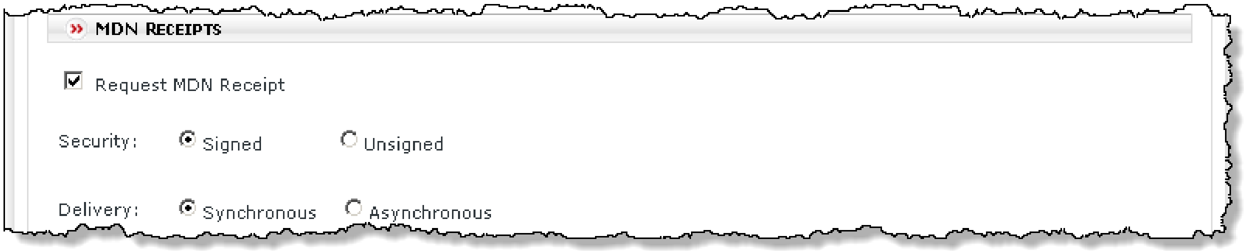
Incoming Message Security: ☑ Require Signature ☑ Require Encryption

Compression: □ Compress Outgoing Data

Connection Timeout (sec): 600

□ Restrict the use of signing and encryption algorithms to FIPS 140-2 compliant algorithms. NOTE: Most standard algorithms are already FIPS compliant.

- MDN Receipts: select the following parameters for your test.



MDN RECEIPTS

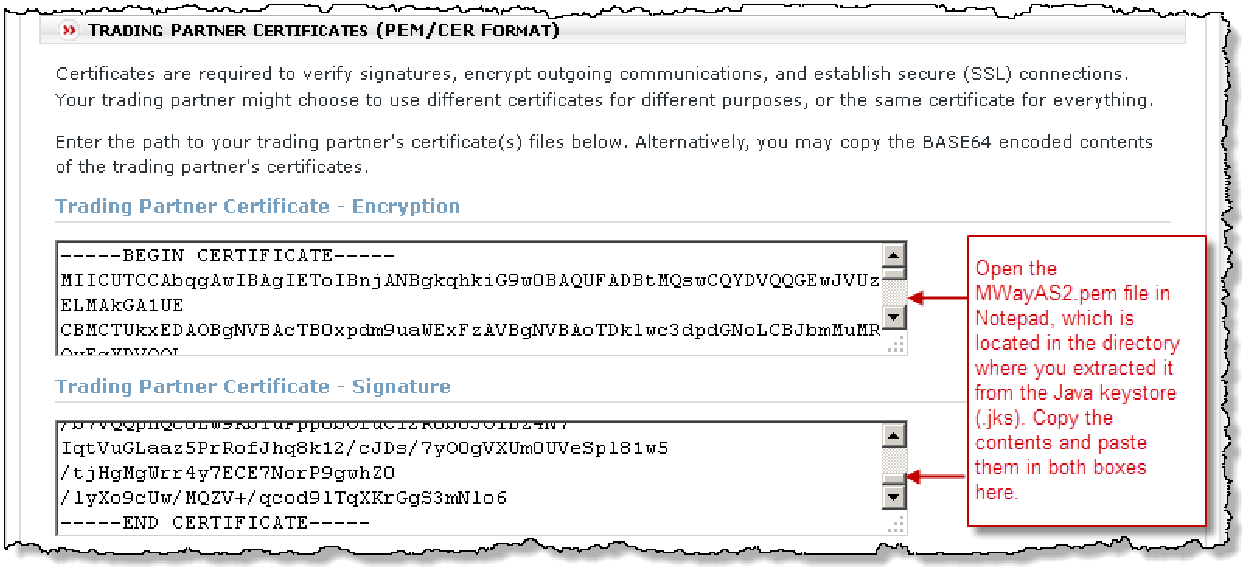
☑ Request MDN Receipt

Security: ● Signed ○ Unsigned

Delivery: ● Synchronous ○ Asynchronous

- Trading Partner Certificates (MWayAS2 public certificate allows TradingPartner1 to decrypt and authenticate signed messages from MWayAS2)
  - Type location of MWayAS2.pem or MWayAS2.cer file in the two boxes

    - or -
  - Copy the contents of MWayAS2.pem to these boxes



Certificates are required to verify signatures, encrypt outgoing communications, and establish secure (SSL) connections. Your trading partner might choose to use different certificates for different purposes, or the same certificate for everything.

Enter the path to your trading partner's certificate(s) files below. Alternatively, you may copy the BASE64 encoded contents of the trading partner's certificates.

Trading Partner Certificate - Encryption

```
-----BEGIN CERTIFICATE-----
MIICUTCCAbqgAwIBAgIEToIBnjANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJVUz
ELMAkGA1UE
CBMCTUkxEDAOBgNVBAcTB0xpdm9uaWExFzAVBgNVBAoTDklwc3dpdGNoLCBJbmMuMR
```

Trading Partner Certificate - Signature

```
IqtVuGLaaz5PrRofJhq8k12/cJDs/7yO0gVXUm0UVeSpl81w5
/tjHgMgWrr4y7ECE7NorP9gwhZ0
/lyXo9cUw/MQZV+/qcod9lTqXKrGgS3mNlo6
-----END CERTIFICATE-----
```

Open the MWayAS2.pem file in Notepad, which is located in the directory where you extracted it from the Java keystore (.jks). Copy the contents and paste them in both boxes here.

7 On the **Trading Partner** tab, click **Save Changes**.

To Test AS2 Inbound to MessageWay

If you do not have an existing trading partner with whom to test or another AS2 testing environment, you can use ***AS2 Connector*** (***http://www.freeas2.com/***).

CAUTION: Whenever you make changes to configurations files, you must restart certain processes to make the changes take effect:

Restart the Web container, such as Apache Tomcat, after you make changes to ***web.xml*** (on page 134) or ***mwas2.conf*** (on page 136);

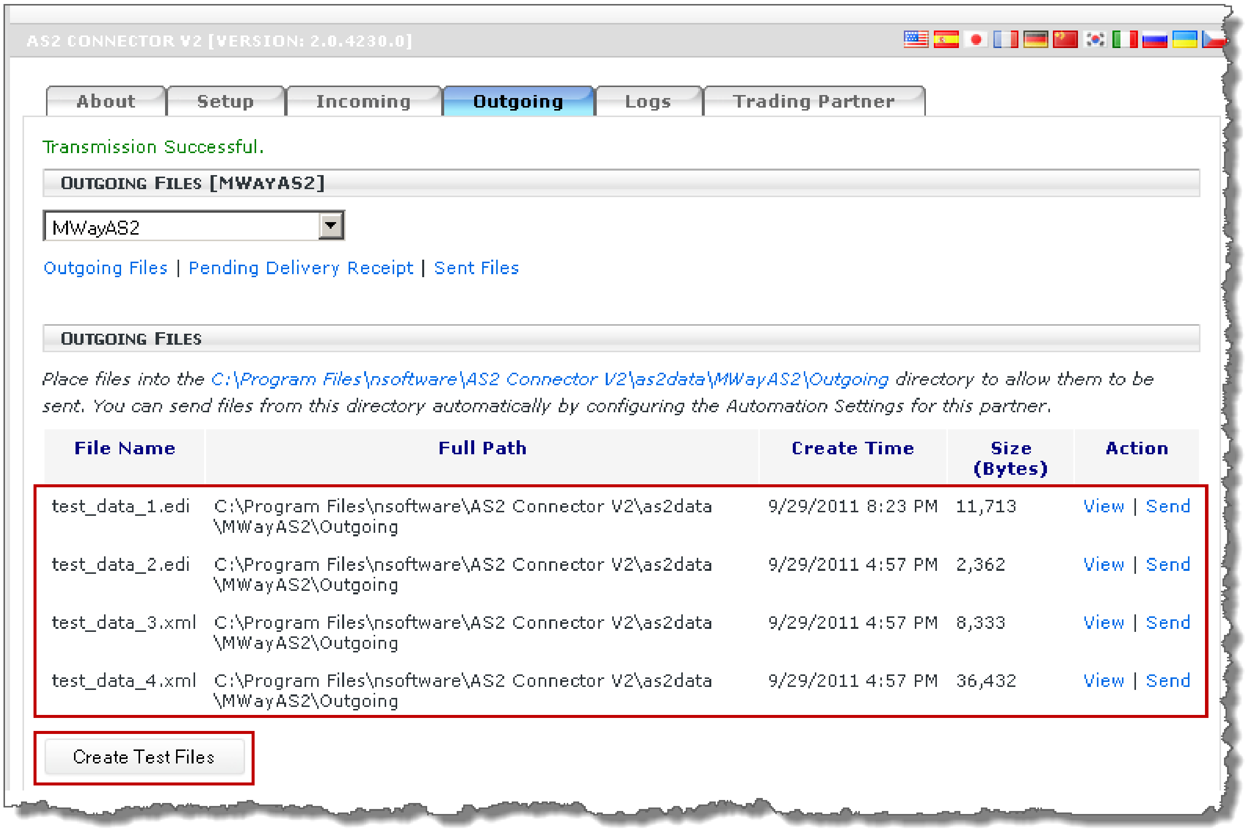
Restart the MessageWay Service Interface after you make changes to ***mwsi.conf*** (on page 145).

1 If necessary, start the AS2 connector.

The Administration Console Web application appears in your browser.

2 On the **Outgoing** tab, click **Create Test Files**.

Four files appear: two in EDI format and two in XML format.



Transmission Successful.

OUTGOING FILES [MWAYAS2]

MWayAS2

Outgoing Files | Pending Delivery Receipt | Sent Files

OUTGOING FILES

Place files into the C:\Program Files\nsoftware\AS2 Connector V2\as2data\MWayAS2\Outgoing directory to allow them to be sent. You can send files from this directory automatically by configuring the Automation Settings for this partner.

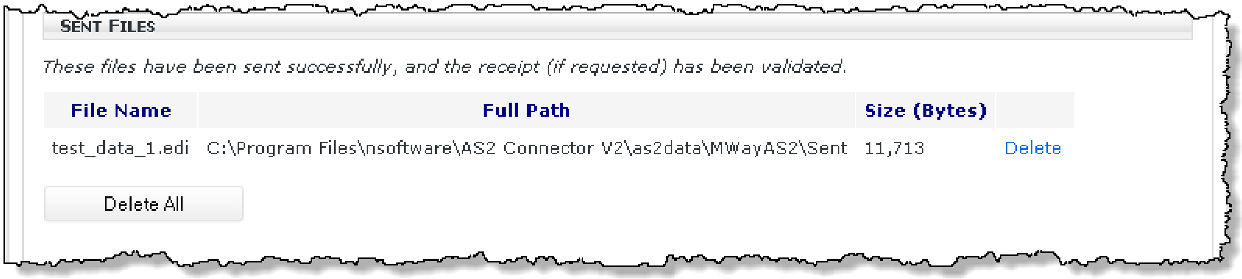
File Name	Full Path	Create Time	Size (Bytes)	Action
test_data_1.edi	C:\Program Files\nsoftware\AS2 Connector V2\as2data \MWayAS2\Outgoing	9/29/2011 8:23 PM	11,713	View | Send
test_data_2.edi	C:\Program Files\nsoftware\AS2 Connector V2\as2data \MWayAS2\Outgoing	9/29/2011 4:57 PM	2,362	View | Send
test_data_3.xml	C:\Program Files\nsoftware\AS2 Connector V2\as2data \MWayAS2\Outgoing	9/29/2011 4:57 PM	8,333	View | Send
test_data_4.xml	C:\Program Files\nsoftware\AS2 Connector V2\as2data \MWayAS2\Outgoing	9/29/2011 4:57 PM	36,432	View | Send

3 Click **Send** for the first file.

If the send was not successful, the file information will turn red, and a notice will appear at the top of the page.

- or -

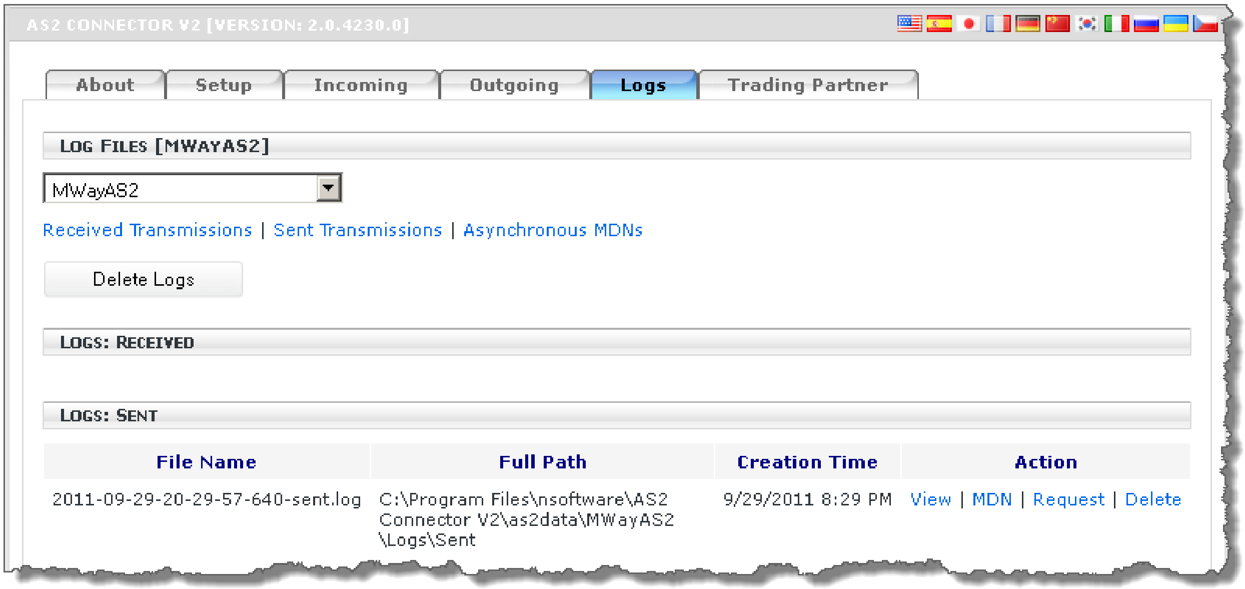
If the send was successful, the file will disappear from the list and appear on the Sent Files list.


SENT FILES

These files have been sent successfully, and the receipt (if requested) has been validated.

File Name	Full Path	Size (Bytes)	
test_data_1.edi	C:\Program Files\nsoftware\AS2 Connector V2\as2data\MWayAS2\Sent	11,713	Delete

4 In either case, click the **Logs** tab to access the log files.


AS2 CONNECTOR V2 [VERSION: 2.0.4230.0]
About
Setup
Incoming
Outgoing
Logs
Trading Partner
Received Transmissions | Sent Transmissions | Asynchronous MDNs
Delete Logs

LOG FILES [MWAYAS2]

MWayAS2

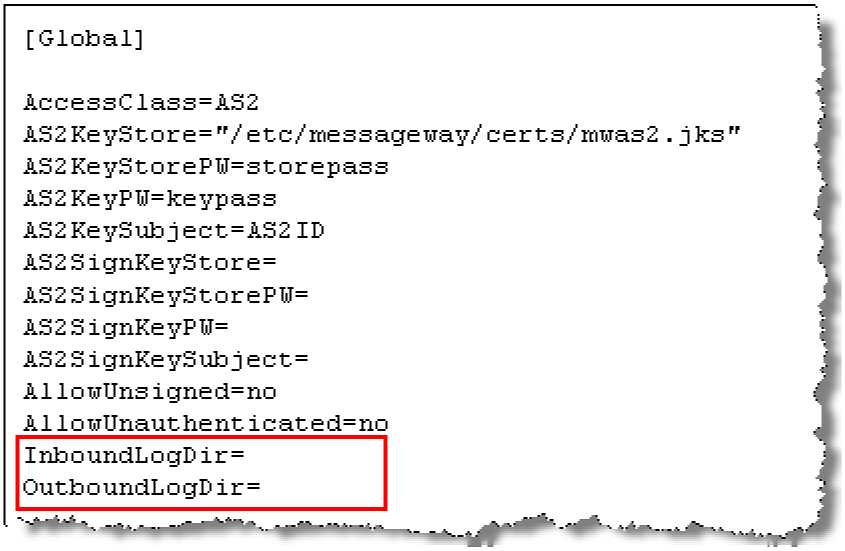
LOGS: RECEIVED

LOGS: SENT

File Name	Full Path	Creation Time	Action
2011-09-29-20-29-57-640-sent.log	C:\Program Files\nsoftware\AS2 Connector V2\as2data\MWayAS2 \Logs\Sent	9/29/2011 8:29 PM	View | MDN | Request | Delete

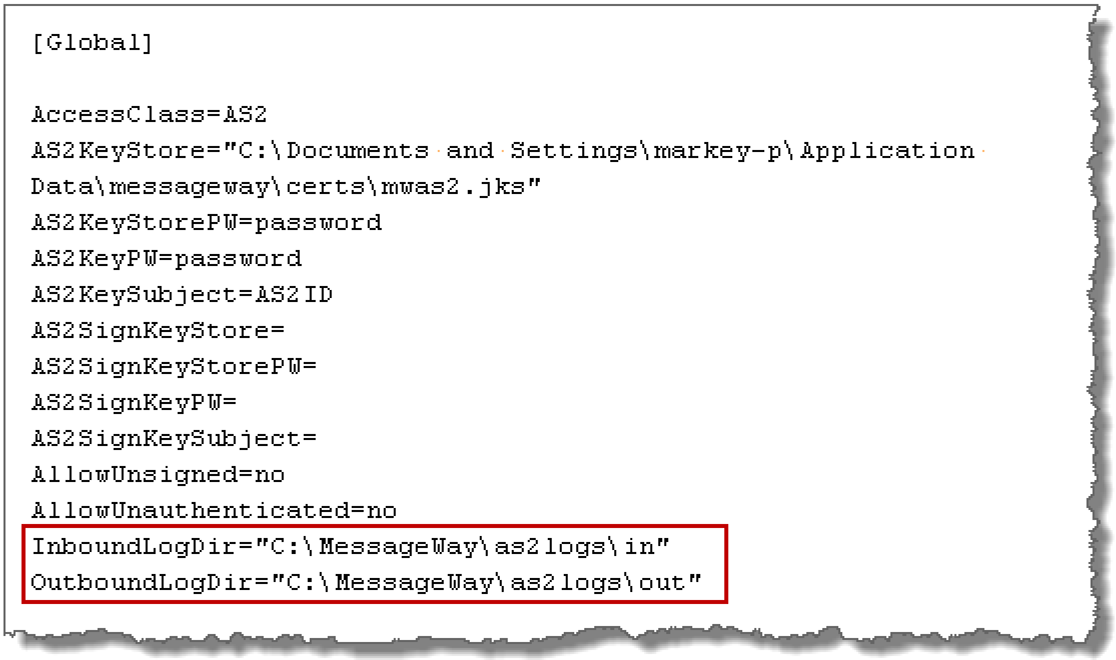
5 For the file in question, click **View** and scroll through the information, which shows you what the trading partner did to the file, if anything.

6 To review similar information on the MessageWay side for troubleshooting, you can specify that MessageWay also generate log files. To do so, you modify the ***InboundLogDir*** (on page 137) parameter in the MessageWay AS2 configuration file, mwas2.conf.



```
[Global]

AccessClass=AS2
AS2KeyStore="/etc/messageway/certs/mwas2.jks"
AS2KeyStorePW=storepass
AS2KeyPW=keypass
AS2KeySubject=AS2ID
AS2SignKeyStore=
AS2SignKeyStorePW=
AS2SignKeyPW=
AS2SignKeySubject=
AllowUnsigned=no
AllowUnauthenticated=no
InboundLogDir=
OutboundLogDir=
```

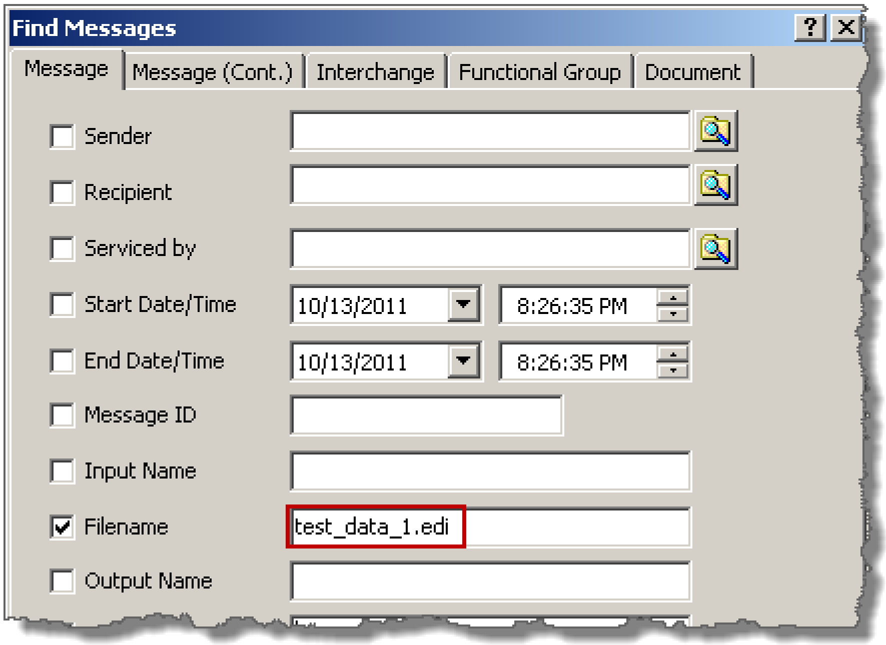
AS2 Configuration File, Global Section, Logging Directories Blank, UNIX/Linux



```
[Global]

AccessClass=AS2
AS2KeyStore="C:\Documents and Settings\markey-p\Application
Data\messageway\certs\mwas2.jks"
AS2KeyStorePW=password
AS2KeyPW=password
AS2KeySubject=AS2 ID
AS2SignKeyStore=
AS2SignKeyStorePW=
AS2SignKeyPW=
AS2SignKeySubject=
AllowUnsigned=no
AllowUnauthenticated=no
InboundLogDir="C:\MessageWay\as2logs\in"
OutboundLogDir="C:\MessageWay\as2logs\out"
```

AS2 Configuration File, Global Section, Logging Directories, Windows

7 From MessageWay Manager, find the inbound message, such as **test_data_1.edi**, using the filename search box.



☐ Sender

☐ Recipient

☐ Serviced by

☐ Start Date/Time 10/13/2011 8:26:35 PM

☐ End Date/Time 10/13/2011 8:26:35 PM

☐ Message ID

☐ Input Name

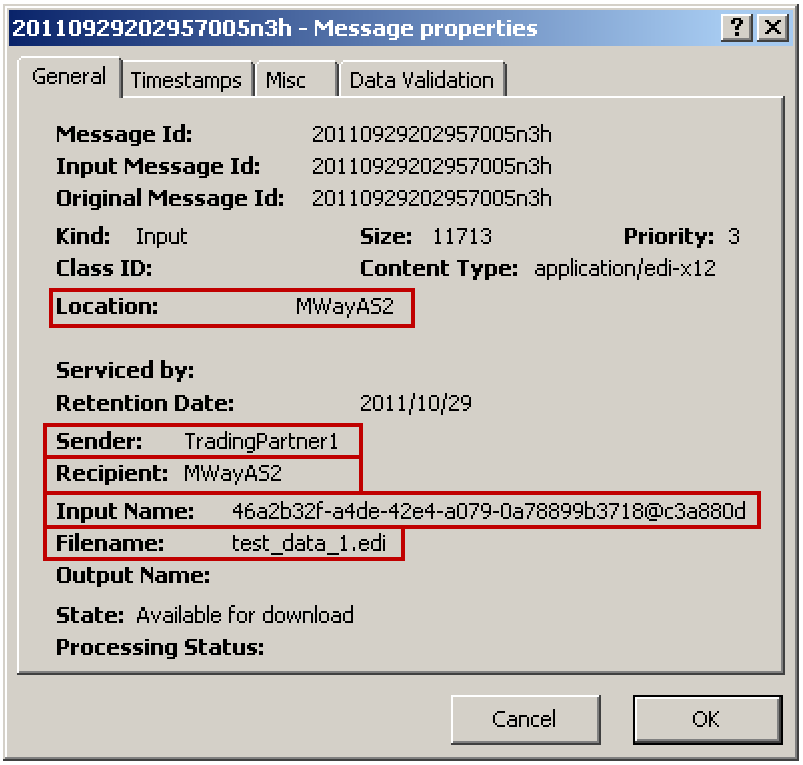
☑ Filename test_data_1.edi

☐ Output Name

A Message List window appears with the message you just sent.

8 In the Message List window, right-click the message and click Properties.

The Message Properties window appears.



Message Id: 20110929202957005n3h
Input Message Id: 20110929202957005n3h
Original Message Id: 20110929202957005n3h
Kind: Input Size: 11713 Priority: 3
Class ID: Content Type: application/edi-x12
Location: MWayAS2

Serviced by:
Retention Date: 2011/10/29
Sender: TradingPartner1
Recipient: MWayAS2
Input Name: 46a2b32f-a4de-42e4-a079-0a78899b3718@c3a880d
Filename: test_data_1.edi
Output Name:
State: Available for download
Processing Status:

Note that you can search for a message using any criteria you happen to know, such as sender, recipient, or file name. These are sent in the AS2 header. The Input Name comes from the Message ID in the AS2 header.

TIP: If an MDN was requested, it will also contain information it received from the trading partner, MWayAS2.

To Test AS2 Outbound From MessageWay

If you do not have an existing trading partner with whom to test or another AS2 testing environment, you can use ***AS2 Connector*** (***http://www.freeas2.com/***). Make sure the AS2 Adapter is started.

CAUTION: Whenever you make changes to configurations files, you must restart certain processes to make the changes take effect:

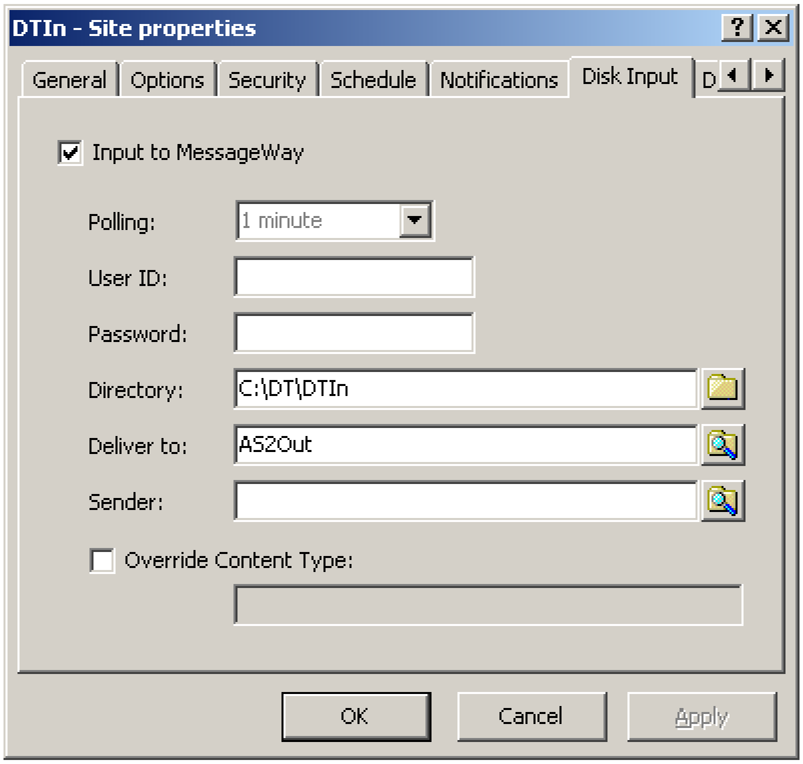
Restart the Web container, such as Apache Tomcat, after you make changes to ***web.xml*** (on page 134) or ***mwas2.conf*** (on page 136).

Restart the MessageWay Service Interface after you make changes to ***mwsi.conf*** (on page 145).

1 If necessary, start the AS2 connector.

The AS2 Connector administrator appears in your browser.

2 Create a disk transfer site or use an existing one to pick a file up from disk or redirect an existing message in MessageWay and send it to the site AS2Out.



☑ Input to MessageWay

Polling: 1 minute

User ID:

Password:

Directory: C:\DT\DTIn

Deliver to: AS2Out

Sender:

□ Override Content Type:

3 From the MessageWay Manager, start the Disk Transfer adapter.

4 Copy a file, such as X850Test, to the directory listed on the **Disk Input** tab.

5 After the file has been successfully sent, from the MessageWay Manager:

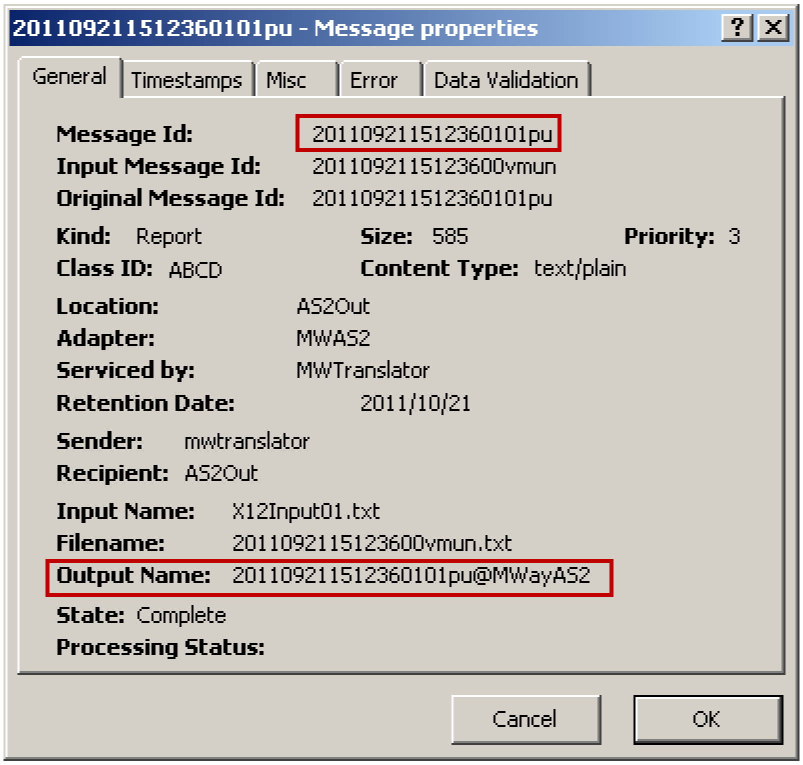
a) In the left pane, click **Locations.**

b) In the right pane, right-click the site, AS2Out.

c) From the menu, click **Show Messages**.

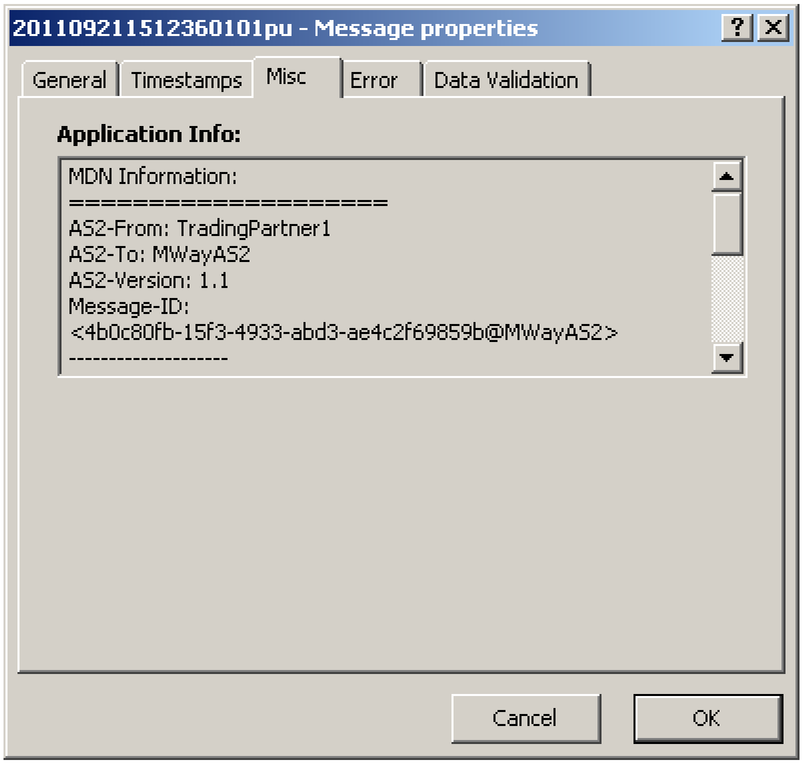
d) From the message list, right-click the message you just sent, and from the menu click **properties**.

The Message Properties window appears. Notice the name of the output file.



Message Id: 201109211512360101pu
Input Message Id: 2011092115123600vmun
Original Message Id: 201109211512360101pu
Kind: Report
Size: 585
Priority: 3
Class ID: ABCD
Content Type: text/plain
Location: AS2Out
Adapter: MWAS2
Serviced by: MWTranslator
Retention Date: 2011/10/21
Sender: mwtranslator
Recipient: AS2Out
Input Name: X12Input01.txt
Filename: 2011092115123600vmun.txt
Output Name: 201109211512360101pu@MWayAS2
State: Complete
Processing Status:

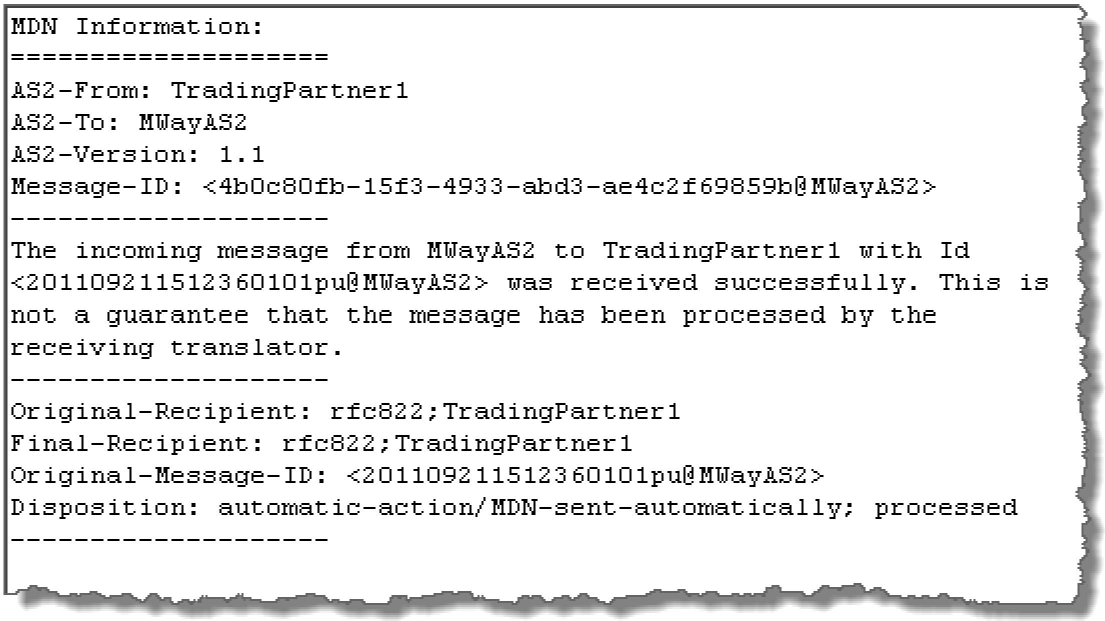
The information about the MDN returned from TradingPartner1 appears on the **Misc** page.



Application Info:

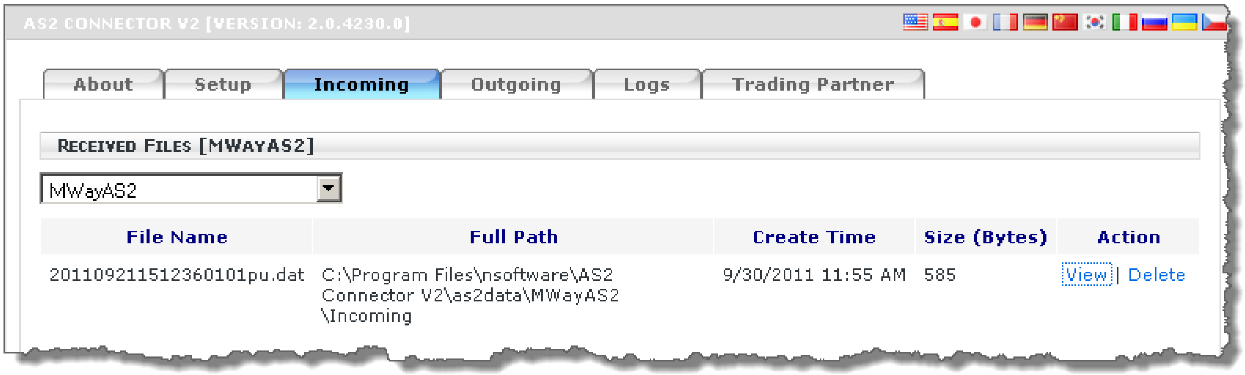
```
MDN Information:
=====================
AS2-From: TradingPartner1
AS2-To: MWayAS2
AS2-Version: 1.1
Message-ID:
<4b0c80fb-15f3-4933-abd3-ae4c2f69859b@MWayAS2>
--------------------
```

This is the full text of the information in the box:



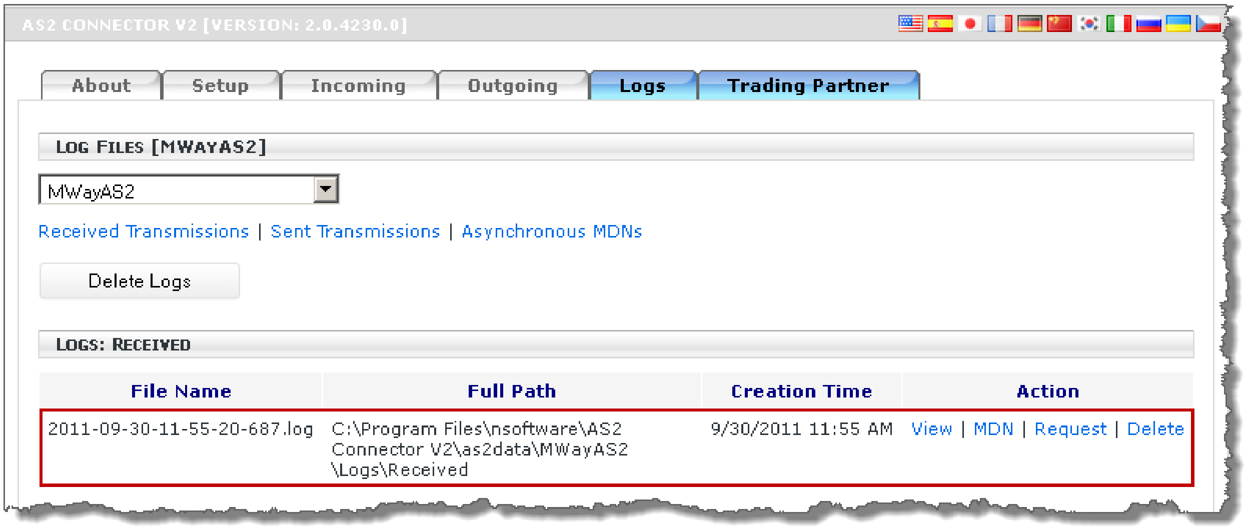
```
MDN Information:
====================
AS2-From: TradingPartner1
AS2-To: MWayAS2
AS2-Version: 1.1
Message-ID: <4b0c80fb-15f3-4933-abd3-ae4c2f69859b@MWayAS2>
--------------------
The incoming message from MWayAS2 to TradingPartner1 with Id
<20110921151236010lpu@MWayAS2> was received successfully. This is
not a guarantee that the message has been processed by the
receiving translator.
--------------------
Original-Recipient: rfc822;TradingPartner1
Final-Recipient: rfc822;TradingPartner1
Original-Message-ID: <20110921151236010lpu@MWayAS2>
Disposition: automatic-action/MDN-sent-automatically; processed
--------------------
```

6 From the AS2 connector, click the **Incoming** tab. Notice the name of the file it received.



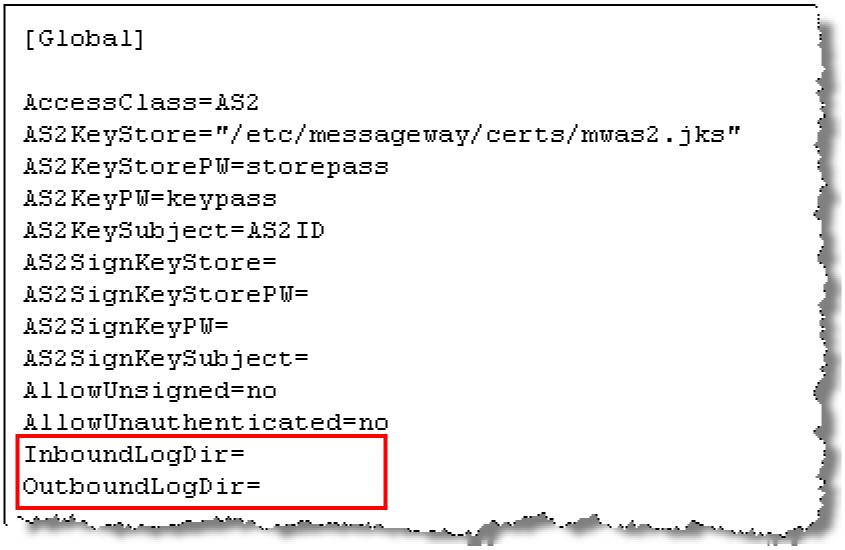
File Name	Full Path	Create Time	Size (Bytes)	Action
20110921151236010lpu.dat	C:\Program Files\nsoftware\AS2 Connector V2\as2data\MWayAS2 \Incoming	9/30/2011 11:55 AM	585	View | Delete

7 Click the **Logs** tab to view the log file for the received message.

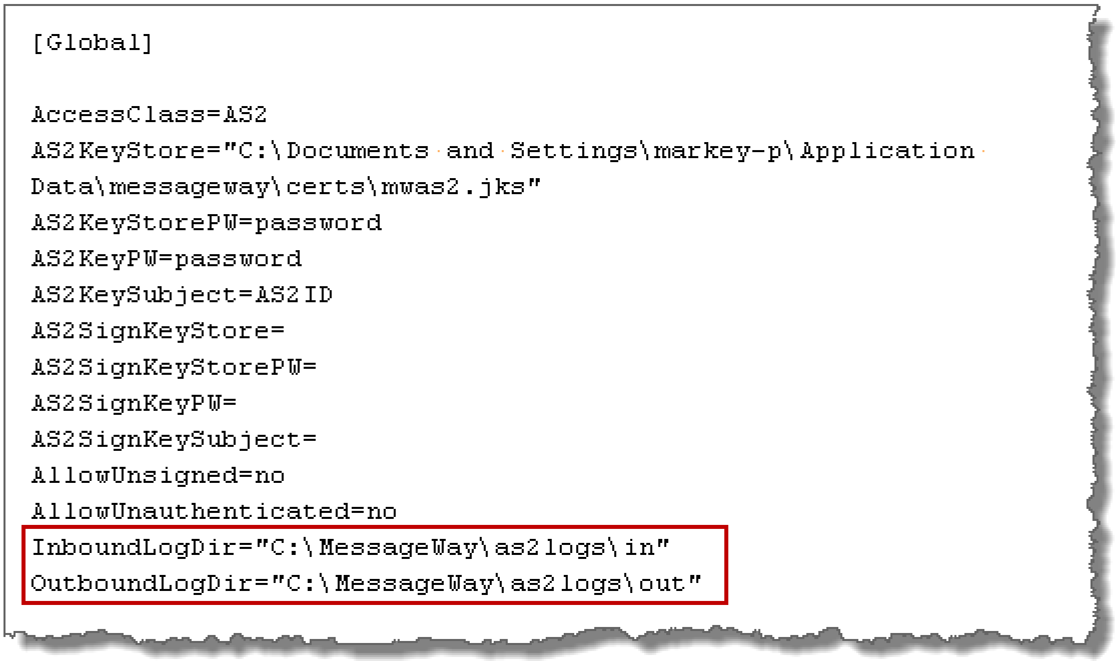

AS2 CONNECTOR V2 [VERSION: 2.0.4230.0]
About
Setup
Incoming
Outgoing
Logs
Trading Partner
LOG FILES [MWAYAS2]
MWayAS2
Received Transmissions | Sent Transmissions | Asynchronous MDNs
Delete Logs
LOGS: RECEIVED

File Name	Full Path	Creation Time	Action
2011-09-30-11-55-20-687.log	C:\Program Files\nsoftware\AS2 Connector V2\as2data\MWayAS2 \Logs\Received	9/30/2011 11:55 AM	View | MDN | Request | Delete

8 To review similar information on the MessageWay side for troubleshooting, you can specify that MessageWay also generate log files. To do so, you modify the ***OutboundLogDir*** (on page 137) parameter in the MessageWay AS2 configuration file, mwas2.conf.



```
[Global]

AccessClass=AS2
AS2KeyStore="/etc/messageway/certs/mwas2.jks"
AS2KeyStorePW=storepass
AS2KeyPW=keypass
AS2KeySubject=AS2ID
AS2SignKeyStore=
AS2SignKeyStorePW=
AS2SignKeyPW=
AS2SignKeySubject=
AllowUnsigned=no
AllowUnauthenticated=no
InboundLogDir=
OutboundLogDir=
```



```
[Global]

AccessClass=AS2
AS2KeyStore="C:\Documents and Settings\markey-p\Application
Data\messageway\certs\mwas2.jks"
AS2KeyStorePW=password
AS2KeyPW=password
AS2KeySubject=AS2ID
AS2SignKeyStore=
AS2SignKeyStorePW=
AS2SignKeyPW=
AS2SignKeySubject=
AllowUnsigned=no
AllowUnauthenticated=no
InboundLogDir="C:\MessageWay\as2logs\in"
OutboundLogDir="C:\MessageWay\as2logs\out"
```

Configuring the FTP Perimeter Server

The MessageWay FTP Perimeter Server provides unsecured and secured implicit and explicit SSL/TLS access to MessageWay from an FTP client. By default for secure transfers, the FTP perimeter server enforces SSL data ***integrity checking*** (on page 217), not file transfer integrity checking (checksum).

IMPORTANT: This is a dedicated MessageWay perimeter server that communicates between FTP clients and MessageWay to access messages in mailboxes. MessageWay supports two ways for clients to view messages: a proprietary view based on message status and a traditional FTP type hierarchical directory view. The two views have different access and location configuration options, which are explained throughout the help file. Which view the client uses for a given session depends on the configuration for the user that logs on to MessageWay. The Default Location on the User Properties window will show either a mailbox that resides in the Locations folder, which uses the proprietary view, or a mailbox that resides in the File System folder, which uses the hierarchical directory view.

This option includes the following components:

- MessageWay FTP Perimeter Server
- MessageWay Service Interface (SI), installed separately with the MessageWay Server

These components typically have the following physical relationships:

- FTP Perimeter Server may reside on any server
- MessageWay Service Interface must reside on the same system as the MessageWay Server

Licensing Requirements for the FTP Perimeter Server

The MessageWay FTP Perimeter Server uses the MessageWay Service Interface to access MessageWay. The MessageWay FTP Perimeter Server requires a license from Progress. For more information, contact MessageWay Technical Support.

Progress has provided certificates with the MessageWay FTP Perimeter Server for users to be able to test secure communications. At least for the final stages of testing, users should obtain their own certificates from a trusted licensing authority.

Overview of the FTP Perimeter Server

File Transfer Protocol (FTP) is a way to move data over the Internet using Transmission Control Protocol/Internet Protocol (TCP/IP). The MessageWay FTP Perimeter Server provides unsecured and secured access to MessageWay from an FTP client. Another component allows the server to act as a proxy to handle connections and commands from the FTP adapter, which is a client. The proxy then connects to an external FTP server.

It allows for both implicit and explicit secured access methods. For secured access, the FTP Perimeter Server uses Secure Sockets Layer (SSL) protocol or its successor protocol, Transport Layer Security (TLS), to create a secure connection with an FTP client. Here, we will use SSL to mean both SSL and TLS.

The FTP perimeter server is based on the following primary references, which you can review at the ***RFC Archive site http://www.rfc-archive.org/***:

- RFC 959 - File Transfer Protocol (FTP)
- RFC 1919 - Classical versus Transparent IP Proxies
- RFC 2228 - FTP Security Extensions
- RFC 4217 - Securing FTP with TLS

The FTP perimeter server is multi-threaded and able to listen on multiple ports and control multiple sessions simultaneously. It runs on Windows as a network service or UNIX/Linux systems as a daemon. It runs as a server to handle connections from external clients or as a proxy server to handle connections from the MessageWay FTP adapter to an external FTP server.

Components and Processes of the FTP Perimeter Server

The main components of the FTP perimeter server system perform the following functions:

- The FTP perimeter server uses dedicated threads to listen on pre-defined TCP/IP ports and to create session threads when external FTP clients connect. Each session thread controls a single FTP session.
- The Service Interface uses dedicated threads to listen on specified HTTP ports and to process requests for MessageWay services that are received from the FTP perimeter server.

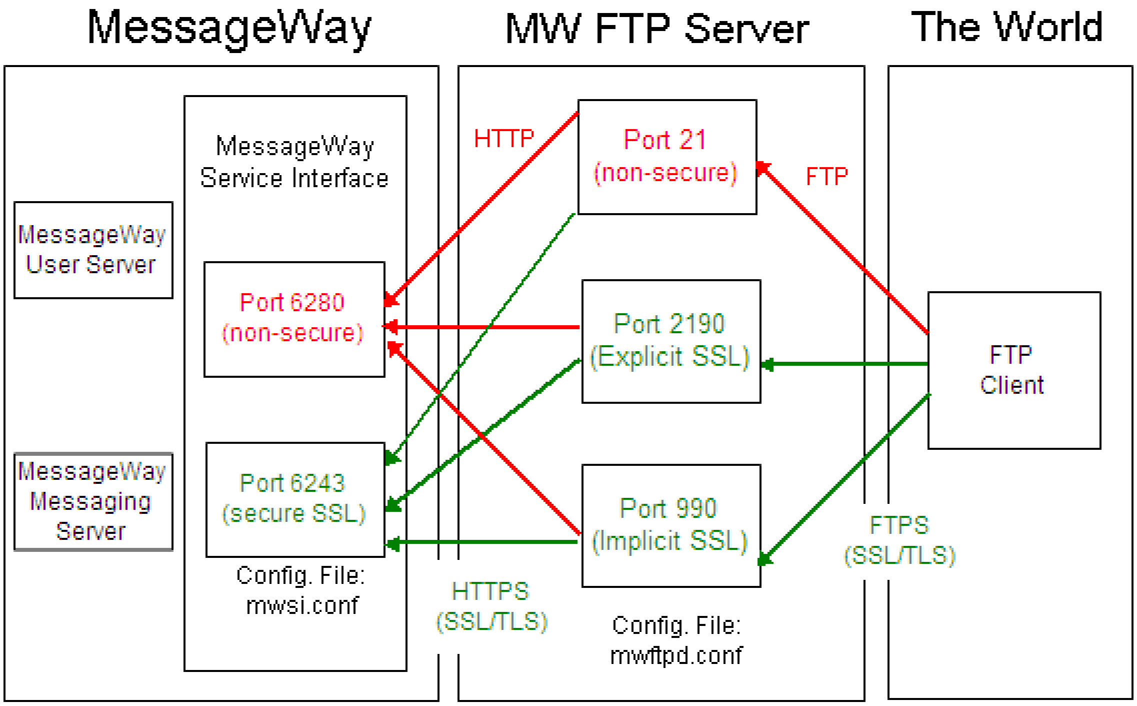
The configurations for the FTP perimeter server and the ***Service Interface*** (on page 95) are in their separate configuration files. The following steps describe the typical process flow between the client and server:

1. FTP perimeter server receives request from FTP client on a port that determines the type of connection.
   - FTP (non-secure) on default port, typically 21
   - FTP SSL (explicit) on dedicated port, 2190 in the example
   - FTP SSL (implicit) on dedicated port, typically 990
2. FTP perimeter server uses configuration information to determine whether client is allowed to connect.
3. If user is allowed to connect, the FTP perimeter server connects to an HTTP Service Interface port specified in the FTP perimeter server configuration for access to MessageWay:
   - HTTP (non-secure) on dedicated port, 6280 in the example
   - HTTP (secure)/HTTPS on dedicated port, 6243 in the example
4. The FTP perimeter server contacts the Service Interface to verify the logon ID and password as a valid:
   - MessageWay User ID and password

     - or -
   - LDAP User ID and password, when user is configured in MessageWay to use LDAP
5. The FTP perimeter server sends commands from the client to the Service Interface, which sends them to MessageWay for processing.

The following diagram provides a high-level view of the communication process:

NOTE: The port to which a connection is made determines whether a connection is secure or non-secure. The MessageWay FTP Perimeter Server may be on the same system as MessageWay, behind a firewall, or on a separate system, for example, in front of the firewall (DMZ).



Components and Processes of the FTP Perimeter Server Acting As Proxy

The main components of the FTP perimeter server when it acts as a proxy server, performs the following functions:

- The FTP perimeter server uses dedicated threads to listen on pre-defined TCP/IP ports and to create session threads when a MessageWay FTP adapter connects. Each session thread controls a single FTP session.
- The FTP perimeter server, functioning as a client, then connects to an external FTP server to push or pull files.

The configurations for the FTP perimeter server determines whether a port is configured for a proxy server. The following steps describe the typical process flow between the client and server:

1 FTP perimeter server receives request from FTP adapter client on a port that determines the type of connection.

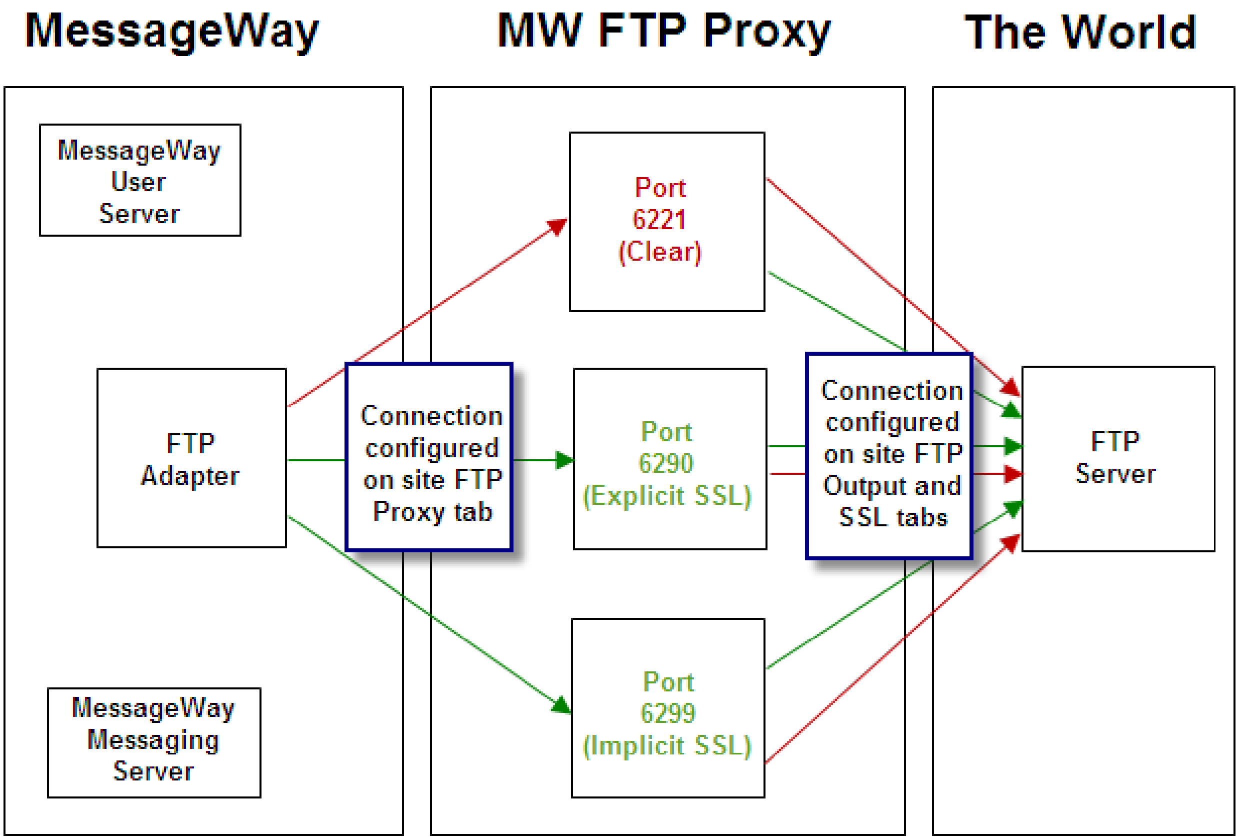
  - FTP (non-secure or clear) on default port, typically 6221
  - FTP SSL (explicit) on dedicated port, typically 6290

- FTP SSL (implicit) on dedicated port, 6299 in the example

2 The FTP perimeter server, acting as a client, connects to an external FTP server using the logon information configured in the MessageWay FTP site.

The following diagram provides a high-level view of the communication process:

NOTE: The port to which a connection is made determines whether a connection is secure or non-secure.



Understanding File Names for FTP

MessageWay has two methods to display file names to client software when they access MessageWay depending on whether the user's default location is in the Locations folder or in the File System folder. If the default location is in the File System folder, the only option is to display the filename property of the message. If the default location is in the Locations folder, additional options are available as described here. For more information about the differences between the two types of locations, refer to the topic, ***Overview of Location Properties*** (on page 453).

For better usability for messages in the Locations folder, you can map the way files are identified on a client system, usually by directory and file name, to the way they are identified in MessageWay. Users configure this parameter, MessageNameFormat, in the configuration file for the FTP server, mwftpd.conf.

The MessageNameFormat parameter defines the format used to name MessageWay messages, as specified in the ***FTP configuration file*** (on page 213). It is used to display the response to a DIR (LIST) command and to interpret the parameters from a GET (RETR), PUT (STOR) or DEL (DELE) command.

The message name format must include either filename (3) or the message ID (1). In addition, it may include the class ID (2).

The message name format is defined as 1 to 3 of the following characters:

1	***Message ID*** (on page 1199)
2	***Class ID*** (on page 1187)
3	***Filename*** (on page 1185)

Each character represents a component of the message name (*msg-name*) to be displayed, separated by a plus character, **+**. The number **1** or **3** must be present and if not found, the listener defaults to **1**.

IMPORTANT: MessageWay allows duplicate file names. Internally this is not a problem, because MessageWay always assigns a unique message ID to a message, whether the user chooses to display it or not. So for messages in locations that are defined in the Locations folder, when users download files, there may be more than one file of the same name. Users should take care to make sure that duplicate file names will not cause a problem for their local system. If there could be a problem, it would be wise to always include the message ID as part of the message name. This will also help troubleshooting, because the message ID includes a date and time stamp. For messages in locations defined in the File System folder, duplicate file names are not displayed or not allowed, depending on the command. If a file name exists in a directory (location) in the File System folder and a client attempts to upload a new file of the same name, the original message is canceled, and then the new file is uploaded. Clients viewing a File System directory structure cannot see canceled or downloaded messages.

Here are some examples based on the MessageNameFormat parameter in the ***listener configuration section*** (on page 217) that is specified in the FTP configuration file. The components create the resulting file name. Note that messages in locations defined under the File System folder do not support Class ID, so Class ID displays as part of the filename.

Parameter	Components	Example of Message Names
3	*Filename*	test.txt
1	*MessageID*	20060301125013015784
21	*ClassID*+ *MessageID*	(Locations) xyz+20060301125013015784 (File System) xyz20060301125013015784
13	*MessageID*+ *Filename*	20060301125013015784+test.txt

231	*ClassID***+** *Filename***+** *MessageID*	(Locations) xyz+test.txt+20060301125013015784 (File System) xyztest.txt+20060301125013015784

Commands for the MessageWay FTP Perimeter Server

The following table lists the raw commands supported by the MessageWay FTP Server as well as some typical user commands supported by clients. The FTP commands must be in uppercase. The client typically converts the commands entered by users to a valid server command string before transmitting it. The associated commands from the client vary based on the client. Not all clients support all commands. For example, DOS client does not support *type ebcdic*, *restart* or *size*. The use of some of the client commands are specific to MessageWay locations in the Locations folder, particularly those that refer to the directories *downloaded* and *canceled*.

There are differences between the commands supported for messages and locations in the Locations folder and those in the File Systems folder. When clients log on to MessageWay, the user's default location determines whether they will view messages from the Locations folder or messages from the File System folder. Some commands are only available to those viewing messages in the File System folder as indicated in the description column in the following table.

Server Command	Typical FTP Client Command	Description
APPE	**append** *local-file* **append** *local-file remote-file*	(File System locations only) Appends current file to existing message. The file to which you append should be in a pickup mailbox, not a service location. You can only append to files with a status of *Available*, *Wait* or *Queued*. The status changes to *Uploading* during the append process, and it will be visible but locked.
AUTH		Sets secure command channel mode.
CCC		Sets Clear Command Channel mode.
CDUP	**cd /** **cd ~** **cd ..**	Change working directory to the default location or home directory.
CWD	**cd canceled** **cd downloaded**	For messages in locations defined under the Locations folder, change working directory to *canceled* or *downloaded* from the location directory.
	cd home **cd /**	(File System locations only) Change working directory. The directory is initially positioned at the Default Location node for the user. If the user has complete access to locations in the File System folder, then a forward slash, / , positions the directory at the top node.

Server Command	Typical FTP Client Command	Description
DELE	**delete** **del** **rm** **mdel**	Delete a message from a MessageWay location. User must have appropriate rights to delete messages for this location.
EPSV		Communicates data connection endpoint information for network protocols through firewalls or network address translators (NATs). Use this extended passive command in place of the *PASV* command for FTP transfers where the control and data connection(s) are being established between the same two machines. Since the server only returns a port number, the client should assume the connection is to the same address to which it originally connected. This type of connection does not require the translation of the network address, so it also supports encrypted data. **Options:** **EPSV** **EPSV 1** **EPSV ALL** **NOTE:** The commands *EPSV* and *EPSV 1* both invoke the IPv4 protocol. The command *EPSV ALL* disables all other related commands, such as *EPRT*, *PORT* and *PASV*. If a 3-way connection is required after issuing an *EPSV ALL* command, you must start a new FTP session.
FEAT		Returns the following feature command set: 211-Features: EPSV REST STREAM SIZE TVFS UTF8 MDTM 211 End
LIST	**dir**, **ls -l**	Display formatted list of messages in the current directory.
	ls */directory/filename* **ls** *filename*	(File System locations only) List the filename property of messages within the directory structure. You can specify either relative or absolute paths. Absolute paths start with a /. You can also use the asterisk, *, as a wildcard after the last slash. Paths can also contain a single dot, for example, *filename.txt* and two dots, for example, *../directory/filename*.

Server Command	Typical FTP Client Command	Description
MDTM	**modtime** *filename*	Returns the last-modified time (Time Received or Sent) of a specified message in GMT. If more than one message meets the selection criteria, the oldest message is returned. The returned format is yyyymmddhhmmss.sss
MKD	mkdir directory	(File System locations only) Make a new directory (location) within the directory (location) where you are currently positioned. This creates a pickup mailbox, which appears to the client as a directory.
NLST	**ls**, **mget**, **mdel, mdelete**	Display an unformatted list of messages, retrieves multiple messages or deletes multiple messages. Must be preceded by PORT or PASV command. The **mget** and **mdel** commands support wild cards, including * and ? (single character) as well as partial names, but they only act against the current location.
NOOP		Do nothing except return a response.
PASS		Send valid password to log on to MessageWay. Must be preceded by the USER command.
PASV		Requests an IP address and port on which the server is listening and to which the client connects, and tells the server to enter passive mode. In passive mode, the client connects to the server rather than the server connecting to a client's port.
PBSZ		Sets protection buffer size to encapsulate protected data over the data channel.
PORT		Specifies an IP address and port to which the client connects for the next file transfer. This is active mode where the server connects to the client.
PROT		Sets secure data channel mode.
PWD	**pwd**	Displays the location name of the current directory.
command	**quote "***command***"**	Sends command to the server as a literal, bypassing any editing of the command by the client. This may be useful when the server supports a command that the client does not.
REST	**restart**	Restart a transfer at byte offset. REST on inbound transfers to locations in the Locations folder is for failed transfers only.
RETR	**get**, **recv**	Retrieve a file from MessageWay. Must be preceded by a PORT or PASV command indicating where the server should send the data.

Server Command	Typical FTP Client Command	Description
RMD	**rmdir** *directory*	(File System locations only) Remove a directory (location). The location cannot have any sub-locations nor any messages.
RNFR	**rename** *Filename From Filename To*	(File System locations only) Rename a file or location from a current *filename* or location. You cannot rename directories (locations) that have messages. This is followed by the To filename with RNTO.
RNTO	(see RNFR)	(File System locations only) Rename a file or location to a new *filename* or location. This is preceded by the From filename with RNFR.
SITE	*option*	Return or send information specific to the current FTP server site.
SIZE	**size**	Returns the size of the remote file (or message in the case of MessageWay)
STAT	**stat**, **status**	Return current time on the server.
STOR	**put**, **send**	Send a file to a MessageWay location. Must be preceded by a PORT or PASV command so the server knows the sending location.
TYPE	**type ascii** **ascii** **type binary** **binary**	Set transfer type: ASCII, EBCDIC or BINARY. The default type is ASCII. Some clients reset the type to ASCII after a list or directory command.
USER	**user**	Send a valid MessageWay user name and password. Must be followed by a valid MessageWay password for the user.

The MessageWay FTP Perimeter Server does not support the following commands for locations defined under the Locations folder:

- APPE (Append a local file to an available message)
- MKD (Make a new directory)
- RMD (Remove a directory)
- RNFR (Rename from c*urrent file name*)
- RNTO (Rename to *new file name*)

Accessing MessageWay from an FTP Client

When FTP clients log on to MessageWay, their MessageWay user configuration defines their ***default location*** (on page 1363) and, optionally, a ***default recipient*** (on page 1363) location. The default location is their FTP mailbox. By default, all messages are uploaded to and downloaded from the default location.

If there is also a default recipient location defined for the user, then all messages are uploaded to this location, unless otherwise stated in the command.

NOTE: Location is a generic term that includes auto-delivery locations, which are service locations and sites, and pickup mailboxes. Mailbox is a specific type of location where users collect messages. A user's default location is always a mailbox. Assuming they have the rights to do so, users may act on locations other than pickup mailboxes. Therefore, here we use the generic term, location.

What type of directory structure a user sees depends on whether the default location is in the Locations folder or in the File System folder. Locations in the File System folder begin with a forward slash, /. For more information about the differences between the two types of locations, refer to the topic, ***Overview of Location Properties*** (on page 453).

IMPORTANT: To use and/or display non-ASCII Unicode characters in users, locations, and file names through the MessageWay FTP and SFTP perimeter servers, FTP and SFTP clients must support Unicode (specifically UTF-8).

CAUTION: In general, do not use the PAUSE/RESUME commands from FTP clients when you transfer files into MessageWay.

Specifically, *do not* pause an inbound file transfer when you transfer files into MessageWay locations that reside in the *Locations* folder (also called the Locations namespace). When you pause file transfers into MessageWay, the status of the file will be marked *Available*. Since MessageWay marks the message as *Available*, a partial file could be available immediately for pickup or delivery, and users might get a partial file. It is *not* possible to resume the transfer when client software sends files to locations in the Locations namespace, because the filename attribute is not unique in that namespace. However, it is possible to resume the transfer when client software sends files to the File System namespace, because the filename attribute *is* unique in that namespace. However, if you pause files to a service location in the File System namespace, the service will probably receive and process a partial file before you are able to resume transmission. Note that there are no problems if you pause and then resume file transfers out of MessageWay.

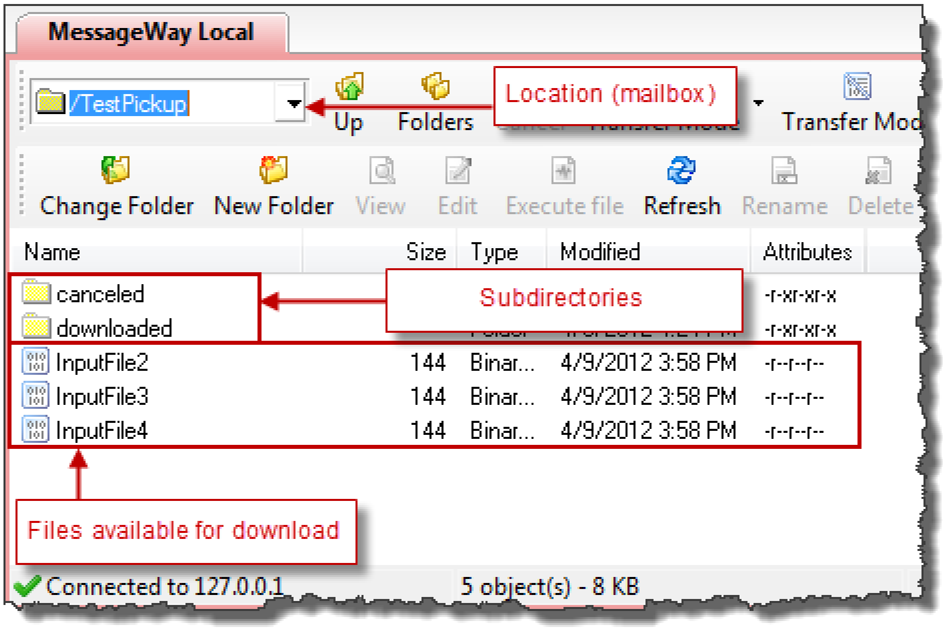
Client View of Messages in Locations Folder (FTP)

For the Locations folder, when an FTP client accesses MessageWay, it sees a default hierarchy:

- A root directory, indicated by the forward slash (/)
  - A user's default location (mailbox) directory
    - *Canceled* directory
    - *Downloaded* directory

TIP: You can hide the *canceled* and *downloaded* directories from the client's view so that it is similar to what FTP clients typically see, and their view will be similar to what they see when using the File System folder. To hide the *canceled* and *downloaded* directories, in the Listeners Configuration section of the FTP Perimeter Server configuration file mwftpd.conf, set the *SuppressCanceledAndDownloadDirs* parameter to *True*. For more information, refer to the topic ***FTP Server, Listener Configuration Section*** (on page 217).

For example, the FTP client may show the following:



Location (mailbox)

Subdirectories

Name	Size	Type	Modified	Attributes
canceled				-r-xr-xr-x
downloaded				-r-xr-xr-x
InputFile2	144	Binar...	4/9/2012 3:58 PM	-r--r--r--
InputFile3	144	Binar...	4/9/2012 3:58 PM	-r--r--r--
InputFile4	144	Binar...	4/9/2012 3:58 PM	-r--r--r--

Files available for download

Connected to 127.0.0.1 5 object(s) - 8 KB

When a user downloads or deletes a message, it moves to the downloaded or canceled directory, respectively. Users can continue to retrieve messages from these directories until the archive program removes them from the system.

Clients view message information from MessageWay in terms of directory structures and file names. From MessageWay Manager, this information is viewed in terms of locations and statuses.

The following table shows these different views. It should help users understand how clients typically view MessageWay.

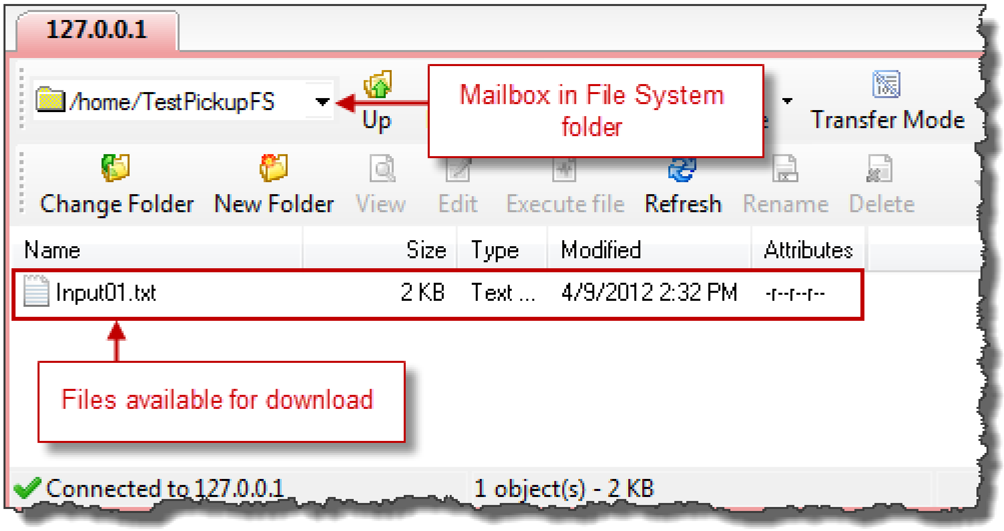
Concept	MessageWay Manger	Client Software
Content	Message ID [Class ID] [filename]	File name
Location	mailbox (current)	/Location directory[/subdirectory]

Status	A = Available
	C = Canceled
	D = Downloaded
		Available = location directory
		Canceled = canceled subdirectory
		Downloaded = downloaded subdirectory

Users can make this link more obvious using the ***file name mapping feature*** (on page 303).

Client View of Messages in File System Folder (FTP)

If the default location for a user is in the File System folder, when an FTP client accesses MessageWay, the user sees a hierarchical directory from the default location.



Name	Size	Type	Modified	Attributes
Input01.txt	2 KB	Text ...	4/9/2012 2:32 PM	-r--r--r--

When a user deletes a message, the message is no longer visible.

Most users do specific things and only need to know a limited set of client commands. The following table describes the most typical tasks, the basic FTP commands users need, and the effect of these commands in MessageWay:

Tasks	FTP Command(s)	Affect in MessageWay
Move around in the MessageWay structure	cd	Allows users to move among directories to which the user has access, which is typically their default location (directory) and its contents.
Delete messages from MessageWay	del, mdel	Cancels messages. User must have the right to cancel messages for this location. When messages are marked canceled, users can no longer access them.
Get directory listings	dir, ls	Displays messages within the immediate directory.
Move files from MessageWay (download)	get, mget	Downloads available messages and changes the status to complete. When messages are marked complete, users can no longer access them.
Move files to MessageWay (upload)	put, mput	Uploads files to any MessageWay locations where user has upload rights.
Set transfer mode	type	Sets transfer mode as ASCII or binary.

For a more comprehensive list of client commands, refer to the topic ***Commands for the MessageWay FTP Server*** (on page 191). The details for FTP client commands and their syntax are described for ***basic use*** (on page 198).

Basic FTP Commands and Syntax

The FTP commands users enter to communicate with the MessageWay FTP Perimeter Server are the same as those supported by most servers.

CD

The CD command allows the user to make any directory the current location directory.

A location directory corresponds to a MessageWay location, but there are more options for locations in the Locations folder. For example, the directories, *canceled* and *downloaded*, are not used for locations in the File System folder. These directories normally correspond to the root's subdirectories. *Canceled* and *downloaded* could also be valid root directories if added as locations within the MessageWay Manager.

The syntax of the command for locations in both the Locations and File System folder is:

cd [**/** | **~** | **..**]

- or -

cd /*location_directory*

Additional syntax options for locations in the Locations folder are:

cd [**canceled**|**downloaded**]

- or -

cd /*location_directory*/[**canceled**|**downloaded**]

The following table shows some examples:

Command	Result
cd / - or - **cd ~** - or - **cd ..**	Resets the current directory to the home or default directory (File System folder only) If a user has access to the root directory, / , then cd / will set the current directory to the root directory rather than the default directory.
cd */location_directory*	Changes the current directory to */location-name*
cd canceled	(Locations folder only) Changes current location directory to its **canceled** subdirectory
cd downloaded	(Locations folder only) Changes current location directory to its **downloaded** subdirectory

Command	Result
cd */location_directory/***downloaded**	(Locations folder only) Changes the current location directory to the **downloaded** subdirectory of the specified location

DEL

The DEL command cancels messages with a status of *Available*. The user must have the appropriate rights to cancel messages for the location, which include the right to ***cancel messages*** (on page 1057).

When a message is deleted, it is moved to the *canceled* directory. Until they are removed by the archive program, canceled messages are available for users to download.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
location-name	Name of the MessageWay location.
msg-name	(Location folder only) Name of the message derived from the MessageNameFormat parameter specified in the FTP configuration file. (File System folder only) Name of the message derived from the filename property. Messages in locations in the File System folder ignore the MessageNameFormat parameter.

The syntax options of the command are as follows:

del [**/**location-name**/**]*msg-name*

Here are some examples:

Command	Description
del *msg-name*	Cancels message in current directory.
del /Remote2/*msg-name*	Cancels message in Remote2 directory.

DIR

The DIR or LS command displays a single message when the message name is used or all messages for the location and status. The message list output depends on the location being queried and the directory in the location. If the command has no arguments, MessageWay returns all messages in the current directory.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
location-name	Name of the MessageWay location.
msg-name	(Location folder only) Name of the message derived from the MessageNameFormat parameter specified in the FTP configuration file. (File System folder only) Name of the message derived from the filename property. Messages in locations in the File System folder ignore the MessageNameFormat parameter.

The syntax of the command for locations in both the Locations and File System folder is::

dir [*****]

- or -

dir *msg-name*

Additional syntax options for locations in the Locations folder are:

dir canceled | **downloaded**

- or -

dir */location-name*[**/canceled**|**/downloaded**]

Here are some basic examples and descriptions of the results.

Command	Result
dir or **dir ***	Lists available messages in the current directory if the current directory is the user's default location; Otherwise, it lists messages uploaded to the current directory by the user that has logged on.
dir canceled	(Locations folder only) Lists canceled messages in the current directory if the current directory is the user's default location; Otherwise it returns, "Access-Denied."
dir downloaded	(Locations folder only) Lists completed messages in the current directory if the current directory is the user's default location; Otherwise it returns, "Access-Denied."
dir */location-name*	Lists available messages in *location-name,* if *location-name* is the user's default location; Otherwise, it lists messages uploaded to the location by the user that has logged on, if the user has the necessary permissions.
dir */location-name*/**canceled**	(Locations folder only) Lists canceled messages in *location-name,* if *location-name* is the users' default location; Otherwise it returns, "Access-Denied."

Command	Result
dir /*location-name***/downloaded**	(Locations folder only) Lists completed messages in *location-name,* if *location-name* is the users' default location; Otherwise it returns, "Access-Denied."

Here are some conditions that affect the results of the command:

- If the user has download rights to the location directory that it queries, but does not have upload rights, then the list displays all messages in the location directory with a status of *available*.
- If the user does not have download rights but does have upload rights to the location that it queries, then the behavior is somewhat different. Instead of displaying messages of a particular status, messages where the sender matches the user's default location are displayed regardless of status. The status of each message, however, is not available and the user cannot view messages in the *canceled* or *downloaded* subdirectories.

GET

The GET command retrieves one or more messages from a location (mailbox) directory.

Users may retrieve messages only if the user who is logged on has the necessary download permissions defined on the location configuration and the user configuration.

Here are descriptions of the parameters used in the syntax:

Parameter	Description
location-name	Name of the MessageWay location directory.
msg-name	(Location folder only) Name of the message derived from the MessageNameFormat parameter specified in the FTP configuration file, which may be a combination of the Message ID, Class ID and Filename. When you use the message ID, all other fields are ignored. **IMPORTANT:** MessageWay allows duplicate filenames, and it returns a specific message with the message name or the oldest message that matches the location and status. If you only use the filename to download messages, and there are messages with duplicate filenames, you will always receive the oldest message. (File System folder only) Name of the message derived from the filename property. Messages in locations in the File System folder ignore the MessageNameFormat parameter. **IMPORTANT:** MessageWay allows duplicate filenames. If you upload a message with a filename that already exists, MessageWay cancels the existing message and uploads the current message.
local-path	Path and/or file name of the downloaded file on the local system.

The basic syntax options of the command are as follows:

get [*****] [**?**] [*local-path*]

- or -

get [*/location-name/*]*msg-name* [*local-path*]

- or -

mget [*|*file** (...)]

IMPORTANT: Some clients do not support the **GET *** command, such as DOS FTP. Also, in some cases, using **GET *** will retrieve the oldest file that meets the criteria, but it may overwrite the first file it finds on your local disk. To avoid this problem, use the command specifying the name of the local file, **GET *** [*local-path*].

Here are some examples:

Command	**Description**
get [*] [*local-path*]	Downloads the oldest message from the current location to the home directory or to an optional local directory
get *msg-name*	Downloads message, optionally using the single-character wildcard (?), from current location directory to the current local directory
get /Remote2	Downloads oldest message from *Remote2* directory to the current local directory
get /Remote2/canceled	(Locations folder only) Downloads oldest message in *canceled* subdirectory in *Remote2* directory to the current local directory
get /Remote2/*msg-name*	Downloads specific message from *Remote2* directory to the current local directory
get /Remote2/downloaded/*msg-name*	(Locations folder only) Downloads specific message in *downloaded* subdirectory in *Remote2* directory to the current local directory
get downloaded	(Locations folder only) Downloads oldest message in *downloaded* subdirectory in current location directory to the current local directory
get canceled/*msg-name*	(Locations folder only) Downloads specific message in *canceled* subdirectory in current location directory to the current local directory
mget *	Downloads all messages in the current location directory to the current local directory

PUT

The PUT command transfers a file from the client's system to a MessageWay location, assuming the user has the necessary permission to upload messages to the location. Users may send messages to their default recipient or to another location directory specified in the command.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
file	Name of the current file on the client system.
new-file	New name for the remote file, which becomes the input file name in MessageWay.
location-name	Name of the MessageWay location to which the file is delivered.

The syntax options of the command are as follows:

put *file*

- or -

put *file /location-name*

- or -

put *file /location-name/new-file*

- or -

mput [*|file* (...)]

Here are some examples:

Command	Description
put *file*	Upload *file* to the current location directory
put *file new-file*	Upload *file* to a message with the filename, *new-file*, in the current location directory
put *file* /**Remote3**	Upload *file* to the *Remote3* directory
put *file* /**Remote3**/*new-file*	Upload *file* with the filename, *new-file*, to the *Remote3* directory
mput *.txt	Upload all files that end in .txt to the current location directory

Advanced FTP Commands and Syntax (Locations Folder)

IMPORTANT: This information is only valid for locations in the Locations folder, not for locations (directories) in the File System folder.

The syntax of the advanced commands show how to use ***class ID*** (on page 1187) to identify messages that belong to a specific group. This extension to the basic FTP commands is specific to MessageWay.

DEL

The DEL command cancels messages with a status of *Available*. When canceled messages are eligible for archive or delete, they will be removed from the MessageWay message store when the archive program runs.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
classID	Class ID specified in MessageWay
location-name	Name of the MessageWay location
msg-name	Name of the message derived from the MessageNameFormat parameter specified in the FTP configuration file

The advanced syntax options of the command are as follows:

del *classID* **@**[*location-name*]**/** *msg-name*

- or -

del **/** *location-name*[**/** *classID* **@**]**/** *msg-name*

DIR

The DIR command displays a single message when the message name is used or all messages for the location, class ID and status. The message list output depends on the location being queried and the directory in the location. If the command has no arguments, MessageWay returns all messages in the current directory.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
classID	Class ID specified in MessageWay
location-name	Name of the MessageWay location
msg-name	Name of the message derived from the MessageNameFormat parameter specified on the FTP configuration file

The advanced syntax options of the command are as follows:

dir canceled | **downloaded** [**/** *classID* **@**][**/** *msg-name*]

- or -

dir *classID***@** [*]

- or -

dir *classID***@**[**canceled**|**downloaded**][**/***msg-name*]

- or -

dir *classID***@**[*location-name*][**/canceled**|**/downloaded**][**/***msg-name*]

- or -

dir /*location-name*[**/canceled**|**/downloaded**][**/***classID***@**][**/***msg-name*]

Here are some conditions that affect the results of the command:

- If msg-name is provided, then that message will be displayed when a provided location and class ID are also correct for that message.
- If the user has download rights to the location directory that it queries, but does not have upload rights, then the list displays all messages in the location directory with a status of *available*.
- If the user does not have download rights but does have upload rights to the location that it queries, then the behavior is somewhat different. Instead of displaying messages of a particular status, messages where the sender matches the user's default location are displayed regardless of status. The status of each message, however, is not available and the user cannot view messages in the *canceled* or *downloaded* subdirectories.

GET

The GET command retrieves one or more messages from a location directory. You may retrieve a specific message with the message name or the oldest message that matches the location, class ID and status.

Users may retrieve messages ONLY if the user who is logged on has the necessary download permissions defined on the location configuration.

Here are descriptions of the parameters used in the syntax:

Parameter	Description
classID	Class ID specified in MessageWay
location-name	Name of the MessageWay location directory
msg-name	Name of the message derived from the MessageNameFormat parameter specified on the FTP configuration file
local-path	Path and/or file name of the downloaded file on the local system

The syntax options of the command are as follows:

get canceled|**downloaded** [**/***classID***@**] [*local-path*]

- or -

get canceled|**downloaded** [*/classID***@**]*/msg-name* [*local-path*]

- or -

get *classID***@**[*location-root_directory*][**/canceled**|**/downloaded**] [*local-path*]

- or -

get *classID***@**[**canceled**|**downloaded**]*/msg-name* [*local-path*]

- or -

get *classID***@**[*location-root_directory*][**/canceled**|**/downloaded**]*/msg-name* [*local-path*]

- or -

get */location-root_directory*[**/canceled**|**/downloaded**][*/classID***@**] [*local-path*]

- or -

get */location-root_directory*[**/canceled**|**/downloaded**][*/classID***@**]*/msg-name* [*local-path*]

PUT

The PUT command transfers a file from the client's system to a MessageWay location, assuming the user has the necessary permission to upload messages to the location. Users may send messages to their default recipient or to another location specified in the command. If you do not specify a location name, the message is stored in the default recipient location.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
classID	Class ID to be associated with the message.
file	Name of the current file on the client system.
new-file	New name for the remote file, which becomes the input file name in MessageWay.
location-name	Name of the MessageWay location to which the file is delivered.

The syntax options of the command are as follows:

put *file /location-name*[*/classID***@**][*/new-file*]

- or -

put *file classID***@**[*location-name*][*/new-file*]

QUOTE

The QUOTE command is not an FTP command. However, most FTP clients support this command. It allows users to send a command to the server as a literal, bypassing any editing of the command by the client. The FTP client sends the values within quotes to the FTP server. This may be useful when the server supports a command that the client does not or when MessageWay has extended the use of the command.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
option	***Any command that the MessageWay FTP Server supports*** (on page 191).

The syntax of the command is as follows:

QUOTE "*option***"**

Here is an example that sets the transfer type to EBCDIC:

QUOTE "type ebcdic"

SITE

This allows users to enter a command that is specific to the current FTP perimeter server, which processes the command following the word SITE. Use this command within the QUOTE command.

The following options are available:

Option	Description
TIME	Returns the local time of the MessageWay server
COMPRESS	Returns data as a compressed (ZIP) file. The **COMPRESS** option is only valid when the **CompressOutbound** parameter is set to **Client** or it is omitted from the mwftpd.conf file. When **CompressOutbound** is set to **True** or **False** in the mwftpd.conf file, an error is returned, "COMPRESS - rejected due to policy reasons."
UNCOMPRESS	Returns data as an uncompressed file. The **UNCOMPRESS** option is only valid when the **CompressOutbound** parameter is set to **Client** or it is omitted from the mwftpd.conf file. When **CompressOutbound** is set to **True** or **False** in the mwftpd.conf file, an error is returned, "COMPRESS - rejected due to policy reasons."
STATUS	Returns the value for the CompressOutbound parameter set in the Listener Configurations section of the mwftpd.conf file
SENDER=*MWayMailbox*	Sets the default sender location for the session, which overrides the default sender configured in the **Default Location** box on the **Locations** tab of the User Properties window. It affects any subsequent **PUT** commands for the session unless changed
HELP	Returns the list of supported **SITE** commands

The syntax options of the command are as follows:

QUOTE "SITE *option***"**

Here are some examples:

QUOTE "site time"

quote "SITE SENDER=MessageWayMailbox"

Advanced FTP Command Examples (Locations Folder)

IMPORTANT: This information is only valid for locations in the Locations folder, not for locations (directories) in the File System folder.

These examples assume that you use the DOS FTP command-line client connected to the MessageWay FTP Server. Results may vary using another command-line client. The mapping defined should behave the same with most user interfaces for FTP clients.

Default location — The ***default location*** (on page 1363) directory of the logged-on user.

Current location — The location named by the root in the current working directory.

Current status — The message status indicated by the location in the current working directory. Messages in the location directory, have a status of *Available* (A). Messages in the **canceled** subdirectory have a status of *Canceled* (C). Messages in the **downloaded** subdirectory have a status of *Downloaded* (D).

These conditions are required for the examples:

- The logged-on user must have download rights to locations Remote1 and Remote2 and upload rights to Remote3.
- The current working directory is /Remote1.

Any examples containing either **canceled** or **downloaded** also applies for the other.

DEL Examples

The DEL command cancels messages with a status of Available.

Here are some examples:

Command	Location	Class ID	Status	Message ID
del *msg-name*	Current	-	Current	from *msg-name*
del /Remote2/*msg-name*	Remote2	-	A	from *msg-name*
del abc@/*msg-name*	Current	abc	Current	from *msg-name*
del /Remote2/abc@/*msg-name*	Remote2	abc	A	from *msg-name*
del abc@Remote2/*msg-name*	Remote2	abc	A	from *msg-name*

DIR Examples

The DIR command lists either a single message when *msg-name* is provided or all messages matching the provided location, class id and status.

Here are some examples:

Command	Location	Class ID	Status	Message ID
dir	Current	-	Current	
dir *	Current	-	Current	
dir *msg-name*	Current	-	Current	from *msg-name*
dir canceled	Current	-	C	-
dir /Remote2	Remote2	-	A	-
dir /Remote2/canceled	Remote2	-	C	-
dir /Remote2/*msg-name*	Remote2	-	A	from *msg-name*
dir /Remote2/canceled/*msg-name*	Remote2	-	C	from *msg-name*
dir abc@	Current	abc	Current	-
dir abc@*	Current	abc	Current	-
dir abc@/*msg-name*	-	abc	-	from *msg-name*
dir abc@canceled	Current	abc	C	-
dir abc@canceled/*msg-name*	Current	abc	C	from *msg-name*
dir abc@Remote2	Remote2	abc	A	-
dir abc@Remote2/canceled	Remote2	abc	C	-
dir abc@Remote2/*msg-name*	Remote2	abc	A	from *msg-name*
dir abc@Remote2/canceled/*msg-name*	Remote2	abc	C	from *msg-name*
dir /Remote2/abc@	Remote2	abc	A	-
dir /Remote2/canceled/abc@	Remote2	abc	C	-
dir /Remote2/abc@/*msg-name*	Remote2	abc	A	from *msg-name*
dir /Remote2/canceled/abc@/*msg-name*	Remote2	abc	C	from *msg-name*
dir canceled/abc@	Current	abc	C	-
dir canceled/abc@/*msg-name*	Current	abc	C	from *msg-name*

GET Examples

The GET command either retrieves a specific message when a message ID is present in the argument or retrieves the oldest message that matches the provided location, class ID and status.

IMPORTANT: Some clients do not support the **GET *** command, such as DOS FTP. Also, in some cases, using **GET *** will retrieve the oldest file that meets the criteria, but it may overwrite the first file it finds on your local disk. To avoid this problem, use the command specifying the name of the local file, **GET *** [*local-path*].

For all commands, a second file name parameter may be used to set the local file name. This has no affect on MessageWay FTP behavior.

Command	Location	Class ID	Status	Message ID
get *msg-name*	Current	-	Current	from *msg-name*
get /Remote2	Remote2	-	A	-
get /Remote2/canceled	Remote2	-	C	-
get /Remote2/*msg-name*	Remote2	-	A	from *msg-name*
get /Remote2/downloaded/*msg-name*	Remote2	-	D	from *msg-name*
get downloaded	Current	-	D	-
get canceled/*msg-name*	Current	-	C	from *msg-name*
get abc@	Current	abc	Current	-
get abc@/*msg-name*	Current	abc	Current	from *msg-name*
get canceled/abc@	Current	abc	C	-
get downloaded/abc@/*msg-name*	Current	abc	D	from *msg-name*
get /Remote2/abc@	Remote2	abc	A	-
get /Remote2/downloaded/abc@	Remote2	abc	D	-
get /Remote2/abc@/*msg-name*	Remote2	abc	A	from *msg-name*
get /Remote2/canceled/abc@/*msg-name*	Remote2	abc	C	from *msg-name*
get abc@Remote2	Remote2	abc	A	-
get abc@downloaded	Current	abc	D	-
get abc@canceled/*msg-name*	Current	abc	C	from *msg-name*
get abc@Remote2/canceled	Remote2	abc	C	-
get abc@Remote2/*msg-name*	Remote2	abc	A	from *msg-name*
get abc@Remote2/downloaded/*msg-name*	Remote2	abc	D	from *msg-name*

PUT Examples

The PUT command transfers a file from the client as a message to a MessageWay location. When a new-file name is not provided in the command, either the name of the input file or *M<msgid>.dat* is used to create the filename value in MessageWay as shown in the table.

Command	Recipient	Class ID	Filename
put *file*	Current	-	*file*
put *file new-file*	Current	-	*new-file*
put *file* **/Remote3**	Remote3	-	*M<msgid>.dat*
put *file* **/Remote3/***new-file*	Remote3	-	*new-file*
put *file* **abc@**	Current	abc	*M<msgid>.dat*
put *file* **abc@/***new-file*	Current	abc	*new-file*
put *file* **/Remote3/abc@**	Remote3	abc	*M<msgid>.dat*
put *file* **/Remote3/abc@/***new-file*	Remote3	abc	*new-file*
put *file* **abc@Remote3**	Remote3	abc	*M<msgid>.dat*
put *file* **abc@Remote3/***new-file*	Remote3	abc	*new-file*

SITE Examples

A few basic examples of client-issued commands and server responses follow. MessageWay accepts both spellings: **quot** or **quote**.

Client Command	Server Responses
quote "SITE TIME"	200 SITE: TIME - 20080108130655250 - or - 200 SITE: TIME - not implemented (occurs when MWaySI version < 4.2.1.12)
quote "SITE COMPRESS"	200 SITE: COMPRESS - outbound compression turned on - or - 200 SITE: COMPRESS - rejected due to policy reasons (occurs when **CompressOutbound** parameter is set to **true** or **false** in mwftpd.conf)
quote "SITE UNCOMPRESS"	200 SITE: UNCOMPRESS - outbound compression turned off - or - 200 SITE: UNCOMPRESS - rejected due to policy reasons (occurs when **CompressOutbound** parameter is set to **true** or **false** in mwftpd.conf)
quote "SITE STATUS"	200 SITE: STATUS - obcompress=true
quote "SITE SENDER=MWayMailbox"	200 SITE: SENDER=MWayMailbox

Client Command	Server Responses
quote "SITE HELP"	200 SITE: HELP - 200 SITE TIME 200 SITE COMPRESS 200 SITE UNCOMPRESS 200 SITE STATUS 200 SITE HELP

Here is an example that retrieves a message in compressed (ZIP or GZIP) format, assuming that the **CompressOutbound** parameter in the Listener Configurations section of the mwftpd.conf is not listed, or if listed, it is set to **Client**:

```
ftp> quot "SITE COMPRESS"

200 SITE: COMPRESS - outbound compression turned on

ftp> get 33537313+MW20071010133537313.DAT+20071010133454006aaa testfile.zip

200 PORT command successful. Consider using PASV

150 Connecting to Data Port...

226 Retrieved Message: [20071010133454006aaa] (compressed) Size: [4005] bytes
```

Changing Your MessageWay Password from an FTP Client

Typically, you can change the password for your MessageWay user ID from an FTP client command line.

From a command line , to change your password during the logon sequence:

1. At the logon command, type your user name only, and click **ENTER**.
2. At the password prompt, type:
   old_password|new_password|repeat_new_password

From a command line, to change your password after you have logged on:

1. Type **user**.
2. At the password prompt, type:
   old_password|new_password|repeat_new_password

Basic Installation Tasks

The installation process installs the components of the MessageWay FTP Perimeter Server. These tasks assume that you have already installed MessageWay, which includes the following components of interest here:

- MessageWay Messaging Server, which processes messaging requests
- MessageWay User Server, which controls access to MessageWay from the Manager
- MessageWay Service Interface, which provides access to MessageWay from the Internet
- MessageWay Manager, which provides the user interface to configure MessageWay

These are the tasks performed during initial installation for testing:

- Install the FTP perimeter server on any system
- ***Set up the configuration file for the Service Interface*** (on page 96) on the MessageWay system
- ***Start the Service Interface*** (on page 103)
- ***Test the connection to the Service Interface*** (on page 104)
- Set up the configuration file for the FTP perimeter server
- For secure transmissions, install the certificate obtained from a licensing authority

NOTE: Progress provides certificates with FTP perimeter server option to use for initial testing. These certificates allow anonymous logon. You should replace these certificates as soon as possible. Also note that these certificates are shared with the default installation of the MessageWay Service Interface Server.

- Configure MessageWay users and locations
- Test the system from end to end

For the actual installation information, refer to the *MessageWay Installation Guide*.

Configuring the FTP Perimeter Server Components

You set the parameters for the FTP Perimeter Server system in the configuration files, mwsi.conf for the Service Interface and mwftpd.conf for the FTP Perimeter Server. You edit the files with a text editor. For information about configuring the Service Interface file, refer to the topic, ***Service Interface*** (on page 95).

The following table shows the default location for the FTP configuration file, which depends on the operating system where the FTP Perimeter Server resides:

Operating System	Location of the FTP Perimeter Server Configuration File
UNIX or Linux	/etc/messageway/mwftpd.conf
Windows	\ProgramData\messageway\mwftpd.conf

New Parameters for the FTP Configuration File

CAUTION: If you already have a configuration file, you must manually insert new parameters that you want to use, since the upgrade process does not overlay existing configuration files.

The new parameters or modifications to existing parameters for the FTP configuration file, mwftpd.conf, are as follows:

Release	Section	Parameters
4.2.0	Listener Configurations	▪ AccessClass ▪ NonStopCompat ▪ MessageNameFormat ▪ ExternalIP
4.2.1	Listener Configurations	▪ CompressOutbound
4.2.2	Listener Configurations	▪ NonStopCompat (modified) ▪ Proxy ▪ ProxyCertVerifyFile
5.0.0	Listener Configurations	▪ Banner control character options: **\n** for newline, **\t** for tab and **\r** for carriage return/linefeed. ▪ DisablePassive ▪ IgnorePortIP ▪ UpshiftPassword ▪ StrictTextDownload ▪ StrictTextUpload
5.0.0 ER03	Listener Configurations	▪ CommandTimeout ▪ DataTimeout ▪ AllowAnonymous ▪ TransferTypePolicy ▪ MapNestedDirectory
5.5.0	No new parameters	
6.0.0	No new parameters	
6.1.0	Listener Configurations	▪ MapNestedDirectory is deprecated; replaced by File System folder option
		▪ SuppressCanceledAndDownloadDirs
6.1.0 HF01	Listener Configurations	▪ FilenameSort

Configurations for the FTP Perimeter Server

The MessageWay FTP Perimeter Server resides anywhere in the LAN or WAN. Users may configure the listener ports to perform normal FTP server functions or to act as a proxy server. In its primary function, the FTP perimeter server receives commands from an FTP client, which is typically outside the network. The FTP perimeter server also acts as a client when it communicates with the Service Interface to provide users access to MessageWay. In its secondary function as a proxy server, a listener port receives commands from an FTP adapter, which, as a client, it then forwards to an external FTP server.

The server also provides secure communications using SSL/TLS. As a server, it uses the information in the *SecurityContextConfig* section. As a client, when it communicates with the Service Interface, which also has security configurations, it uses the information in the *ServiceInterfaceConfig* section.

There are seven sections in the configuration file, mwftpd.conf. The following table describes the purpose of each section. Parameters listed in italics will be named by users.

Section	**Purpose**
Global	▪ Connection parameters
Listeners	▪ Pointers to FTP listener configurations in this file
AllowHosts	▪ IP addresses allowed to connect
DenyHosts	▪ IP addresses not allowed to connect
FTPListenerConfig	▪ IP address of FTP Server and listening port ▪ Security type ▪ Reference to Security context configuration ▪ SSL method and security information ▪ Timeouts ▪ Reference to Service Interface configuration ▪ Option to set a listener as a proxy server ▪ Various parameters to further customize data transfers
SecurityContextConfig	▪ Public and private key information
ServiceInterfaceConfig	▪ IP address and port on which Service Interface listens ▪ Security type of HTTP connection ▪ Security certificate information

Global Section

The following table explains the parameters used in the **[Global]** section of mwftpd.conf.

Parameter	**Description**
MaxConnections	Maximum concurrent connections each listener will accept

Parameter	Description
PortRange	Use this only when the FTP client requests a *passive* data transfer. The starting port number should be greater than 1024. In this case, the FTP server actively sends a random port number within this range, and the client opens that data port on the server. A client might request a passive data connection when: ▪ Client is on a network behind some types of router-based firewalls ▪ Client is on network behind a service requiring passive transfers ▪ Transfers are erratic ▪ Client receives repeated failed data channel errors

FTP Server, Listeners Section

This table explains the parameters used in the **[Listeners]** section of mwftpd.conf.

Parameter	Description
FTPListenerConfig	Pointer to FTP listener configurations specified in this file, with one listener configuration per FTP Server port. There should be separate listeners for the FTP/SSL standard server and the FTP/SSL proxy server.

AllowHosts Section

This table explains the parameters used in the **[AllowHosts]** section of mwftpd.conf.

Parameter	Description
IP address	List IP addresses, one per line, of clients that are allowed to connect to the FTP Server. ▪ You may enter a range of addresses on a line, using the syntax typically used to denote subnetworks: 192.168.1.0/255.255.255.0 or 192.168.1.0/24, which both allow connections from 192.168.1.0 to 192.168.1.255. ▪ When a specific IP address allowed here also falls within a range of denied addresses, the connection will be allowed. ▪ When there are no entries in the AllowHosts section, all IP addresses are allowed.

DenyHosts Section

This table explains the parameters used in the **[DenyHosts]** section of mwftpd.conf.

Parameter	Description
IP address	List of IP addresses, one per line, of clients that are not allowed to connect to the FTP Server. ▪ You may enter a range of addresses on a line, using the syntax typically used to denote subnetworks: 192.168.2.0/255.255.255.0 or 192.168.2.0/24, which both allow connections from 192.168.2.0 to 192.168.2.255. ▪ When a specific IP address denied here falls within a range of allowed addresses, the connection will be denied. ▪ When there are no entries in the DenyHosts section, no IP address is denied.

Listener Configurations Section

This table explains the parameters used in the **[***FTPListenerConfig***]** section of mwftpd.conf. There should be a configuration for each port on which the FTP Server listens. Note that some parameters are valid for both servers and proxy servers, some only for servers and some only for proxy servers.

CAUTION: Every listener configured here MUST be referenced by a listener in the Listeners section. If a configuration exists in this section but is not referenced, the FTP server will not start.

Parameter for Servers and Proxy Servers	Description
Banner	Sign-on banner sent once to each listener when the listener starts. It may be a file name or a string literal. If it is file name, it should exist; its size should be greater than zero, and the process should have access to it. This is an example: **Banner="C:\somefile.txt"** If it is a literal, the banner text should be enclosed in quotation marks. It may include the following control characters: ▪ **\n** newline character ▪ **\t** tab character ▪ **\r** carriage return/linefeed character This is an example: **Banner="MessageWay FTP Server Version 5.0"**

Parameter for Servers and Proxy Servers	**Description**
IP	IP address of the host that is running the FTP perimeter server. When the host has multiple Network Interface Cards (NICs), use an asterisk, *****, to listen on all IP addresses on the server.
Port	Port number on which the FTP perimeter server listens. The typical default values are: ▪ **21** for FTP non-secure ▪ **2190** for FTP explicit secure ▪ **990** for FTP implicit secure ▪ **6221** for proxy non-secure ▪ **6290** for proxy explicit secure ▪ **6299** for proxy implicit secure
Security	Enter a security type. Non-secure listeners must be set to **None**. Secure listeners must be set to **SSL** or **TLS**. Valid values: ▪ **None** ▪ **SSL** ▪ **TLS**
SecurityContext	Pointer to one of security context configurations specified in this file.
SSLMethod	Determines how the client communicates with the FTP perimeter server during connection negotiations, and the port where the server is listening. For *Explicit SSL*, often called just SSL, the client starts the connection without security and then attempts to make a secure data connection before the user name and password have been verified. For *Implicit SSL*, the client sends commands to the server in a secure manner. Implicit SSL connections use a default port of 990, so any attempt to connect to a server that is not configured for Implicit SSL will fail. Valid values: ▪ **Explicit** ▪ **Implicit** The default is *Explicit* when the Security parameter is set to **SSL** or **TLS**.
SSLCommandSecurity	Minimum security allowed for the command channel. Use only when **SSLMethod=Explicit**. Valid values: ▪ **None** ▪ **Logon** ▪ **Full** (default)
SSLDataSecurity	Minimum security allowed for the data channel. Use only when **SSLMethod=Explicit**. Valid values: ▪ **None** ▪ **Full** (default)

Parameter for Servers and Proxy Servers	Description
SSLDataIntegrityStrict	For data integrity, set this to **True** to ensure that a complete message has been received on an SSL connection before storing the message in MessageWay. If set to **False**, then the connection is vulnerable to truncation attacks, where an attacker forces the truncation of the transferred data without the knowledge of either the client or server. When not used, the default setting is **True**. ▪ **False** ▪ **True** (default) **CAUTION:** Setting this to **True** may not be compatible with some clients.
Trace	Allows trace of the FTP session. Trace information is stored in the following locations, depending on the operating system: ▪ Windows: ..\program files\messageway\bin\ftp\ in the MWFTPserver.log ▪ UNIX/Linux: /var/log/mwftpd.log Valid values are any combination of the following, separated by commas: ▪ **ftp** ▪ **ftp-data** ▪ **dirlog**
LogonTimeout	Number of seconds the FTP server or proxy server will wait for the client to respond with logon information before it terminates the connection.
IdleTimeout	Number of seconds the FTP server or proxy server will wait when the line is idle before it terminates the connection.
CommandTimeout	Time (in seconds) that the FTP server or proxy will wait for a command from a connected client. When set, this overrides **IdleTimeout**. When both CommandTimeout and DataTimeout are set to zero, the server never terminates the connection; the connection is, in effect, infinite.
DataTimeout	Time (in seconds) that the FTP server or proxy will wait for data from a connected client. When set, this overrides **IdleTimeout**. When both CommandTimeout and DataTimeout are set to zero, the server never terminates the connection; the connection is, in effect, infinite.
ConnectionTimeout	Number of seconds the FTP server or proxy server will wait for the client to respond to send data to a port number sent by the server during an active transfer.
ExternalIP	Specifies an external IP address to allow passive mode when the FTP Server is behind a Network Address Translation (NAT) firewall. The IP address is used in the 227 response to the **PASV** command.
DisablePassive	When set to **True**, does not allow clients to use passive mode and returns a 502 error.
IgnorePortIp	When set to **True**, the FTP server will ignore the internal IP address in the **PORT** command for an active data session. Instead, it uses the external IP address of the remote client that has made the connection to the server.

Parameter for Servers and Proxy Servers	Description
UpshiftPassword	When set to **True**, the server converts all passwords to uppercase characters before it validates them against the MessageWay database.

Parameter for Servers Only	Description
MaxLogonAttempts	Number of consecutive times user can fail to log on before server disconnects the session.
CompressOutbound	Allows FTP clients to pull messages in compressed mode. The options are: ▪ **True** all downloaded messages will be compressed in ZIP or GZ file format **CAUTION:** Compressed files are not renamed, so users should change the extension to ZIP (Windows) or GZ (UNIX/Linux) after the file reaches its destination. ▪ **False** or option is blank downloaded messages will not be compressed, which is the default when an option is not specified for the parameter ▪ **Client** or when the **CompressOutbound** parameter is omitted **SITE COMPRESS** and **SITE UNCOMPRESS** commands will be honored to allow client control of outbound compression
MSI	Pointer to one of the MessageWay Service Interface configurations defined in this file.
AccessClass	Restricts access to MessageWay via this listener to only those users whose configuration does not include an access class list or includes this value in their access class list. This value should be alphanumeric and is case-sensitive. It must match exactly what is specified for the user. Optional, but if used, only one access class value is allowed.

Parameter for Servers Only	Description
NonStopCompat	Invokes NonStop compatibility. There are 5 options as follows. : ▪ **0** or blank No compatibility with NonStop ▪ **1** Limited NonStop compatibility ▪ **2** Full NonStop compatibility ▪ **3** Full NonStop Compatibility, but does not display *Canceled* or *Downloaded* directories, and the positioning of the file names when displayed has been changed to match the positioning used on NonStop. ▪ **4** Full NonStop Compatibility, but limits behavior to that of NonStop MIX display and commands. The MessageNameFormat parameter will be ignored.
MessageNameFormat	(File System folder only) This parameter is ignored. The Filename is always used. (Locations folder only) Defines the format for naming MessageWay messages (file name seen by FTP client). The format is defined as 1 to 3 of the following characters: ▪ **1** Message ID (default) ▪ **2** Class ID ▪ **3** Filename Each character represents a component to be displayed separated by **+**. The number **1** or **3** must be present. When neither is used, **1**, Message ID, is used as the default.
StrictTextDownload	Parameter can be used only if the listener is connecting to a MessageWay running on either a Linux or Unix platform. When set to *True*, EOL conversions for ASCII transfers are done on end-of-line chars native to MessageWay: NL->CRLF; CR's are treated as data and not converted.
StrictTextUpload	Parameter can be used only if the listener is connecting to a MessageWay running on either a Linux or Unix platform. When set to *True*, EOL conversions for ASCII transfers are done strictly on FTP protocol EOL chars: CRLF->NL; Standalone CR, LF characters are treated as data and not converted.

Parameter for Servers Only	Description
AllowAnonymous	Allows remote users to connect to MessageWay using **anonymous** as the user id. When users send this id, they will be prompted for a password, but the password is not required, or if supplied, it is ignored. The options are: ▪ **True** ▪ **False** or option is blank (default) This default requires users to have a valid user ID and password configured in MessageWay that they must use to connect.
TransferTypePolicy	When set, it enforces the transfer mode between the remote FTP client and the MessageWay FTP server, overriding the client request. Rejects client TYPE commands. Use the Binary option to force all communications into binary mode, which is required when you are also using integrity checking. The options are: ▪ Blank (default) ▪ **Binary** ▪ **ASCII**
SuppressCanceledAndDownloadDirs	(Locations Folder only) Allows the FTP server to not display messages in the Canceled and Downloaded directories. This mimics the behavior of the File System folder and is typical of most FTP server displays. The options are: ▪ **True** ▪ **False** or option is blank (default)
FilenameSort	When set to **True**, the sort order for the message list is by file name. This overrides the default sort order, which is by the message time received or sent. The options are: ▪ **True** ▪ **False** or option is blank (default)

Parameter for Proxy Servers Only	Description
Proxy	Controls whether a listener functions as a client proxy server. The options are: ▪ **True** Listener functions as a client proxy server ▪ **False** or option is blank (default) Listener functions as normal FTP perimeter server
ProxyCertVerifyFile	When the listener is operating in proxy mode; this value should be the fully qualified file name of the certificate file that is used to verify the remote server certificate. This is used when the Remote Server Certificate fingerprint is not sent by the FTP client.
ProxyTrace	Allows tracing on the client side of the proxy. This works in conjunction with the trace parameter above. ▪ **True** Allows tracing ▪ **False** or the option is blank (default) Does not allow tracing

Security Context Configurations Section

This table explains the parameters used in the **[***SecurityContextConfig***]** section of mwftpd.conf. These parameters refer to the security information used by the FTP Server to connect to an FTP client.

The default values in this section for a secure connection reference security files that are installed with the server. Users should be able to test a secure FTP connection using these default configurations and security files without making any further changes.

CAUTION: Every Security Context configured here MUST be referenced by a SecurityContext value in FTPListenerConfig section. If a configuration exists in this section but is not referenced, the FTP server will not start.

Parameter	Description
CertificateFile	Fully qualified file name (path and file name) of the Public Key file.
PrivateKeyFile	Fully qualified file name (path and file name) of the Private Key file.
PrivateKeyPassPhrase	Pass phrase to use when the PrivateKeyFile is encrypted.
CipherList	Identifies the encrypted algorithm, such as RC4, AES and Triple DES. For more information refer to OpenSSL documentation.

Service Interface Configuration Section

This table explains the parameters used in the **[***ServiceInterfaceConfig***]** section of mwftpd.conf. These parameters refer to the security information used by the FTP Server functioning as a client to connect to the MessageWay Service Interface (SI).

For secure connections, the default fingerprint in this section references security files that are installed with SI. Users should be able to test a secure FTP connection using these default configurations and security files without making any further changes.

CAUTION: When you reinstall or upgrade the MessageWay FTP Server, your configuration file is not replaced. However, when you reinstall or upgrade the MessageWay Server, the default certificates for the Service Interface may be replaced. Whenever SI certificates are replaced, the fingerprint shown here must be changed to match the new SI certificates. In the case where the SI files do not match the fingerprint, you will receive an application error, 7011, which is visible in the Events Viewer on Windows or the Event log on UNIX/Linux. Simply copy the peer certificate fingerprint shown there to this section in your configuration file and retest.

CAUTION: Every Service Interface configured here MUST be referenced by an MSI value in the FTPListenerConfig section. If a configuration exists in this section but is not referenced, the FTP server will not start.

Parameter	Description
IP	IP address of the host that is running the MessageWay Service Interface (SI).
Port	Port where the SI is listening.
Security	Security type. Non-secure listeners must be set to **None**. Secure listeners must be set to **SSL** or **TLS**. Valid values: ▪ **None** ▪ **SSL** ▪ **TLS**
CertVerifyFile	Fully qualified file name (path and file name) of the certificate file on the FTP Server that is used to verify the certificate file sent to the FTP server by the Service Interface to establish a secure connection. Use either the CertVerifyFile parameter or the CertFingerprint parameter. This value should be blank if not used. **CAUTION:** Do not delete this parameter.
CertFingerprint	SHA1 or MD5 digest of the certificate. Use either the CertVerifyFile parameter or the CertFingerprint parameter. This value should be blank if not used. **CAUTION:** Do not delete this parameter.

Parameter	Description
ConnectionTimeout	Number of seconds the FTP Server waits for a connection to the SI.
RequestTimeout	Number of seconds the FTP Server waits for a request from the SI.
Trace	Allows a trace of the MWSI session. Valid values include any combination of: ▪ **http** ▪ **http-body**
ClientCertFile	Fully qualified file name of the client certificate file on the FTP server. That certificate is used by the MessageWay Service Interface to identify the FTP server as a trusted authentication agent. This is required when ftp "anonymous" user access is used.
ClientKeyFile	Fully qualified file name of the private key that is used to identify the SFTP server. Required if ClientCertFile is provided.
ClientKeyPassphrase	Pass phrase to use if the ClientKeyFile is encrypted.
AuthAgent	Name of the trusted authentication agent as identified by the Common Name on the client certificate. This name must match the Common Name that is stored in the ClientCertFile and must be included in the MWSI agents file (i.e. trusted by MWSI).

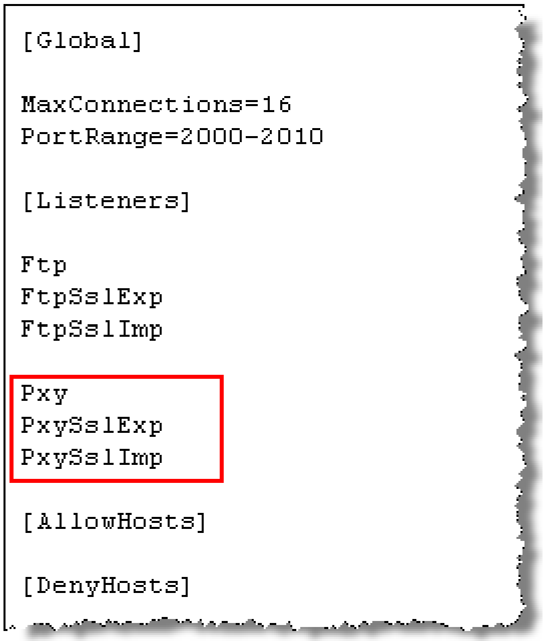
Configuring the FTP Perimeter Server Acting As A Proxy

Users may set a port on the FTP perimeter server to function as a proxy server. The server acts initially as a server when the port receives commands from a MessageWay FTP adapter. It then functions as a client and forwards the commands to and handles responses from an external server.

You must also ***configure an FTP location*** (on page 238) that will communicate with the proxy server port.

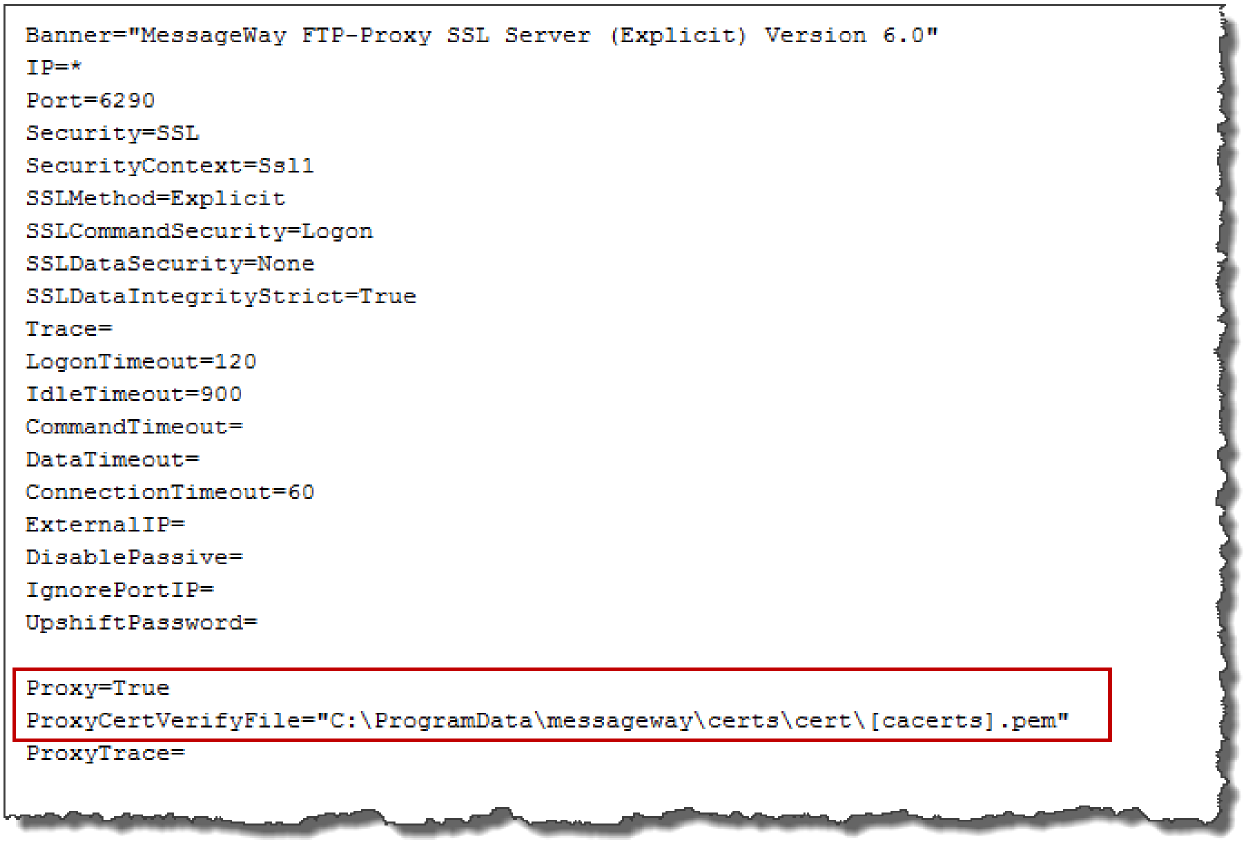
To configure a listener to function as an FTP proxy, in addition to the normal settings for your FTP server, do the following in the FTP configuration file, mwftpd.conf:

1 In the Listeners Section, identify a listener, such as, ***Pxy, PxySslExp or PxySslImp*** (on page 227), depending on whether or not you want security and what type.



```
[Global]

MaxConnections=16
PortRange=2000-2010

[Listeners]

Ftp
FtpSslExp
FtpSslImp

Pxy
PxySslExp
PxySslImp

[AllowHosts]

[DenyHosts]
```

2 To use a certificate to verify the client, identify the location and file name of the certificate file or bundle in the parameter, ProxyCertVerifyFile. Alternatively, if you use a fingerprint, you would configure that on the **Proxy** tab of the FTP site.



```
Banner="MessageWay FTP-Proxy SSL Server (Explicit) Version 6.0"
IP=*
Port=6290
Security=SSL
SecurityContext=Ssl1
SSLMethod=Explicit
SSLCommandSecurity=Logon
SSLDataSecurity=None
SSLDataIntegrityStrict=True
Trace=
LogonTimeout=120
IdleTimeout=900
CommandTimeout=
DataTimeout=
ConnectionTimeout=60
ExternalIP=
DisablePassive=
IgnorePortIP=
UpshiftPassword=

Proxy=True
ProxyCertVerifyFile="C:\ProgramData\messageway\certs\cert\[cacerts].pem"
ProxyTrace=
```

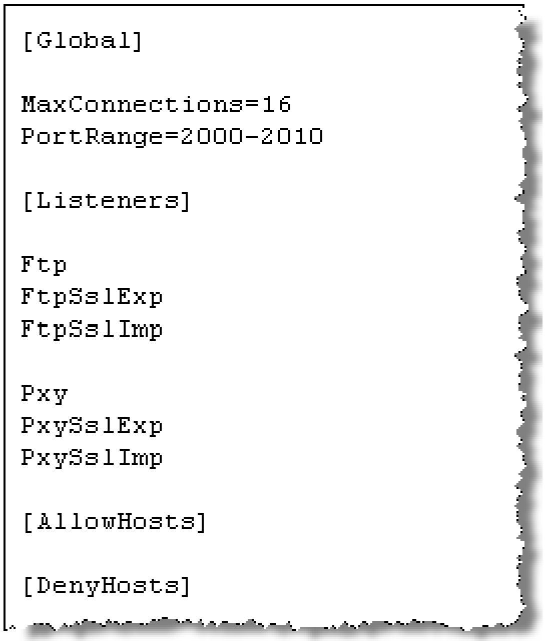
IMPORTANT: the ***example configurations*** (on page 227) do not use the SI parameter, because the proxy server function does not require the MessageWay Service Interface (SI). It also does not use AccessClass, NonStopCompat or MessageNameFormat parameters.

Examples of Configurations for the FTP Perimeter Server

These examples show the configurations that permit the FTP perimeter server running on a Windows system to negotiate external connection and data transfer requests. They also show configurations that allow it to function as a proxy server. These configurations are for initial testing only.

FTP Server, Global, Listeners, AllowHosts, DenyHosts Examples

The following part of the file shows the first four sections: Global, Listeners, AllowHosts and DenyHosts. Notice that there are no entries in the latter two, which means that anyone can connect to the FTP server.



```
[Global]

MaxConnections=16
PortRange=2000-2010

[Listeners]

Ftp
FtpSslExp
FtpSslImp

Pxy
PxySslExp
PxySslImp

[AllowHosts]

[DenyHosts]
```

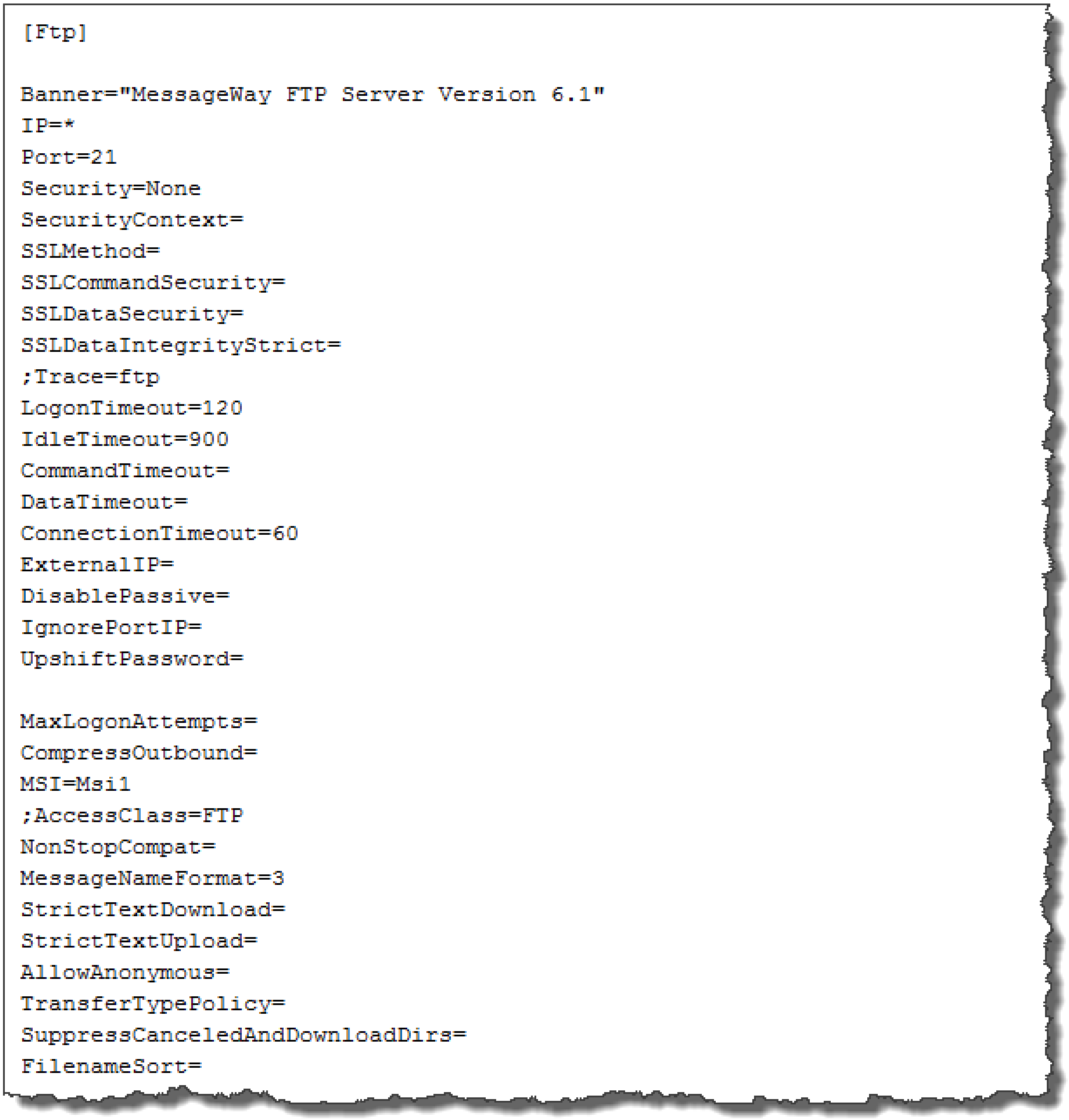
FTP Server, Listener Configurations Examples

This example configures the listener called Ftp, listed previously in the Listeners section. This is the default, non-secure listener that listens on port 21. For testing, we often use port 2121 to avoid conflict with any other FTP listener that might already use the default port, 21. It is pointing to a configuration for the MessageWay Service Interface, Msi1, which appears later in this file. Note that the example assigns 3, filename, to the MessageNameFormat parameter. This is also where you would allow anonymous access to MessageWay.

IMPORTANT: MessageWay allows duplicate file names. Internally this is not a problem, because MessageWay always assigns a unique message ID to a message, whether the user chooses to display it or not. So for messages in locations that are defined in the Locations folder, when users download files, there may be more than one file of the same name. Users should take care to make sure that duplicate file names will not cause a problem for their local system. If there could be a problem, it would be wise to always include the message ID as part of the message name. This will also help troubleshooting, because the message ID includes a date and time stamp. For messages in locations defined in the File System folder, duplicate file names are not displayed or not allowed, depending on the command. If a file name exists in a directory (location) in the File System folder and a client attempts to upload a new file of the same name, the original message is canceled, and then the new file is uploaded. Clients viewing a File System directory structure cannot see canceled or downloaded messages.

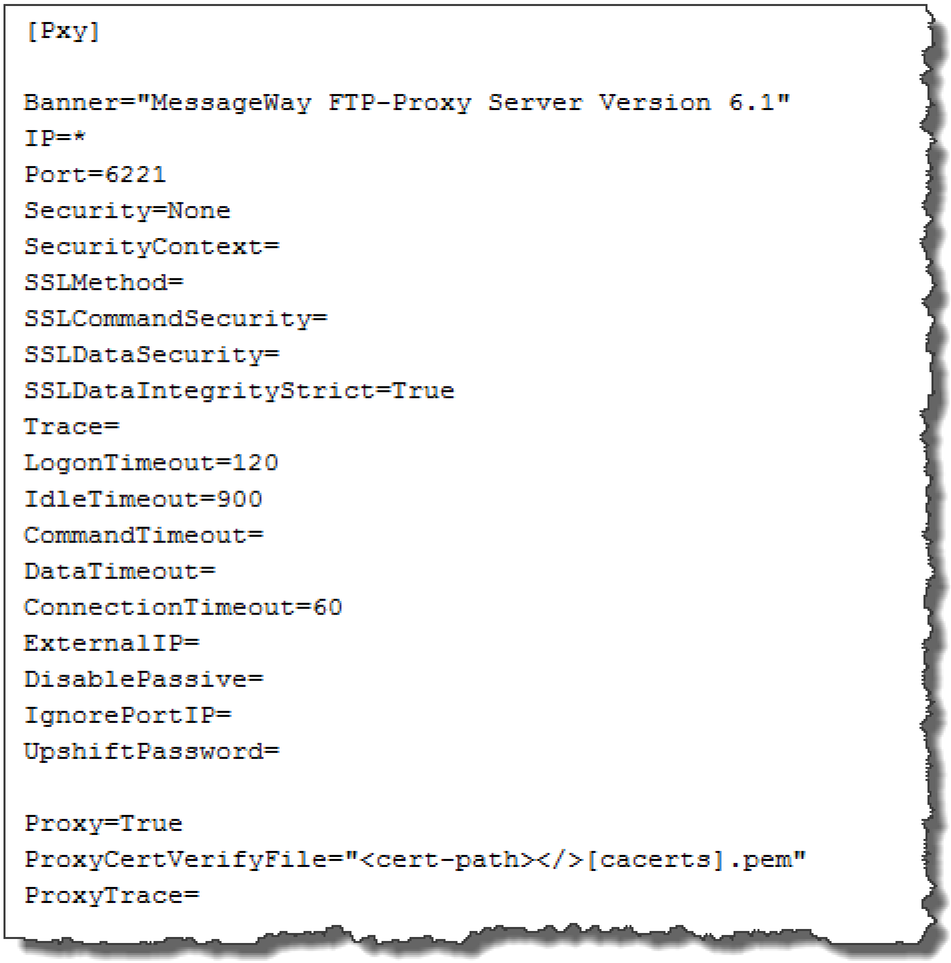
Note the following:

- When both *CommandTimeout* and *DataTimeout* are set to zero, the server never terminates the connection: the connection is, in effect, infinite.
- Compressed files are not renamed, so users should change the extension to ZIP (Windows) or GZ (UNIX/Linux) after the file reaches its destination.



```
[Ftp]

Banner="MessageWay FTP Server Version 6.1"
IP=*
Port=21
Security=None
SecurityContext=
SSLMethod=
SSLCommandSecurity=
SSLDataSecurity=
SSLDataIntegrityStrict=
;Trace=ftp
LogonTimeout=120
IdleTimeout=900
CommandTimeout=
DataTimeout=
ConnectionTimeout=60
ExternalIP=
DisablePassive=
IgnorePortIP=
UpshiftPassword=

MaxLogonAttempts=
CompressOutbound=
MSI=Msi1
;AccessClass=FTP
NonStopCompat=
MessageNameFormat=3
StrictTextDownload=
StrictTextUpload=
AllowAnonymous=
TransferTypePolicy=
SuppressCanceledAndDownloadDirs=
FilenameSort=
```

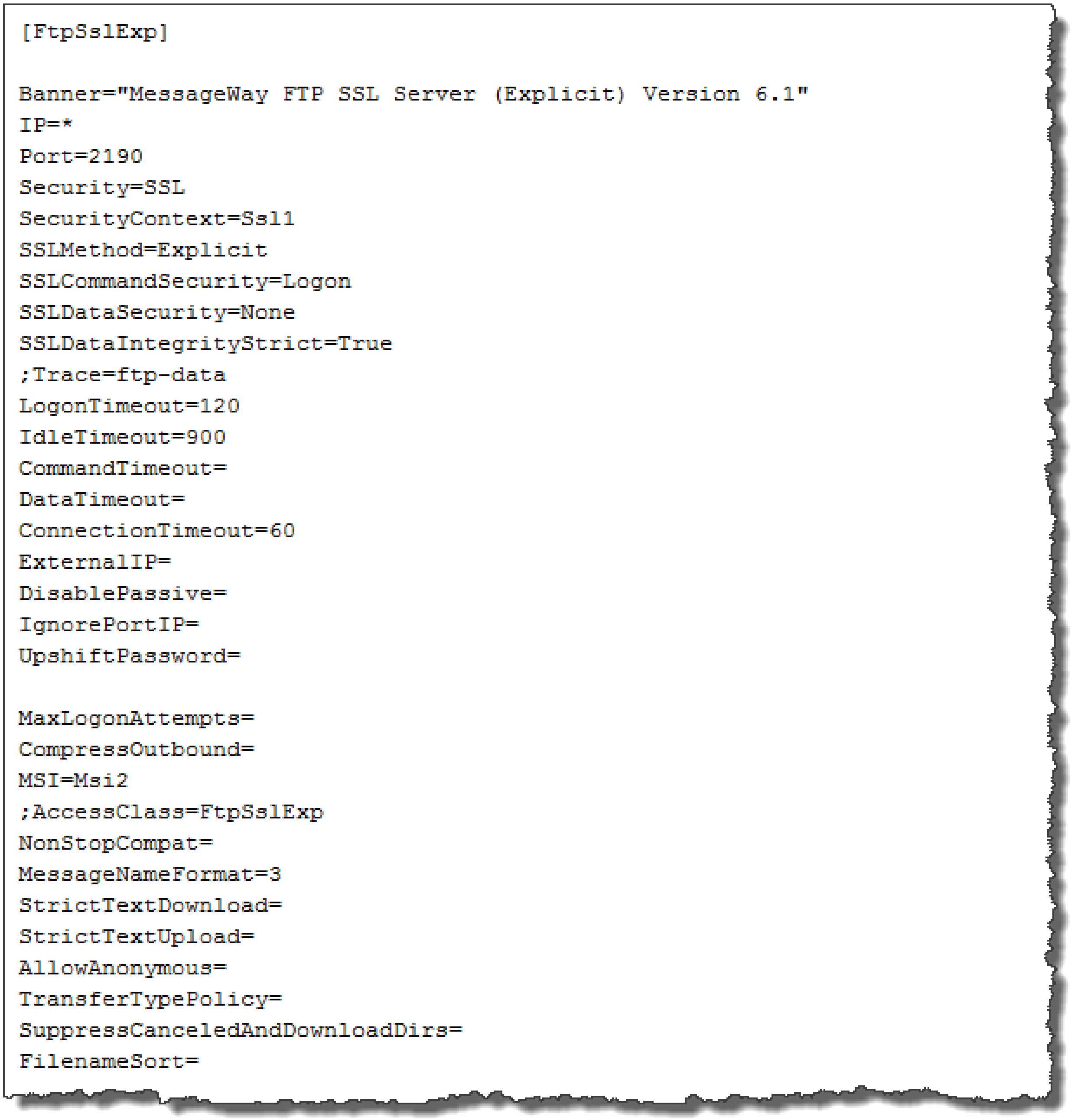
This example configures the listener called Pxy, listed previously in the Listeners section, to function as a proxy client. This is the default, non-secure listener that listens on port 6221. The proxy server does not require access to the Service Interface, so there is no MSI parameter.



```
[Pxy]

Banner="MessageWay FTP-Proxy Server Version 6.1"
IP=*
Port=6221
Security=None
SecurityContext=
SSLMethod=
SSLCommandSecurity=
SSLDataSecurity=
SSLDataIntegrityStrict=True
Trace=
LogonTimeout=120
IdleTimeout=900
CommandTimeout=
DataTimeout=
ConnectionTimeout=60
ExternalIP=
DisablePassive=
IgnorePortIP=
UpshiftPassword=

Proxy=True
ProxyCertVerifyFile="<cert-path></>[cacerts].pem"
ProxyTrace=
```

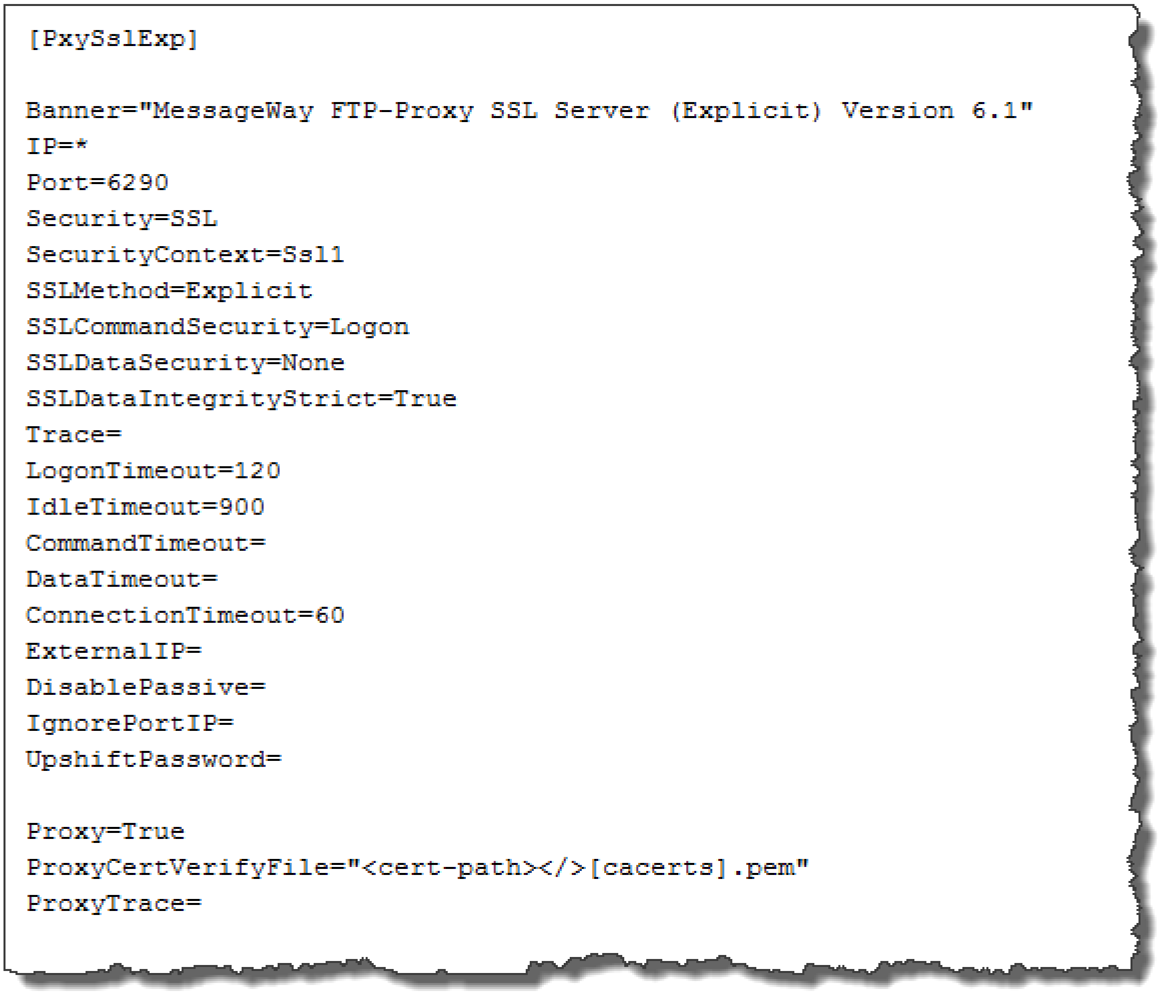
This example configures the listener called FtpSslExp, listed previously in the Listeners section. This is the explicit secure listener that listens on port 2190. It points to a configuration for the SSL security context, Ssl1 and to a configuration for the MessageWay Service Interface, Msi2. Both appear later in this file.

NOTE: Integrity checking (SSLDataIntegrityStrict = True) is set by default to ensure that the entire file has been received.



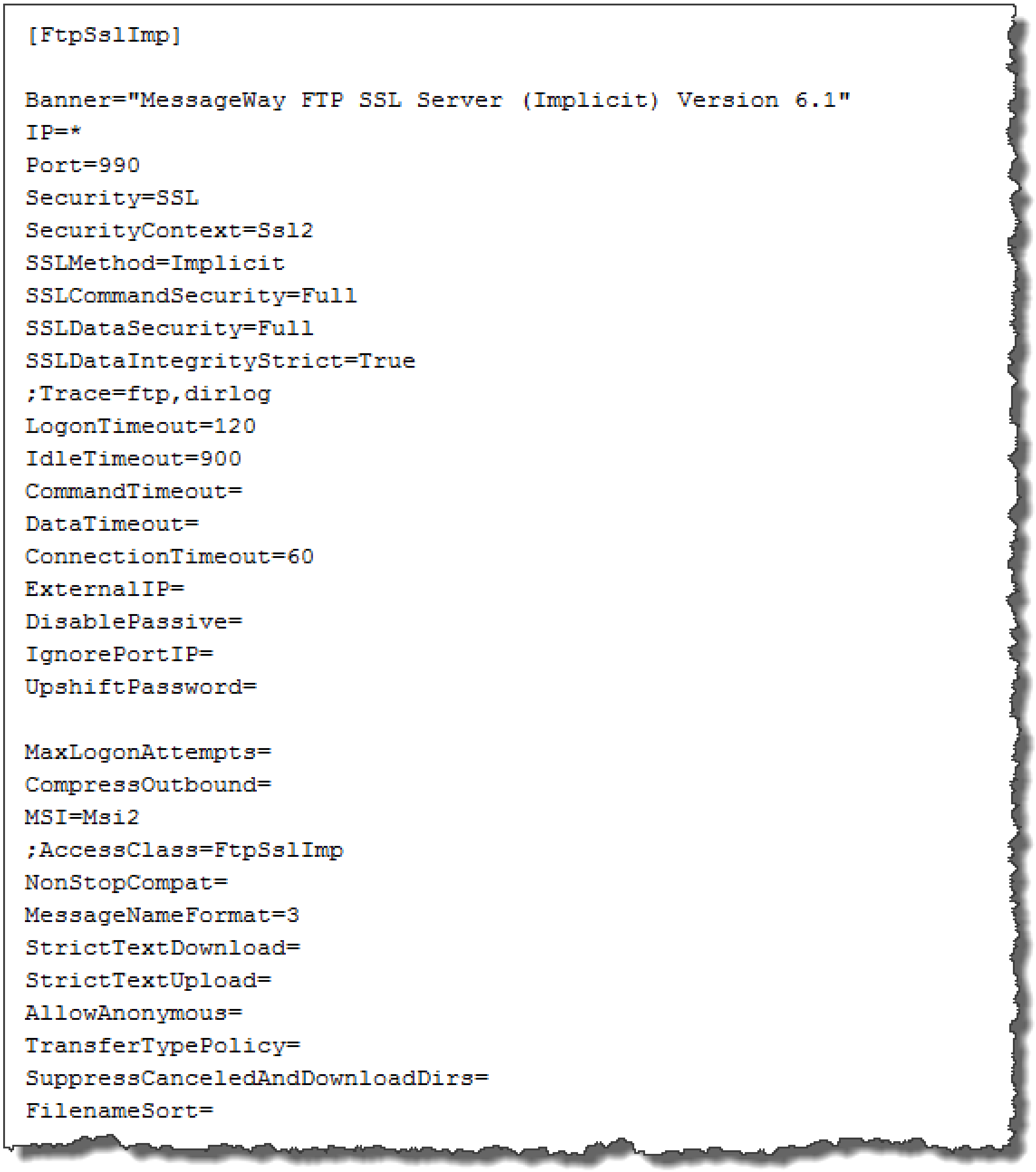
```
[FtpSslExp]

Banner="MessageWay FTP SSL Server (Explicit) Version 6.1"
IP=*
Port=2190
Security=SSL
SecurityContext=Ssl1
SSLMethod=Explicit
SSLCommandSecurity=Logon
SSLDataSecurity=None
SSLDataIntegrityStrict=True
;Trace=ftp-data
LogonTimeout=120
IdleTimeout=900
CommandTimeout=
DataTimeout=
ConnectionTimeout=60
ExternalIP=
DisablePassive=
IgnorePortIP=
UpshiftPassword=

MaxLogonAttempts=
CompressOutbound=
MSI=Msi2
;AccessClass=FtpSslExp
NonStopCompat=
MessageNameFormat=3
StrictTextDownload=
StrictTextUpload=
AllowAnonymous=
TransferTypePolicy=
SuppressCanceledAndDownloadDirs=
FilenameSort=
```

This example configures the listener called PxySslExp, listed previously in the Listeners section, to function as a proxy client. This is the explicit secure listener that listens on port 6290. It points to a configuration for the SSL security context, Ssl1. The proxy server does not require access to the Service Interface, so there is no MSI parameter.



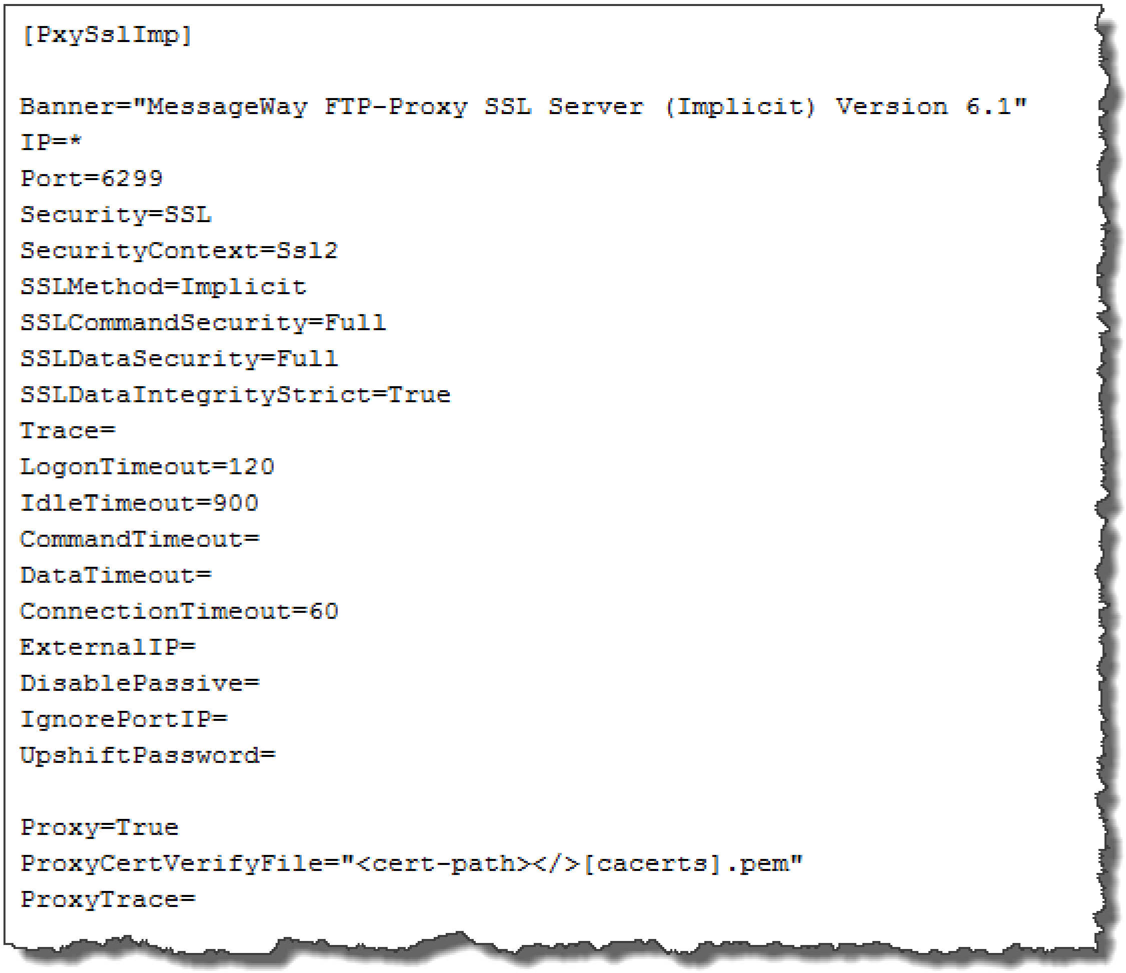
```
[PxySslExp]

Banner="MessageWay FTP-Proxy SSL Server (Explicit) Version 6.1"
IP=*
Port=6290
Security=SSL
SecurityContext=Ssl1
SSLMethod=Explicit
SSLCommandSecurity=Logon
SSLDataSecurity=None
SSLDataIntegrityStrict=True
Trace=
LogonTimeout=120
IdleTimeout=900
CommandTimeout=
DataTimeout=
ConnectionTimeout=60
ExternalIP=
DisablePassive=
IgnorePortIP=
UpshiftPassword=

Proxy=True
ProxyCertVerifyFile="<cert-path></>[cacerts].pem"
ProxyTrace=
```

This example configures the listener called FtpSslImp, listed previously in the Listeners section. This is the default, implicit secure listener that listens on port 990. It points to a configuration for the SSL security context, Ssl2 and to a configuration for the MessageWay Service Interface, Msi2. Both appear later in this file.



```
[FtpSslImp]

Banner="MessageWay FTP SSL Server (Implicit) Version 6.1"
IP=*
Port=990
Security=SSL
SecurityContext=Ssl2
SSLMethod=Implicit
SSLCommandSecurity=Full
SSLDataSecurity=Full
SSLDataIntegrityStrict=True
;Trace=ftp,dirlog
LogonTimeout=120
IdleTimeout=900
CommandTimeout=
DataTimeout=
ConnectionTimeout=60
ExternalIP=
DisablePassive=
IgnorePortIP=
UpshiftPassword=

MaxLogonAttempts=
CompressOutbound=
MSI=Msi2
;AccessClass=FtpSslImp
NonStopCompat=
MessageNameFormat=3
StrictTextDownload=
StrictTextUpload=
AllowAnonymous=
TransferTypePolicy=
SuppressCanceledAndDownloadDirs=
FilenameSort=
```

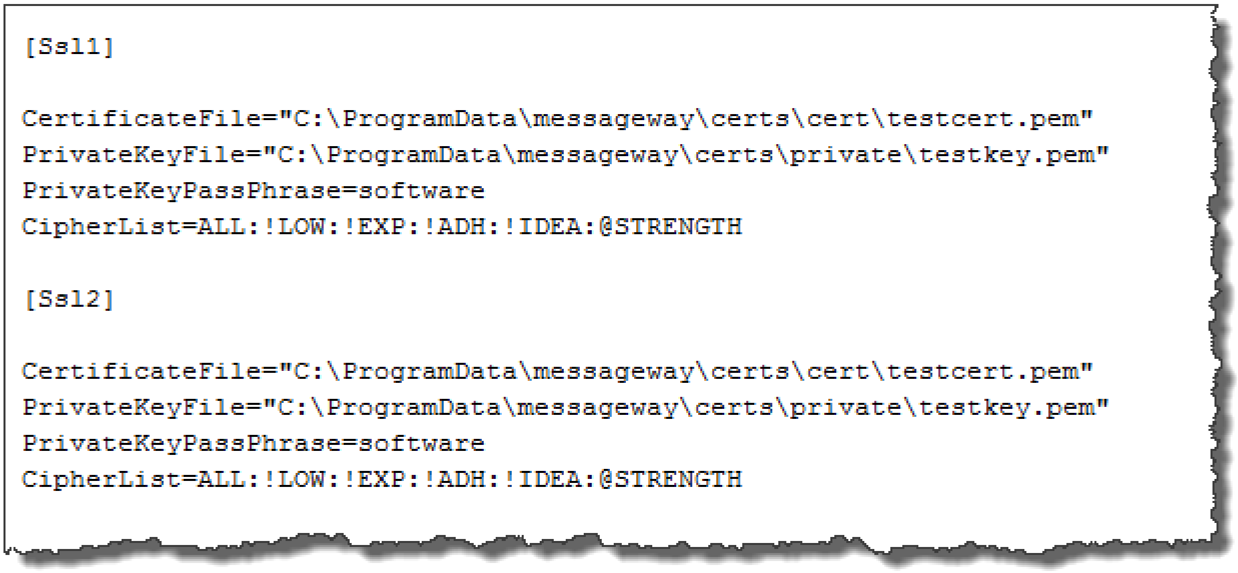
This example configures the listener called PxySslImp, listed previously in the Listeners section, to function as a proxy client. This is the default, implicit secure listener that listens on port 6299. It points to a configuration for the SSL security context, Ssl2. The proxy server does not require access to the Service Interface, so there is no MSI parameter.



```
[PxySslImp]

Banner="MessageWay FTP-Proxy SSL Server (Implicit) Version 6.1"
IP=*
Port=6299
Security=SSL
SecurityContext=Ssl2
SSLMethod=Implicit
SSLCommandSecurity=Full
SSLDataSecurity=Full
SSLDataIntegrityStrict=True
Trace=
LogonTimeout=120
IdleTimeout=900
CommandTimeout=
DataTimeout=
ConnectionTimeout=60
ExternalIP=
DisablePassive=
IgnorePortIP=
UpshiftPassword=

Proxy=True
ProxyCertVerifyFile="<cert-path></>[cacerts].pem"
ProxyTrace=
```

FTP Server, Security Context Configurations Examples

This section contains the security context, Ssl1, for SSL and the security context, Ssl2, for the SSL Implicit port. They are referenced in the sections FtpSslExp, PxySslExp, FtpSslImp and PxySslImp. This section specifies the security files required to communicate with FTP clients. These files are installed with the FTP Server. Together with the default FTP configuration file with these default settings, users can test a secure connection with no further configuration.



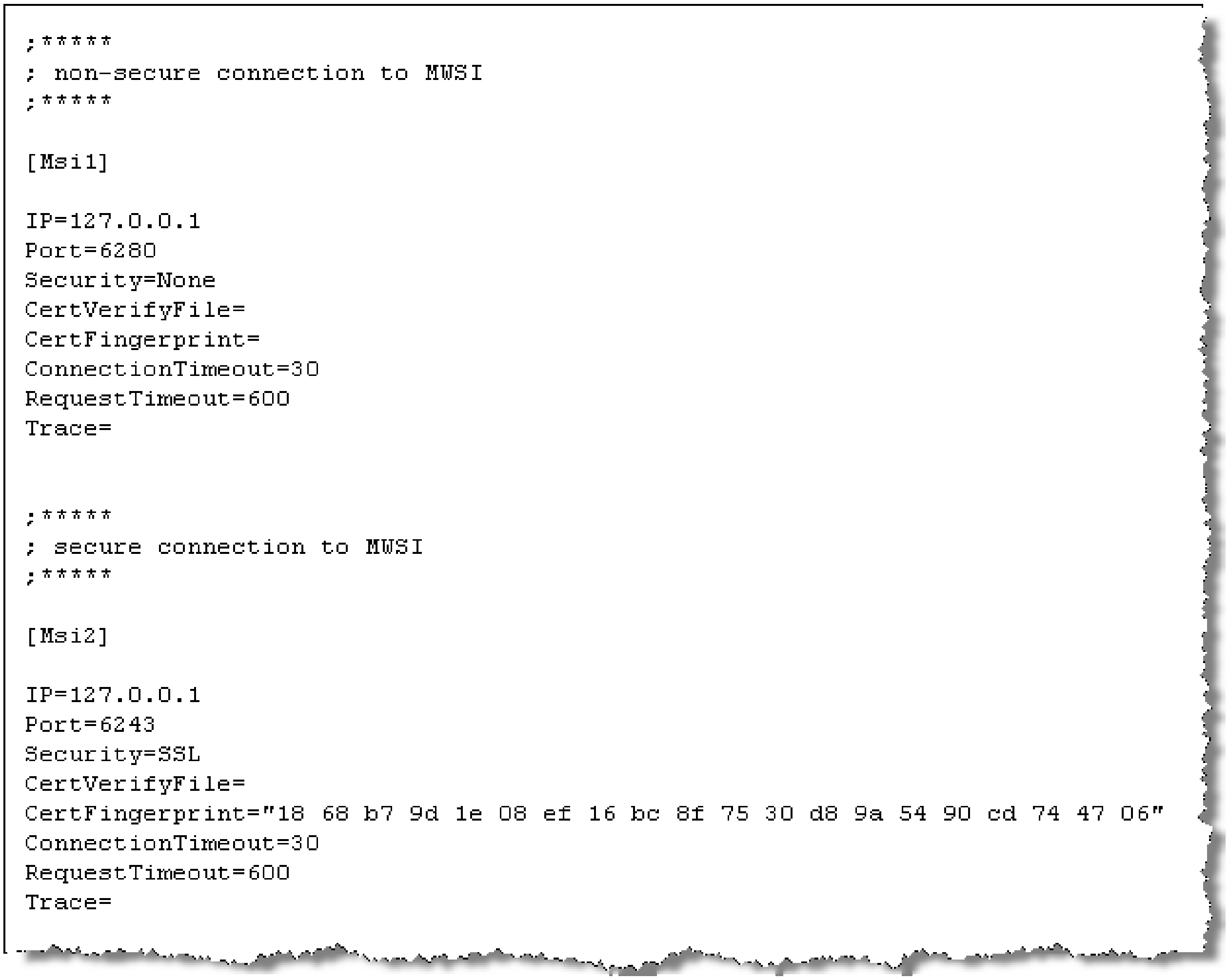
```
[Ssl1]

CertificateFile="C:\ProgramData\messageway\certs\cert\testcert.pem"
PrivateKeyFile="C:\ProgramData\messageway\certs\private\testkey.pem"
PrivateKeyPassPhrase=software
CipherList=ALL:!LOW:!EXP:!ADH:!IDEA:@STRENGTH

[Ssl2]

CertificateFile="C:\ProgramData\messageway\certs\cert\testcert.pem"
PrivateKeyFile="C:\ProgramData\messageway\certs\private\testkey.pem"
PrivateKeyPassPhrase=software
CipherList=ALL:!LOW:!EXP:!ADH:!IDEA:@STRENGTH
```

FTP Server, Service Interface Configuration Examples

This section provides the FTP server with the information to connect to the MessageWay Service Interface (SI). The first section, Msi1, connects with the non-secure HTTP port, 6280. For testing purposes, it is also using the loopback IP address, 127.0.0.1, to point to the SI.

The second section, Msi2, connects with the secure HTTPS port, 6243. This section references the security files required to communicate with SI. The security files installed with SI, which is installed with the MessageWay Server, work with a fingerprint, shown here. Together with the default settings in the SI configuration file, users can test a secure connection with no further configuration.

CAUTION: When you reinstall or upgrade the MessageWay FTP Server, your configuration file is not replaced. However, when you reinstall or upgrade the MessageWay Server, the default certificates for the Service Interface may be replaced. Whenever SI certificates are replaced, the fingerprint shown here must be changed to match the new SI certificates. In the case where the SI files do not match the fingerprint, you will receive an application error, 7011, which is visible in the Events Viewer on Windows or the Event log on UNIX/Linux. Simply copy the peer certificate fingerprint shown there to this section in your configuration file and retest.



```
;*****
; non-secure connection to MWSI
;*****

[Msi1]

IP=127.0.0.1
Port=6280
Security=None
CertVerifyFile=
CertFingerprint=
ConnectionTimeout=30
RequestTimeout=600
Trace=


;*****
; secure connection to MWSI
;*****

[Msi2]

IP=127.0.0.1
Port=6243
Security=SSL
CertVerifyFile=
CertFingerprint="18 68 b7 9d 1e 08 ef 16 bc 8f 75 30 d8 9a 54 90 cd 74 47 06"
ConnectionTimeout=30
RequestTimeout=600
Trace=
```

Configuring MessageWay Users and Locations

In order to send and retrieve messages, you must configure users in MessageWay with security to do the tasks you want. You must also configure locations where the messages are stored. Your tasks are as follows:

- To allow users to send messages, configure locations capable of output or pickup
- To allow users to retrieve messages, configure pickup mailboxes
- To access MessageWay through an FTP client, configure remote users
- To set location security, assign users and rights to locations

Configuring Locations for Clients to Send Messages

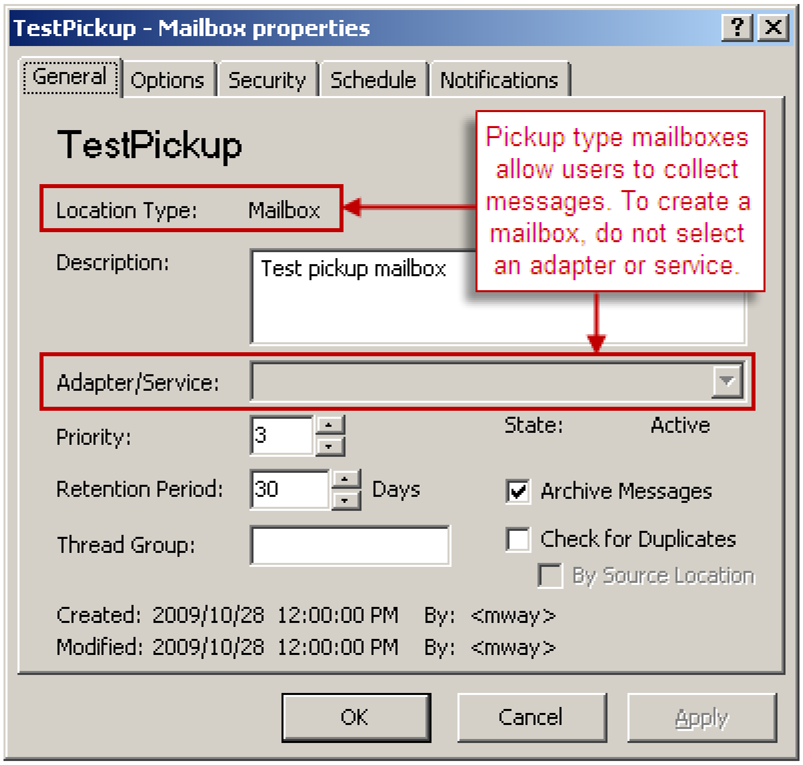
To allow users to send messages to MessageWay through the FTP Perimeter Server, you ***create locations*** (on page 453) in MessageWay to receive the messages. You create different types of locations, depending on whether the FTP client user will access locations in the Locations folder or locations in the File System folder. For more information about the differences between the two, refer to the topic, ***Overview of Location Properties*** (on page 453).

- In the Locations folder, when you create locations to receive messages, they must be of the type I/O, output, service or pickup. They may not be solely an input type.
- In the File System folder, users can only create pickup mailboxes, but MessageWay Manager users can also create service locations.

Configuring a Pickup Mailbox in the Locations Folder

MessageWay allows users to pick up messages from a location through a perimeter server, such as the FTP server, the SFTP server, or the Web Client via the Service Interface, rather than have them delivered by MessageWay through an adapter. To create a pickup type location, you do not specify an adapter or service. For more information about creating locations, refer to the topic, ***Configuring Locations*** (on page 453).

Notice on the **General** page of the Mailbox Properties window, when you do not select an adapter or service, the location type is *Mailbox*. This type of location is often called a pickup mailbox. Notice also that there is no special adapter or service tab.



TestPickup - Mailbox properties

TestPickup

Location Type: Mailbox

Pickup type mailboxes allow users to collect messages. To create a mailbox, do not select an adapter or service.

Description: Test pickup mailbox

Adapter/Service:

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

☐ By Source Location

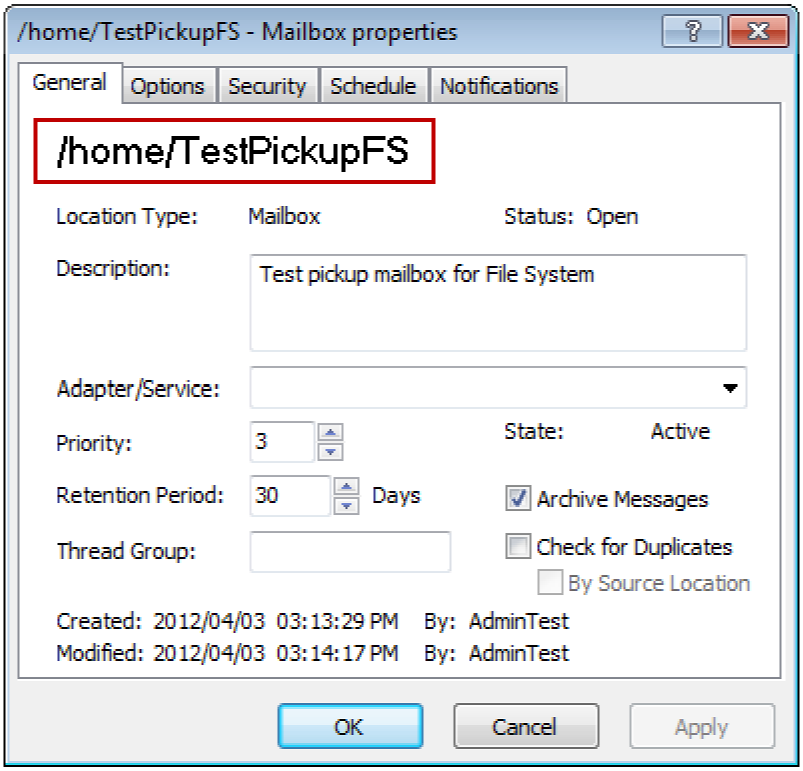
Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/10/28 12:00:00 PM By: <mway>

Configuring a Pickup Mailbox in the File System Folder

When you create a pickup mailbox in the File System folder, you also create a directory node of the same name. The mailbox name will reflect the full pathname of the directory, including slashes.

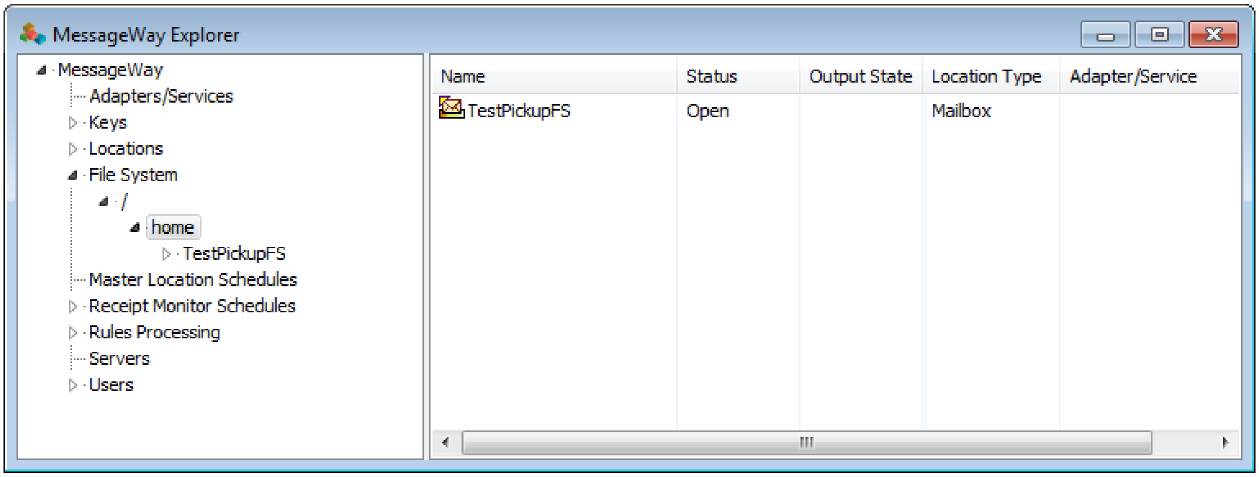
As for locations in the Locations folder, you do not select any adapter or service.



/home/TestPickupFS

Location Type: Mailbox
Status: Open
Description: Test pickup mailbox for File System
Adapter/Service:
Priority: 3
State: Active
Retention Period: 30 Days
☑ Archive Messages
Thread Group:
☐ Check for Duplicates
☐ By Source Location
Created: 2012/04/03 03:13:29 PM By: AdminTest
Modified: 2012/04/03 03:14:17 PM By: AdminTest

Note that the directory structure appears in the left pane of MessageWay Explorer, and the mailbox in the right. To access the properties of the mailbox, you must right-click the mailbox and select **Properties**.



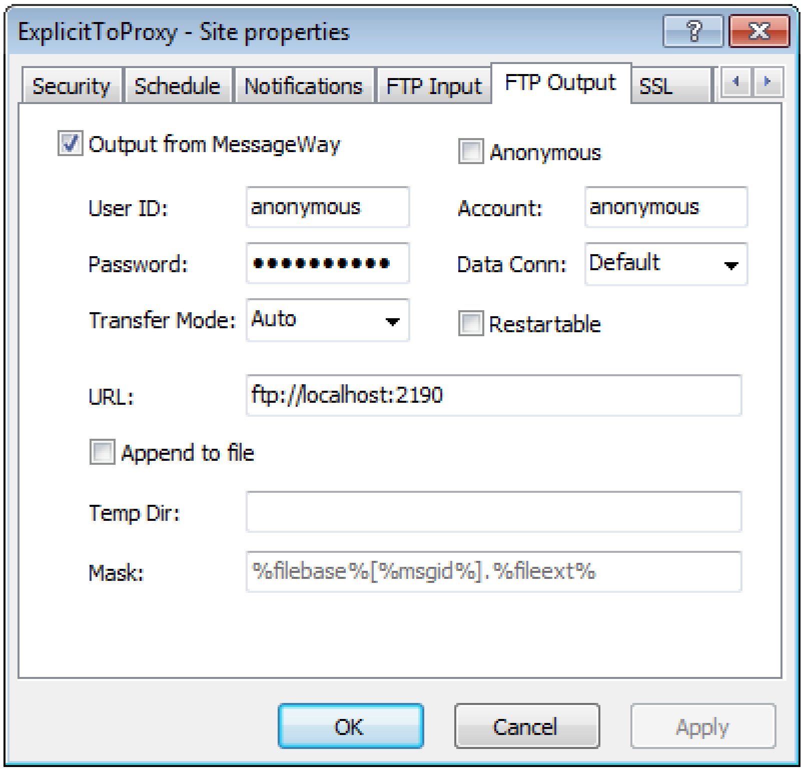
Name	Status	Output State	Location Type	Adapter/Service
TestPickupFS	Open		Mailbox	

Configuring an FTP Site for the Proxy Server

To have an FTP site connect to a proxy server, instead of directly to an external FTP server, you configure parameters on the **Proxy** tab of the location properties window. Note that some of the settings may be inherited from the FTP adapter configurations, visible on the **Proxy** tab of the FTP Adapter Properties window. Proceed as follows:

1 Configure a normal ***FTP Output site*** (on page 605), including any security settings required by the external FTP server, specifically, settings on the **FTP Output** tab and the **SSL** tab.

NOTE: These configurations control the connection between the Proxy Server acting as a client and the external FTP server.



ExplicitToProxy - Site properties

Security | Schedule | Notifications | FTP Input | FTP Output | SSL

☑ Output from MessageWay

☐ Anonymous

User ID: anonymous

Account: anonymous

Password: ●●●●●●●●●●●

Data Conn: Default

Transfer Mode: Auto

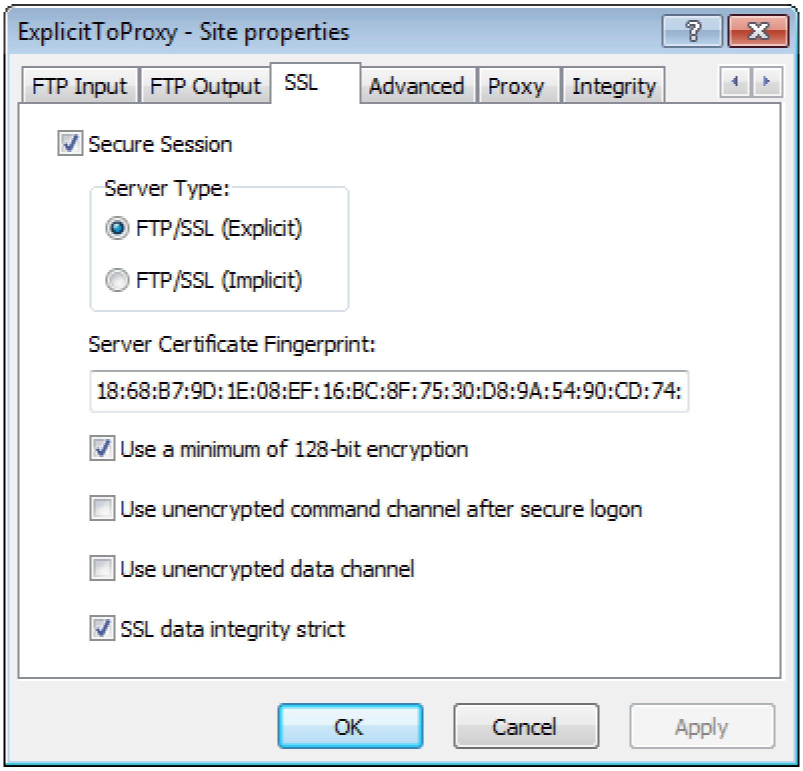
☐ Restartable

URL: ftp://localhost:2190

☐ Append to file

Temp Dir:

Mask: %filebase%[%msgid%].%fileext%



☑ Secure Session

Server Type:

● FTP/SSL (Explicit)

○ FTP/SSL (Implicit)

Server Certificate Fingerprint:

18:68:B7:9D:1E:08:EF:16:BC:8F:75:30:D8:9A:54:90:CD:74:

☑ Use a minimum of 128-bit encryption

□ Use unencrypted command channel after secure logon

□ Use unencrypted data channel

☑ SSL data integrity strict

2 On the **Proxy** tab, check the **Proxy** box.

NOTE: These configurations control the connection between the FTP adapter and the Proxy Server.

3 In the Server box, type the URL and port for the proxy server.

NOTE: The port must be ***defined as a proxy port*** (on page 225) in the FTP configuration file, mwftpd.conf.

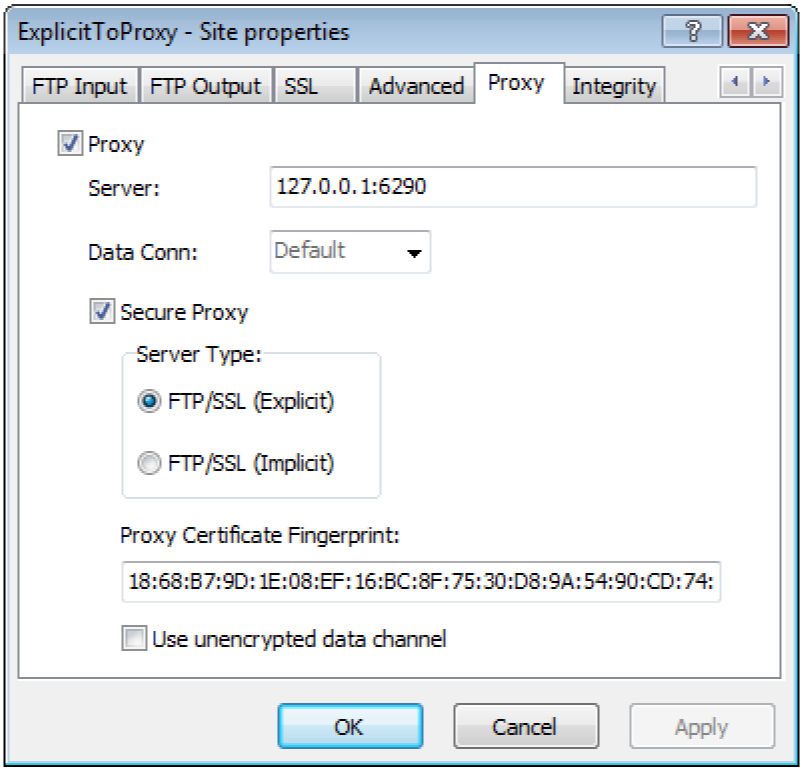
4 To configure a secure connection between the adapter and the proxy server:

a) Check the **Secure Proxy** box.

b) Click the type of data connection, explicit or implicit.

c) To use a fingerprint rather than the certificate itself, enter the fingerprint in the **Proxy Certificate Fingerprint** box.

d) To use an unencrypted data channel, check the box, **Use unencrypted data channel**. The default is an encrypted data channel.



ExplicitToProxy - Site properties

☑ Proxy

Server: 127.0.0.1:6290

Data Conn: Default

☑ Secure Proxy

Server Type:

● FTP/SSL (Explicit)

○ FTP/SSL (Implicit)

Proxy Certificate Fingerprint:

18:68:B7:9D:1E:08:EF:16:BC:8F:75:30:D8:9A:54:90:CD:74:

☐ Use unencrypted data channel

Configuring Remote Users

When given proper security, remote users should be able to pick up (download) messages from MessageWay to their systems and send (upload) messages from their systems to MessageWay locations. Additional rights will allow users to cancel messages.

The user must have a logon ID and password, a default location and the appropriate rights to access necessary locations. To do this, we will take advantage of a user group, which allows us to configure the rights for the user at the group level. For more information about creating users and user groups, refer to the topic, ***Configuring User Security*** (on page 375).

To configure our remote user for testing purposes, proceed as follows:

1 From MessageWay Explorer, modify the Remote Users group to include the right, **Cancel Messages**.

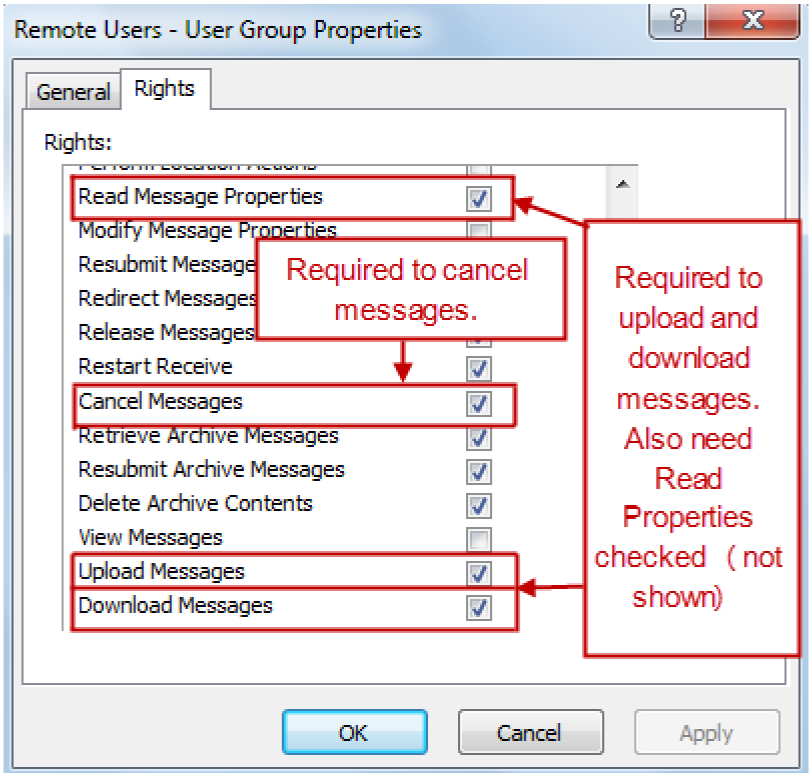
a) In the left pane click **Users** and in the right pane double-click the group, **Remote Users**.

The User Group Properties window appears.

b) Click the **Rights** tab, and in the Rights box, check **Cancel Messages**.

Remote users should typically be able to upload and download messages. When you check the **Download Messages** or **Upload Messages** right in the Rights box for the user group, the other related boxes are automatically checked. For our test, we also want remote users to be able to cancel messages, so we checked **Cancel Messages**.

The following boxes should be checked, at minimum.



Rights:

- Read Message Properties ☑
- Modify Message Properties □
- Resubmit Message
- Redirect Messages
- Release Messages
- Restart Receive ☑
- Cancel Messages ☑
- Retrieve Archive Messages ☑
- Resubmit Archive Messages ☑
- Delete Archive Contents ☑
- View Messages □
- Upload Messages ☑
- Download Messages ☑

Required to cancel messages.

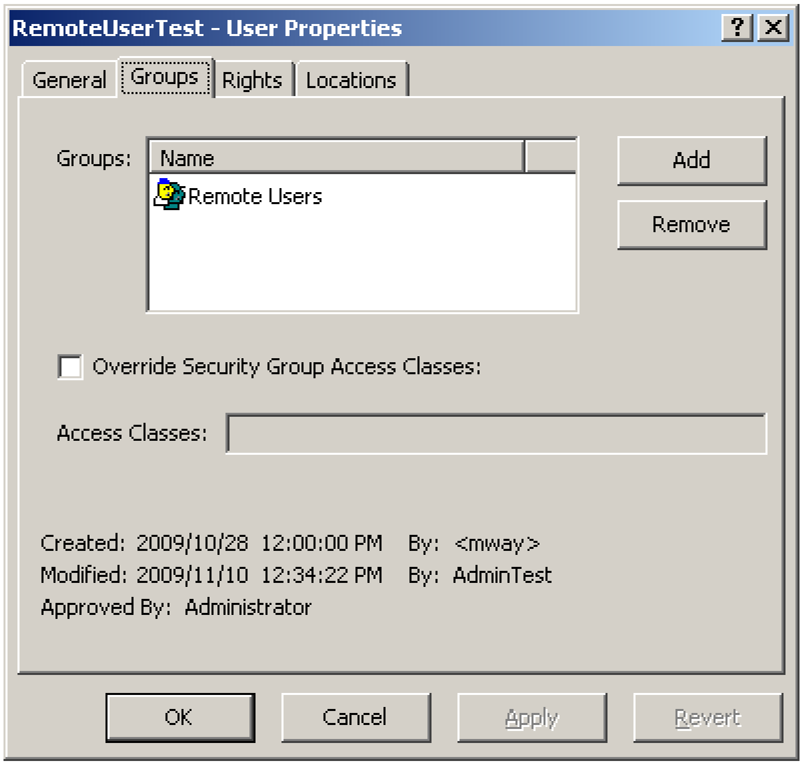
Required to upload and download messages. Also need Read Properties checked (not shown)

2 ***Create a user*** (on page 381) with the following information:

- User ID of **RemoteUserTest** or **RemoteUserTestFS**
- Password of **password**
- Group of **Remote Users**

This is an efficient way to consistently set the rights for users who have common needs. Access classes control user access through the Web Client, the SFTP Server, the FTP Server and the AS2 Interface, but we will ignore them for our test.

Note that the information at the bottom of the page will show when and by whom the entity was created, and when and by whom it was modified. When using the optional ***Maker/Checker feature*** (on page 893), it also shows who approved the changes.



Groups:

Name	
Remote Users	

□ Override Security Group Access Classes:

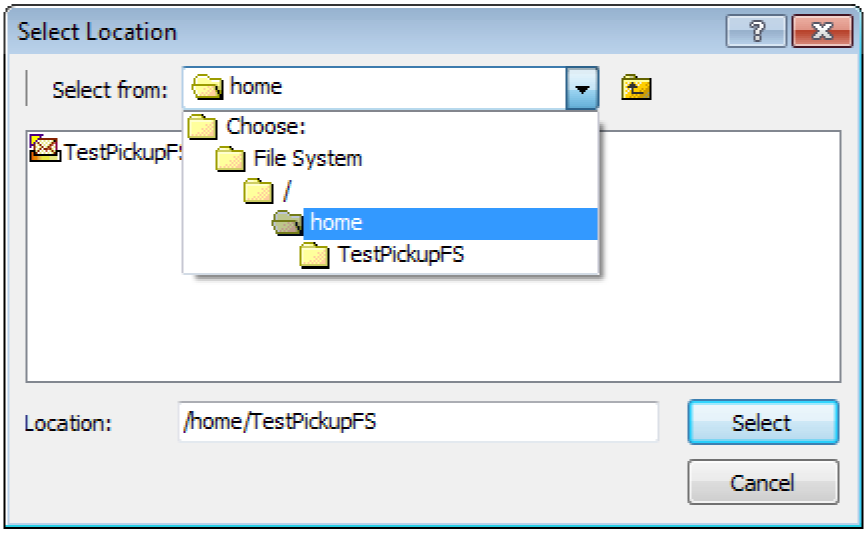
Access Classes:

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/10 12:34:22 PM By: AdminTest
Approved By: Administrator

3 On the Locations tab, add a default location.

- For users whose default location is in the Locations folder, type **TestPickup**
- For users whose default location is in the File System folder, type **TestPickupFS**

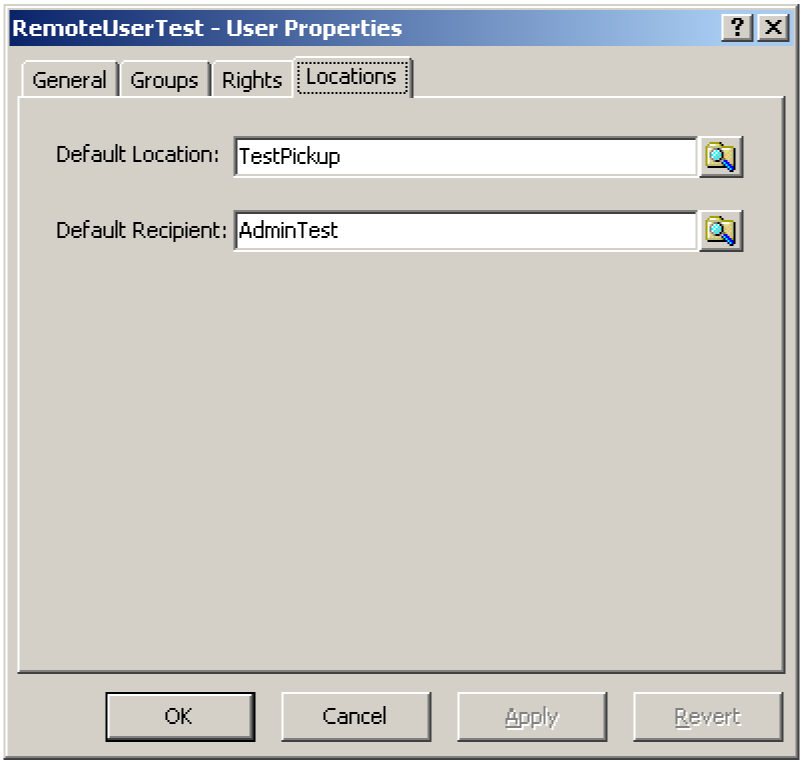
  To browse to locations in the File System folder, click the **Browse** button, and then the down button on the Select from box, and click **Choose**. When the File System folder appears, double click to choose.



Location: /home/TestPickupFS

Each user accessing MessageWay through the Service Interface must be assigned a default location. When the user logs on to MessageWay, the contents of this mailbox displays first. Users may then switch to another location to which they have access. This location also provides the source location for any uploaded messages.

4 Optionally, add a default recipient, to upload messages to a location other then the Default Location. If not provided, messages are uploaded to the Default Location.



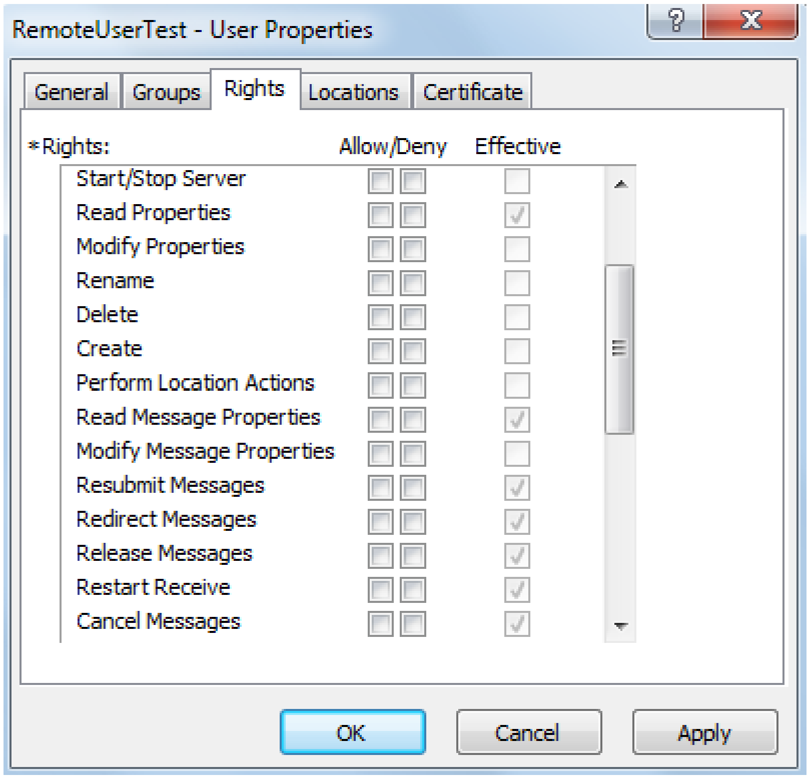
Default Location: TestPickup

Default Recipient: AdminTest

5 Check that at least the user rights are checked as shown here.

The user's rights are the combined rights of all groups to which the user belongs. In this case, the user only belongs to the Remote Users group, whose rights appear in the Effective column on the Rights page of the User Properties window.

TIP: The default rights for the Remote Users group do not include the property *Cancel Messages*. If you have not changed the rights at the group level as suggested previously, you can add that right for your user by checking the *Allow* column.



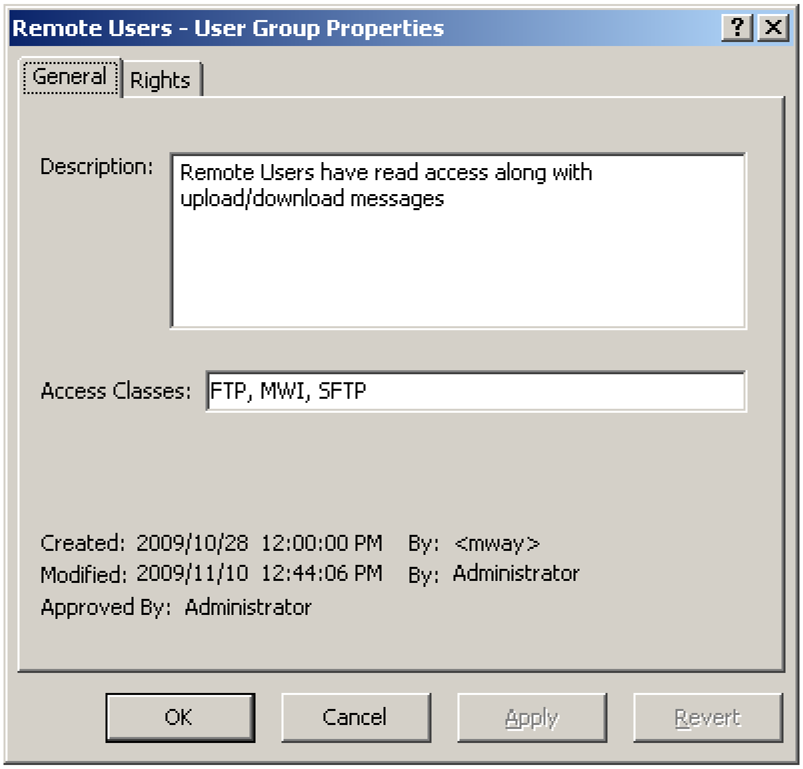
*Rights:	Allow/Deny		Effective
Start/Stop Server	□	□	□
Read Properties	□	□	☑
Modify Properties	□	□	□
Rename	□	□	□
Delete	□	□	□
Create	□	□	□
Perform Location Actions	□	□	□
Read Message Properties	□	□	☑
Modify Message Properties	□	□	□
Resubmit Messages	□	□	☑
Redirect Messages	□	□	☑
Release Messages	□	□	☑
Restart Receive	□	□	☑
Cancel Messages	□	□	☑

Controlling User Access with Access Classes (FTP Server)

To limit the access paths to MessageWay for a user or group of users, you assign an access class. When an access class is set for a user, they will not be able to log on to MessageWay unless the FTP Server configuration file also has that access class listed.

IMPORTANT: Access class names are case-sensitive. They must match the access class names configured in the configuration file for the FTP Server (mwftpd.conf).

Access classes may be assigned to a user group. You do this on the **General** page of the User Group Properties window.

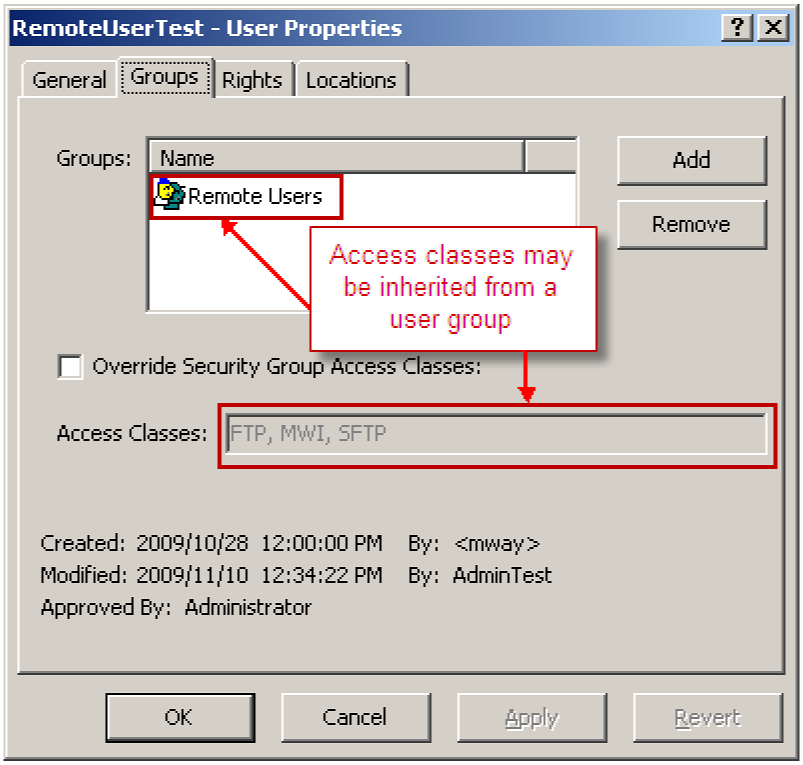


Description: Remote Users have read access along with upload/download messages

Access Classes: FTP, MWI, SFTP

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/10 12:44:06 PM By: Administrator
Approved By: Administrator

This access class is then assigned to users that belong to that group.



Groups:

Name
Remote Users

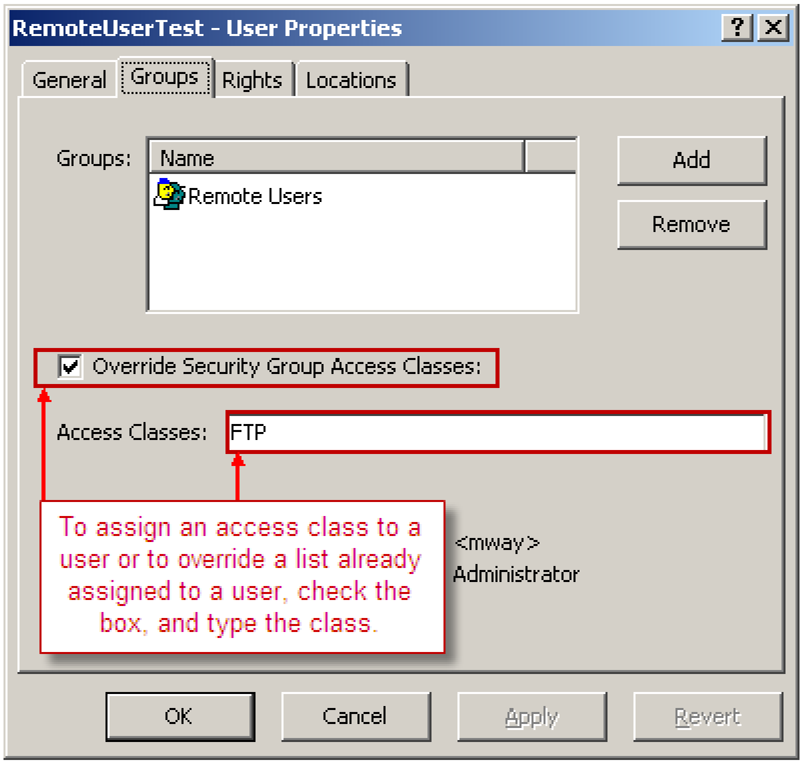
Access classes may be inherited from a user group

☐ Override Security Group Access Classes:

Access Classes: FTP, MWI, SFTP

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/10 12:34:22 PM By: AdminTest
Approved By: Administrator

To assign one or more access classes to a single user or override access classes already assigned to a user, you specify them on the **Groups** page of the User Properties window, separated by commas.

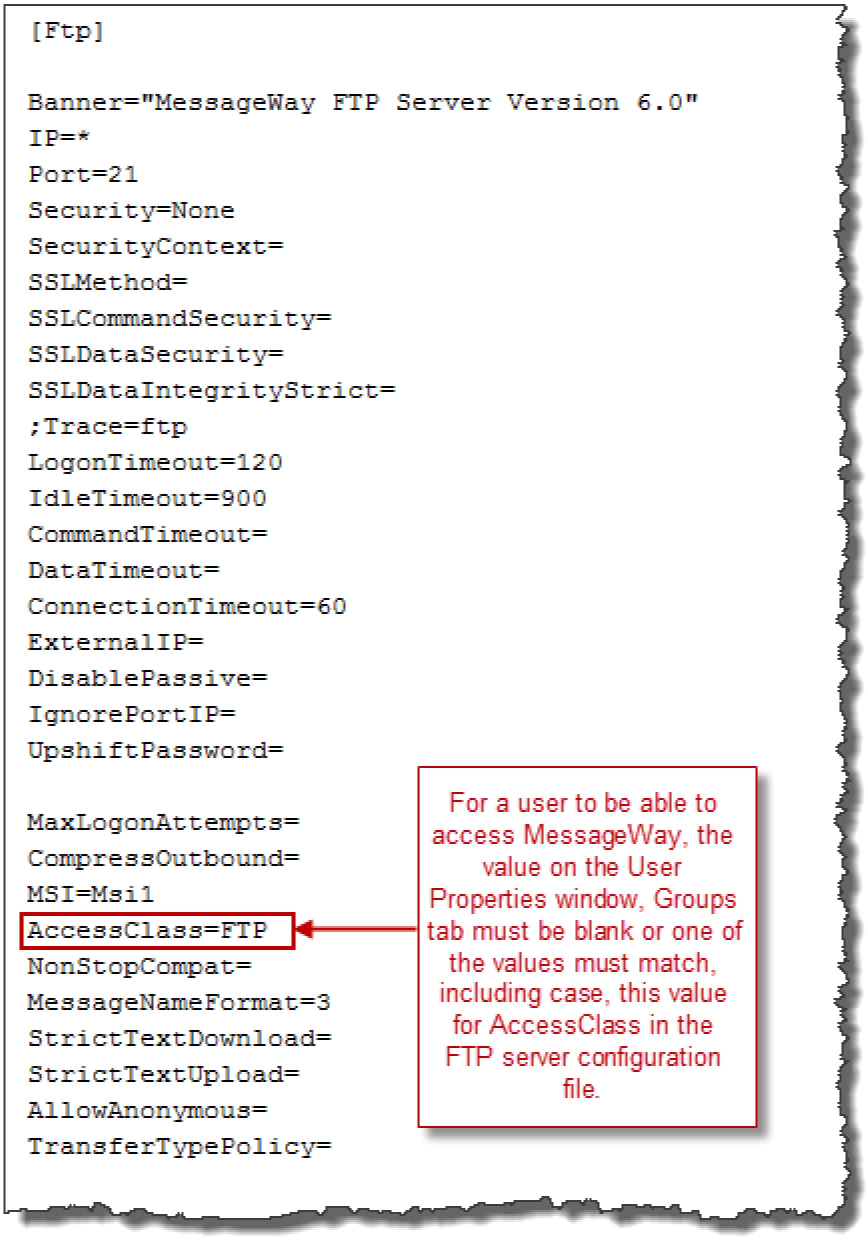


☑ Override Security Group Access Classes:

Access Classes: FTP

To assign an access class to a user or to override a list already assigned to a user, check the box, and type the class.

This access class must be listed in the FTP configuration file, mwftpd.conf. If the access class in the configuration file is blank, then the access class for the user must also be blank. If the access class in the configuration file is not blank, then the access class for the user must either match the access class in the configuration file or be blank.



```
[Ftp]

Banner="MessageWay FTP Server Version 6.0"
IP=*
Port=21
Security=None
SecurityContext=
SSLMethod=
SSLCommandSecurity=
SSLDataSecurity=
SSLDataIntegrityStrict=
;Trace=ftp
LogonTimeout=120
IdleTimeout=900
CommandTimeout=
DataTimeout=
ConnectionTimeout=60
ExternalIP=
DisablePassive=
IgnorePortIP=
UpshiftPassword=

MaxLogonAttempts=
CompressOutbound=
MSI=Msi1
AccessClass=FTP
NonStopCompat=
MessageNameFormat=3
StrictTextDownload=
StrictTextUpload=
AllowAnonymous=
TransferTypePolicy=
```

For a user to be able to access MessageWay, the value on the User Properties window, Groups tab must be blank or one of the values must match, including case, this value for AccessClass in the FTP server configuration file.

Assigning Rights for Locations

Once you have assigned rights to your user, you must make sure that the user is able to access the necessary locations. To do so, you assign appropriate rights to the locations, which are called access lists, that determine who can do what to locations.

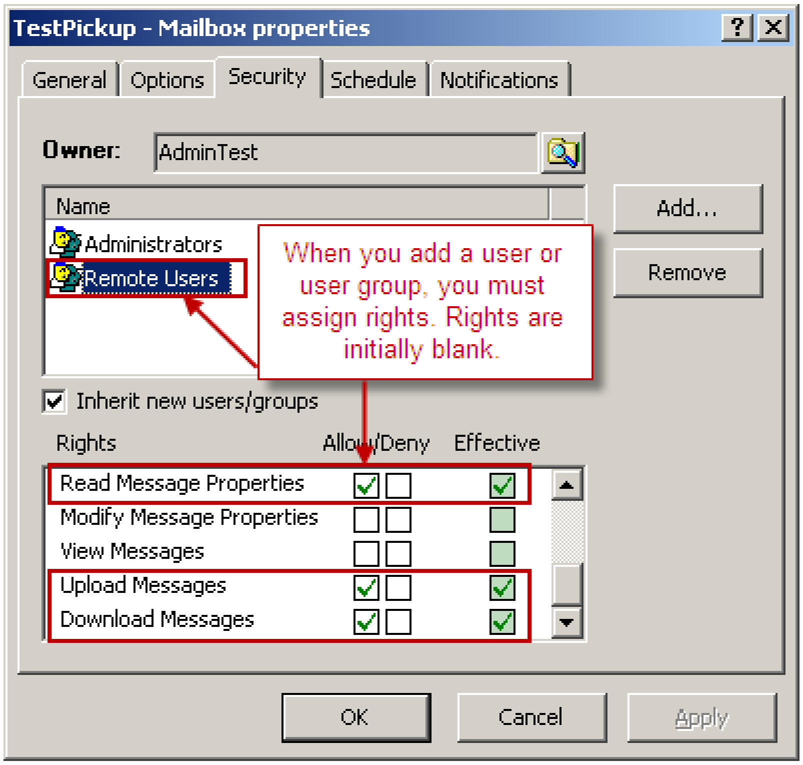
To create an access list, you add user groups or users to the **Names** box and specify the rights in the **Rights** box. You set these rights separately from the rights set for the user. When a user attempts to access a location, the rights of the location are compared with the rights of the user, and only those rights that match are allowed. The user must be a member of one of the listed groups or must be listed separately. For more information, refer to the topic ***Configuring User Security*** (on page 375).

A mailbox is a special type of location that allows users to pickup or collect messages. In the following example, the Remote Users group has been added to the Security page of the mailbox, TestPickUp, and we set the same rights for the mailbox as we set for the Remote Users user group, not all of which are currently visible.

Notice that we had to check the **Allow** boxes for the rights *Upload Messages* and *Download Messages*. This is because the Remote Users group was added to this specific mailbox rather than being inherited from its folder. That is, the Remote Users group is not listed on the **Security** tab of the **Folder** Properties window for the **Locations** folder, so its rights could not be inherited. Had Remote Users group been inherited from the **Locations** folder, this mailbox would have inherited the rights set at the folder level. Since they weren't inherited, we had to specifically set the rights for the mailbox.

Since the rights for our user match the rights for the mailbox, the user will be able to access messages in this mailbox.

IMPORTANT: For users to be able to access messages in locations other than their default mailbox, they must have access rights to those other locations.



Owner: AdminTest

Name
Administrators
Remote Users

When you add a user or user group, you must assign rights. Rights are initially blank.

☑ Inherit new users/groups

Rights	Allow	Deny	Effective
Read Message Properties	☑	□	☑
Modify Message Properties	□	□	□
View Messages	□	□	□
Upload Messages	☑	□	☑
Download Messages	☑	□	☑

Access List for TestPickup Mailbox (Mailbox Properties Window, Security Page)

Configuring Anonymous Access

The MessageWay FTP Perimeter Server may be configured to allow users to log on to MessageWay as anonymous. Proper configuration of MessageWay to do this requires the following:

- ***Define a MessageWay user called*** *anonymous* (on page 250)
- ***Configure the MessageWay FTP server to allow anonymous access*** (on page 254)
- ***Configure the MessageWay Service Interface to allow anonymous access*** (on page 256)
- ***Configure the agents file to allow access for localhost*** (on page 259)

IMPORTANT: After you have finished these tasks, make sure you restart the perimeter server and the ***Service Interface*** (on page 103) so they will read the changed configuration files.

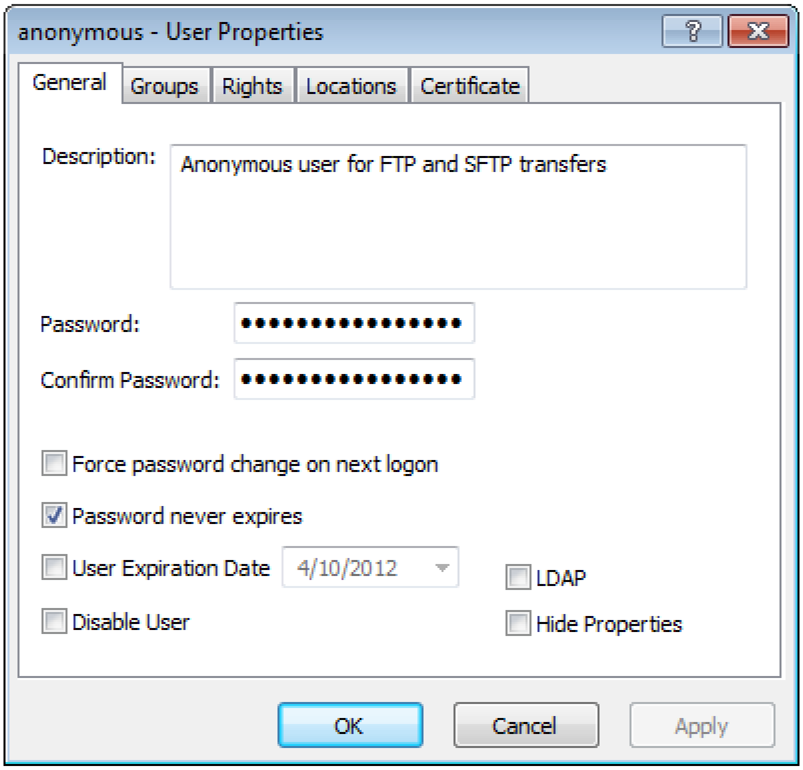
To Define an Anonymous MessageWay FTP or SFTP User

To configure an anonymous user who will access MessageWay from an FTP or SFTP client, proceed as follows:

1 Add a user called **anonymous**.

2 On the **General** page, type a description, a password and choose your password expiration policy.

NOTE: You must enter a password, but it is ignored during an FTP session.



anonymous - User Properties

Description: Anonymous user for FTP and SFTP transfers

Password: ••••••••••••••••

Confirm Password: ••••••••••••••••

□ Force password change on next logon

☑ Password never expires

□ User Expiration Date 4/10/2012

□ LDAP

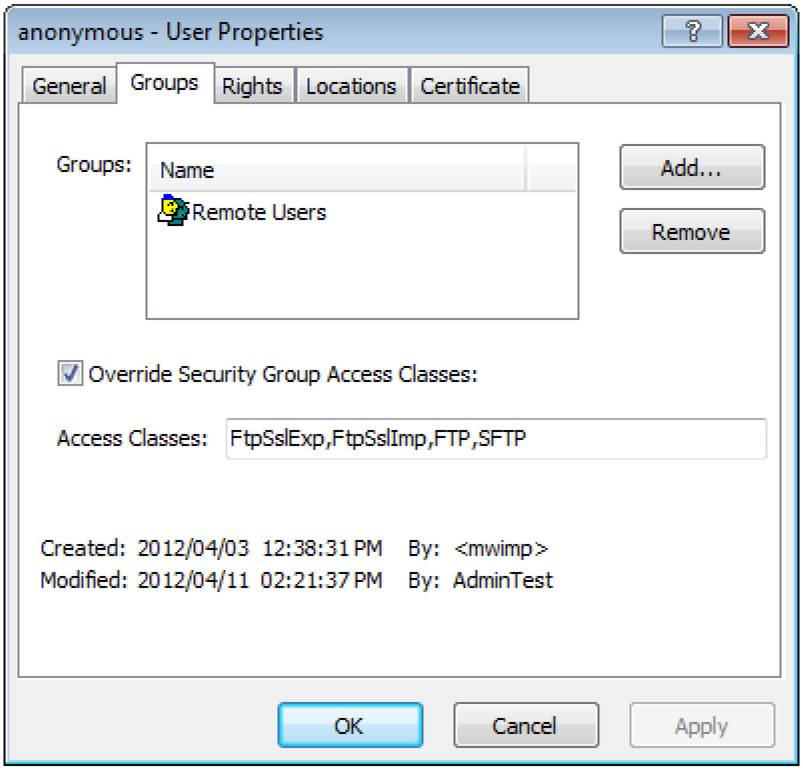
□ Disable User

□ Hide Properties

3 On the **Groups** page, add this user to the *Remote Users* group.

4 Check the Override Security Group Access Classes, and type the access class or classes that you support, separated by commas. They must match *exactly* what you have specified on the FTP server configuration file, mwftpd.conf or on the SFTP server configurations file, mwsftpd.conf.

CAUTION: Access class names are *case-sensitive*.



Groups:

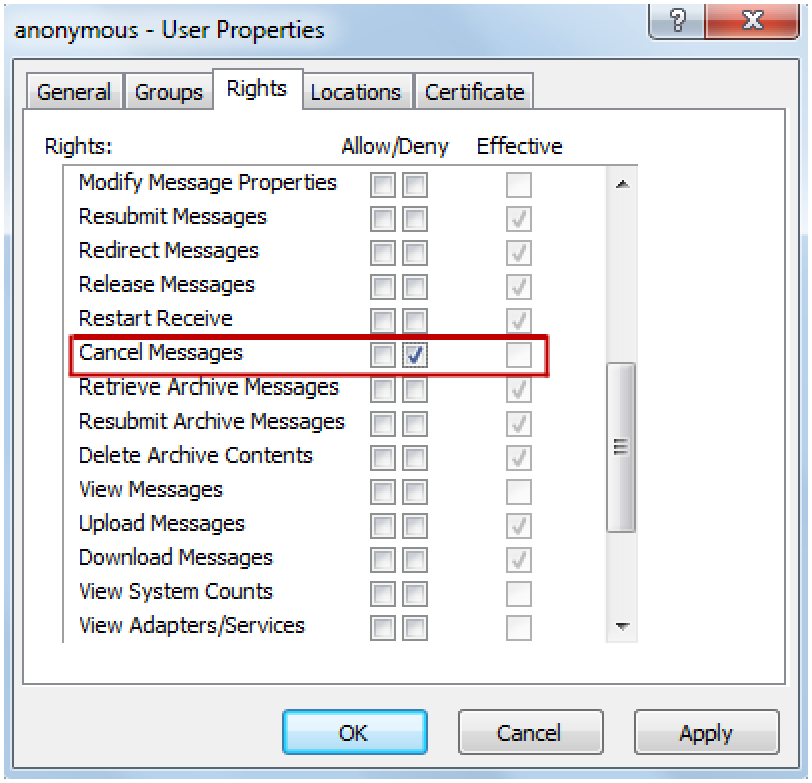
Name
Remote Users

☑ Override Security Group Access Classes:

Access Classes: FtpSslExp,FtpSslImp,FTP,SFTP

Created: 2012/04/03 12:38:31 PM By: <mwimp>
Modified: 2012/04/11 02:21:37 PM By: AdminTest

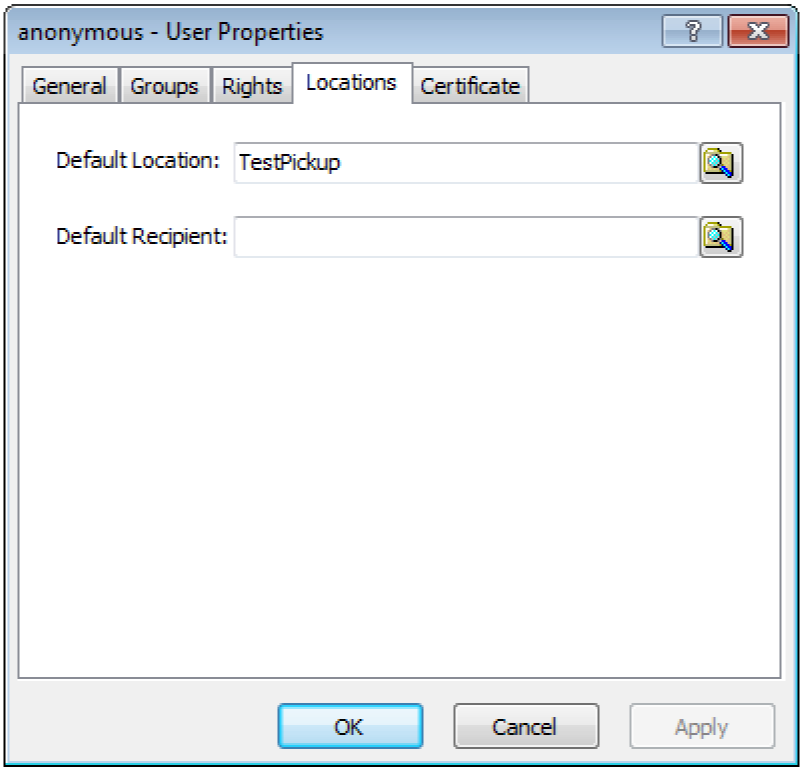
5 On the **Rights** page, appropriate rights will be inherited from the group *Remote Users*. You do not need to change anything, ***unless you have configured the group to be able to cancel messages*** (on page 241). If you do not want to give this privilege to anonymous users, you need to deny, **Cancel Messages**.



Rights:	Allow/Deny		Effective
Modify Message Properties	□	□	□
Resubmit Messages	□	□	☑
Redirect Messages	□	□	☑
Release Messages	□	□	☑
Restart Receive	□	□	☑
Cancel Messages	□	☑	□
Retrieve Archive Messages	□	□	☑
Resubmit Archive Messages	□	□	☑
Delete Archive Contents	□	□	☑
View Messages	□	□	□
Upload Messages	□	□	☑
Download Messages	□	□	☑
View System Counts	□	□	□
View Adapters/Services	□	□	□

6 On the **Locations** page, select a ***pickup mailbox*** (on page 237) for the default location and select an optional ***default recipient location*** (on page 236). The default recipient location is useful if all anonymous users will be sending files to a specific location, such as for translation, and they don't want to always specify the location in their PUT commands. Make sure you select or type the appropriate default location depending on whether it is in the Locations folder or the File System folder. For a description of the differences, refer to the topic ***Overview of Location Properties*** (on page 453).

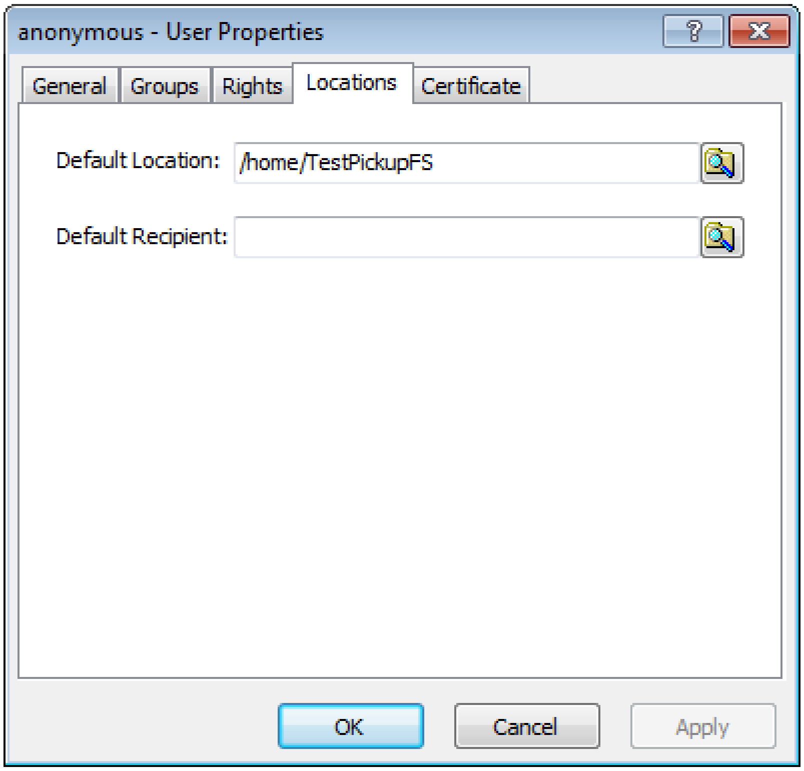
The following default location is in the Locations folder.



Default Location: TestPickup

Default Recipient:

This location is in the File System folder.



Default Location: /home/TestPickupFS

Default Recipient:

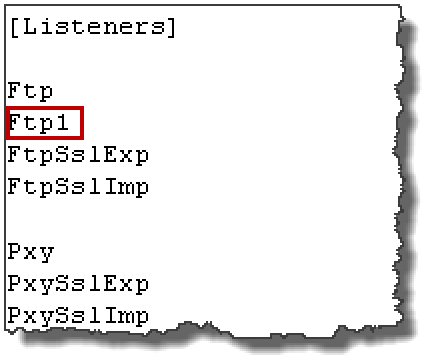
7 Click **OK**.

To Configure the FTP Server for Anonymous Access

To configure the FTP server for anonymous access, you must make the following changes to the ***FTP server configuration file*** (on page 213), mwftpd.conf:

1 If you are creating a new listener:

a) Add that listener to the Listeners Section, for example Ftp1.



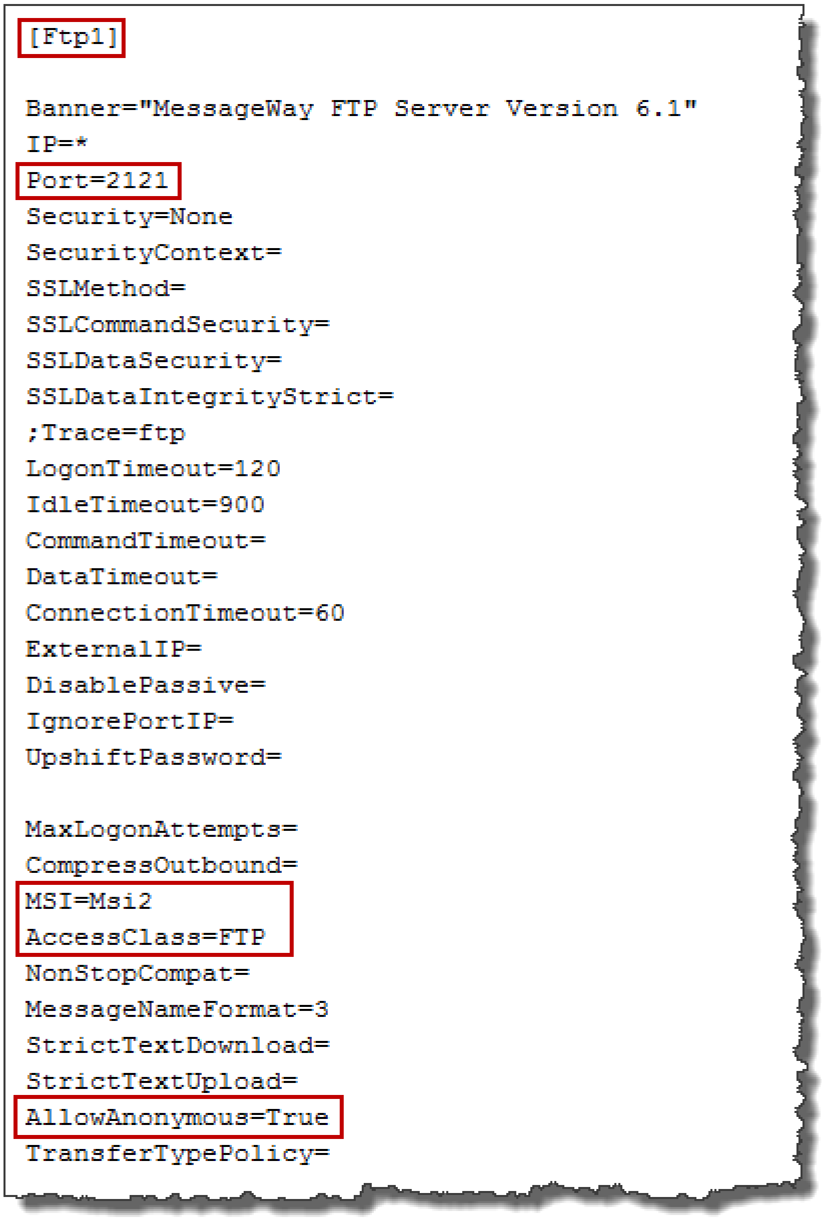
```
[Listeners]

Ftp
Ftp1
FtpSslExp
FtpSslImp

Pxy
PxySslExp
PxySslImp
```

b) In the Listener Configurations Section, copy an appropriate existing listener configuration, for example [Ftp] and name it what you called it in the Listeners Section, for example Ftp1.

2 In the Listeners Configuration Section, review the following parameters and change as necessary:

- Type a port number that will not conflict with others in use, for example **Port=2121**
- **MSI=Msi2**
- **AccessClass=FTP** (uncomment if commented)

- **AllowAnonymous=True**

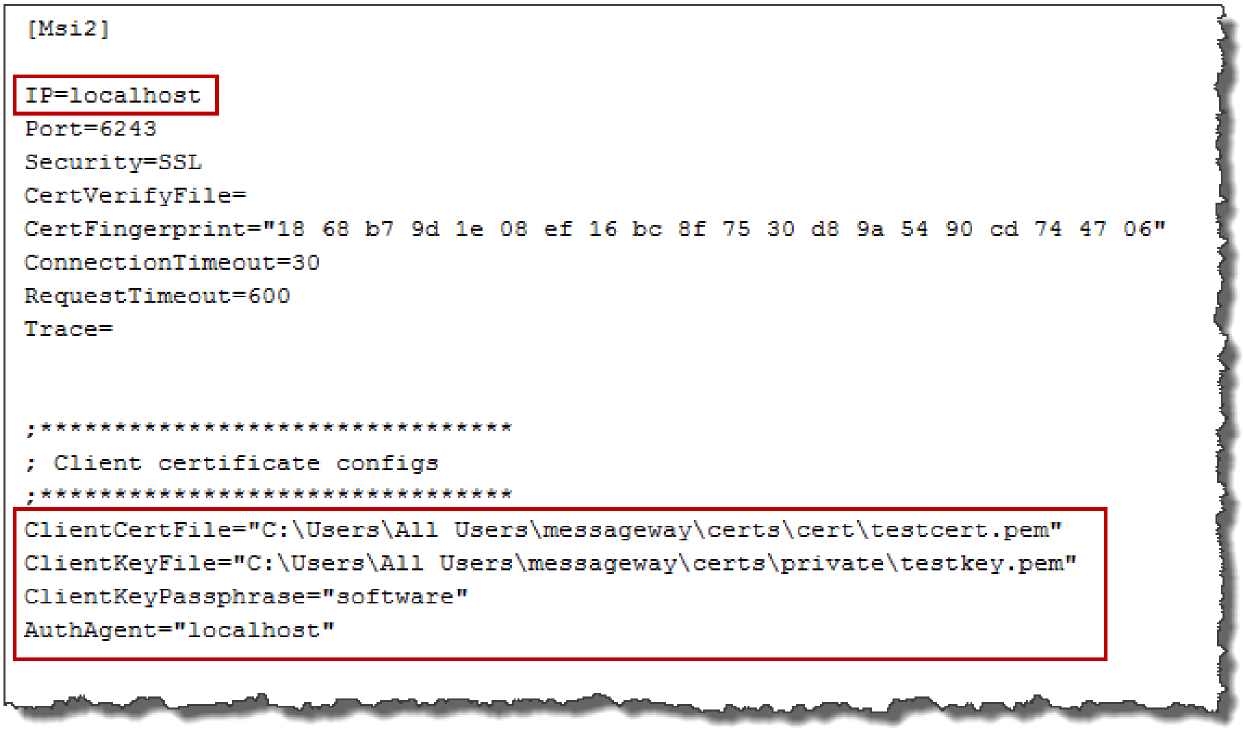


```
[Ftp1]

Banner="MessageWay FTP Server Version 6.1"
IP=*
Port=2121
Security=None
SecurityContext=
SSLMethod=
SSLCommandSecurity=
SSLDataSecurity=
SSLDataIntegrityStrict=
;Trace=ftp
LogonTimeout=120
IdleTimeout=900
CommandTimeout=
DataTimeout=
ConnectionTimeout=60
ExternalIP=
DisablePassive=
IgnorePortIP=
UpshiftPassword=

MaxLogonAttempts=
CompressOutbound=
MSI=Msi2
AccessClass=FTP
NonStopCompat=
MessageNameFormat=3
StrictTextDownload=
StrictTextUpload=
AllowAnonymous=True
TransferTypePolicy=
```

3 In the Service Interface Configurations Section, review the following parameters for Msi2, and make changes as required:

- **IP=localhost**
- Client certificate files are correct for your system, but you can leave them as is if you are using the default test certificate files
- **AuthAgent="localhost"**

MessageWay uses a file, by default called *agents*, to specify who can connect to the service interface. The AuthAgent you specify here, must be configured in that file and must be the same as the IP name specified here.



```
[Msi2]

IP=localhost
Port=6243
Security=SSL
CertVerifyFile=
CertFingerprint="18 68 b7 9d 1e 08 ef 16 bc 8f 75 30 d8 9a 54 90 cd 74 47 06"
ConnectionTimeout=30
RequestTimeout=600
Trace=


;********************************
; Client certificate configs
;********************************
ClientCertFile="C:\Users\All Users\messageway\certs\cert\testcert.pem"
ClientKeyFile="C:\Users\All Users\messageway\certs\private\testkey.pem"
ClientKeyPassphrase="software"
AuthAgent="localhost"
```

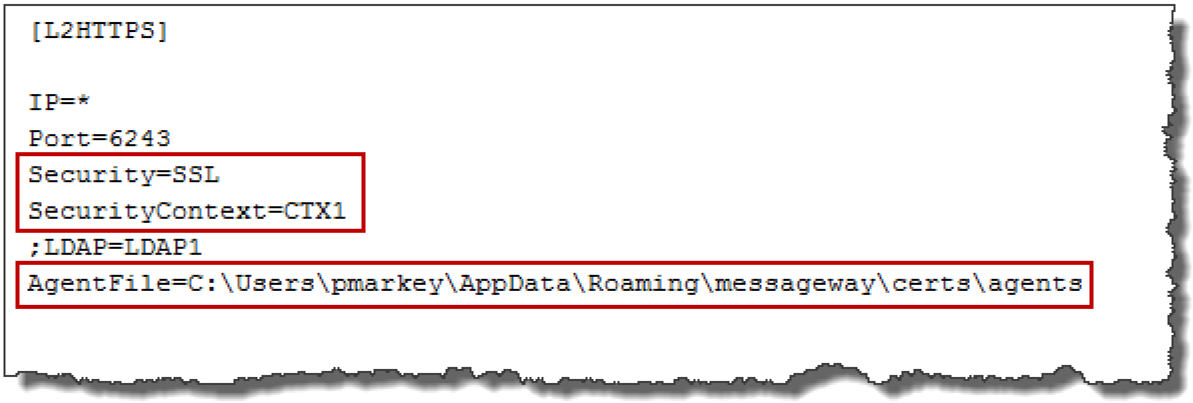
4 Save your changes.

5 ***Restart the FTP perimeter server*** (on page 260) so that it will read the new configuration file.

To Configure the MessageWay Service Interface

The MessageWay Service Interface acts as a server to the MessageWay FTP Perimeter Server when it attempts a connection to MessageWay. For connections that serve anonymous users, this must be SSL. To configure the ***MessageWay Service Interface configuration file, mwsi.conf*** (on page 95), to allow access to MessageWay for anonymous users, proceed as follows:

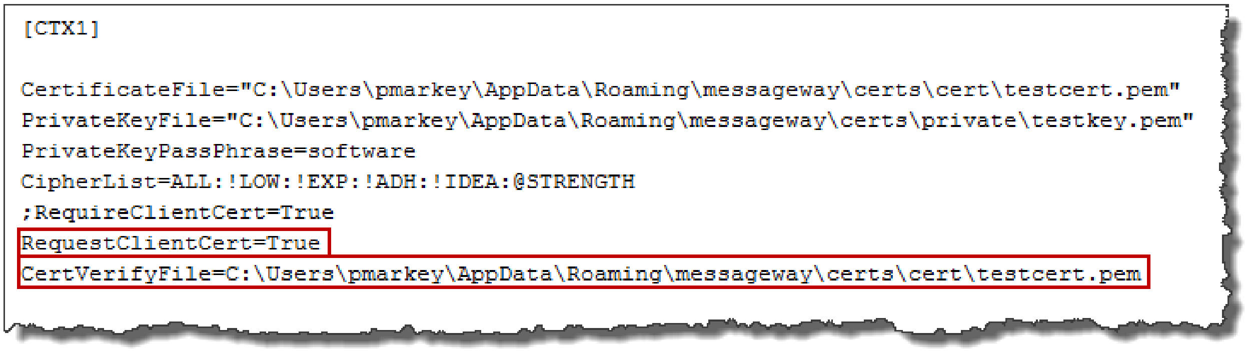
1 In the HTTP Listener Configurations Section, make sure the agents file is in the location specified. If not, you will need to change the location here to point to the correct location or ***create the file*** (on page 259).



```
[L2HTTPS]

IP=*
Port=6243
Security=SSL
SecurityContext=CTX1
;LDAP=LDAP1
AgentFile=C:\Users\pmarkey\AppData\Roaming\messageway\certs\agents
```

2 In the Security Context Configurations Section, review the [CTX1] configuration and change as necessary:

- Client certificates specify the correct location. You can leave these as is if you are using the default test certificates.
- Uncomment the RequestClientCert parameter, and set it to **True**.
- Uncomment the CertVerifyFile and specify the full path name of the certificate file to verify the connecting server.



```
[CTX1]

CertificateFile="C:\Users\pmarkey\AppData\Roaming\messageway\certs\cert\testcert.pem"
PrivateKeyFile="C:\Users\pmarkey\AppData\Roaming\messageway\certs\private\testkey.pem"
PrivateKeyPassPhrase=software
CipherList=ALL:!LOW:!EXP:!ADH:!IDEA:@STRENGTH
;RequireClientCert=True
RequestClientCert=True
CertVerifyFile=C:\Users\pmarkey\AppData\Roaming\messageway\certs\cert\testcert.pem
```

3 Save your changes.

4 ***Restart the Service Interface*** (on page 103), so that it will read the new configuration file.

Configuring the Agents File

To enable public key client authentication, the MessageWay Service Interface (SI) uses the agents file to authenticate MessageWay servers that present themselves as clients to SI and to authenticate the users they represent.

Syntax for the Agents File

You must create the agents file in the location specified in the parameter, AgentFile, in the mwsi.conf file.

By default, a sample file called agents.sample is installed in the following locations, depending on the operating system:

Operating System	Location of the Agents Sample File
UNIX or Linux	/etc/messageway/certs/agents.sample
Windows	\Users\MessageWayUser\AppData\Roaming\messageway\certs\agents.sample

The general rules for the agents file are as follows:

- Must list the AuthAgent value in the appropriate configuration file, such as mwas2.conf or mwsftpd.conf or mwftpd.conf if you are configuring anonymous user access
- Must list all groups and users allowed or denied connection for a given agent

The syntax rules for the agents file are as follows:

- Use Semi-colon (;) to comment a line
- Use separate lines for each AuthAgent and its users and groups list
  - AuthAgent must be first item on the line separated from list of users by at least one space or tab character
    - AuthAgent must match the common name (CN) used in the client certificate
    - Users and groups must be users or groups configured in MessageWay
  - Users and groups follow AuthAgent on the same line
    - Items in this list are separated by commas
    - Items may be in any order
    - Allowed or denied status of user overrides status of group
    - Allowed or denied status of group or user overrides asterisk (*)
    - Use an exclamation mark (!) to deny access to a user or group
    - Enclose group names in greater than (<) and less than (>) signs
    - Optionally use quotation marks (" ") around user names

The following table provides some examples for the user list:

User List Syntax	Description
!*user* - or - **!"***user***"**	Deny access to this user. This access overrides any access for a group to which the user belongs.
user - or - **"***user***"**	Allow access to this user. This access overrides any access for a group to which the user belongs.
!<*group***>**	Deny access to this group. Individual user access overrides group access.

User List Syntax	Description
<*group*>	Allow access to this group. Individual user access overrides group access.
*	Allow all users. Individual user or group access overrides this access.

To Create or Modify the Agents File

The default location of the agents file and the agents.sample file is as follows:

Operating System	Location of the Agents Sample File
UNIX or Linux	/etc/messageway/certs/agents.sample
Windows	\Users\MessageWayUser\AppData\Roaming\messageway\certs\agents.sample

Other processes also use the agents file, so it may already exist. If it doesn't exist or you want to create a new one, start with step 1, otherwise go to step 2.

1 In Windows, using a text editor, create an empty file called **agents** (no extension) in the same location specified in the AgentFile parameter of the HTTP Listeners Configuration section in the MessageWay Service Interface configuration file, ***mwsi.conf*** (on page 145).

CAUTION: When you save the file, make sure there is no extension attached to the end.

2 On a new line in the agents file, type the following:

a) The case-sensitive name that matches the common name (CN) on the FTP client certificate.

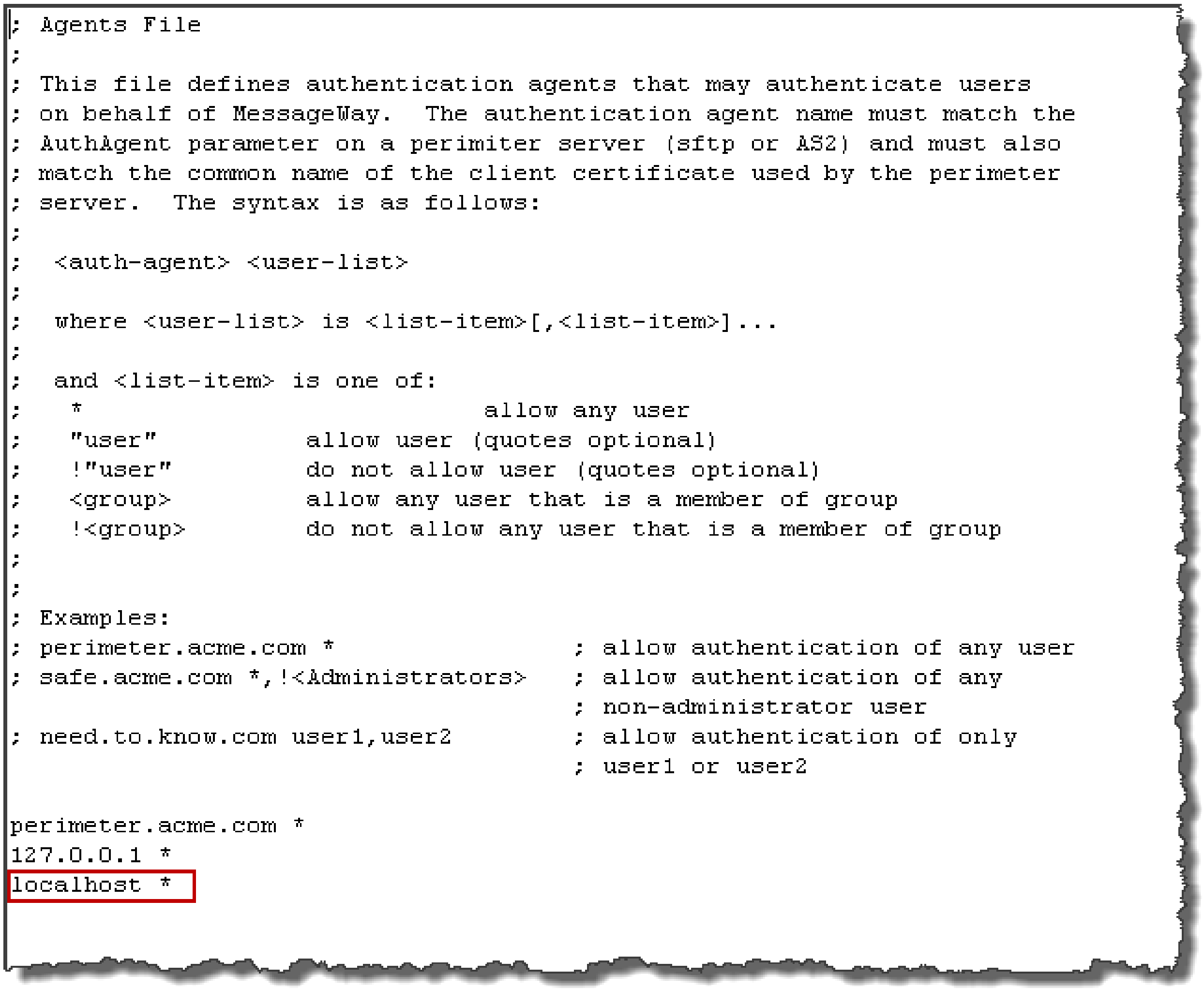
This name is also the AuthAgent value in the server configuration file.

b) At least one space or tab character.

c) MessageWay groups and users that will be allowed to send messages to MessageWay, with names separated by commas or an asterisk (*) for anyone.

Following our example, type:

localhost *



```
; Agents File
;
; This file defines authentication agents that may authenticate users
; on behalf of MessageWay.  The authentication agent name must match the
; AuthAgent parameter on a perimiter server (sftp or AS2) and must also
; match the common name of the client certificate used by the perimeter
; server.  The syntax is as follows:
;
;  <auth-agent> <user-list>
;
;  where <user-list> is <list-item>[,<list-item>]...
;
;  and <list-item> is one of:
;   *                           allow any user
;   "user"          allow user (quotes optional)
;   !"user"         do not allow user (quotes optional)
;   <group>         allow any user that is a member of group
;   !<group>        do not allow any user that is a member of group
;
;
; Examples:
; perimeter.acme.com *                ; allow authentication of any user
; safe.acme.com *,!<Administrators>   ; allow authentication of any
                                      ; non-administrator user
; need.to.know.com user1,user2        ; allow authentication of only
                                      ; user1 or user2

perimeter.acme.com *
127.0.0.1 *
localhost *
```

NOTE: There may be other lines for agents and users in the file. Any MessageWay servers or interfaces that use public key authentication for input or that allow anonymous access to MessageWay must be listed as an agent.

Testing the FTP Perimeter Server

To test the FTP Server process from end to end, make sure you have completed the installation tasks, described in the topic, ***Basic Installation Tasks*** (on page 212).

Start the FTP Perimeter Server

You start the FTP perimeter server differently, depending on the operating system where the server resides: UNIX/Linux or Windows.

To Start the FTP Perimeter Server on Windows

To start the FTP perimeter server on Windows, proceed as follows:

1 From the **Start** menu, select **Programs|Administrative Tools|Computer Management**.

The Computer Manager window appears.

2 In the left pane, expand the folder **Services and Applications**, and click **Services**.

The Services window appears.

3 In the right pane, scroll to the service, **MessageWay FTP Server**.

4 Right-click **MessageWay FTP Server**, and select **Start** from the menu.

The Status column should display **Started**.

To Start the FTP Perimeter Server on UNIX or Linux

On UNIX or Linux, you start the FTP perimeter server with a startup script. The startup script, **mwftpd**, has the following options:

FTP script options	Description
condrestart	Restarts only if the FTP server is running. The script determines if the FTP server is running by looking for the PID file on disk. This process rereads the configuration file.
restart	Stops the server and then starts the server. This process rereads the configuration file.
start	Starts the server. This process rereads the configuration file.
status	Provides the status of the server.
stop	Sends the FTP server process a TERM signal; waits for 1 second; checks if the process is still running, and if it is, then sends the process a KILL signal.
stopnowait	Sends the FTP server a TERM signal and exits the script. This will cause the FTP server to stay around until the IdleLogonTime (configured in the Listeners section of the configuration file) before shutting down.
wait	Sends the FTP server a KILL signal and waits to make sure that the server is stopped.

IMPORTANT: The script and the daemon process that the script starts and stops can be started only by the user, **root**. Check the system logs for errors if the server daemon process fails to start.

To start the FTP perimeter server on UNIX or Linux, proceed as follows:

1 Make sure you are logged on as the user, **root**.

NOTE: When running, MessageWay temporarily requires root access for the remote execution server, the SFTP proxy server and the FTP and SFTP perimeter servers. The FTP and SFTP perimeter servers require root access because they must listen on low ports (<1024), and both Linux and Solaris require root access to listen on low ports.

2 Go to the subdirectory where the script resides by typing:

cd /etc/init.d

3 To start the server daemon process, type:

./mwftpd start

- or -

To check the server status, type:

./mwftpd status

- or -

To stop the server, type:

./mwftpd stop

- or -

To restart the server, type:

./mwftpd restart

NOTE: For Red Hat 7.x, MessageWay supports the systemctl utility, including automatically starting MessageWay when the application server is rebooted, and automatically starting MessageWay perimeter servers when the perimeter server is rebooted. The systemctl files are named *messageway.service*, *mwftpd.service*, *mwproxy.service*, *mwresd.service* and *mwsftpd.service*, and are located in **/usr/lib/systemd/system/**, with symbolic links being added in **/etc/systemd/system/multi-user.target.wants/**. See above systemctl files for more details.

Test the Non-secure FTP Connection

In this test, we will send and retrieve a message using the loopback IP address, 127.0.0.1, and the default FTP port, 21.

If you have not already done so, start the following:

- MessageWay Manager
- MessageWay Server (starts the Messaging Server, the Service Interface and the User Server)
- MessageWay FTP Perimeter Server

NOTE: You must decide what type of client you will use to send commands to the FTP Server. You could use a command-line or GUI interface, such as WS_FTP Pro.

1 Start the FTP client.

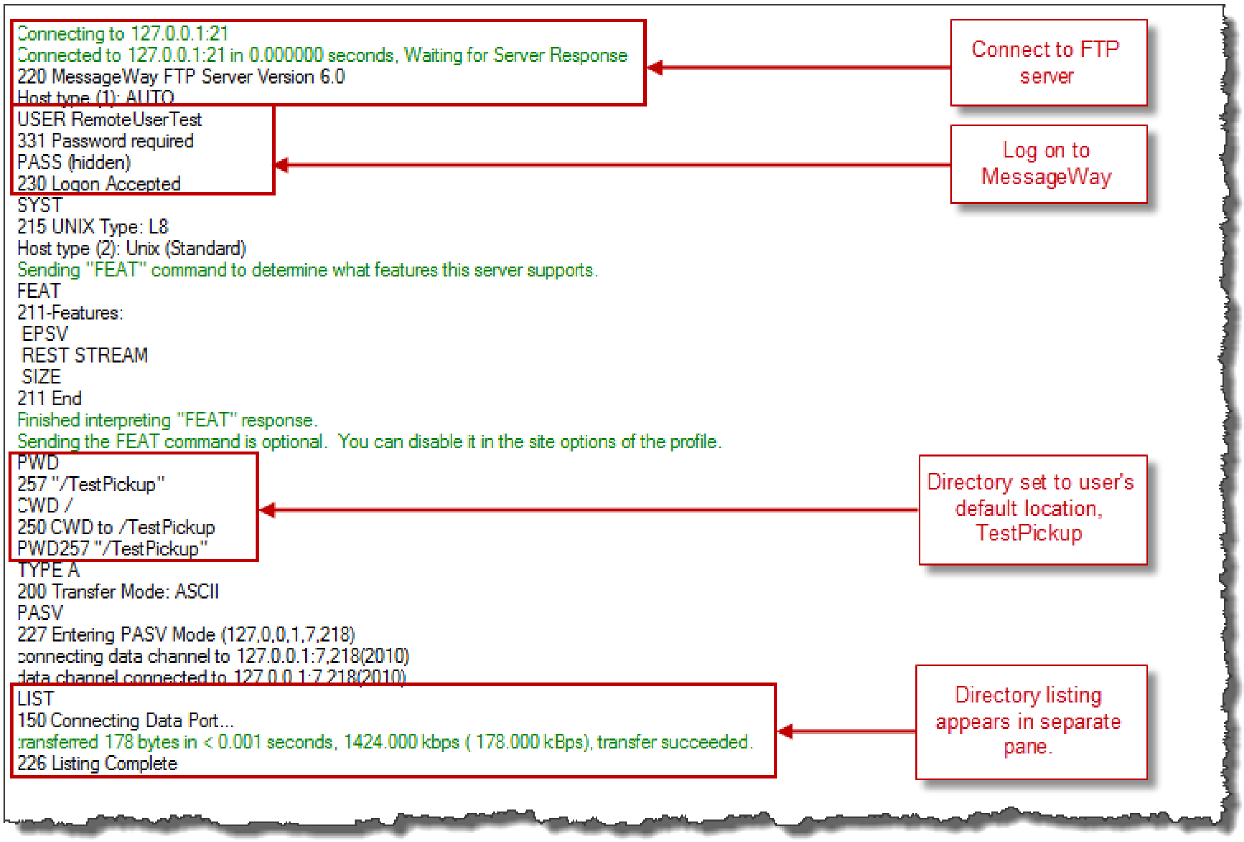
2 Connect to the FTP Server and log on to MessageWay, using the following information:

User ID	**RemoteUserTest**
Password	*password for the user ID*

Address (includes location name)	**ftp://127.0.0.1**
Port	Default (**21**)

For instructions to add a user and mailbox for MessageWay, refer to the topic, ***Configuring MessageWay Users and Locations*** (on page 236). For instructions to specify the address and port for the server, refer to the topic, ***Configuring the FTP Server Components*** (on page 213).

If you are using a client such as WS_FTP Pro, you should see something like the following exchange of information:



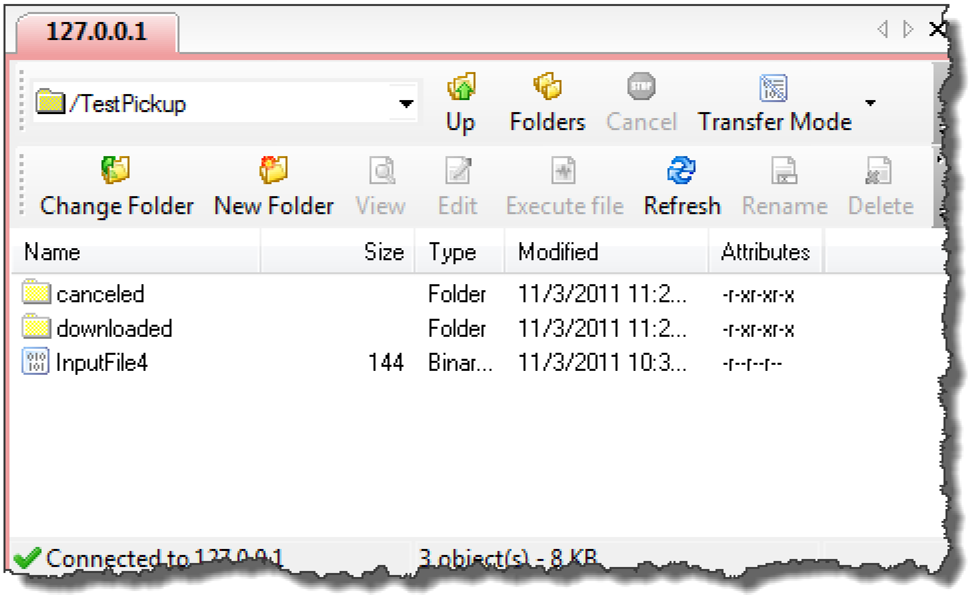
```
Connecting to 127.0.0.1:21
Connected to 127.0.0.1:21 in 0.000000 seconds, Waiting for Server Response
220 MessageWay FTP Server Version 6.0
Host type (1): AUTO
USER RemoteUserTest
331 Password required
PASS (hidden)
230 Logon Accepted
SYST
215 UNIX Type: L8
Host type (2): Unix (Standard)
Sending "FEAT" command to determine what features this server supports.
FEAT
211-Features:
 EPSV
 REST STREAM
 SIZE
211 End
Finished interpreting "FEAT" response.
Sending the FEAT command is optional.  You can disable it in the site options of the profile.
PWD
257 "/TestPickup"
CWD /
250 CWD to /TestPickup
PWD257 "/TestPickup"
TYPE A
200 Transfer Mode: ASCII
PASV
227 Entering PASV Mode (127,0,0,1,7,218)
connecting data channel to 127.0.0.1:7,218(2010)
data channel connected to 127.0.0.1:7,218(2010)
LIST
150 Connecting Data Port...
ransferred 178 bytes in < 0.001 seconds, 1424.000 kbps ( 178.000 kBps), transfer succeeded.
226 Listing Complete
```

Connect to FTP server

Log on to MessageWay

Directory set to user's default location, TestPickup

Directory listing appears in separate pane.

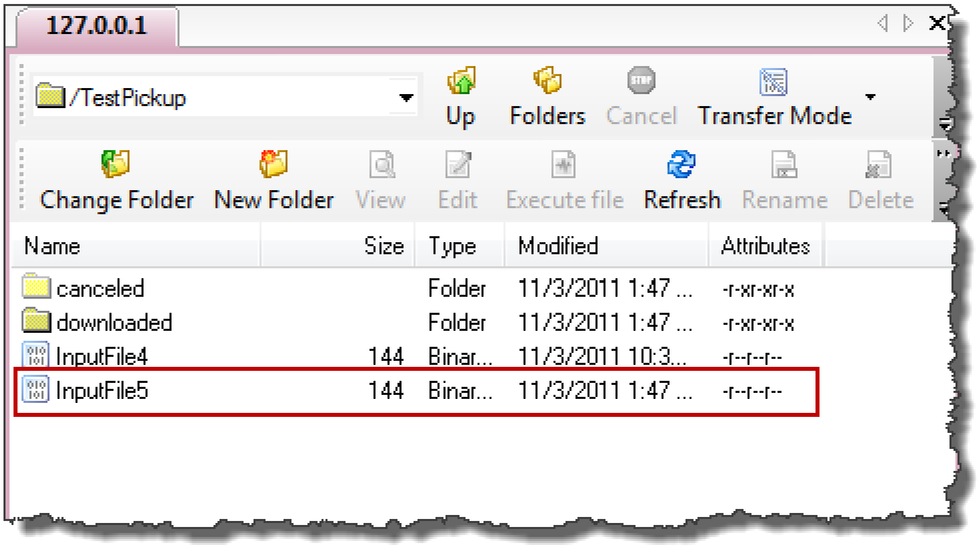


Name	Size	Type	Modified	Attributes
canceled		Folder	11/3/2011 11:2...	-r-xr-xr-x
downloaded		Folder	11/3/2011 11:2...	-r-xr-xr-x
InputFile4	144	Binar...	11/3/2011 10:3...	-r--r--r--

Connected to 127.0.0.1 3 object(s) - 8 KB

3 Send a file, for example InputFile5, to the MessageWay mailbox TestPickup.

The user RemoteUserTest must have upload rights to the location to which you are uploading the file, so for simplicity, we are uploading the file to the user's default location, TestPickUp.



Name	Size	Type	Modified	Attributes
canceled		Folder	11/3/2011 1:47 ...	-r-xr-xr-x
downloaded		Folder	11/3/2011 1:47 ...	-r-xr-xr-x
InputFile4	144	Binar...	11/3/2011 10:3...	-r--r--r--
InputFile5	144	Binar...	11/3/2011 1:47 ...	-r--r--r--

4 (Optional) To view information about the message from the MessageWay Manager, in the MessageWay Explorer window:

a) In the left pane, select **Locations**.

b) In the right pane, right-click your mailbox, **TestPickUp**.

c) From the menu, select **Show Messages**.

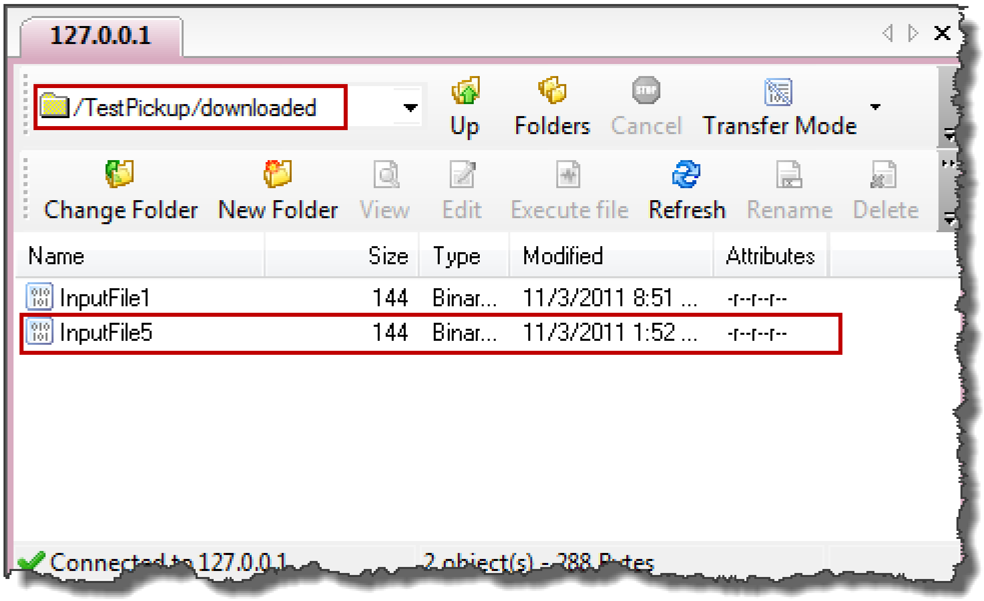
d) Right-click on the most recent message.

e) From the menu, select **Properties**.

The state at the bottom of the Message properties window is *Available for download*. This message is now available for us to retrieve.

5 Retrieve your message from MessageWay. Note that the file is now listed under the directory, /downloaded.

You should see something like the following:



Name	Size	Type	Modified	Attributes
InputFile1	144	Binar...	11/3/2011 8:51 ...	-r--r--r--
InputFile5	144	Binar...	11/3/2011 1:52 ...	-r--r--r--

Test the Secure FTP Connection

In this test, we will send and retrieve a message using the loopback IP address, 127.0.0.1.

CAUTION: This example uses a fingerprint for the Msi2 configuration in the mwftpd.conf file to communicate with the MessageWay Service Interface (SI). If this is not a new installation of MessageWay, you may have to change the fingerprint. You will have to change the fingerprint if the certificates have changed, in order to match the new fingerprints. Contact your security administrator or MessageWay Technical Support for further instructions.

If you have not already done so, start the following:

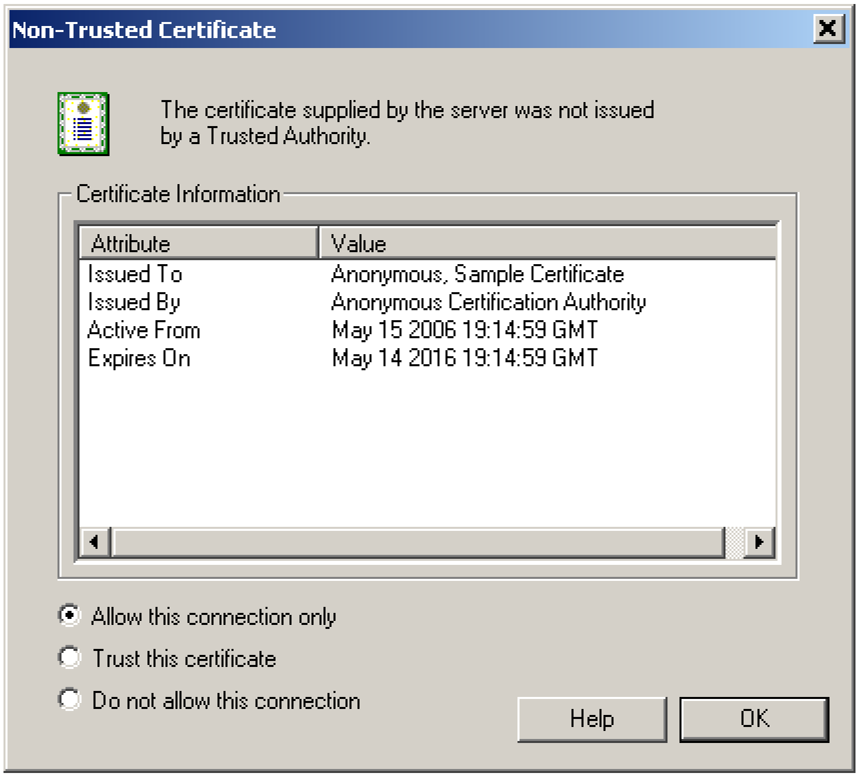
- MessageWay Manager
- MessageWay Server (starts the Messaging Server, the Service Interface and the User Server)
- MessageWay FTP Perimeter Server

NOTE: You must decide what type of client you will use to send commands to the FTP Server. The client must support SSL connections, either implicit or explicit. With WS_FTP Pro, you must use version 8.0.3 or higher in order to test both Explicit and Implicit types of connections.

1 Start the FTP client.

2 Connect to the FTP Server with a secure SSL connection.

A warning message should appear indicating that this is a non-trusted certificate, similar to the following:


Non-Trusted Certificate

The certificate supplied by the server was not issued by a Trusted Authority.

Certificate Information

Attribute	Value
Issued To	Anonymous, Sample Certificate
Issued By	Anonymous Certification Authority
Active From	May 15 2006 19:14:59 GMT
Expires On	May 14 2016 19:14:59 GMT

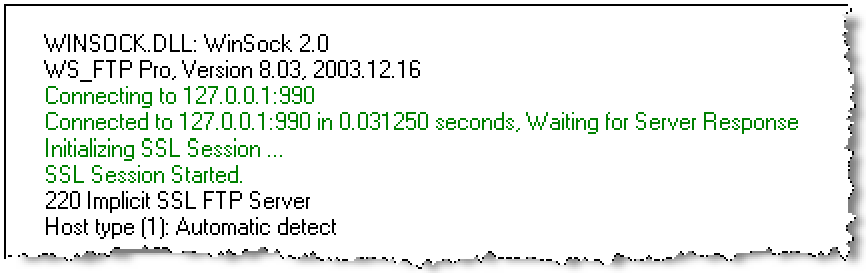
● Allow this connection only

○ Trust this certificate

○ Do not allow this connection

3 Respond to the warning by allowing the connection.

If you are using a client such as WS_FTP Pro, you should see something like the following exchange of information:



```
WINSOCK.DLL: WinSock 2.0
WS_FTP Pro, Version 8.03, 2003.12.16
Connecting to 127.0.0.1:990
Connected to 127.0.0.1:990 in 0.031250 seconds, Waiting for Server Response
Initializing SSL Session ...
SSL Session Started.
220 Implicit SSL FTP Server
Host type (1): Automatic detect
```

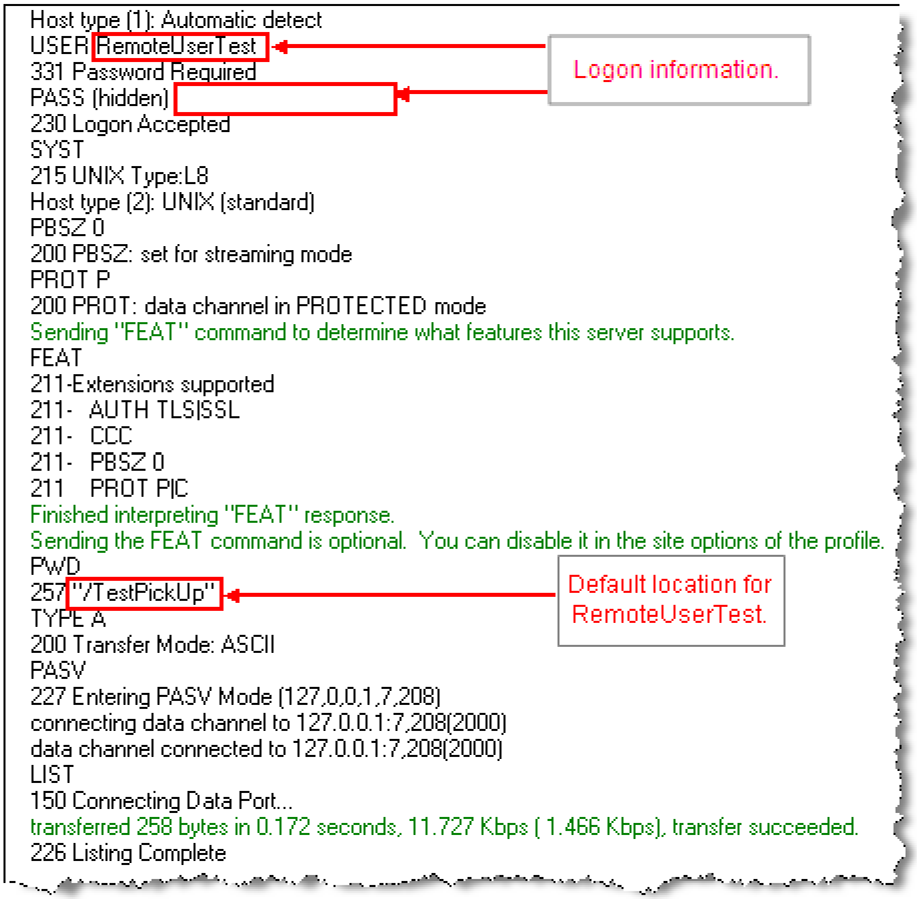
4 Log on to MessageWay, using the following information:

User ID	**RemoteUserTest**
Password	*password for the user ID*
Address (includes mailbox name)	**ftp://127.0.0.1**
Port	Default (**990**)

For instructions to add a user and location for MessageWay, refer to the topic, ***Configuring MessageWay Users and Locations*** (on page 236). For instructions to specify the address and port for the server, refer to the topic, ***Configuring Files for the FTP Server Components*** (on page 213).

The client connects to your system using the loopback address, and points to the default location for the user, TestPickUp.

If you are using a client such as WS_FTP Pro, you should see something like the following exchange of information:



```
Host type (1): Automatic detect
USER RemoteUserTest
331 Password Required
PASS (hidden)
230 Logon Accepted
SYST
215 UNIX Type:L8
Host type (2): UNIX (standard)
PBSZ 0
200 PBSZ: set for streaming mode
PROT P
200 PROT: data channel in PROTECTED mode
Sending "FEAT" command to determine what features this server supports.
FEAT
211-Extensions supported
211-   AUTH TLS|SSL
211-   CCC
211-   PBSZ 0
211    PROT P|C
Finished interpreting "FEAT" response.
Sending the FEAT command is optional.  You can disable it in the site options of the profile.
PWD
257 "/TestPickUp"
TYPE A
200 Transfer Mode: ASCII
PASV
227 Entering PASV Mode (127,0,0,1,7,208)
connecting data channel to 127.0.0.1:7,208(2000)
data channel connected to 127.0.0.1:7,208(2000)
LIST
150 Connecting Data Port...
transferred 258 bytes in 0.172 seconds, 11.727 Kbps ( 1.466 Kbps), transfer succeeded.
226 Listing Complete
```

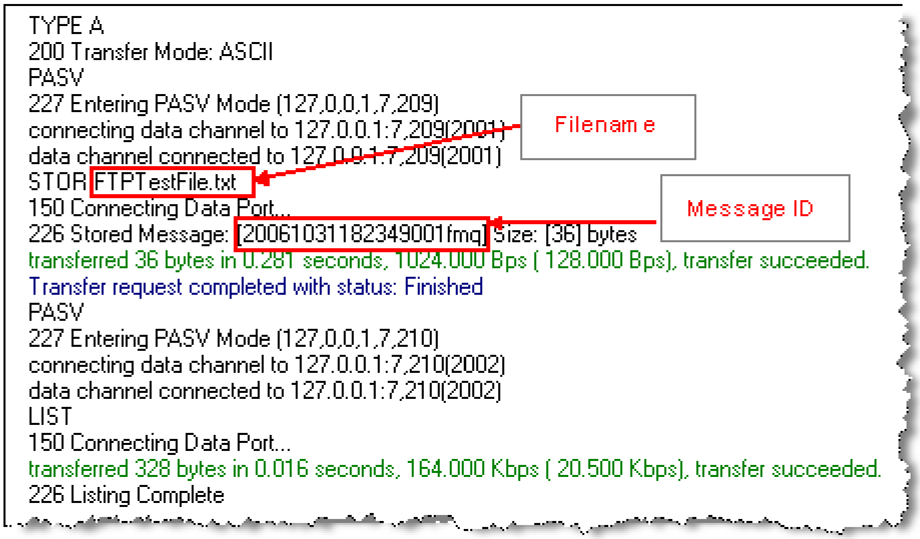
Logon information.

Default location for RemoteUserTest.

5 Send a file to the MessageWay address listed previously.

The user RemoteUserTest must have upload rights to the location to which you are uploading the file, so for simplicity, we are uploading the file to the user's default location, TestPickUp.

If you are using a client such as WS_FTP Pro, you should see something like the following exchange of information:

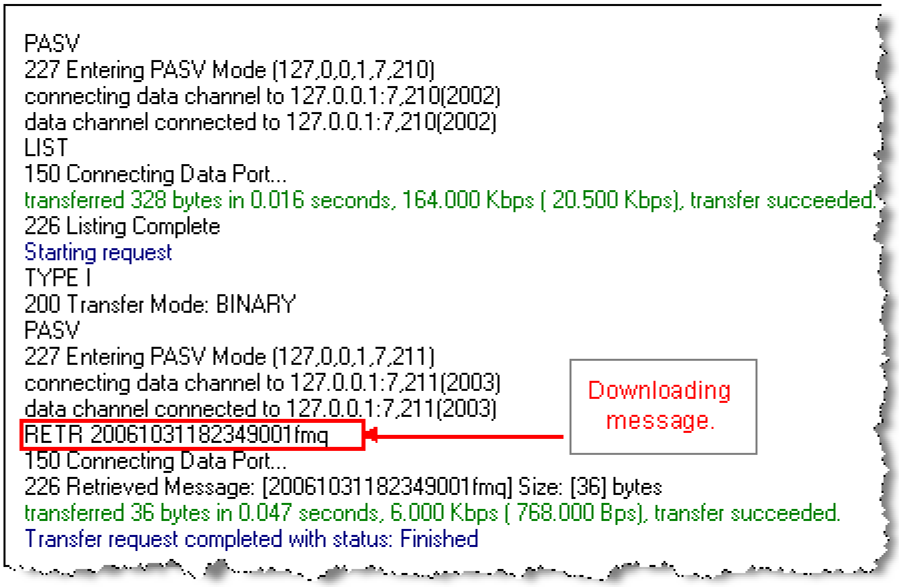


```
TYPE A
200 Transfer Mode: ASCII
PASV
227 Entering PASV Mode (127,0,0,1,7,209)
connecting data channel to 127.0.0.1:7,209(2001)
data channel connected to 127.0.0.1:7,209(2001)
STOR FTPTestFile.txt
150 Connecting Data Port...
226 Stored Message: [20061031182349001fmq] Size: [36] bytes
transferred 36 bytes in 0.281 seconds, 1024.000 Bps ( 128.000 Bps), transfer succeeded.
Transfer request completed with status: Finished
PASV
227 Entering PASV Mode (127,0,0,1,7,210)
connecting data channel to 127.0.0.1:7,210(2002)
data channel connected to 127.0.0.1:7,210(2002)
LIST
150 Connecting Data Port...
transferred 328 bytes in 0.016 seconds, 164.000 Kbps ( 20.500 Kbps), transfer succeeded.
226 Listing Complete
```

6 If your connection times out, you may need to reconnect. To reconnect to the FTP Server and MessageWay from your FTP Client, repeat step 2.

7 Retrieve your message from MessageWay.

You should see something like the following exchange of information:



```
PASV
227 Entering PASV Mode (127,0,0,1,7,210)
connecting data channel to 127.0.0.1:7,210(2002)
data channel connected to 127.0.0.1:7,210(2002)
LIST
150 Connecting Data Port...
transferred 328 bytes in 0.016 seconds, 164.000 Kbps ( 20.500 Kbps), transfer succeeded.
226 Listing Complete
Starting request
TYPE I
200 Transfer Mode: BINARY
PASV
227 Entering PASV Mode (127,0,0,1,7,211)
connecting data channel to 127.0.0.1:7,211(2003)
data channel connected to 127.0.0.1:7,211(2003)
RETR 20061031182349001fmq
150 Connecting Data Port...
226 Retrieved Message: [20061031182349001fmq] Size: [36] bytes
transferred 36 bytes in 0.047 seconds, 6.000 Kbps ( 768.000 Bps), transfer succeeded.
Transfer request completed with status: Finished
```

Configuring the Remote Execution Perimeter Server (RES)

The Remote Execution Server (RES) is a perimeter server that provides secure execution of scripts, programs or commands invoked from MessageWay and that are run on a remote machine. The system provides the ability to execute remote scripts, to report the status of execution and to monitor the status of remote servers.

NOTE: (Windows) The MessageWay Remote Execution Server and the MWRES utility *do not* currently support Unicode characters on Windows systems. They *do* support Unicode on UNIX/Linux systems.

For example, when you are not allowed to execute file transfers from the application server, you can use RES to perform transfers from the perimeter server.You can also use RES as a command center to drive programs on other servers running various operating systems. Operators have visibility into all RES processing from the MessageWay Manager.

RES activity is initiated from scripts used with the ***Custom Processing Service*** (on page 414) or the ***Custom IO Adapter*** (on page 410).

This option includes the following components:

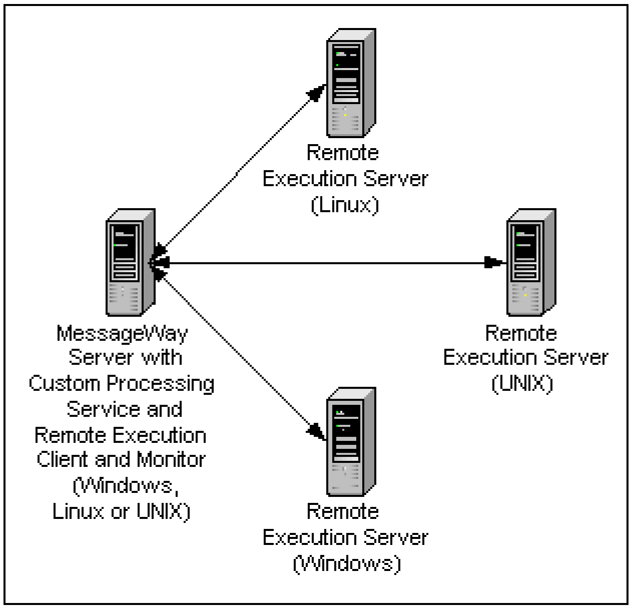
- Remote Execution Server (RES)
- Remote Execution Client (part of the MessageWay Server)
- Remote Server Monitor (part of MessageWay Scheduling Server)

These components typically have the following physical relationships:

- The client resides with the MessageWay Server
- The monitor functionality is in the MessageWay Scheduling Server, which resides with the MessageWay Server
- The RES resides on a remote machine

NOTE: Although it is not shown in the following diagram, a Remote Execution Server does not need to be on a different physical machine. You may also run the server on the same machine as the MessageWay Server, which is useful for initial testing.

The following diagram shows a typical relationship among the RES components.


Remote Execution Server (Linux)
MessageWay Server with Custom Processing Service and Remote Execution Client and Monitor (Windows, Linux or UNIX)
Remote Execution Server (UNIX)
Remote Execution Server (Windows)

Licensing Requirements for the Remote Execution Server

The MessageWay Remote Execution Server (RES) is a licensed component of MessageWay from Progress. For more information, contact MessageWay Technical Support.

Basic Installation Tasks

The installation process installs or upgrades the components of the Remote Execution Server (RES) system, at which time you also set up the configuration file. These tasks assume that you have already installed MessageWay, which includes the MessageWay Server and the MessageWay Manager. The Remote Execution Client is by default installed with the MessageWay Server.

These are the tasks performed during initial installation for testing:

- Install the Remote Execution Server, typically on a system that is not where the client runs.

NOTE: You may want to install the server on the same machine as the client for testing purposes.

- Set up the configuration file for the client, and optionally, the monitor.
- Set up the configuration file for the server, typically on the remote machine.
- Configure shared keys for the client and server.
- Configure logon security for the user ID that will access the server.
- If needed, for the monitor, configure a location to receive the notifications.
- Start the Remote Execution Server.
- Test the connection to the server.
- Configure a Custom Processing or Custom IO location to invoke the client.
- Test the system from end to end.

For the actual installation information, refer to the *MessageWay Installation Guide*.

Overview of the Remote Execution Server

The main components of the Remote Execution Server system perform the following functions:

- The Remote Execution Client processes the command line received from a MessageWay Custom Processing or Custom IO location and passes it to the Remote Execution Server (RES).
- The optional Remote Server Monitor tracks the status, running or not, of all Remote Execution Servers and sends notifications to various locations.
- The RES authenticates the user and executes the command sent from the Remote Execution Client.

The configurations on a Custom Processing or Custom IO location initiate client activity and specify what the server should do. The following steps describe the typical process flow between the client and server:

1. Message trigger or action request sent to location

   - or -

   Closed schedule opens
2. Script or command invokes the RES client.
3. RES client reads its configuration file, contacts server and sends encrypted command.
4. Server reads its configuration file, authenticates the client and executes the command. It may also log its activity.

The Remote Monitor is part of the MessageWay Scheduling Server. These steps describe what the Remote Monitor does:

1. On MessageWay startup, Scheduling Server looks for the RES configuration file.
   - If found, it reads information from appropriate sections.

     - or -
   - If not found, it assumes the RES is not used.
2. When the configuration file exists, it checks the **Enabled** parameter for the Remote Monitor.
3. When the Remote Monitor is enabled, it will contact the listed servers at the specified interval to make sure the servers are running. It may also log its activity.

Tasks for the Server

The Remote Execution Server (RES) executes the command sent from the Remote Execution Client.

The server will perform its tasks based on the information it finds in the configuration file. These are the normal tasks the server performs:

1. ***Reads the appropriate information from the configuration file*** (on page 275).
2. Listens on the specified port(s) for connections from the specified client(s).
3. Receives a connection request from a valid client and generates and sends a session-specific key, which is encrypted using the shared key.
4. Receives encrypted data from the client and decrypts it by using the session-specific key.
5. Validates the user ID and password and executes the command line sent to it from the client.
6. Sends completion code and information that was written to standard error and standard out to the client, all of which must be completed within the timeout limit for the session.

Tasks for the Client

The Remote Execution Client processes the command line received from a MessageWay Custom Processing or Custom IO location and passes it to the Remote Execution Server (RES).

The client will perform its tasks based on the information it receives from the location in the command line. These are the normal tasks the client performs:

1. Receives and parses information from a Custom Processing or Custom IO location.
2. ***Reads the appropriate information from the configuration file*** (on page 278).
3. Initiates a connection to the server and receives a session-specific key, which is encrypted using the shared key.
4. Encrypts the data using the session-specific key.
5. Passes the encrypted user ID and password and remote command line to the server.
6. Waits for a response from the server, which must be within the timeout limit.
7. If a response is not received within the timeout limit, the client returns a non-zero code and an error message to MessageWay.

   - or -

   If a response is received within the timeout limit, the client passes the completion code, standard error and standard out information received from the server to MessageWay.

Tasks for the Monitor

The optional monitor component of the Remote Execution Server system is part of the MessageWay Schedule Server and resides with the MessageWay Server. The Remote Server Monitor tracks the status, running or not, of all Remote Execution Servers and sends notifications to various locations. The monitor may be enabled in the configuration file, mwres.conf.

The monitor will perform its tasks based on the information it finds in the configuration file. These are the normal tasks the monitor performs:

1 ***Reads the appropriate information from the configuration file*** (on page 280). If the file is not found, it assumes that the Remote Execution Server system is not used.

2 Initiates connections to the server and requests a date and time stamp.

3 If the server responds within the ConnectTimeout period that is specified in seconds, it may log the information to the system log file depending on your remote monitor configurations.

   a) If the NotifyRecipient has a location and NotifyLevel is set to **Info**, it also sends a notification message with the date and time stamp to the specified location.

   – otherwise –

   b) It does not send a notification message to the location.

4 If the server does not respond within the ConnectTimeout period, it assumes the server is not running, and it may log a warning or error message to the system log depending on your remote monitor configurations.

   a) If the NotifyRecipient has a location and NotifyLevel is set to **Error**, **Warn** or **Info**, it also sends a notification message to the specified location.

   – otherwise –

   b) It does not send a notification message to the location.

5 While the error condition exists, and the ErrorRepeatLevel is greater than zero minutes, it will create the notification at the interval specified. A value of zero means the error is only reported once.

6 While the warning condition exists, and the WarnRepeatLevel is greater than zero minutes, it will create the notification at the interval specified. A value of zero means the warning is only reported once.

7 Repeat the previous steps at the interval in seconds that is specified for the MonitorLoopDelay.

Configuration Files for the RES Components

You set the parameters for the Remote Execution Server system in the configuration files: one for the client and the monitor, mwres.conf. and one for the server, mwresd.conf. You edit the files with a text editor. Copies of the files reside on the same machine as its component.

The following table shows the default location for the configuration file for the client and monitor, which depends on the operating system where the client and server reside:

Operating System	Location of the RES Client Configuration File
UNIX or Linux	/etc/messageway/mwres.conf
Windows	\Users*MessageWayUser*\AppData\Roaming\messageway\mwres.conf

The following table shows the default location for the configuration file for the server:

Operating System	Location of the RES Server Configuration File
UNIX or Linux	/etc/messageway/mwresd.conf
Windows	\ProgramData\messageway\mwresd.conf

Configurations for the RES Server

The server component of the Remote Execution Server system typically resides on a different machine than the MessageWay Server. It receives commands from the client, which it processes and then returns a completion code and any standard error (STDERR) and standard out (STDOUT) information.

The following table explains the configuration options for the server that appear in the mwresd.conf file.

Section and Parameter	Description of Parameter
Global Section	
timeout	I/O time in seconds the server will maintain the session thread.
address	The IP address and port where the server listens. When the host has multiple Network Interface Cards (NICs), use ***** to have the listener listen on all IP addresses on the server: ▪ *IP address* - Internet Protocol address or ***** for any address ▪ **:***Port* - valid port Examples: ▪ **192.168.1.1:6235** ▪ ***:6235**
max-connections	Maximum number of simultaneous sessions the server will handle.
logging	Turns on and off server logging. Logs to the file **mwres_audit***yyyymmdd***.txt**. ▪ **0** turns off server logging ▪ **1** logs attempts to connect and remote requests ▪ **2** logs responses to remote requests ▪ **3** logs all connects, requests and responses
logdir	Defines the directory to create server logs. If not defined, then a directory is found as follows: ▪ Environment Variable: **MWRES_LOGDIR** ▪ Windows: executable directory ▪ UNIX or Linux: **/var/log** ▪ UNIX or Linux: **~** (home directory)
Authorized Clients Section	
clients	Clients to which the server is authorized to connect (syntax follows)

Control logging on the RES server to limit the amount of information sent to the log. The following table shows in more detail the type of information that the server logs, based on setting for the Logging parameter in the [global] section.

Value	Description	Example

1	log-Connect
	Logged anytime a connection is attempted on the port where the RES server is listening.
		Cmd=CONNECT
		From=100.10.10.167
		Status=ACCEPTED/REJECTED

	log-Status-Request
	Status request comes from MWSched (the scheduling server) or from the mwres client (-x option)
		Req=STATUS
		From=100.10.10.167

	log-Execute-Request
	Execute request are requests by the mwres client to execute a command on the server where RES is running.
		Req=EXECUTE
		From=100.10.10.167
		Blksize=65535
		User=guest
		Cmd=dosorunix -s ofile nfile

2	log-Status-Response
	Status response sent back to the client
		Rsp=STATUS
		To=100.10.10.167
		20051004100013

	log-Execute-Response
	Execute responses show the completion code and any output that the program sent to its stdout.
		Rsp=EXECUTE
		To=100.10.10.167
		RetCode=100

3	Turn on all logging	All of the above.

List the clients one per line after the [clients] section. The syntax for the client entries is as follows:

[clients]
Client IP Address,*Path to Key File*l*keyfile*.**mkf**[,**"***Passphrase***"**]

This table explains the options.

Parameter	Description
Client IP Address	Internet Protocol (IP) address for the client that is allowed to connect to this server.

Parameter	Description
Location of Key File	Where the encryption key file resides that was generated to connect to this client.
keyfile	Name of the key file, which should have an extension of **.mkf**.
Passphrase	Optional. Allows users to modify the shared key for more security. When used, the server will compute an MD5 hash of the passphrase and apply it to the encryption key before use. The passphrase must be enclosed in double quotation marks.

Here are some Windows examples:

192.168.2.1,c:\Program Files\MessageWay\utils\keyfile.mkf

192.168.2.2,c:\Program Files\MessageWay\utils\keyfile.mkf,"passphrase"

Here are some UNIX and Linux examples:

192.168.2.1,/opt/messageway/utils/keyfile.mkf

192.168.2.2,/opt/messageway/utils/keyfile.mkf,"passphrase"

IMPORTANT: When the Remote Execution Client is installed on each node of a cluster, the RES configuration file on each remote box running the server must have an entry in the [client] section for each node of the cluster. You cannot use a single entry for the virtual IP of the cluster. The RES configuration file on each node of the cluster where the client is installed should have identical entries in the [server] section. The following example is for the server. For a corresponding example for cluster configurations for Remote Execution Clients, refer to the topic, ***Configurations for the Client*** (on page 278).

Here is an example of the clients listed in the configuration file for the server on each remote system with entries for each node of the cluster where the clients run:

192.168.2.1,/opt/messageway/utils/keyA.mkf,"Test Passphrase"

192.168.2.2,/opt/messageway/utils/keyA.mkf,"Test Passphrase"

IMPORTANT: After the necessary changes have been made to the server configuration file, mwresd.conf, ensure that the file is at one of the locations in the following list.

For Windows systems during startup, the server looks for it's configuration file in the following locations, in the order shown:

1. Location identified in the environment variable, **MWRESD_CONF**

   NOTE: Users must create this variable.

2. MessageWay user's application folder,
   \Users\MessageWayUser\AppData\Roaming\messageway
3. All users or common application folder,
   \ProgramData\messageway

4 Directory where the program was started

For UNIX or Linux systems during startup, the server looks for it's configuration file in the following locations, in the order shown:

1 Location identified in the **ENV** variable, **MWRESD_CONF**, which is invoked from the startup script

IMPORTANT: If you install RES in a location other than the default, /etc/messageway, you should modify the ENV variable in the shell script to point to the install location.

2 **HOME** directory (**$HOME**) of the user, **root**, who starts the server

3 In /etc/messageway, because **install.sh** creates a copy here for the server

Configurations for the RES Client

The client component of the Remote Execution Server system resides with the MessageWay Server. It receives commands from a Custom Processing or Custom IO location, which it passes to the server listed in the command.

The following table explains the configuration options for the client, which shares the configuration file, mwres.conf, with the monitor.

Section and Parameter	Description of Parameter
Global Section	
timeout	Time (seconds) for connection and response timeouts. Connection timeout is used to timeout connection attempts. It is limited to a max. of 30 seconds. Response timeout is used to limit the amount of time to wait for response from the remote server. Default: unlimited. Overridden by -t switch.
retry	Number of times a connection attempt will be tried after initial failure. Connection retries (integer) specifies the number of times a connection attempt will be retried. Default: no retries. Overridden by -r switch.
delay	Time in seconds to wait between retry attempts. Default: no delay. Overridden by -d switch.
Authorized Servers Section	
servers	Servers where the client is authorized to connect (syntax follows).

List the servers one per line after the [servers] section. The syntax for the server entries is as follows:

[servers]
Server Name,*Server IP Address*[/Secondary IP Address]:*Port*,*Path to Key File/keyfile***.mfk**[,**"***Passphrase***"**]

This table explains the options.

Parameter	Description
Server Name	Server name may or may not be the same as the system hostname of the machine where the RES server is installed. This parameter is used by the RES client to determine which RES server to execute from either a Custom Processing or Custom IO location.
Server IP Address	Primary Internet Protocol (IP) address for this server.
Secondary IP Address	Secondary IP address for this server. Used when the **-s** option is set in the command line.
Port	Port number on the server to which the client connects.
Path to Key File	Where the encryption key file resides that was generated for this server.
keyfile	Name of the key file, which uses an extension of **.mfk**.
Passphrase	Optional. Allows users to modify the shared key for more security. When used, the client will compute an MD5 hash of the passphrase and apply it to the encryption key before use. The passphrase must be enclosed in double quotation marks.

Here are some Windows examples:

```
Server1,192.168.1.1:6235,c:\Program Files\MessageWay\utils\keyfile.mkf
```

```
Server2,192.168.1.2/192.168.1.3:6235,c:\Program Files\MessageWay\utils\keyfile.mkf,"passphrase"
```

Here are some UNIX and Linux examples:

```
Server1,192.168.1.1:6235,/opt/messageway/utils/keyfile.mkf
```

```
Server2,192.168.1.2/192.168.1.3:6235,/opt/messageway/utils/keyfile.mkf,"passphrase"
```

IMPORTANT: When the Remote Execution Client is installed on each node of a cluster, the RES configuration file on each remote box running the server must have an entry in the [client] section for each node of the cluster. You cannot use a single entry for the virtual IP of the cluster. The RES configuration file on each node of the cluster where the client is installed should have identical entries in the [server] section. The following example is for the client. For a corresponding example for cluster configurations for Remote Execution Servers, refer to the topic, ***Configurations for the Server*** (on page 275).

Here is an example of the server listed in the configuration file for the client on each node of a cluster:

```
RedHat, 192.168.2.3:6235,/opt/messageway/utils/keyA.mkf,"Test Passphrase"
```

IMPORTANT: After the necessary changes have been made to the client configuration file, mwres.conf, ensure that the file is at one of the locations in the following list.

For Windows systems during startup or when invoked, the client looks for it's configuration file in the following locations, in the order shown:

1 Location identified in the environment variable, **MWRES_CONF**

NOTE: Users must create this variable.

2 MessageWay user's application folder, \Users\MessageWayUser\AppData\Roaming\messageway

3 All Users or common application folder, \ProgramData\messageway

4 Directory where the program was started

For UNIX or Linux, when started or invoked, the client looks for it's configuration file in the following locations, in the order shown:

1 Location identified in the **ENV** variable, **MWRES_CONF**

IMPORTANT: Unlike the ENV variable for the RES server, users must create the ENV variable for the client, and then define it in the bash profile.

2 **HOME** directory (**$HOME**) of the user/process, **mway**, which usually invokes the client

3 In /etc/messageway

Configurations for the RES Monitor

The optional monitor component of the Remote Execution Server system is part of the MessageWay Schedule Server and resides with the MessageWay Server. The Remote Execution Server Monitor tracks the status, running or not, of all Remote Execution Servers listed in the configuration file and sends notifications to various locations.

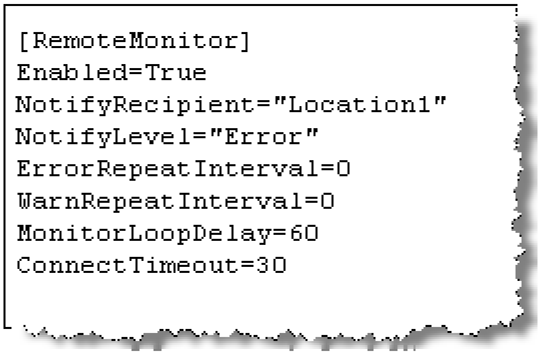
IMPORTANT: You must restart the MessageWay Scheduling Server after the RES Monitor is enabled in the configuration file.

The following table explains the configuration options for the monitor in the mwres.conf file, which it shares with the client.

Section and Parameter	Description of Parameter
RemoteMonitor Section	
Enabled	▪ **True** - monitor will check connections to servers ▪ **False** or *commented out* - monitor will not run
NotifyRecipient	Send notifications to this MessageWay location as well as the system event log
NotifyLevel	▪ **Error** - only send notifications when there are errors ▪ **Warn** - send notifications when there are errors or warnings ▪ **Info** - send notifications for all events
ErrorRepeatInterval	Send notifications errors at this interval in minutes, while the server is not running: ▪ **0** - Report this error only once ▪ *>0* - Repeat error at this interval

Section and Parameter	Description of Parameter
WarnRepeatInterval	Send notification warnings at this interval in minutes, while the server is not running: ▪ **0** - Report this error only once ▪ *>0* - Repeat warning at this interval
MonitorLoopDelay	Time in seconds that the monitor should repeat its cycle to contact the servers
ConnectTimeout	Time in seconds for the monitor to wait for a response from the server. If the connection does not succeed within this time, the monitor considers the server in a state of not running.

The Remote Monitor section is used by the MessageWay Scheduling Server to control monitoring of remote RES servers. The following example shows a typical configuration.



```
[RemoteMonitor]
Enabled=True
NotifyRecipient="Location1"
NotifyLevel="Error"
ErrorRepeatInterval=0
WarnRepeatInterval=0
MonitorLoopDelay=60
ConnectTimeout=30
```

Configuring Security for the Remote Execution Server

The Remote Execution Server system authorizes script execution and protects data exchanged between the client and server machines from public access. To do so, it uses three methods: connection security, script security context and logon security.

The RES uses a session-specific key to encrypt the data passing through the connection between the client and server. The remote server generates the session key, which it encrypts using the shared key and passes to the client at the beginning of the session.

If a passphrase is provided, the server will use it to modify the shared key before it is used. Users must manually distribute the key to the server system the first time. The key could be updated on a regular basis for increased security.

The server accepts connections only from a list of approved client IP addresses from the configuration file. All other connections are refused. A separate key may be configured for each IP address.

You set the security context of the script by passing a user ID and password over the encrypted connection.

Logon security controls access to the Remote Execution Server.

Generating the Shared Key File

You generate the shared key on the system where the client resides and distribute a copy to the server.

The default location for the program that generates the key files, mwkeygen, and the key files themselves depends on the operating system, as shown in the following table:

Operating System	Default Location of Key Files
UNIX or Linux	**/opt/messageway/utils/mwkeygen**
Windows	**C:\Program Files\MessageWay\utils\mwkeygen.exe**

The syntax for the shared-key generation program is simply the executable followed by the file name of the key file you want to create. Once you create the key file on the client system, you should put a copy on the system where the server resides. When both the client and server are on the same system, they will share the one key file.

The syntax for the file name is as follows:

{*fully-qualified file name*|*file name*}[**.***suffix*]

- When a suffix is not supplied, the default suffix .mkf is used.
- File names that are not fully qualified are created in the current directory.

Here are some Windows examples that are executed from a command prompt where the program resides:

mwkeygen keyA	Creates a key file, **keyA.mkf**, in the current directory.
mwkeygen keyA.key	Creates a key file, **keyA.key**, in the current directory.
mwkeygen c:\keyfiles\keyA	Creates a key file, **keyA.mkf**, in the **c:\keyfiles** directory. The directory must exist.

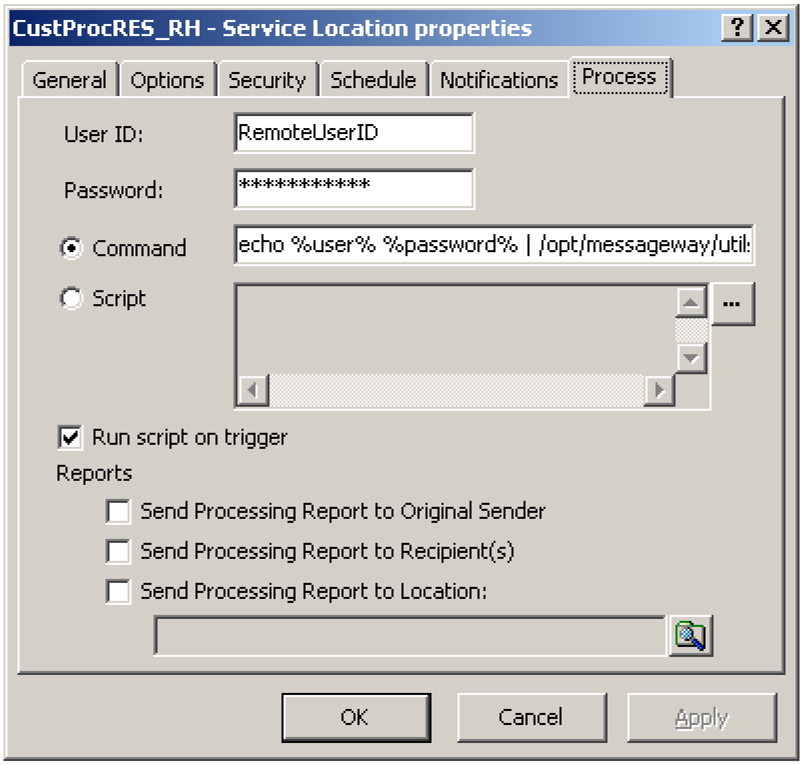
Here are some UNIX and Linux examples that are executed from a command prompt where the program resides:

./mwkeygen keyA	Creates a key file, **keyA.mkf**, in the current directory.
./mwkeygen keyA.key	Creates a key file, **keyA.key**, in the current directory.
./mwkeygen /opt/keyfiles/keyA	Creates a key file, **keyA.mkf**, in the **/opt/keyfiles** directory. The directory must exist.

Security Context of Remote Script

IMPORTANT: You maintain the security of the script by not showing your password in clear text. The client will pass encrypted text to the server. Users should take care to make sure the password is not displayed as clear text in the location configuration.

You do this by configuring the password within the location configuration and then using the %password% replaceable parameter in the script. This way, the password never appears in clear text in the configuration files, as you can see in the following example. When you use the %password% token, you typically also use the %user% token, although either could be typed in clear text.



User ID: RemoteUserID

Password: ***********

● Command echo %user% %password% | /opt/messageway/util:

○ Script

☑ Run script on trigger

Reports

□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

□ Send Processing Report to Location:

Logon Security

The Remote Execution Server requires certain security settings to enable the client to log on to the system on which the server resides.

You will perform different tasks, depending on where the server resides, UNIX/Linux or Windows.

Setting Logon Security for Windows

When the client sends a user ID to the Remote Execution Server, that user ID must have special privileges on the Windows system. If you need a special user ID to log on to Windows for this, create that user before you perform this task.

To grant the privileges, do the following:

1 From the **Start** menu, select **Programs|Administrative Tools|Local Security Policy**.

- or -

From the Control Panel window, select **Administrative Tools|Local Security Policy**.

The Local Security Settings window appears.

2 In the left pane, within the Local Policies folder, select **User Rights Assignment**.

3 In the right pane, double-click **Log on as a batch job**.

The Log on as a batch job Properties window appears.

4 Select the **Add User or Group** button.

The Select Users or Groups window appears.

5 Do the following:

a) In Enter the object names to select, type the following:

machine name\user ID to be passed by the client

b) Select **Check Names** and then **OK** twice to return to the Local Security Settings window.

If the object name is valid, the properties window appears with the user ID added to the **Member Of** tab.

Setting Logon Security for UNIX or Linux

For a UNIX or Linux system, the RES Server uses Pluggable Authentication Modules (PAM) to authenticate the remote user specified by the RES Client. PAM uses system-supplied shared objects for user authentication. The installation provides files that contain instructions to setup PAM on the system where the RES Server will be running.

For Linux, copy the mwresd.pam.gcc file as follows:

From Location	To Location
/opt/messageway/res/mwresd.pam.gcc	/etc/pam.d/mwresd

For UNIX, append the mwresd.pam.sol file as follows:

From Location	To Location
/opt/messageway/res/mwresd.pam.sol	/etc/pam.conf

For more information about PAM, visit the site ***http://www.kernel.org/pub/linux/libs/pam/*** (***http://www.kernel.org/pub/linux/libs/pam/***).

Configuring the Command Line for the Client

On the **Process** tab of the Custom Processing service location or the **Input** or **Output** tabs of the Custom IO site, you enter the command that will eventually go to the server. The client must send the following information to the server:

- User ID and password to log on to the server
- Command that the server is to execute

IMPORTANT: For clients installed on Windows, you must add the install directory to the system path. On Windows XP, go to My Computer>Properties>Advanced tab>Environment Variables button>System

Variables box, select the **path** variable and click the **Edit** button. Then add the install directory for the RES client, C:\Program Files\messageway\utils.

The normal syntax of the command that must go in the **Command** box or in the **Script** box is as follows:

mwres **-u** *user* **-p** *password* [**-r** *retries* **-d** *delay*] [**-s**] [**-t** *timeout*] *remote_server* **"***remote_command_line***"**

In the **Script** window or from the command line, you may also specify the user ID and password followed by a pipe mark in front of the client program, in which case the values will be passed using the standard-in process:

echo *user password* | *mwres* [**-r** *retries* **-d** *delay*] [**-s**] [**-t** *timeout*] *remote_server* **"***remote_command_line***"**

- For more information about how to use the tokens %user% and %password%, refer to the topic, ***Using Replaceable Parameters (Custom Processing Service Location)*** (on page 571).
- When *user* is blank or *remote_server* is not defined, then the client will return an error without contacting the server.

The following table describes the syntax.

Options	Description
mwres	This is the client program. Assuming the program is in the current directory, the syntax for the different operating systems is as follows: ▪ UNIX or Linux: **/opt/messageway/utils/mwres** ▪ Windows: **mwres**
user	A valid user to log on to the server, which may be represented by one of the following: ▪ %user% - token, typically used with %password% ▪ **-u** followed by name of the user
password	A valid password for the user, which may be represented by one of the following: ▪ %password% - token, typically used with %user% and followed by a pipe symbol (**|**) ▪ **-p** followed by password
-r *retries*	Number of times to retry after failed connections; Used with *delay*.
-d *delay*	Number of seconds to delay before next retry attempt; Used with *retries*.
-s	If a secondary IP address is specified in the configuration file, then the client will attempt to connect to the secondary IP address after all attempts to connect to the primary IP address have failed. If the **-r** and **-d** options are also set, then the secondary IP connection will follow the same retry rules as the primary.
-t *timeout*	Amount of time in seconds the client will wait for a response from the server. Overrides setting in the configuration file.

Options	Description
remote_server	Use the server name. The name of the remote server must match the name of the server given in the servers section of the configuration file that is associated with the IP address of the server.
"*remote_command_line*"	This is the command, in quotation marks, that the remote server will execute. To execute DOS commands on Windows, use the syntax, **"cmd.exe /c** ***command*****"**

Here are some examples for a Windows client that you would enter in the Command box:

- **echo %user% %password% | mwres WindowsXP "cmd.exe /c cd"**
- **mwres -u MyUserID -p MyPassword Solaris "ls -al"**
- **mwres -u %user% -p %password% Solaris "hostname"**

Here are some examples for a UNIX or Linux client that you would enter in the Command box:

- **echo %user% %password% | /opt/messageway/utils/mwres WindowsXP "cmd.exe /c cd"**
- **/opt/messageway/utils/mwres -u MyUserID -p MyPassword RedHat "ls -al"**
- **/opt/messageway/utils/mwres -u %user% -p %password% RedHat "hostname"**

Configuring Events to Initiate Commands

There are three types of events that will cause a Custom Processing service location to execute its command to invoke the remote execution client:

- For the Custom Processing service location, the **Run script on trigger** is checked on the **Process** page of the Custom Processing service location window, and:
  - A message trigger is sent to a Custom Processing service location

    - or -
  - An operator issues the **Execute Now** command, from the MessageWay Manager
- For the schedule for the Custom Processing Service Location, a schedule item is configured to generate a trigger message when the schedule opens, which requires:
  - Day and time when schedule opens
  - **Trigger** box checked, and the **Input or Execute Now** option selected

Sending a Message Trigger

Messages that may or may not have content, when the message itself is not sent out of MessageWay, is called a message trigger. For the Remote Execution Server, you use message triggers to invoke the command configured for the Custom Processing service location or Custom IO site. This command initiates the process that will typically run on a remote server.

To use this method, you send a small message from MessageWay to the Custom Processing service location or Custom IO site. These are normal messages or notifications, and will queue to the location until they can be delivered. You can always track trigger messages, because they will be logged as soon as they enter MessageWay.

Issuing the Execute Now Command

For testing the Remote Execution Server, you can issue the **Execute Now** command from the MessageWay Manager to activate the command configured for the Custom Processing service location. This command initiates the process that will typically run on a remote server.

The Custom Processing service must be running and the **Run script on trigger** must be checked.

IMPORTANT: This command will override a closed schedule or a location that is on hold.

To manually create a trigger message, proceed as follows:

1. From the left pane of MessageWay Explorer, select **Locations**.
2. From the right pane, right-click a custom processing service location, and select **Execute Now** from the menu.

   A confirmation dialog box appears to make sure you want to execute the action.
3. Click **OK**.

When the **Execute Now** command is processed, a dummy message will be generated using the name of the Custom Processing service location as both its source and destination locations.

NOTE: If the Custom Processing service is not running, the trigger message is ignored and discarded. You must start the service and re-issue the command.

Configuring a Schedule to Send a Trigger Message

You can also configure the location to queue an action when the schedule for the Custom Processing service location sends a trigger message at a specific day and time.

The Custom Processing service must be running.

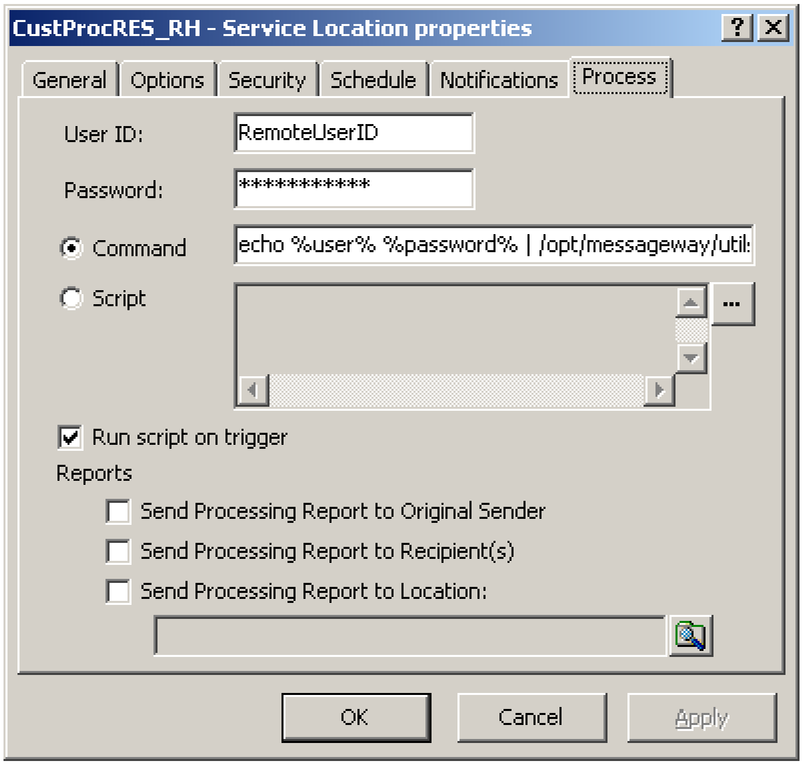
To queue an action using this method:

1. In the right pane, right-click the Custom Processing service location.

   A menu appears.
2. From the menu, select **Properties**.

   The Service Location Properties window appears.
3. From the Service Location Properties window, select the **Process** tab.

4 Check the box, **Run script on trigger**.



User ID: RemoteUserID

Password: ***********

● Command echo %user% %password% | /opt/messageway/util:

○ Script

☑ Run script on trigger

Reports

□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

□ Send Processing Report to Location:

5 Select the **Schedule** tab.

6 For **Schedule Option**, click **Schedule**, and then do one of the following:

a) ***Create a local schedule*** (on page 498)

- or -

b) ***Create or use a master schedule that has already been created*** (on page 496)

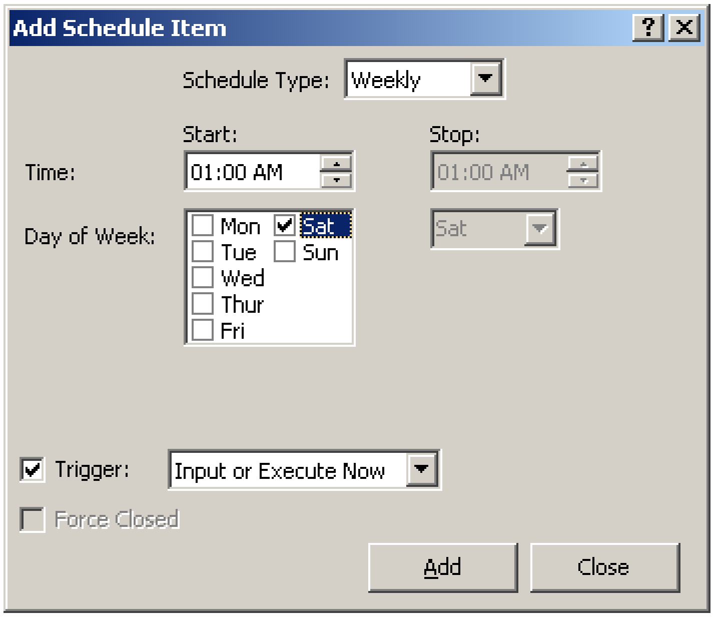
7 From the schedule window, add a schedule item with the following configurations:

a) Check the box, **Trigger**.

b) Select **Input or Execute Now** from the options list.

c) Select **Schedule Type**.

d) Select the appropriate parameters for day, date, time for the type of schedule when you want to open the schedule and send the trigger message.



Add Schedule Item

Schedule Type: Weekly

Time: Start: 01:00 AM Stop: 01:00 AM

Day of Week: □ Mon ☑ Sat □ Tue □ Sun □ Wed □ Thur □ Fri Sat

☑ Trigger: Input or Execute Now

□ Force Closed

When the schedule opens, the service location queues a trigger message to itself to run the script.

When the script is processed, a dummy message will be generated using the name of the Custom Processing service location as both its source and destination locations.

Testing the Remote Execution Server

To test the Remote Execution Server process from end to end, make sure you have completed the installation tasks, described in the topic, ***Basic Installation Tasks*** (on page 271).

Start the Remote Execution Server

You start the Remote Execution Server (RES) differently, depending on the operating system where the server resides: UNIX/Linux or Windows.

To Start the Remote Execution Server on Windows

To start the Remote Execution Server on Windows, proceed as follows:

1. From the **Start** menu, select **Programs|Administrative Tools|Computer Management**.

   The Computer Manager window appears.
2. In the left pane, expand the folder Services and Applications, and click **Services**.

   The Services window appears.
3. In the right pane, scroll to the service, **MessageWay RES**.
4. Right-click **MessageWay RES**, and select **Start** from the menu.

The Status column should display **Started**.

5 To start the service automatically when the operating system boots:

a) Right-click **MessageWay RES**, and select **Properties** from the menu.

The MessageWay RES Properties window appears.

b) On the **General** tab, from the Startup type list, select **Automatic**,and click **OK**.

The Startup Type column should display **Automatic**.

To Start the Remote Execution Server on UNIX or Linux

On UNIX or Linux, you start the Remote Execution Server with a startup script. The startup script, **mwresd**, has the options, **start**,**stop**,**restart** and **status**.

IMPORTANT: The script and the daemon process that the script starts and stops can be started only by the user, **root**. Check the system logs for errors if the server daemon process fails to start.

To start the Remote Execution Server on UNIX or Linux, proceed as follows:

1 Make sure you are logged on as the user, **root**.

NOTE: The remote execution server requires root access because it allows sessions to log on and this requires root access. Note that only port listening and credential validation is performed as root; thereafter, the session thread runs as the logged-on user.

2 Go to the subdirectory where the script resides by typing:

```
cd /etc/init.d
```

3 To start the server daemon process, type:

```
./mwresd start
```

- or -

To check the server status, type:

```
./mwresd status
```

- or -

To stop the server, type:

```
./mwresd stop
```

- or -

To restart the server, type:

```
./mwresd restart
```

Test the Connection Between the Client and Server

You test the connection between the client and the server to verify that the secure connection works. A successful test assures you that shared keys and IP address are correct and that the encryption is working properly.

You can test the connection between the client and server from a command line. The command actually mimics the process the monitor uses to check the status of servers.

1 Make sure the Remote Execution Server is started. For more information, refer to the topic, ***Start the Remote Execution Server*** (on page 289).

2 From a command line, go to the location where the RES client runs:

Windows	**cd \Program Files\MessageWay\utils**
UNIX or Linux	**cd /opt/messageway/utils**

3 Type the command that invokes the client to check the status of a server:

The name of the server must be the same name you specified in the [servers] section of the configuration file. Do not use the IP address.

Windows	**mwres -x** *name of server*
UNIX or Linux	**./mwres -x** *name of server*

4 Review the information in the log for the server, whose location is specified in the RES configuration file as follows, depending on the operating system:

All systems	Environment Variable	**MWRES_LOGDIR**
Windows	Executable Directory	**\Program Files\MessageWay\res \mwres_audit***yyyymmdd***.txt**
UNIX or Linux		**/var/log/mwres_audit***yyyymmdd***.txt**
UNIX or Linux	HOME directory	**~**

Test the Syntax of the Command from the Client

You test the command that the client sends to the server to verify the syntax. A successful test assures you that the syntax is correct and that the shared keys and IP address are correct and that the encryption is working properly.

You can test the command from a command line. The command actually mimics the process the client uses when it receives the command from MessageWay.

1 Make sure the Remote Execution Server is started. For more information, refer to the topic, ***Start the Remote Execution Server*** (on page 289).

2 From a command line, go to the location where the RES client runs:

Windows	**cd \Program Files\MessageWay\utils**
UNIX or	**cd /opt/messageway/utils**

Linux

3 Type the command that invokes the client to send a command to a server:

The name of the server must be the same name you specified in the [servers] section of the configuration file. Do not use the IP address. For information and examples of the command syntax, refer to the topic, ***Configuring the Command Line for the Client*** (on page 284).

Windows	**mwres** *command syntax*
UNIX or Linux	**./mwres** *command syntax*

NOTE: You cannot use MessageWay tokens at a system command line, so you must use actual values. For example, type a command similar to the following:
mwres -u MyUserID -p My Password WindowsXP "hostname"

4 Review the information in the system log for the server, whose location is specified in the configuration file as follows, depending on the operating system:

All systems	Environment Variable	**MWRES_LOGDIR**
Windows	Executable Directory	**\Program Files\MessageWay\res \mwres_audit***yyyymmdd***.txt**
UNIX or Linux		**/var/log/mwres_audit***yyyymmdd***.txt**
UNIX or Linux	HOME directory	**~**

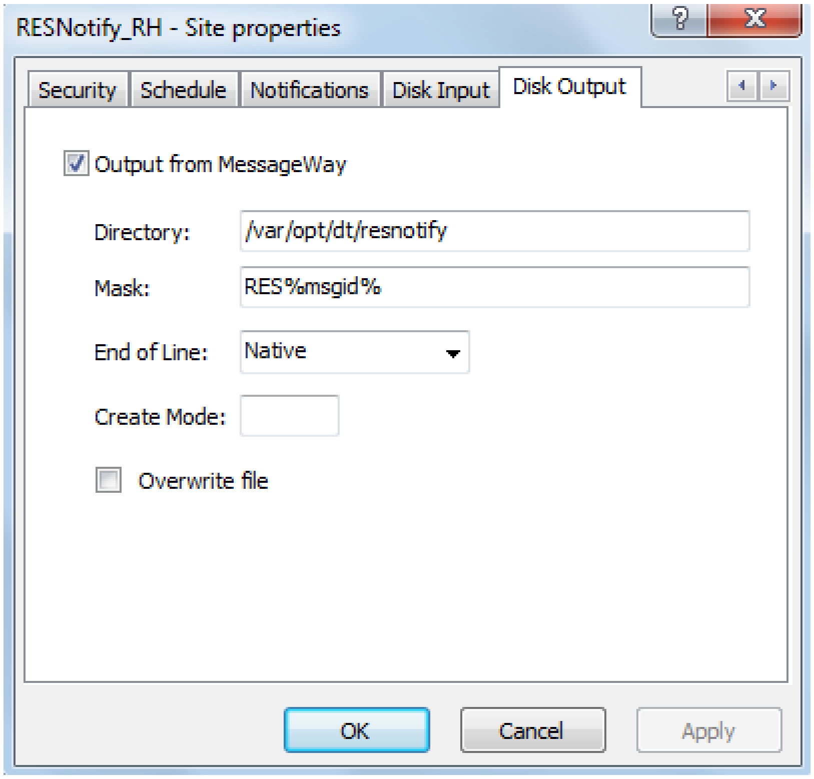
Create a Disk Transfer Site for Notifications from the RES Monitor

The RES monitor periodically contacts the server to determine if it is still running. Users can configure the monitor to create notifications back to a location every time it successfully contacts the server.

If you are unfamiliar with how to create a disk transfer site, refer to the topic, ***Configuring Locations Properties*** (on page 453).

1 Create a directory, and make sure the owner of MessageWay or its group has security to write to the directory.

2 On the **Disk Output** tab, enter an appropriate directory and a mask to create the file name.


RESNotify_RH - Site properties

☑ Output from MessageWay

Directory: /var/opt/dt/resnotify

Mask: RES%msgid%

End of Line: Native

Create Mode:

□ Overwrite file

Test the Monitor

The optional monitor component of the Remote Execution Server system is part of the MessageWay Scheduling Server and resides with the MessageWay Server. The Remote Server Monitor tracks the status, running or not, of all Remote Execution Servers and sends notifications to various locations.

The monitor will perform its tasks based on the information it finds in the configuration file.For information about what the monitor does, refer to the topic, ***Tasks for the Monitor*** (on page 273).

1 Make sure the monitor is configured to start as follows:

- **Enabled=True**
- **NotifyRecipient=***valid MessageWay location*
- **NotifyLevel=Info**

For more information, refer to the topic, ***Configurations for the Monitor*** (on page 280).

2 Make sure the Remote Execution Server is started. For more information, refer to the topic, ***Start the Remote Execution Server*** (on page 289).

3 Start or restart the MessageWay Server:

- ***MessageWay Startup and Shutdown for UNIX and Linux*** (on page 27)
- ***MessageWay Startup and Shutdown for Windows*** (on page 30)

4 After an appropriate period of time that the monitor should have contacted the server, check the location specified in NotifyRecipient for messages. The sender will be MWSched.

- or -

Review the information in the system log for the server, whose location is specified in the configuration file as follows, depending on the operating system:

All systems	Environment Variable	**MWRES_LOGDIR**
Windows	Executable Directory	**\Program Files\MessageWay\res \mwres_audit***yyyymmdd***.txt**
UNIX or Linux		**/var/log/mwres_audit***yyyymmdd***.txt**
UNIX or Linux	HOME directory	**~**

Messages begin with **Warn**, **Error** or **Info**.

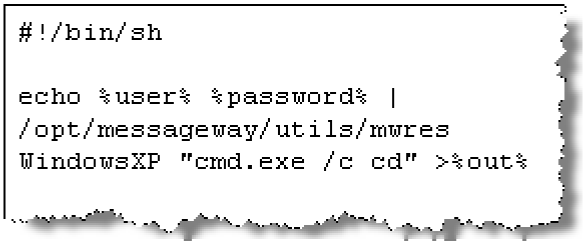
Create a Custom Processing Service Location

For this test, we are going to create a custom processing service location. If you are unfamiliar with how to create this type of location, refer to the topic, ***Configuring a Custom Processing Service Location*** (on page 565).

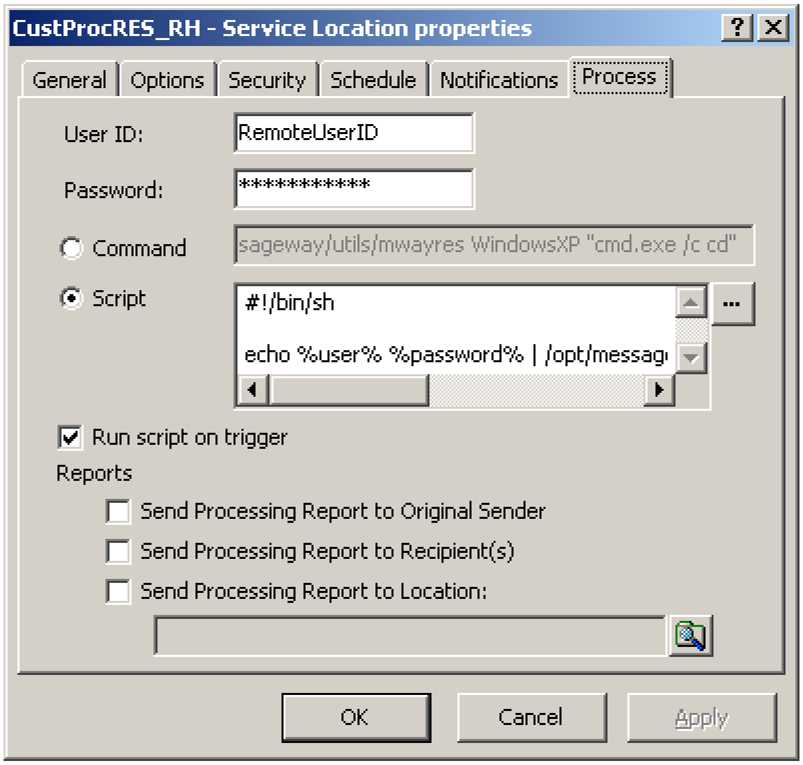
You will use the user and password tokens to keep your password secure and out of view. MessageWay will replace the tokens with the values in the User ID and Password fields before the client sends them to the server.

1. On the **Process** tab, type the user ID and password that the client will send to the server to execute the command as a batch user.
2. Check the box, **Run script on trigger or schedule**.

3 Select **Script**, and enter the information to send a test command, such as the example below where the client is on Linux and the RES server is on Windows:



```
#!/bin/sh

echo %user% %password% |
/opt/messageway/utils/mwres
WindowsXP "cmd.exe /c cd" >%out%
```



CustProcRES_RH - Service Location properties

User ID: RemoteUserID

Password: ************

○ Command sageway/utils/mwayres WindowsXP "cmd.exe /c cd"

● Script

```
#!/bin/sh

echo %user% %password% | /opt/messagi
```

☑ Run script on trigger

Reports

☐ Send Processing Report to Original Sender

☐ Send Processing Report to Recipient(s)

☐ Send Processing Report to Location:

Test the System End-to-End

To test the entire system, you will have MessageWay generate a trigger to send a command to a client that will, in turn, send the command to the Remote Execution Server.

This set of tasks assumes you have performed the preceding tasks. Proceed as follows:

1 From the MessageWay Manager, start the Custom Processing service, MWCustomProc.

2 Start the Disk Transfer adapter, MWDisk, so the notification location will distribute notifications.

3 Issue the ***Execute Now command*** (on page 287).

4 Review the message that pertains to your test, which is a dummy message generated by the **Execute Now** command.

a) Within the MessageWay Manager monitor, from the **Complete** box of the **Service** area, double-click the number.

A Message List window appears.

b) In the Message List window, double-click a recent message whose sender is MWSCHED, which should be the trigger message generated when you selected **Execute Now** command.

A Message window appears with information about the trigger that the command generated.

5 Find the output of the script command in:

- The logging directory, if you have logging enabled and reporting responses

  - or -

- A message delivered to the {Unknown} system location, if you followed the example in the script box and send the output to %out%.
  The default destination for output returned to a Custom Processing service location when you use the Execute Now command to trigger a process where the output is sent to %out% is a location called UNKNOWN. When that location is not defined, the message is sent to the system mailbox, {Unknown}. This is a simple test, but in reality, you would probably have a more extensive script that would create a status file to control what MessageWay does with the output.

Troubleshooting Remote Execution Server

This table contains a list of errors that the client component of the Remote Execution Server might generate. When the client generates errors, it returns an error code and error text that is sent to standard out. Error text begins with **mwres:**.

IMPORTANT: The Windows MessageWay MWRES.exe utility does not support non-ASCII Unicode characters for any command line options. An ASCII path to the executable, an ASCII username/password, and ASCII options are required for the utility to function as intended. Keep this in mind when configuring Custom I/O adapters or Custom Proc services configured through the MessageWay Manager. Similarly, the Windows MessageWay MWRES perimeter server does not support commands with non-ASCII Unicode characters from any MWRES client.

Any error codes outside of this range would be from the remote server.

Error Code	Cause	Error Text
100	Invalid command line options used.	Displays **mwres** usage syntax
101	Server name not supplied or empty.	**mwres: Missing Server Name**
102	Error in configuration file mwres.conf.	**mwres: Config file error:** *detailed description*
103	Unable to find Server in mwres.conf.	**mwres: Unable to find server -** *detailed description*
104	Unable to create a socket (rare).	**mwres: Unable to create a remote socket connection**
105	Missing user name.	**mwres: Missing user name**

Error Code	Cause	Error Text
106	Unable to establish a socket connection to the remote server.	**mwres: Connect failure to remote server -** *detailed description*
107	A timeout has occurred waiting for a response from the remote server.	**mwres: Receive timeout exceeded**

This table contains a list of errors that the server component of the Remote Execution Server might generate.

Error Code	Cause	Error Text
503	RES server returned a response to the client that its service was unavailable.	**RES service unavailable**
7005	Logs this event if the server has trouble reading and loading the mwres.conf parameters into memory. This is done at startup and causes the service/daemon to stop.	**Load error RES config file**
7006	This error is logged when the listener (the thread that accepts connection from remote) encounters errors. All errors on the listener are considered critical and will cause the program to halt. An exception is the **Max connections exceeded** event, which is logged as a Warning event.	**Listener error**
7007	This event can be generated for several reasons; some of the common ones might be: ▪ Client configuration entry not found in mwres.conf ▪ Shared key file not found or could not be read (security;bad format;corrupt) ▪ Shared Key file mismatch	**Remote client connection failure**

Error Code	Cause	Error Text
7008	This event is generated when a valid **Command** request is sent but there is a user authentication failure; (user not found, user unable to login at this time, invalid password, etc.).	**User authentication failure**

Configuring the SFTP Perimeter Server

The MessageWay SFTP Perimeter Server provides secure access to MessageWay from an external SFTP client using Secure Shell (SSH) and SFTP protocol. The MessageWay SFTP Perimeter Server does not provide SCP server capability.

IMPORTANT: This is a dedicated MessageWay perimeter server that communicates between SFTP clients and MessageWay to access messages in mailboxes. MessageWay supports two ways for clients to view messages: a proprietary view based on message status and a traditional FTP type hierarchical directory view. The two views have different access and location configuration options, which are explained throughout the help file. Which view the client uses for a given session depends on the configuration for the user that logs on to MessageWay. The Default Location on the User Properties window will show either a mailbox that resides in the Locations folder, which uses the proprietary view, or a mailbox that resides in the File System folder, which uses the hierarchical directory view.

This option uses the following components:

- MessageWay SFTP Perimeter Server
- MessageWay Service Interface (SI), installed separately with the MessageWay Server

These components typically have the following physical relationships:

- SFTP Perimeter Server may reside on any server
- MessageWay Service Interface must reside on the same system as the MessageWay Server

Licensing Requirements for the SFTP Perimeter Server

The MessageWay SFTP Perimeter Server, the MessageWay SFTP Adapter and the MessageWay SFTP Proxy Server are all included in the MessageWay base license, although you install and configure them separately. For more information, contact MessageWay Technical Support.

The SSH host keys are generated during MessageWay SFTP Perimeter Server installation to enable secure communications between SFTP clients and the SFTP Perimeter Server. These keys are production-ready and do not require replacement. The configuration file is pre-configured to use the keys generated during installation.

Progress has provided certificates with the MessageWay installation as part of the Service Interface for users to be able to test SSL communications between the MessageWay SFTP Perimeter Server and the Service Interface. At least for the final stages of testing, users should obtain their own certificates from a trusted licensing authority.

To install the SFTP Server on Windows, you must first install ***Cygwin*** (***http://www.cygwin.com/***), which is open software that provides a Linux-like environment on a Windows system.

Overview of the SFTP Perimeter Server

Secure Shell (SSH) File Transfer Protocol (SFTP) is a way to move data securely from computer to computer. The MessageWay SFTP Perimeter Server provides secure access to MessageWay from an SFTP client over SSH. Since SFTP does not provide security, it runs as a subsystem under SSH file transfer protocol, which provides the authentication and security.

On Linux or UNIX, the SFTP Perimeter Server runs in native mode. On Windows, the SFTP Perimeter Server runs under the open software, ***Cygwin*** (***http://www.cygwin.com/***), which provides a Linux API emulation layer.

The SFTP Perimeter Server is based on the following references:

- ***SFTP, DS version 02, protocol version 3*** (***http://tools.ietf.org/pdf/draft-ietf-secsh-filexfer-02.pdf***)
- SSH, OpenSSH, version 2 only
- OpenSSH version 7.4p1
- SSL 3.0/TLS 1.0 ***RFC 2246*** (***http://tools.ietf.org/html/rfc2246***)

Components and Processes of the SFTP Perimeter Server

The main components of the SFTP perimeter server system perform the following functions:

- The SSH Server uses dedicated threads to listen on a pre-defined port and to create session threads when SFTP clients connect. After SSH authenticates the user, it spawns an SFTP server session. Each session thread controls a single SFTP session.
- The SFTP perimeter server controls the information exchange between the MessageWay Service Interface (SI) and the SFTP client.
- The Service Interface uses dedicated threads to listen on specified HTTP ports and to process:
  - Requests to authenticate users that are received from the SSH server.
  - Requests for MessageWay services that are received from the SFTP Perimeter Server.

The configurations for the SSH server and SFTP perimeter server and the ***Service Interface*** (on page 95) are in separate configuration files. The following steps describe the typical process flow between the SFTP client and MessageWay:

1 At process initialization, the SSH server reads both configuration files, mwsftpd_config and mwsftpd.conf.

2 SSH server receives connection request from SFTP client.

- Default port is typically 22.
- MWay example configuration uses port 6222 to avoid collision with any pre-existing SSH services listening on port 22.

3 The SSH server connects to an HTTP Service Interface port specified in the SFTP perimeter server configuration file, mwsftpd.conf, for access to MessageWay:

- HTTP (non-secure) on dedicated port, 6280 in the example.
- HTTP (secure)/HTTPS on dedicated port, 6243 in the example.

4 MessageWay determines whether the client is allowed to access MessageWay.

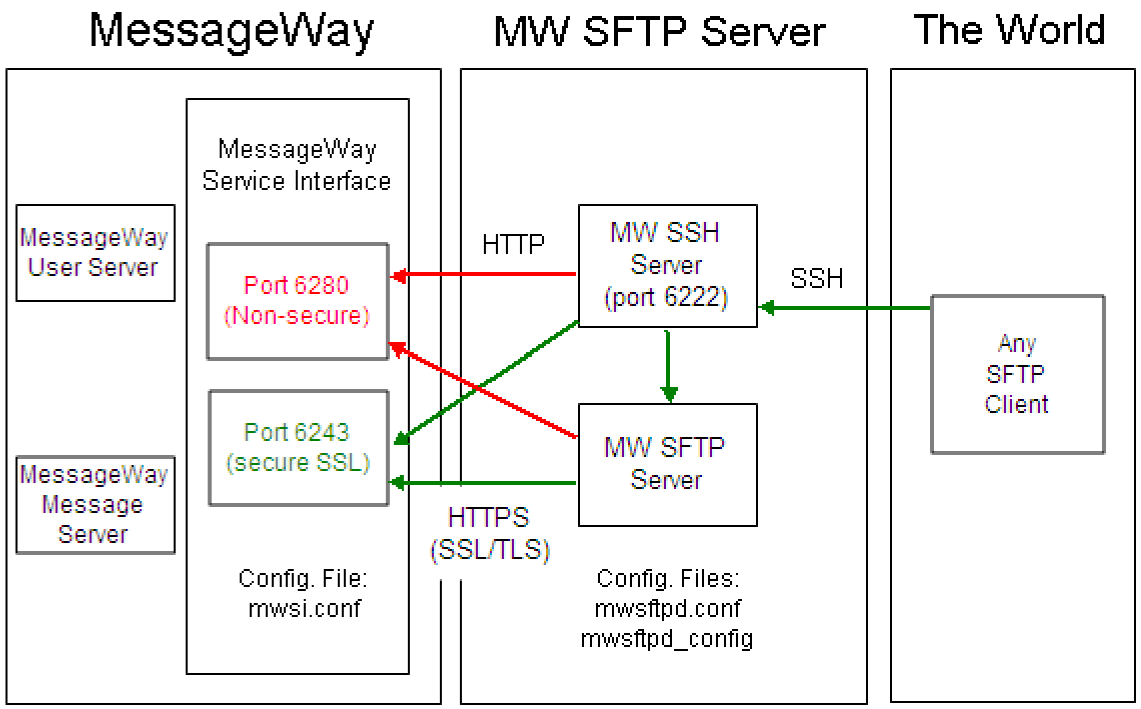
5 If the client is allowed access, the SSH server spawns an SFTP perimeter server to continue the dialog.

6 The SFTP perimeter server saves the authenticated logon information from the SSH server.

7 The SFTP perimeter server controls information between the client and Service Interface.

The following diagram provides a high-level view of the communication process:

NOTE: The MessageWay port to which a connection is made determines whether a connection is secure or non-secure. In the diagram, green indicates a secure connection and red a non-secure connection.



Accessing MessageWay from an SFTP Client

When SFTP clients log on to MessageWay, their MessageWay user configuration defines their ***default location*** (on page 1363) and, optionally, a ***default recipient*** (on page 1363) location. The default location is their SFTP mailbox. By default, all messages are uploaded to and downloaded from the default location. If there is also a default recipient location defined for the user, then all messages are uploaded to this location, unless otherwise stated in the command.

NOTE: Location is a generic term that includes auto-delivery locations, which are service locations and sites, and pickup mailboxes. Mailbox is a specific type of location where users collect messages. A user's default location is always a mailbox. Assuming they have the rights to do so, users may act on locations other than pickup mailboxes. Therefore, here we use the generic term, location.

What type of directory structure a user sees depends on whether the default location is in the Locations folder or in the File System folder. Locations in the File System folder begin with a forward slash, /. For more information about the differences between the two types of locations, refer to the topic, ***Overview of Location Properties*** (on page 453).

IMPORTANT: To use and/or display non-ASCII Unicode characters in users, locations, and file names through the MessageWay FTP and SFTP perimeter servers, FTP and SFTP clients must support Unicode (specifically UTF-8).

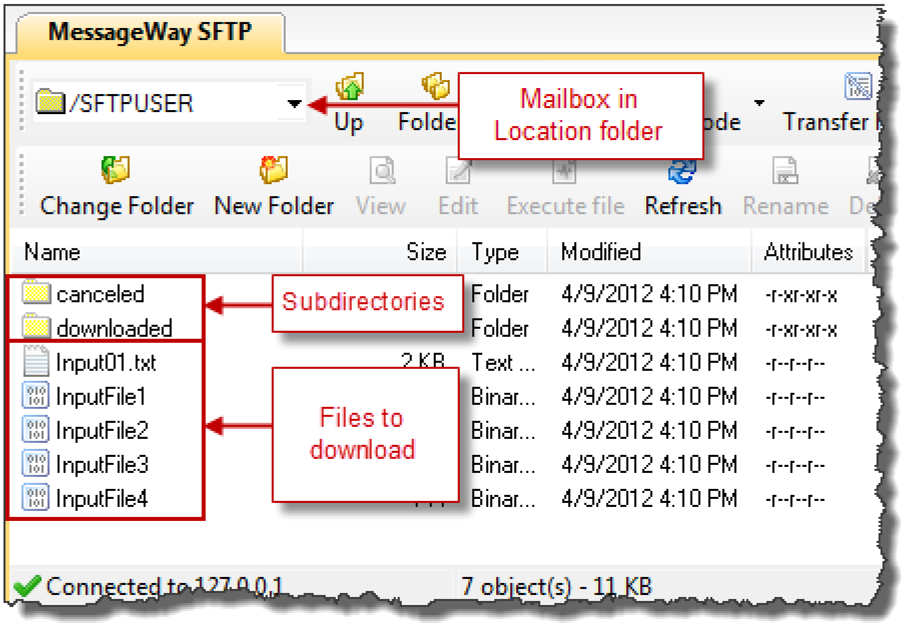
Client View of Messages in Locations Folder (SFTP)

For the Locations folder, when an SFTP client accesses MessageWay, it sees a default hierarchy:

- A root directory, indicated by the forward slash (/)
  - A user's default location (mailbox) directory
    - *Canceled* directory
    - *Downloaded* directory

TIP: You can hide the *canceled* and *downloaded* directories from the client's view so that it is similar to what SFTP clients typically see, and their view will be similar to what they see when using the File System folder. To hide the *canceled* and *downloaded* directories, in the Global section of the SFTP Perimeter Server configuration file mwsftpd.conf, set the *SuppressCanceledAndDownloadDirs* parameter to *True*. For more information, refer to the topic ***SFTP Server, Global Section*** (on page 322).

For example, the SFTP client may show the following:



Mailbox in Location folder

Subdirectories

Files to download

Name	Size	Type	Modified	Attributes
canceled		Folder	4/9/2012 4:10 PM	-r-xr-xr-x
downloaded		Folder	4/9/2012 4:10 PM	-r-xr-xr-x
Input01.txt	2 KB	Text ...	4/9/2012 4:10 PM	-r--r--r--
InputFile1		Binar...	4/9/2012 4:10 PM	-r--r--r--
InputFile2		Binar...	4/9/2012 4:10 PM	-r--r--r--
InputFile3		Binar...	4/9/2012 4:10 PM	-r--r--r--
InputFile4		Binar...	4/9/2012 4:10 PM	-r--r--r--

Connected to 127.0.0.1 7 object(s) - 11 KB

When a user downloads or deletes a message, it moves to the downloaded or canceled directory, respectively. Users can continue to retrieve messages from these directories until the archive program removes them from the system.

Clients view message information from MessageWay in terms of directory structures and file names. From MessageWay Manager, this information is viewed in terms of locations and statuses.

The following table shows these different views. It should help users understand how clients typically view MessageWay.

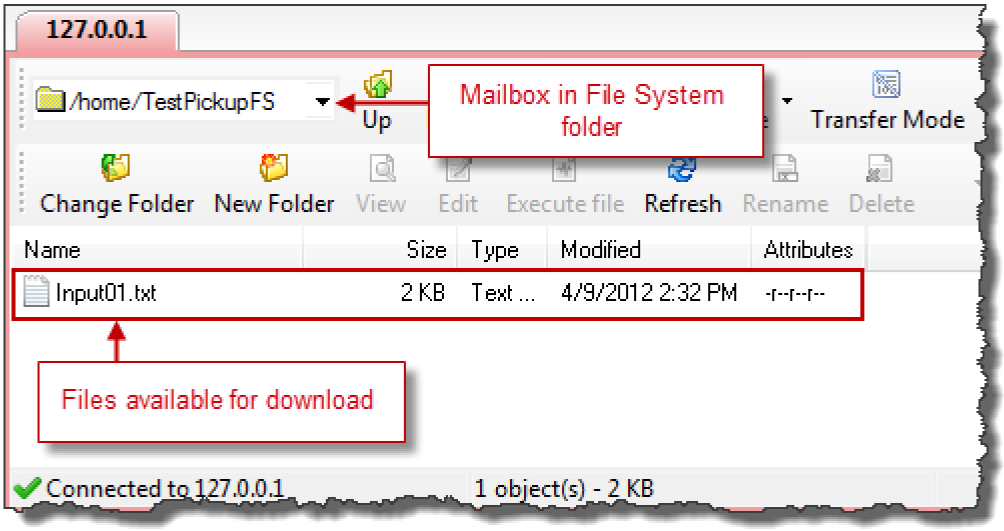
Concept	MessageWay Manger	Client Software
Content	Message ID [Class ID] [filename]	File name
Location	mailbox (current)	/Location directory[/subdirectory]

Status	A = Available
	C = Canceled
	D = Downloaded
		Available = location directory
		Canceled = canceled subdirectory
		Downloaded = downloaded subdirectory

Users can make this link more obvious using the ***file name mapping feature*** (on page 303).

Client View of Messages in File System Folder (SFTP)

If the default location for a user is in the File System folder, when an SFTP client accesses MessageWay, the user sees a hierarchical directory from the default location.



Name	Size	Type	Modified	Attributes
Input01.txt	2 KB	Text ...	4/9/2012 2:32 PM	-r--r--r--

When a user deletes a message, the message is no longer visible.

Understanding Message Names for SFTP

MessageWay has two methods to display file names to client software when they access MessageWay depending on whether the user's default location is in the Locations folder or in the File System folder. If the default location is in the File System folder, the only option is to display the filename property of the message. If the default location is in the Locations folder, additional options are available as described here. For more information about the differences between the two types of locations, refer to the topic, ***Overview of Location Properties*** (on page 453).

For better usability for messages in the Locations folder, you can map the way files are identified on a client system, usually by directory and file name, to the way they are identified in MessageWay. Users configure this parameter, MessageNameFormat, in the configuration file for the SFTP server, mwsftpd.conf.

The MessageNameFormat parameter defines the format used to display file names for MessageWay messages to the client, as specified in the Global section of the SFTP configuration file, mwsftpd.conf. The file names appear in response to an LS command, and the client must use them to perform a GET or RM command.

The message name format must always include either the message ID or filename. In addition, it may include the class ID. If message ID or filename are not part of the defined MessageNameFormat parameter, then message ID will be appended to the displayed message name.

The message name format is defined as 1 to 3 of the following characters:

1	***Message ID*** (on page 1199)
2	***Class ID*** (on page 1187)
3	***Filename*** (on page 1185)

Each character represents a component of the message name (*msg-name*) to be displayed, separated by a plus character, **+**. The number **1** or **3** must be present and if not found, the listener defaults to **1**.

IMPORTANT: MessageWay allows duplicate file names. Internally this is not a problem, because MessageWay always assigns a unique message ID to a message, whether the user chooses to display it or not. So for messages in locations that are defined in the Locations folder, when users download files, there may be more than one file of the same name. Users should take care to make sure that duplicate file names will not cause a problem for their local system. If there could be a problem, it would be wise to always include the message ID as part of the message name. This will also help troubleshooting, because the message ID includes a date and time stamp. For messages in locations defined in the File System folder, duplicate file names are not displayed or not allowed, depending on the command. If a file name exists in a directory (location) in the File System folder and a client attempts to upload a new file of the same name, the original message is canceled, and then the new file is uploaded. Clients viewing a File System directory structure cannot see canceled or downloaded messages.

Here are some examples based on the MessageNameFormat parameter in the Global section that is specified in the SFTP configuration file. The components create the resulting file name:

Parameter	Components	Example of File Name
3	*Filename*	text.txt
1	*MessageID*	20060301125013015784
21	*ClassID***+***MessageID*	xyz+20060301125013015784
13	*MessageID***+***Filename*	20060301125013015784+test.txt
231	*ClassID***+***Filename***+***MessageID*	xyz+test.txt+20060301125013015784

Commands for the MessageWay SFTP Perimeter Server

The following table lists the raw commands supported by the SFTP Server as well as some typical client commands. The associated commands from the client vary based on the client.

NOTE: Location is a generic term that includes auto-delivery locations, which are service locations and sites, and pickup mailboxes. Mailbox is a specific type of location where users collect messages. A user's default location is always a mailbox. Assuming they have the rights to do so, users may act on locations other than pickup mailboxes. Therefore, here we use the generic term, location.

There are differences between the commands supported for messages and locations in the Locations folder and those in the File Systems folder. When clients log on to MessageWay, the user's default location determines whether they will view messages from the Locations folder or messages from the File System folder.

Server Command	Typical SFTP Client Command	Description
CDUP	**cd ..**	Change working directory to the parent of the current directory. (Locations folder only) Only valid from *canceled* and *downloaded* directories.
CWD	**cd** *absolute-path* **cd** */pathname*	Change working directory. (Locations folder only) *canceled* and *downloaded* are the only valid subdirectories.
DELE	**rm**	Cancel a message in a MessageWay mailbox. (Locations folder only) The canceled message is then displayed in the *canceled* subdirectory. (File System folder only) The canceled message is no longer visible to the client.
LIST	**ls**, **ls -l**	Display formatted list of messages.
PWD	**pwd**	Display the current working directory (*/location-root_directory*[*/subdirectory*])
RETR	**get**	Retrieve a file from MessageWay.
STOR	**put**	Send a file to a MessageWay location. **NOTE:** Compound addresses allow users to send files through one or more service processes in MessageWay before final delivery. The SFTP Perimeter Server does not directly support compound addresses during uploads, either in explicit paths typed by a user or in the Default Location or Default Recipient fields on the Locations tab of the User Properties window. A workaround is to upload files to a Distribution List location that sends the file to a location that then uses the compound address.

Basic SFTP Commands and Syntax

Most users do specific things and only need to know a limited set of client commands. The following table describes the most typical tasks, the basic SFTP commands users need, and the effect of these commands in MessageWay:

Tasks	SFTP Command(s)	Affect in MessageWay
Move around in the MessageWay structure	cd	Allows users to move among directories.

Delete messages from MessageWay	rm	Changes status of message to canceled, awaiting archive process before the message is removed from the system. User must have the right to cancel messages for this location. (Locations folder only) Places messages in *Canceled* subdirectory. (File System folder only) Removes messages from view.
Get directory listings	ls, dir	Displays messages in a directory.
Move files from MessageWay (download)	get	Downloads messages from a directory.
Move files to MessageWay (upload)	put	Uploads messages to any MessageWay locations where user has upload rights.

For a more comprehensive list of client commands, refer to the topic ***Commands for the MessageWay SFTP Perimeter Server*** (on page 304). For details about SFTP client commands and their syntax for advanced use, refer to the topic ***Advanced SFTP Syntax*** (on page 311).

CD

The CD command allows the user to make any directory the current root directory. A root directory corresponds to a location, but there are more options for locations in the Locations folder. For example, the directories, *canceled* and *downloaded*, are not used for locations in the File System folder. The directories Canceled and Downloaded normally correspond to the root's subdirectories. Canceled and Downloaded would also be valid root directories if added as locations within the MessageWay Manager.

The syntax of the command for locations in both the Locations and File System folder is:

cd /|~

- or -

cd */location-root_directory*

Additional syntax options for locations in the Locations folder are:

cd canceled|downloaded

- or -

cd */location-root_directory*/**canceled|downloaded**

The following table shows some examples:

Command	Result
cd /	Resets the current root directory to the home or default directory

Command	Result
cd ~	Resets the current root directory to the home or default directory
cd */location-root_directory*	Changes the current root directory to */ocation-root_directory*
cd canceled	(Locations folder only) Changes current root directory to the /canceled subdirectory
cd downloaded	(Locations folder only) Changes current root directory to the /downloaded subdirectory
cd */location-root_directory*/**downloaded**	(Locations folder only) Changes the current root directory to the /downloaded subdirectory of the specified */location-root_directory*

GET

The GET command retrieves one or more messages from a location (root directory).

Users may retrieve messages ONLY if the user who is logged on has the necessary download permissions defined on the location configuration and the user configuration.

Here are descriptions of the parameters used in the syntax:

Parameter	Description
msg-name	(Locations folder only) Name of the message derived from the MessageNameFormat parameter specified on the SFTP configuration file, unless you only use the message ID. When you only use the message ID, the MessageNameFormat requirements are ignored. (File System folder only) File name.
local-path	Path and/or file name of the downloaded file on the local disk
^	(Locations folder only) Only required for SFTP (FTP SSH) when no message name is provided. When used, only the oldest message meeting the *get* criteria will be downloaded

NOTE: Depending on your SFTP client or system, you may also be able to use wild card characters, such as the asterisk, *, or question mark, ? to specify a message name mask. The OpenSSH client supports wild cards.

The syntax options of the command for locations in both the Locations folder and the File System folder are as follows:

get [*****] [**?**]

- or -

get *msg-name*

- or -

get *msg-name local-path*

Additional syntax options of the command for locations in the Locations folder are:

get *msg-name***^**

- or -

get *msg-name***^** *local-path*

LS

The LS command displays a single message, when the message name is used, or all messages for the location (root directory) and status. The message list output depends on the location (root directory) being queried and potentially the subdirectory. If the command has no arguments, MessageWay returns the messages in the current directory.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	**Description**
location-root_directory	Name of the MessageWay location or root directory.
msg-name	(Locations folder only) Name of the message derived from the MessageNameFormat parameter specified on the SFTP configuration file. (File System folder only) File name of the message.

NOTE: Depending on your SFTP client or system, you may also be able to use wild card characters, such as the asterisk, *, or question mark, ? to specify a message name mask. The OpenSSH client supports wild cards. Additionally, you may be able to use the DIR command.

The syntax options of the command for locations in both the Locations folder and the File System folder are as follows:

ls [**-al**] [*****] [**?**]

- or -

ls *msg-name*

- or -

ls /*location-root_directory*

Additional syntax options of the command are available for locations in the Locations folder as follows:

ls /canceled|downloaded

- or -

ls /canceled|downloaded/*msg-name*

- or -

ls */location-root_directory/***canceled**|**downloaded**

- or -

ls */location-root_directory/***canceled**|**downloaded/***msg-name*

Here are some conditions that affect the results of the command:

- If *msg-name* is provided, then that message will be displayed when a provided location and class ID are also correct for that message.
- If the user has download rights to the location (root directory) that it queries, but does not have upload rights, then the list displays all messages in the location (root directory) with a status of A, available.
- If the user does not have download rights but does have upload rights to the location that it queries, then the behavior is somewhat different. Instead of displaying messages of a particular status, messages where the sender matches the user's default location are displayed regardless of status. The status of each message, however, is not available and the user cannot view messages in the Canceled or Downloaded subdirectories.

Here are some basic examples and descriptions of the results.

Command	**Result**
ls or **ls -l**	Lists available messages in the current directory if the current directory is the user's default location; Otherwise, it lists messages uploaded to the current directory by the user that has logged on.
ls *msg-name*	Lists the message. The message name must match the format specified for the MessageNameFormat in the SFTP configuration file, unless you use only the message ID. When you only use the message ID, the MessageNameFormat is ignored.
ls */location-root_directory*	Lists available messages in *location-root_directory,* if *location-root_directory* is the user's default location; Otherwise, it lists messages uploaded to the location by the user that has logged on, if the user has the necessary permissions.
ls canceled	(Locations folder only) Lists canceled messages in the /canceled subdirectory of the current directory if the current-directory is the user's default location; Otherwise it returns, "Access-Denied."
ls downloaded	(Locations folder only) Lists completed messages in the /downloaded subdirectory of the current directory if the current directory is the user's default location; Otherwise it returns, "Access-Denied."

Command	Result
ls */location-root_directory/***canceled**	(Locations folder only) Lists canceled messages in the /canceled subdirectory*,* if the *location-root_directory* is the same as the user's default location; Otherwise it returns, "Access-Denied."
ls */location-root_directory/***downloaded**	(Locations folder only) Lists completed messages in the /downloaded subdirectory*,* if *location-root_directory* is the same as the user's default location; Otherwise it returns, "Access-Denied."

PUT

The PUT command transfers a file from the client as a message to a MessageWay location. You may send messages to the current directory or to a directory specified in the command. If you do not specify a destination location, the message is stored in the current directory or location as configured in the default recipient field for the logged on user, assuming the user has the necessary permissions to upload messages to the location.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
file	Name of the current file on the client system
new-file	New name for the remote file, which becomes the input file name in MessageWay
location-root_directory	Name of the MessageWay location to which the file is delivered **NOTE:** Compound addresses allow users to send files through one or more service processes in MessageWay before final delivery. The SFTP Perimeter Server does not directly support compound addresses during uploads, either in explicit paths typed by a user or in the Default Location or Default Recipient fields on the Locations tab of the User Properties window. A workaround is to upload files to a Distribution List location that sends the file to a location that then uses the compound address.

The syntax options of the command are as follows:

put *file*

- or -

put *file new-file*

- or -

put *file /location-root_directory/new-file*

RM

The RM command cancels messages that have a status of *Available*. For locations in the Locations folder, it displays them in the Canceled subdirectory. When canceled messages are eligible for archive or delete, they will be removed from the MessageWay message store when the Archive program runs. For locations in the File System folder, canceled messages are no longer available to SFTP clients.

Here are descriptions of the basic replaceable parameters used in the syntax:

Parameter	Description
location-root_directory	Name of the MessageWay location.
msg-name	(Locations folder only) Name of the message derived from the MessageNameFormat parameter specified on the SFTP configuration file. (File System folder only) File name.

NOTE: Depending on your SFTP client or system, you may also be able to use wild card characters, such as the asterisk, *, or question mark, ? to specify a message name mask. The OpenSSH client supports wild cards.

The syntax options of the command are as follows:

rm *msg-name*

- or -

rm */location-root_directory/msg-name*

Advanced SFTP Syntax (Locations Folder)

IMPORTANT: This information is only valid for locations in the Locations folder, not for locations (directories) in the File System folder.

The syntax of the advanced commands show how to use ***class ID*** (on page 1187) to identify messages that belong to a specific group. The following information shows advanced syntax for the commands supported by the SFTP Server as well as some typical client commands. The associated commands from the client vary based on the client.

NOTE: Location is a generic term that includes auto-delivery locations, which are service locations and sites, and pickup mailboxes. Mailbox is a specific type of location where users collect messages. A user's default location is always a mailbox. Assuming they have the rights to do so, users may act on locations other than pickup mailboxes. Therefore, here we use the generic term, location.

GET

The GET command retrieves one or more messages from a location (root directory). You may retrieve a specific message with the message ID, or the msg-name as determined by the MessageNameFormat parameter, or the oldest message that matches the location, class ID and status. When the message ID is used, all other fields are ignored. Additional syntax allows users to access messages based on class ID.

Users may retrieve messages ONLY if the user who is logged on has the necessary download permissions defined on the location configuration.

Here are descriptions of the parameters used in the syntax:

Parameter	**Description**
classID	Class ID specified in MessageWay
location-root_directory	Name of the MessageWay location, which is the same as the root directory
msg-name	Name of the message derived from the MessageNameFormat parameter specified on the SFTP configuration file
local-path	Path and/or file name of the downloaded file on the local disk
^	Only required for SFTP (FTP SSH) when no message name is provided. When used, only the oldest message meeting the 'get' criteria will be downloaded

NOTE: Depending on your SFTP client or system, you may also be able to use wild card characters, such as the asterisk, *, or question mark, ? to specify a message name mask. The OpenSSH client supports wild cards.

The advanced syntax options of the command are as follows:

get canceled|**downloaded** [*/classID*@]**^** [*local-path*]

- or -

get canceled|**downloaded** [*/classID*@]*/msg-name* [*local-path*]

- or -

get *classID*@[*location-root_directory*][**/canceled**|**/downloaded**]**^** [*local-path*]

- or -

get *classID*@[**canceled**|**downloaded**]*/msg-name* [*local-path*]

- or -

get *classID*@[*location-root_directory*][**/canceled**|**/downloaded**]*/msg-name* [*local-path*]

- or -

get */location-root_directory*[**/canceled**|**/downloaded**][*/classID*@]**^** [*local-path*]

- or -

get */location-root_directory*[**/canceled**|**/downloaded**][*/classID*@]*/msg-name* [*local-path*]

LS

The LS command displays a single message, when the message name is used, or all messages for the location (root directory), class ID and status. The message list output depends on the location (root directory) being queried and potentially the subdirectory. If the command has no arguments, MessageWay returns the available, canceled or downloaded messages in the current directory. Additional syntax allows users to access messages based on class ID.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
classID	Class ID specified in MessageWay.
location-root_directory	Name of the MessageWay location or root directory.
msg-name	Name of the message derived from the MessageNameFormat parameter specified on the SFTP configuration file.

NOTE: Depending on your SFTP client or system, you may also be able to use wild card characters, such as the asterisk, *, or question mark, ? to specify a message name mask. The OpenSSH client supports wild cards. Additionally, you may be able to use the DIR command.

The advanced syntax options of the command are as follows:

ls canceled | **downloaded** [/*classID***@**][/*msg-name*]

- or -

ls *classID***@**

- or -

ls *classID***@**[**canceled**|**downloaded**][/*msg-name*]

- or -

ls *classID***@**[*location-root_directory*][**/canceled**|**/downloaded**][/*msg-name*]

- or -

ls /*location-root_directory*[**/canceled**|**/downloaded**][/*classID***@**][/*msg-name*]

Here are some conditions that affect the results of the command:

- If *msg-name* is provided, then that message will be displayed when a provided location and class ID are also correct for that message.
- If the user has download rights to the location (root directory) that it queries, but does not have upload rights, then the list displays all messages in the location (root directory) with a status of **A**, available.
- If the user does not have download rights but does have upload rights to the location that it queries, then the behavior is somewhat different. Instead of displaying messages of a particular status, messages where the sender matches the user's default location are displayed regardless of status. The

status of each message, however, is not available and the user cannot view messages in the Canceled or Downloaded subdirectories.

PUT

The PUT command transfers a file from the client as a message to a MessageWay location. You may send messages to the current directory or to a directory specified in the command. Optionally, you may specify a class ID in the command to set the Message class of the message. If you do not specify a destination location, the message is stored in the current directory or location as configured in the default recipient field for the logged on user, assuming the user has the necessary permissions to upload messages to the location.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
classID	Class ID to be associated with the message
file	Name of the current file on the client system
new-file	New name for the remote file, which becomes the input file name in MessageWay
location-root_directory	Name of the MessageWay location to which the file is delivered **NOTE:** Compound addresses allow users to send files through one or more service processes in MessageWay before final delivery. The SFTP Perimeter Server does not directly support compound addresses during uploads, either in explicit paths typed by a user or in the Default Location or Default Recipient fields on the Locations tab of the User Properties window. A workaround is to upload files to a Distribution List location that sends the file to a location that then uses the compound address.

The advanced syntax options of the command are as follows:

put *file /location-root_directory*[*/classID***@**][*/new-file*]

- or -

put *file classID***@**[*location-root_directory*][*/new-file*]

RM

The RM command cancels messages that have a status of *Available* and displays them in the Canceled subdirectory. When canceled messages are eligible for archive or delete, they will be removed from the MessageWay message store when the Archive program runs. Additional syntax allows users to access messages based on class ID.

Here are descriptions of the replaceable parameters used in the syntax:

Parameter	Description
classID	Class ID specified in MessageWay.
location-root_directory	Name of the MessageWay location.
msg-name	Name of the message derived from the MessageNameFormat parameter specified on the SFTP configuration file.

NOTE: Depending on your SFTP client or system, you may also be able to use wild card characters, such as the asterisk, *, or question mark, ? to specify a message name mask. The OpenSSH client supports wild cards.

The advanced syntax options of the command are as follows:

rm *classID*@[*location-root_directory*]/*msg-name*

- or -

rm /*location-root_directory*[/*classID*@]/*msg-name*

Advanced SFTP Command Examples (Locations Folder)

IMPORTANT: This information is only valid for locations in the Locations folder, not for locations (directories) in the File System folder.

These examples assume that you use a command-line client to connect to the MessageWay SFTP Perimeter Server. Results may vary depending on the command-line client. The mapping defined should behave the same with most user interfaces for SFTP clients.

Here are descriptions of some important terms:

Default location — The ***default location*** (on page 1363) or root directory of the logged-on user.

Current location — The location named by the root in the current working directory.

Current status — The message status indicated by the location in the current working directory. Messages in the root directory, have a status of Available(A). Messages in the /canceled subdirectory have a status of Canceled(C). Messages in the /downloaded subdirectory have a status of Downloaded(D).

These conditions are required for the examples:

- The logged-on user must have download rights to locations, Remote1 and Remote2, and upload rights to Remote3.
- The current working directory is /Remote1.

Any examples containing either **canceled** or **downloaded** also applies for the other.

RM Examples

The RM command cancels messages with a status of Available, **A**. Canceled messages then appear in the /canceled subdirectory.

NOTE: Depending on your SFTP client or system, you may also be able to use wild card characters, such as the asterisk, *, or question mark, ? to specify a message name mask. The OpenSSH client supports wild cards.

Here are some examples:

Command	Location	Class ID	Status	Message ID
rm *msg-name*	Current	-	Current	from *msg-name*
rm /Remote2/*msg-name*	Remote2	-	A	from *msg-name*
rm abc@/*msg-name*	Current	abc	Current	from *msg-name*
rm /Remote2/abc@/*msg-name*	Remote2	abc	A	from *msg-name*
rm abc@Remote2/*msg-name*	Remote2	abc	A	from *msg-name*

LS Examples

The LS command lists either a single message when *msg-name* is provided or all messages that match the provided location, class id and status.

NOTE: Depending on your SFTP client or system, you may also be able to use wild card characters, such as the asterisk, *, or question mark, ? to specify a message name mask. The OpenSSH client supports wild cards. Additionally, you may be able to use the DIR command.

Here are some examples:

Command	Location	Class ID	Status	Message ID
ls [-al]	Current	-	Current	
ls *msg-name*	Current	-	Current	from *msg-name*
ls canceled	Current	-	C	-
ls canceled/*msg-name*	Current	-	C	from *msg-name*
ls downloaded	Current	**-**	D	-

Command	Location	Class ID	Status	Message ID
ls /Remote2	Remote2	-	A	-
ls /Remote2/canceled	Remote2	-	C	-
ls /Remote2/*msg-name*	Remote2	-	A	from *msg-name*
ls /Remote2/downloaded/*msg-name*	Remote2	-	D	from *msg-name*
ls abc@	Current	abc	Current	-
ls abc@/*msg-name*	Current	abc	Current	from *msg-name*
ls abc@canceled	Current	abc	C	-
ls abc@downloaded	Current	abc	D	-
ls abc@canceled/*msg-name*	Current	abc	C	from *msg-name*
ls abc@Remote2	Remote2	abc	A	-
ls abc@Remote2/canceled	Remote2	abc	C	-
ls abc@Remote2/*msg-name*	Remote2	abc	A	from *msg-name*
ls abc@Remote2/downloaded/*msg-name*	Remote2	abc	D	from *msg-name*
ls /Remote2/abc@	Remote2	abc	A	-
ls /Remote2/downloaded/abc@	Remote2	abc	D	-
ls /Remote2/abc@/*msg-name*	Remote2	abc	A	from *msg-name*
ls /Remote2/canceled/abc@/*msg-name*	Remote2	abc	C	from *msg-name*
ls canceled/abc@	Current	abc	C	-
ls canceled/abc@/*msg-name*	Current	abc	C	from *msg-name*

GET Examples

The GET command either retrieves a specific message when a message ID is present in the argument, or retrieves the msg-name as determined by the MessageNameFormat parameter, or retrieves the oldest message that matches the provided location, class ID and status. If the message ID is used, then all other fields are ignored.

For all commands, a second file name parameter may be used to set the local file name.

NOTE: Depending on your SFTP client or system, you may also be able to use wild card characters, such as the asterisk, *, or question mark, ? to specify a message name mask. The OpenSSH client supports wild cards.

Command	Location	Class ID	Status	Message ID
get *	Current	-	Current	-
get *msg-name*	Current	-	Current	from *msg-name*
get /Remote2^	Remote2	-	A	-
get /Remote2/canceled^	Remote2	-	C	-
get /Remote2/*msg-name*	Remote2	-	A	from *msg-name*
get /Remote2/downloaded/*msg-name*	Remote2	-	D	from *msg-name*
get downloaded^	Current	-	D	-
get canceled/*msg-name*	Current	-	C	from *msg-name*
get abc@^	Current	abc	Current	-
get abc@/*msg-name*	Current	abc	Current	from *msg-name*
get canceled/abc@^	Current	abc	C	-
get downloaded/abc@/*msg-name*	Current	abc	D	from *msg-name*
get /Remote2/abc@^	Remote2	abc	A	-
get /Remote2/downloaded/abc@^	Remote2	abc	D	-
get /Remote2/abc@/*msg-name*	Remote2	abc	A	from *msg-name*
get /Remote2/canceled/abc@/*msg-name*	Remote2	abc	C	from *msg-name*
get abc@Remote2^	Remote2	abc	A	-
get abc@downloaded^	Current	abc	D	-
get abc@canceled/*msg-name*	Current	abc	C	from *msg-name*
get abc@Remote2/canceled^	Remote2	abc	C	-
get abc@Remote2/*msg-name*	Remote2	abc	A	from *msg-name*
get abc@Remote2/downloaded/*msg-name*	Remote2	abc	D	from *msg-name*

PUT Examples

The PUT command transfers a file from the client as a message to a MessageWay location. When a new-file name is not provided in the command, either the name of the input file or *M<msgid>.dat* is used to create the filename value in MessageWay.

Command	Recipient	Class ID	InputName
put *file*	Current	-	*file*
put *file new-file*	Current	-	*new-file*

put *file* **/Remote3**	Remote3	-	*file*
put *file* **/Remote3/***new-file*	Remote3	-	*new-file*
put *file* **abc@**	Current	abc	*file*
put *file* **abc@/***new-file*	Current	abc	*new-file*
put *file* **/Remote3/abc@**	Remote3	abc	*file*
put *file* **/Remote3/abc@/***new-file*	Remote3	abc	*new-file*
put *file* **abc@Remote3**	Remote3	abc	*file*
put *file* **abc@Remote3/***new-file*	Remote3	abc	*new-file*

Basic Installation Tasks

This installation process installs the components of the SFTP Perimeter Server. These tasks assume that you have already installed MessageWay, which includes the following components of interest here:

- MessageWay Messaging Server, which processes messaging requests
- MessageWay User Server, which controls access to MessageWay
- MessageWay Service Interface, which provides access to MessageWay from MessageWay servers and the Internet
- MessageWay Manager, which provides the user interface to configure MessageWay

These are the basic tasks to install the SFTP Perimeter Server:

- For UNIX or Linux, install the MWay SFTP Perimeter Server

  - or -
- For Windows
  - Install the open source product Cygwin to provide a Linux-like environment for SFTP
  - Install the MessageWay SFTP Perimeter Server to run under Cygwin

NOTE: The SSH host keys are generated during the MessageWay SFTP Server installation. The mwsftpd.conf is pre-configured with these production-ready keys.

After you have installed the SFTP Perimeter Server, you must perform the following tasks to configure and test the system:

- Set up the configuration file for the Service Interface on the MessageWay system
- Start the Service Interface
- Test the connection to the Service Interface
- Set up the configuration file for the SFTP Perimeter Server
- Install the certificate obtained from a licensing authority to perform SSL communications, if desired, between the MWay SFTP Server and Service Interface

NOTE: Progress provides certificates with the MessageWay installation as part of the Service Interface to use for initial testing. These certificates allow anonymous logon. You should replace these certificates as soon as possible. If the SFTP Server is not installed on the local MessageWay box, the value in the CertFingerprint parameter, which comes pre-configured in the MSI section of mwsftpd.conf, must be used in order to establish an SSL connection using the provided test certificates. If the SFTP Server is installed locally, an SSL connection can be established using either the CertFingerprint or CertVerifyFile parameter. Only one of the two parameters must be active.

- Configure MessageWay users and locations
- Test the system from end to end

For the actual installation information, refer to the *MessageWay Installation Guide*.

Configuring the SFTP Server Components

You set the parameters for the SFTP Server system in the configuration files:

- **mwsi.conf** for the Service Interface
- **mwsftpd.conf** for the SFTP Server.

Use a text editor to edit the files.

For information about configuring the Service Interface file, refer to the topic, ***Service Interface*** (on page 95).

IMPORTANT: Another configuration file, **mwsftpd_config**, provides the default settings to support the MessageWay implementation of SFTP. Users typically do not need to change any settings in this file. The settings in the **mwsftpd.conf** file will override the default settings in the **mwsftpd_config** file. The **mwsftpd_config** file may be overlaid with new updates, so all user changes should be made to the **mwsftpd.conf** file, which will not be overlaid.

The following table shows the default location for the SFTP configuration file:

Operating System	Location of the SFTP Server Configuration File
UNIX or Linux - or - Windows under Cygwin	/etc/messageway/mwsftpd.conf
Windows, Explorer	\Cygwin installation directory\etc\messageway\mwsftpd.conf

TIP: When editing the configuration files, you can either use the UNIX/Linux editor, vi, from a command prompt or a text editor in Windows. You may need to convert the format from DOS to UNIX or UNIX to DOS, depending which system you choose. Programs to do this, dos2unix and unix2dos, are typically available free of charge from the Internet, if you don't already have them.

Configurations for the SFTP Server

The MessageWay SFTP Server resides anywhere in the LAN or WAN. It receives commands from an SFTP client, which is typically outside the network. The SFTP server also acts as a client when it communicates with the MessageWay Service Interface (SI) to provide users access to MessageWay. The server provides secure communications using Secure Shell (SSH) to communicate with clients. Users can configure whether to use a secure HTTP connection to communicate with the SI.

There are four sections in the configuration file, mwsftpd.conf. The following table describes the purpose of each section.

Section	Purpose
Global	▪ Connection parameters between the SFTP Server and SFTP clients ▪ For locations in the **Locations** folder, ability to suppress Canceled and Downloaded directories from client view ▪ Sort message lists on file name rather than time sent or received
MSI	▪ IP address and port on which Service Interface listens ▪ Security type of HTTP connection ▪ Security certificate information ▪ Timeouts ▪ Optional trace file settings ▪ Client certificate information for public key authentication
SSHD	▪ Security information, such as ciphers, host keys and MACs ▪ Other SSHD configuration parameters
SFTP	▪ User under which SFTP Server process runs ▪ Logging parameters

New Parameters for the SFTP Configuration File

CAUTION: If you already have a configuration file, you must manually insert new parameters that you want to use, since the upgrade process does not overlay existing configuration files.

The new parameters or modifications to existing parameters for the SFTP configuration file, mwsftpd.conf, are as follows:

Release	Section	Parameters
6.1.0	Global	▪ SuppressCanceledAndDownloadDirs
6.1.0 HF01	Global	▪ FilenameSort

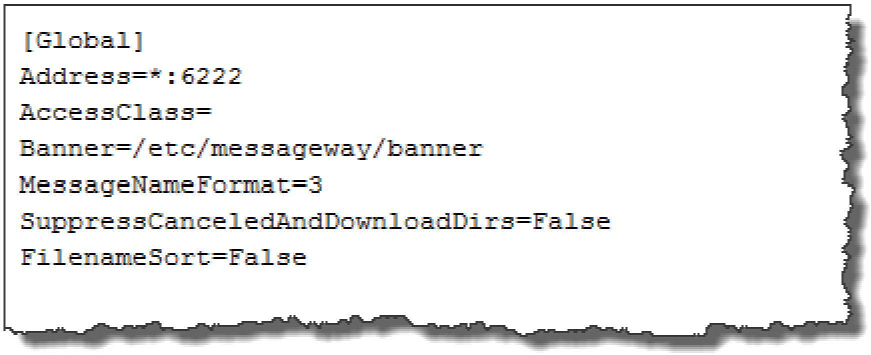
Global Section

The global section specifies the basic connection between the SFTP server and SFTP clients. The following table explains the parameters used in the **[Global]** section of the SFTP Server configuration file, mwsftpd.conf.

Parameter	Description
Address	The IP address and port number where the SFTP server should listen for incoming SFTP clients. Replace the IP address with an asterisk, *****, to listen on any IP address. The typical port default value is **22**. However, in case there is a pre-existing SSH process using that port, you must select another port. To avoid such conflict, the examples use port **6222**.
AccessClass	Restricts access to MessageWay via this listener to only those users whose configuration does not include an access class list or includes this value in their access class list. This value should be alphanumeric and is case-sensitive. It must match exactly what is specified for the user. Optional, but if used, only one access class value is allowed.
Banner	Fully qualified file name that contains the sign-on banner, which is sent to all connections.
MessageNameFormat	Defines the format for naming MessageWay messages (file name seen by SFTP client). The format is defined as 1 to 3 of the following characters: ▪ **1** Message ID ▪ **2** Class ID ▪ **3** Filename Each character represents a component to be displayed separated by plus signs **+**. The number **1** or **3** must be present. When neither is used, **1**, Message ID, will be appended to the displayed message name. This is the same as a MessageNameFormat of **21**.
SuppressCanceledAndDownloadDirs	(Locations Folder only) Allows the SFTP server to not display messages in the Canceled and Downloaded directories. This mimics the behavior of the File System folder and is typical of most SFTP server displays. The options are: ▪ **True** ▪ **False** or option is blank (default)

Parameter	Description
FilenameSort	When set to **True**, the sort order for the message list is by file name. This overrides the default sort order, which is by the message time received or sent. The options are: ▪ **True** ▪ **False** or option is blank (default)

Here is an example of a global section in the mwsftpd.conf file. This default configuration will listen on any IP address. The typical port is 22, which may conflict with other processes that might be using the default SSH port, 22. To avoid possible collisions, the default port was changed to 6222. The MessageNameFormat creates an external file name with a MessageWay message ID, as well as a class ID.



```
[Global]
Address=*:6222
AccessClass=
Banner=/etc/messageway/banner
MessageNameFormat=3
SuppressCanceledAndDownloadDirs=False
FilenameSort=False
```

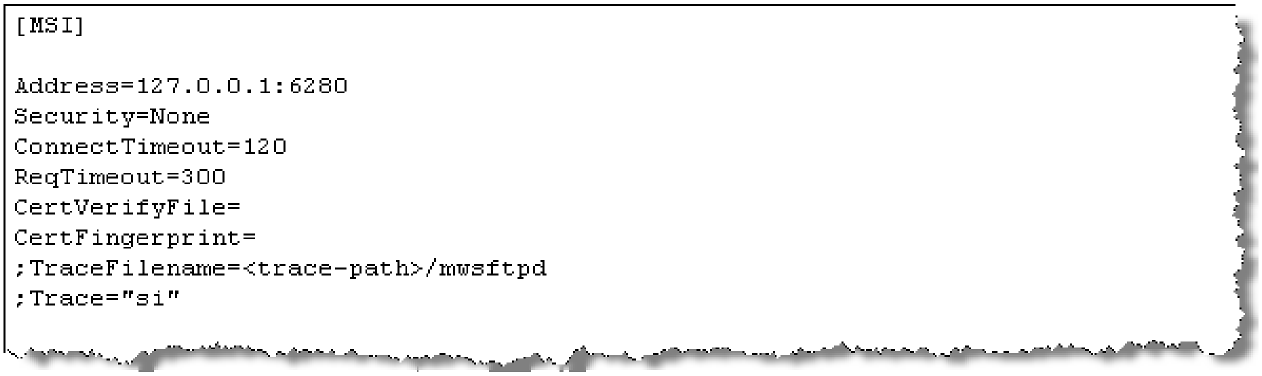
MSI Section

This section specifies how the SFTP server communicates with the MessageWay Service Interface (SI). Users may choose different authentication types: MessageWay user ID and password authentication, which is the default, or ***public key authentication with certificates*** (on page 343), ***with or without encryption*** (on page 342). The following table explains the parameters used in the **[MSI]** section of mwsftpd.conf.

Parameter	Description
Address	The IP address and port number where the SFTP server should connect to the MessageWay SI. The default ports configured for SI are: ▪ **6280** for a non-secure connection ▪ **6243** for a secure connection
Security	Enter a security type. Valid values: ▪ **None** (for a non-secure port) ▪ **SSL** ▪ **TLS**

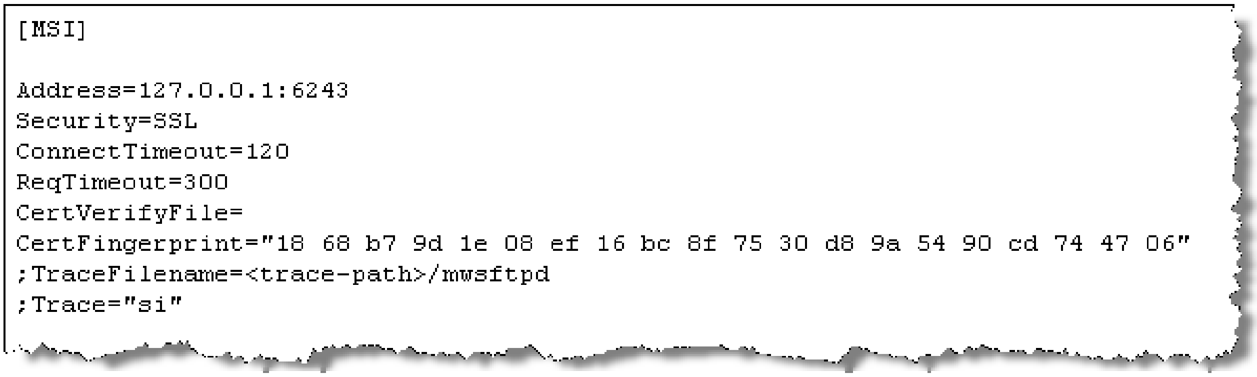
Parameter	Description
ConnectTimeout	Time (in seconds) that the SFTP server will wait when trying to connect to MessageWay SI.
ReqTimeout	Time (in seconds) that the SFTP server will wait for responses from MessageWay SI.
CertVerifyFile	Fully qualified file name of the certificate file for the SFTP server when establishing a secure connection with the MessageWay SI, which is used to verify the certificate received from SI. The default certificate file is shared with the MessageWay SI Server for quick testing. Users should configure either a verify file or a fingerprint to establish a secure connection.
CertFingerprint	SHA1 or MD5 digest of the certificate. The default fingerprint is shared with the MessageWay SI Server for quick testing. Users should configure either a verify file or a fingerprint to establish a secure connection.
TraceFilename	Defines the trace filename (for tracing MWSI) including the directory path. A suffix of .yymmddhhmmss.log will be appended to this name. For example, if the file name is mwsftpd, the log will be mwsftpd.091204134411.log. This parameter is optional.
Trace	Optional parameter to trace the activity between the SFTP server and the MessageWay SI. Use any combination of the following values, separated by a comma when you use more than one: ▪ **http** ▪ **httpbody** ▪ **tcp** ▪ **si**
ClientCertFile	Fully qualified file name of the client certificate file on the SFTP server. That certificate is used by the MessageWay Service Interface to identify the SFTP server as a trusted authentication agent. This is required when sftp "publickey" authentication is used.
ClientKeyFile	Fully qualified file name of the private key that is used to identify the SFTP server. Required if ClientCertFile is provided.
ClientKeyPassphrase	Pass phrase to use if the PrivateKeyFile is encrypted.
AuthAgent	Name of the trusted authentication agent as identified by the Common Name on the client certificate. This name must match the Common Name that is stored in the ClientCertFile and must be included in the mwsi agents file (i.e. trusted by mwsi).

The following configuration is for a non-secure connection to SI:



```
[MSI]

Address=127.0.0.1:6280
Security=None
ConnectTimeout=120
ReqTimeout=300
CertVerifyFile=
CertFingerprint=
;TraceFilename=<trace-path>/mwsftpd
;Trace="si"
```

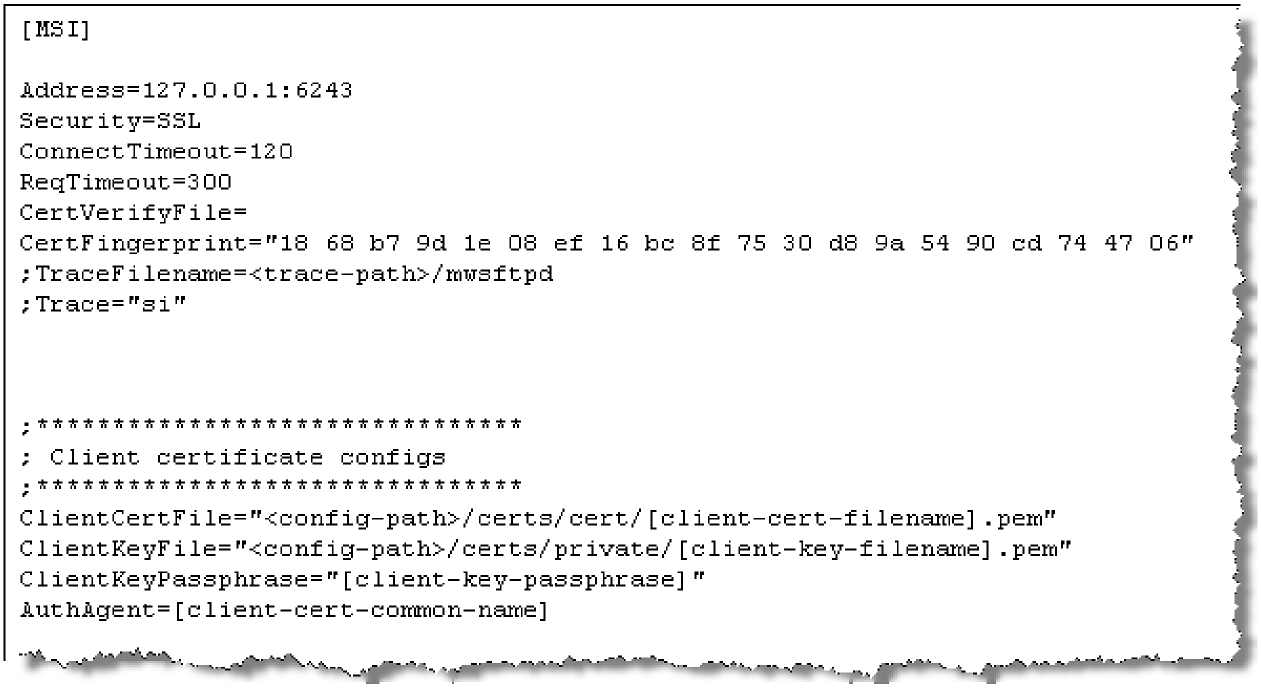
Here is an example of an MSI section in the mwsftpd.conf file that uses MessageWay user ID and password to authenticate the user. The security files installed with SI, which is installed with the MessageWay Server, work with a fingerprint, shown here. Together with the default settings in the SI configuration file, users can test a secure connection with no further configuration.



```
[MSI]

Address=127.0.0.1:6243
Security=SSL
ConnectTimeout=120
ReqTimeout=300
CertVerifyFile=
CertFingerprint="18 68 b7 9d 1e 08 ef 16 bc 8f 75 30 d8 9a 54 90 cd 74 47 06"
;TraceFilename=<trace-path>/mwsftpd
;Trace="si"
```

Here is an example of an MSI section in the mwsftpd.conf file that supports client certificate and public key authentication. This is for a trusted agent, SFTP Server, to provide authentication to SI. In this case, the SFTP server acts as the client to SI. For the following example, users must specify the client certificates, the client passphrase and must add the common name used in the client certificate in the ***Agents file*** (on page 346).

IMPORTANT: To use this type of authentication, you must also configure SI to support client certificate and agent authentication.



```
[MSI]

Address=127.0.0.1:6243
Security=SSL
ConnectTimeout=120
ReqTimeout=300
CertVerifyFile=
CertFingerprint="18 68 b7 9d 1e 08 ef 16 bc 8f 75 30 d8 9a 54 90 cd 74 47 06"
;TraceFilename=<trace-path>/mwsftpd
;Trace="si"



;********************************
; Client certificate configs
;********************************
ClientCertFile="<config-path>/certs/cert/[client-cert-filename].pem"
ClientKeyFile="<config-path>/certs/private/[client-key-filename].pem"
ClientKeyPassphrase="[client-key-passphrase] "
AuthAgent=[client-cert-common-name]
```

SSHD Section

This section specifies how the SFTP server, in its capacity as an SSH server, communicates with SFTP clients.

IMPORTANT: The MessageWay SFTP Server supports Protocol Version 2 of OpenSSH.

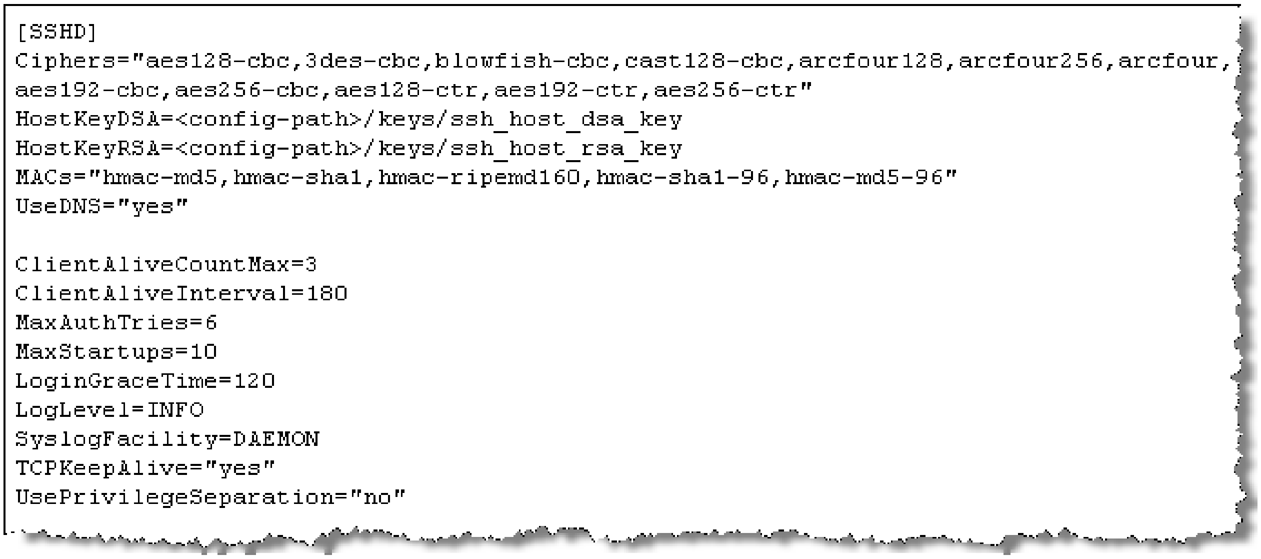
The following table explains the parameters used in the **[SSHD]** section of mwsftpd.conf.

Parameter	Description
Ciphers	Specifies the ciphers allowed for protocol version 2. Multiple ciphers must be comma-separated. The supported ciphers are: ▪ **3des-cbc** ▪ **aes128-cbc** ▪ **aes192-cbc** ▪ **aes256-cbc** ▪ **aes128-ctr** ▪ **aes192-ctr** ▪ **aes256-ctr** ▪ **arcfour128** ▪ **arcfour256** ▪ **arcfour** ▪ **blowfish-cbc** ▪ **cast128-cbc** The default is: `"aes128-cbc,3des-cbc,blowfish-cbc, cast128-cbc,arcfour128,arcfour256, arcfour,aes192-cbc,aes256-cbc, aes128-ctr,aes192-ctr,aes256-ctr"`
HostKeyDSA	This file contains a private DSA host key used by SSH protocol version 2. The default is: `/opt/messageway/keys/ssh_host_dsa_key`. Note that sshd(8) will refuse to use a file if it is group/world-accessible. It is possible to have multiple host key files.
HostKeyRSA	This file contains a private RSA host key used by SSH protocol version 2. The default is: `/opt/messageway/keys/ssh_host_rsa_key`. Note that sshd(8) will refuse to use a file if it is group/world-accessible. It is possible to have multiple host key files.
MACs	Specifies the available message authentication code (MAC) algorithms. The MAC algorithm is used in protocol version 2 for data integrity protection. Multiple algorithms must be comma-separated. The default is: `"hmac-md5,hmac-sha1,hmac-ripemd160, hmac-sha1-96,hmac-md5-96"`
UseDNS	Specifies whether sshd(8) should look up the remote host name and check that the resolved host name for the remote IP address maps back to the very same IP address.
ClientAliveMaxCount	Sets the number of client-alive messages which may be sent without sshd(8) receiving any messages back from the client.

Parameter	Description
ClientAliveInterval	Sets a timeout interval in seconds after which if no data has been received from the client, sshd(8) will send a message through the encrypted channel to request a response from the client. The default is **0**, zero, indicating that these messages will not be sent to the client.
MaxAuthTries	Specifies the maximum number of authentication attempts permitted per connection. Once the number of failures reaches half this value, additional failures are logged.
MaxStartups	Specifies the maximum number of concurrent unauthenticated connections to the SSH daemon. Additional connections will be dropped until authentication succeeds or the LoginGraceTime expires for a connection. The default is **10**. Alternatively, random early drop can be enabled by specifying the three colon separated values **"***start***:***rate***:***full***"** , for example, `"10:30:60"`.
LoginGraceTime	Sets the time in seconds to complete login after which the sshd(8) will disconnect the client connection. It is used to limit the amount of time an unauthenticated session to the client is kept alive.
LogLevel	Gives the verbosity level that is used when logging messages from sshd(8). The possible values are: ▪ **QUIET** ▪ **FATAL** ▪ **ERROR** ▪ **INFO** ▪ **VERBOSE** ▪ **DEBUG** or **DEBUG1** (these are the same) ▪ **DEBUG2** ▪ **DEBUG3** The default is `INFO`.
SyslogFacility	Gives the facility code that is used when logging messages from sshd(8). The possible values are: ▪ **DAEMON** ▪ **USER** ▪ **AUTH** ▪ **LOCAL0** ▪ **LOCAL1** ▪ **LOCAL2** ▪ **LOCAL3** ▪ **LOCAL4** ▪ **LOCAL5** ▪ **LOCAL6** ▪ **LOCAL7** The default is `AUTH`.

Parameter	Description
TCPKeepAlive	Specifies whether the system should send TCP keepalive to the other side.
UsePrivilegesSeparation	Specifies whether sshd(8) separates privileges by creating an unprivileged child process to deal with incoming network traffic. After successful authentication, another process will be created that has the privilege of the authenticated user.
PasswordAuthentication	Determines if Password Authentication is supported. This uses the MessageWay user ID and password to validate the client. Valid values are **yes** or **no**. The default is **yes**.
PubkeyAuthentication	Determines if Public Key Authentication is to be used, rather than MessageWay user ID and password authentication. Valid values are **yes** or **no**. The default is **no**.
AuthorizedKeysFile	Identifies the location of the public key files. You must store the keys of authorized users here. Each file must be named the same as the associated MessageWay user ID and is case-sensitive.

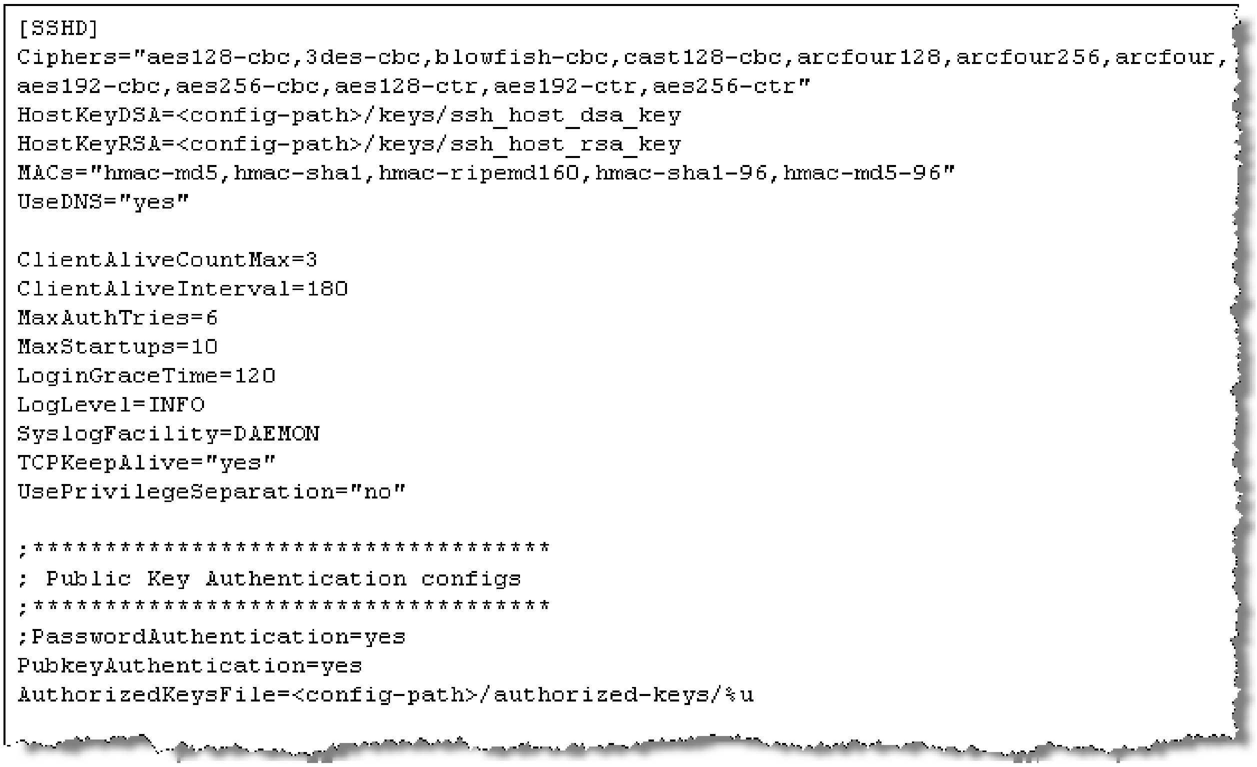
Here is an example of the default settings used in the mwsftpd.conf file. Users must supply the path information where required.



```
[SSHD]
Ciphers="aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,
aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr"
HostKeyDSA=<config-path>/keys/ssh_host_dsa_key
HostKeyRSA=<config-path>/keys/ssh_host_rsa_key
MACs="hmac-md5,hmac-sha1,hmac-ripemd160,hmac-sha1-96,hmac-md5-96"
UseDNS="yes"

ClientAliveCountMax=3
ClientAliveInterval=180
MaxAuthTries=6
MaxStartups=10
LoginGraceTime=120
LogLevel=INFO
SyslogFacility=DAEMON
TCPKeepAlive="yes"
UsePrivilegeSeparation="no"
```

Here is an example that uses public key authentication rather than authentication with MessageWay user ID and password. Notice that the PasswordAuthentication parameter is commented to turn off MessageWay user ID and password authentication, and the PubkeyAuthentication and AuthorizedKeysFile parameters are not commented.

IMPORTANT: To use this type of authentication, you must also configure SI to support client certificate and agent authentication.



```
[SSHD]
Ciphers="aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,
aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr"
HostKeyDSA=<config-path>/keys/ssh_host_dsa_key
HostKeyRSA=<config-path>/keys/ssh_host_rsa_key
MACs="hmac-md5,hmac-sha1,hmac-ripemd160,hmac-sha1-96,hmac-md5-96"
UseDNS="yes"

ClientAliveCountMax=3
ClientAliveInterval=180
MaxAuthTries=6
MaxStartups=10
LoginGraceTime=120
LogLevel=INFO
SyslogFacility=DAEMON
TCPKeepAlive="yes"
UsePrivilegeSeparation="no"

;*************************************
; Public Key Authentication configs
;*************************************
;PasswordAuthentication=yes
PubkeyAuthentication=yes
AuthorizedKeysFile=<config-path>/authorized-keys/%u
```

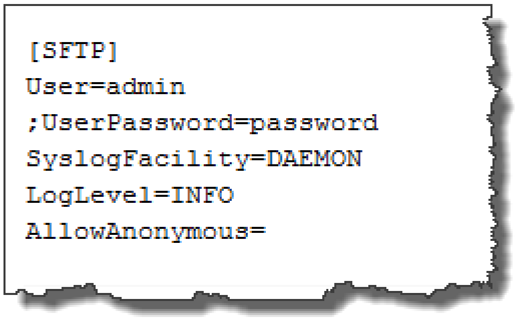
SFTP Section

The SFTP section specifies how the SFTP server runs on the system. The following table explains the parameters used in the **[SFTP]** section of mwsftpd.conf.

Parameter	Description
User	Defines the user under which the SFTP server process will run when created by the sshd daemon. This parameter is required.
UserPassword	Defines the password for User. This parameter is optional.

Parameter	Description
SyslogFacility	Gives the facility code that is used when logging messages from SFTP server. The possible values are: - **DAEMON** - **USER** - **AUTH** - **LOCAL0** - **LOCAL1** - **LOCAL2** - **LOCAL3** - **LOCAL4** - **LOCAL5** - **LOCAL6** - **LOCAL7** The default is `AUTH`. This is optional.
LogLevel	Gives the verbosity level that is used when logging messages from SFTP server. The possible values are: - **QUIET** - **FATAL** - **ERROR** - **INFO** - **VERBOSE** - **DEBUG** - **DEBUG1** - **DEBUG2** - **DEBUG3** The default is `INFO`.
AllowAnonymous	Permits anonymous user logon. Requires secure connection with client certification for the back-end connection to MessageWay. Possible values: - **True** - **False** The default is *False*.

Here is an example of an SFTP section in the mwsftpd.conf file.



```
[SFTP]
User=admin
;UserPassword=password
SyslogFacility=DAEMON
LogLevel=INFO
AllowAnonymous=
```

Configuring MessageWay Users and Locations

In order to send and retrieve messages, you must configure users in MessageWay with security to do the tasks you want. You must also configure locations where the messages are stored. Your tasks are as follows:

- To allow users to send messages, configure locations capable of output or pickup
- To allow users to retrieve messages, configure pickup mailboxes
- To access MessageWay through an SFTP client, configure remote users
- To set location security, assign users and rights to locations

NOTE: Compound addresses allow users to send files through one or more service processes in MessageWay before final delivery. The SFTP Perimeter Server does not directly support compound addresses during uploads, either in explicit paths typed by a user or in the Default Location or Default Recipient fields on the Locations tab of the User Properties window. A workaround is to upload files to a Distribution List location that sends the file to a location that then uses the compound address.

Configuring Mailboxes for Clients to Send Messages

To allow users to send messages to MessageWay through the SFTP Perimeter Server, you ***create locations*** (on page 453) in MessageWay to receive the messages. You create different types of locations, depending on whether the SFTP client user will access locations in the Locations folder or locations in the File System folder. For more information about the differences between the two, refer to the topic, ***Overview of Location Properties*** (on page 453).

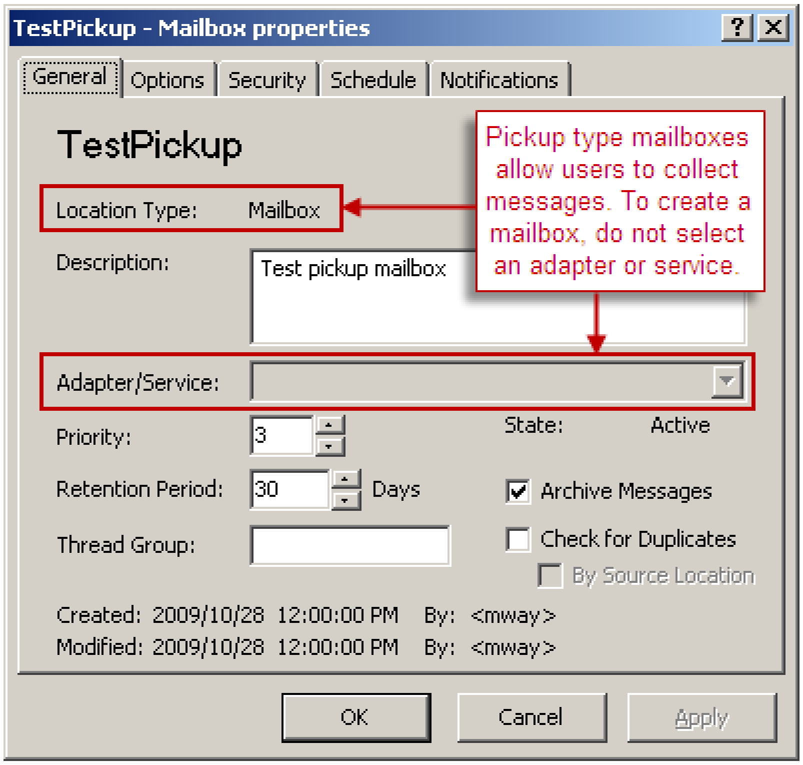
- In the Locations folder, when you create locations to receive messages, they must be of the type I/O, output, service or pickup. They may not be solely an input type.
- In the File System folder, users can only create pickup mailboxes, but MessageWay Manager users can also create service locations.

Configuring a Pickup Mailbox in the Locations Folder

When SFTP clients collect their messages from MessageWay, they access a pickup mailbox through the SFTP Server and the MessageWay Service Interface.

The Service Interface allows users to pick up messages rather than have them delivered by MessageWay through an adapter. Therefore, when you create a location to use with the Service Interface, you do not specify an adapter. When you do not select an adapter, this location becomes a mailbox. For more information about creating locations, refer to the topic, ***Configuring Location Properties*** (on page 453).

Notice on the **General** page of the Mailbox Properties window, the location type of Mailbox is the result of not selecting an adapter or service. Notice also that there is no special adapter or service page.



TestPickup

Location Type: Mailbox

Description: Test pickup mailbox

Adapter/Service:

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

□ Check for Duplicates

□ By Source Location

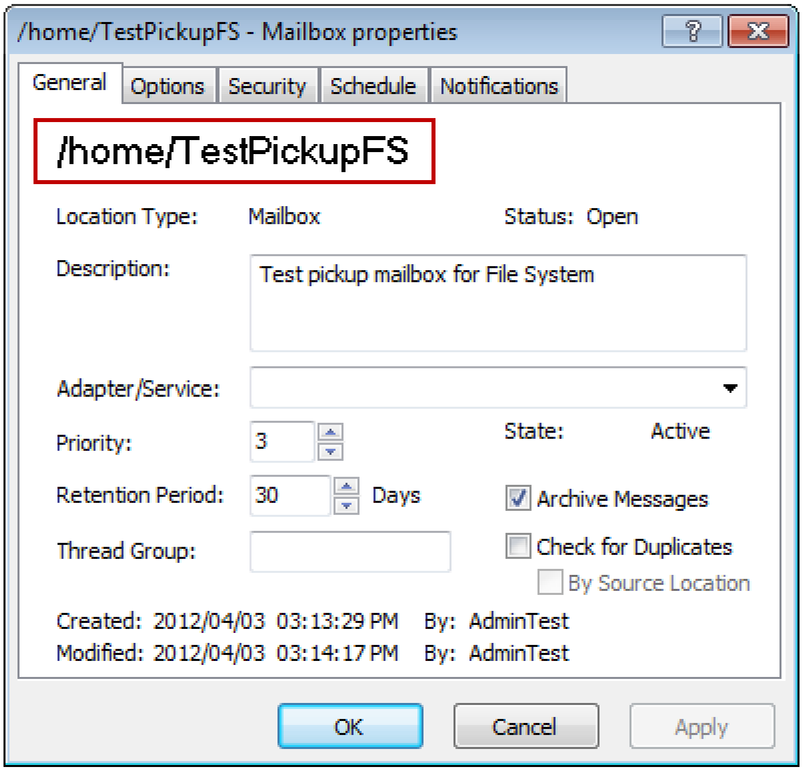
Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/10/28 12:00:00 PM By: <mway>

Pickup type mailboxes allow users to collect messages. To create a mailbox, do not select an adapter or service.

Configuring a Pickup Mailbox in the File System Folder

When you create a pickup mailbox in the File System folder, you also create a directory node of the same name. The mailbox name will reflect the full pathname of the directory, including slashes.

As for locations in the Locations folder, you do not select any adapter or service.



/home/TestPickupFS - Mailbox properties

/home/TestPickupFS

Location Type: Mailbox Status: Open

Description: Test pickup mailbox for File System

Adapter/Service:

Priority: 3 State: Active

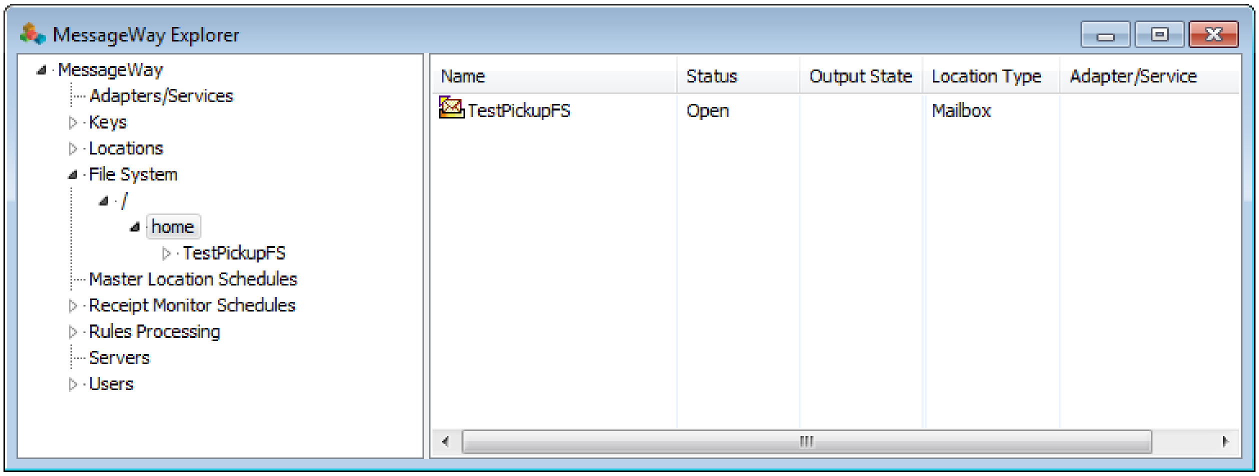
Retention Period: 30 Days ☑ Archive Messages

Thread Group: ☐ Check for Duplicates

☐ By Source Location

Created: 2012/04/03 03:13:29 PM By: AdminTest
Modified: 2012/04/03 03:14:17 PM By: AdminTest

Note that the directory structure appears in the left pane of MessageWay Explorer, and the mailbox in the right. To access the properties of the mailbox, you must right-click the mailbox and select **Properties**.



MessageWay Explorer

- MessageWay
  - Adapters/Services
  - Keys
  - Locations
  - File System
    - /
      - home
        - TestPickupFS
  - Master Location Schedules
  - Receipt Monitor Schedules
  - Rules Processing
  - Servers
  - Users

Name	Status	Output State	Location Type	Adapter/Service
TestPickupFS	Open		Mailbox	

Configuring Remote Users

When given proper security, remote users should be able to pick up (download) messages from MessageWay to their systems and send (upload) messages from their systems to MessageWay locations. Additional rights will allow users to cancel messages.

The user must have a logon ID and password, a default location and the appropriate rights to access necessary locations. To do this, we will take advantage of a user group, which allows us to configure the rights for the user at the group level. For more information about creating users and user groups, refer to the topic, ***Configuring User Security*** (on page 375).

To configure our remote user for testing purposes, proceed as follows:

1 From MessageWay Explorer, modify the Remote Users group to include the right, **Cancel Messages**.

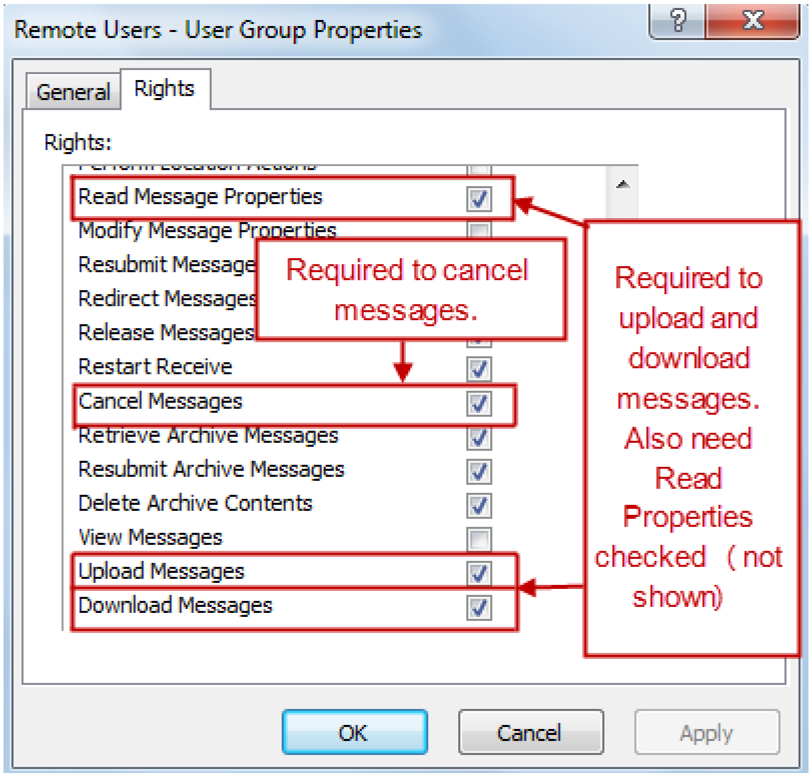
a) In the left pane click **Users** and in the right pane double-click the group, **Remote Users**.

The User Group Properties window appears.

b) Click the **Rights** tab, and in the Rights box, check **Cancel Messages**.

Remote users should typically be able to upload and download messages. When you check the **Download Messages** or **Upload Messages** right in the Rights box for the user group, the other related boxes are automatically checked. For our test, we also want remote users to be able to cancel messages, so we checked **Cancel Messages**.

The following boxes should be checked, at minimum.



Rights:

- Read Message Properties ☑
- Modify Message Properties □
- Resubmit Message
- Redirect Messages
- Release Messages
- Restart Receive ☑
- Cancel Messages ☑
- Retrieve Archive Messages ☑
- Resubmit Archive Messages ☑
- Delete Archive Contents ☑
- View Messages □
- Upload Messages ☑
- Download Messages ☑

Required to cancel messages.

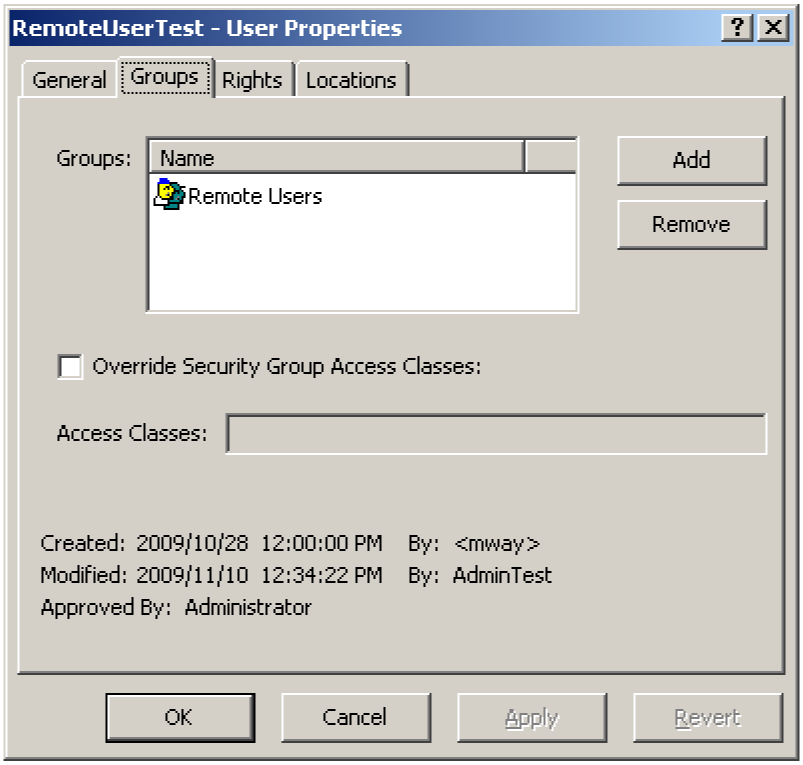
Required to upload and download messages. Also need Read Properties checked (not shown)

2 ***Create a user*** (on page 381) with the following information:

- User ID of **RemoteUserTest** or **RemoteUserTestFS**
- Password of **password**
- Group of **Remote Users**

This is an efficient way to consistently set the rights for users who have common needs. Access classes control user access through the Web Client, the SFTP Server, the FTP Server and the AS2 Interface, but we will ignore them for our test.

Note that the information at the bottom of the page will show when and by whom the entity was created, and when and by whom it was modified. When using the optional ***Maker/Checker feature*** (on page 893), it also shows who approved the changes.



Groups:

Name
Remote Users

□ Override Security Group Access Classes:

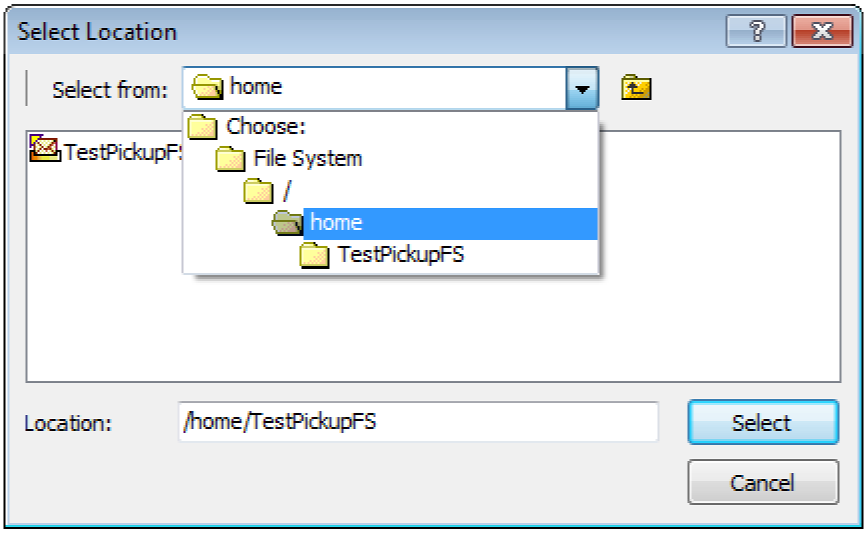
Access Classes:

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/10 12:34:22 PM By: AdminTest
Approved By: Administrator

3 On the Locations tab, add a default location.

- For users whose default location is in the Locations folder, type **TestPickup**
- For users whose default location is in the File System folder, type **TestPickupFS**

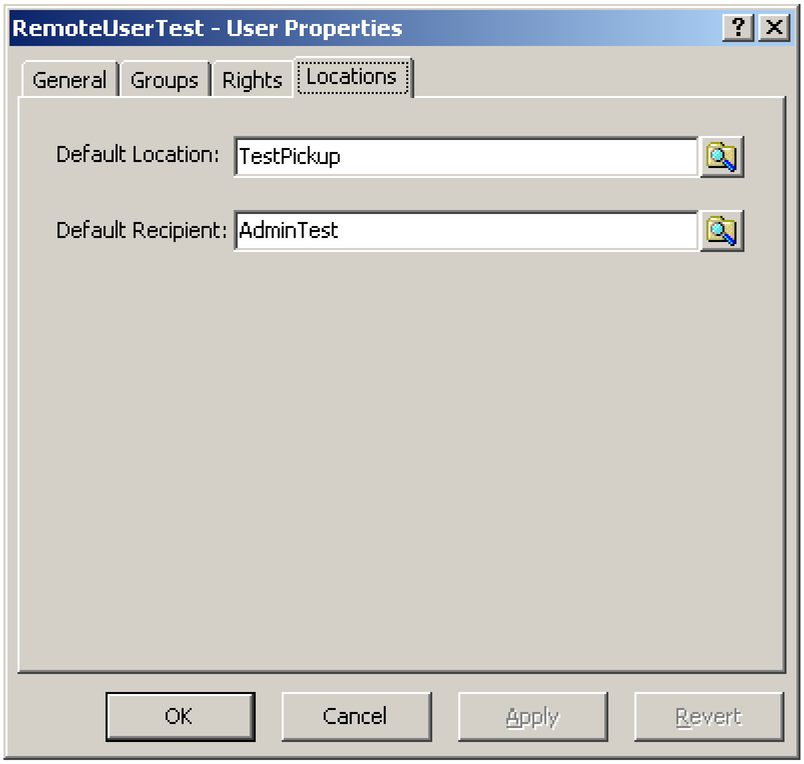
To browse to locations in the File System folder, click the **Browse** button, and then the down button on the Select from box, and click **Choose**. When the File System folder appears, double click to



Location: /home/TestPickupFS

Each user accessing MessageWay through the Service Interface must be assigned a default location. When the user logs on to MessageWay, the contents of this mailbox displays first. Users may then switch to another location to which they have access. This location also provides the source location for any uploaded messages.

4 Optionally, add a default recipient, to upload messages to a location other then the Default Location. If not provided, messages are uploaded to the Default Location.



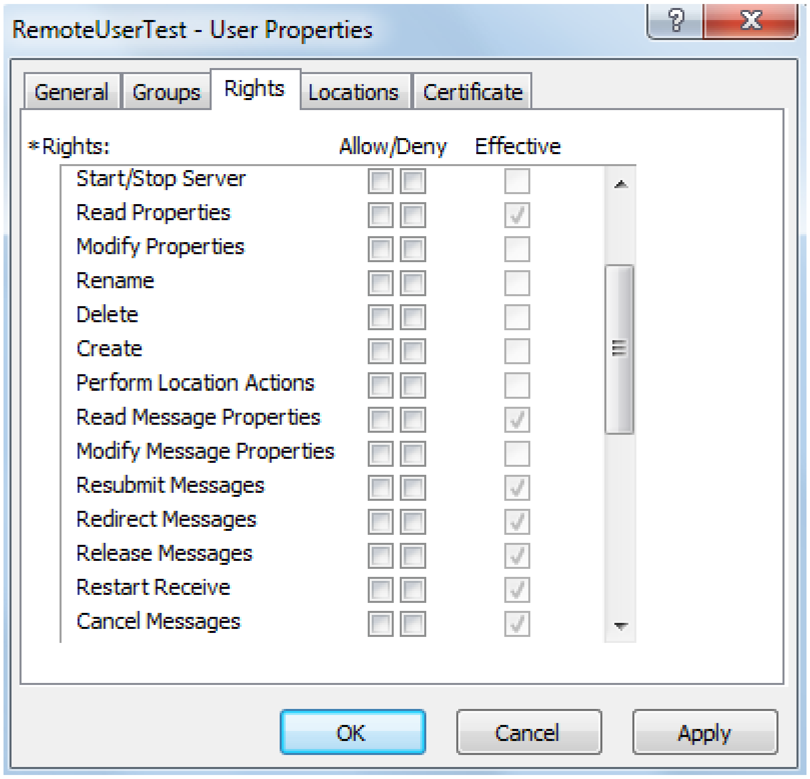
Default Location: TestPickup

Default Recipient: AdminTest

5 Check that at least the user rights are checked as shown here.

The user's rights are the combined rights of all groups to which the user belongs. In this case, the user only belongs to the Remote Users group, whose rights appear in the Effective column on the Rights page of the User Properties window.

TIP: The default rights for the Remote Users group do not include the property *Cancel Messages*. If you have not changed the rights at the group level as suggested previously, you can add that right for your user by checking the *Allow* column.



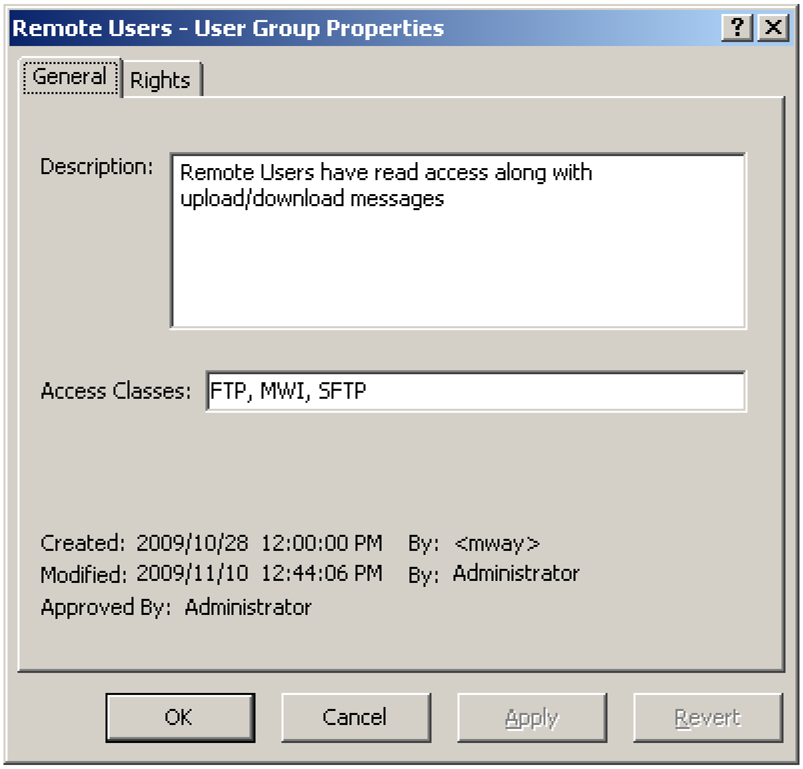
*Rights:	Allow/Deny		Effective
Start/Stop Server	□	□	□
Read Properties	□	□	☑
Modify Properties	□	□	□
Rename	□	□	□
Delete	□	□	□
Create	□	□	□
Perform Location Actions	□	□	□
Read Message Properties	□	□	☑
Modify Message Properties	□	□	□
Resubmit Messages	□	□	☑
Redirect Messages	□	□	☑
Release Messages	□	□	☑
Restart Receive	□	□	☑
Cancel Messages	□	□	☑

Controlling User Access with Access Classes

To limit the access paths to MessageWay for a user or group of users, you assign an access class. When an access class is set for a user, they will not be able to log on to MessageWay unless the SFTP Perimeter Server configuration file also has that access class listed. The user must be configured either with no access classes or with at least the access class defined for the perimeter server.

IMPORTANT: Access class names are case sensitive. They must match the access class names configured in the Global section of the configuration file for the SFTP Perimeter Server (mwsftpd.conf).

Access classes may be assigned to a user group. You do this on the **General** page of the User Group Properties window.



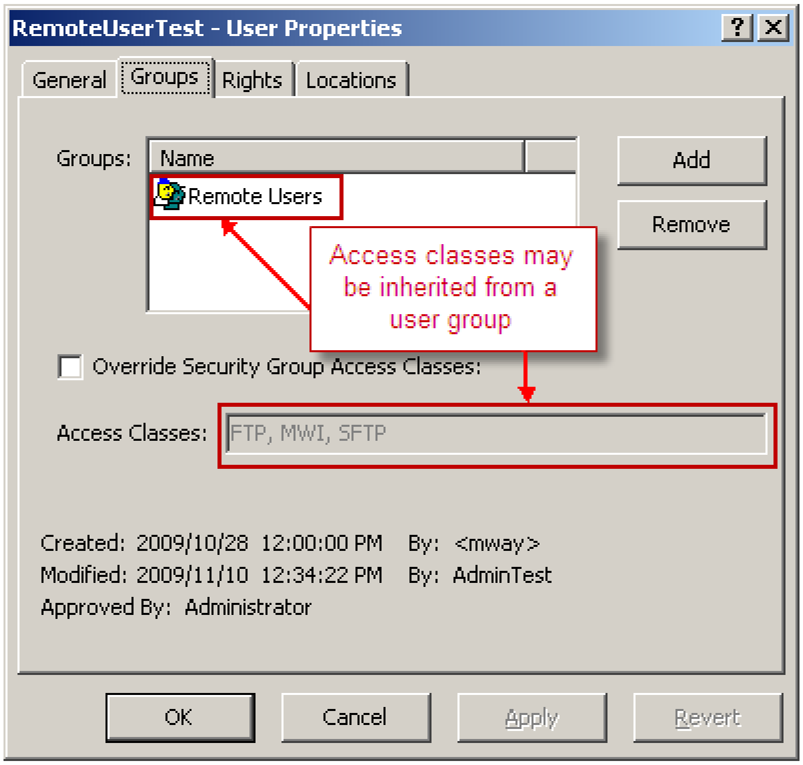
Remote Users - User Group Properties

Description: Remote Users have read access along with upload/download messages

Access Classes: FTP, MWI, SFTP

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/10 12:44:06 PM By: Administrator
Approved By: Administrator

Access classes on the group list are then assigned to users that belong to that group.



RemoteUserTest - User Properties

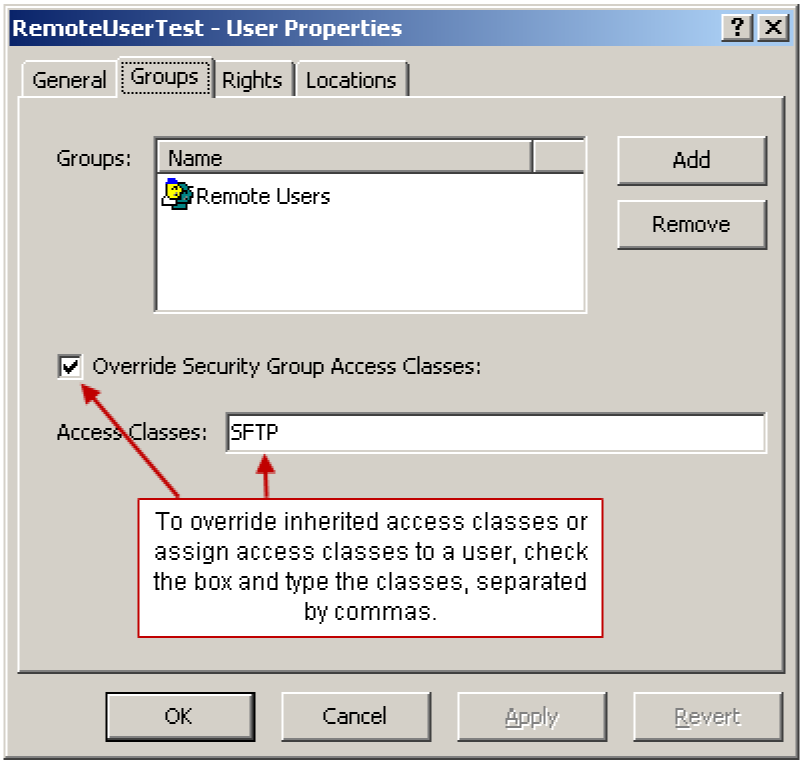
Access classes may be inherited from a user group

☐ Override Security Group Access Classes:

Access Classes: FTP, MWI, SFTP

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/10 12:34:22 PM By: AdminTest
Approved By: Administrator

To assign one or more access classes to a single user or override access classes inherited from a group, you specify them on the **Groups** page of the User Properties window, separated by commas.



Groups:

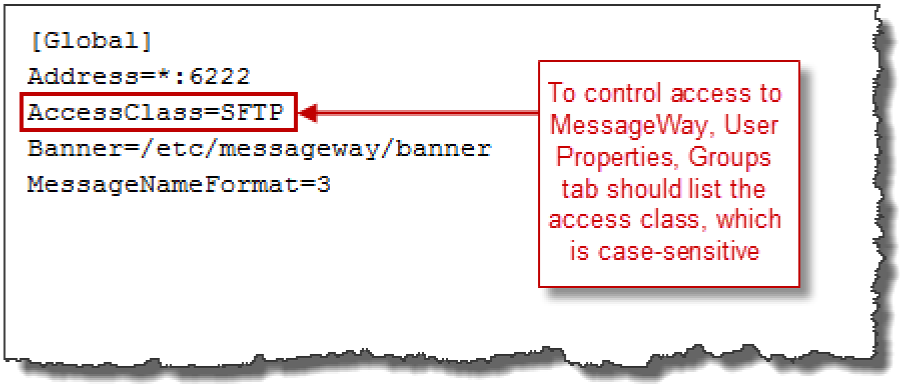
Name
Remote Users

☑ Override Security Group Access Classes:

Access Classes: SFTP

To override inherited access classes or assign access classes to a user, check the box and type the classes, separated by commas.

This access class must be listed in the SFTP configuration file, mwsftpd.conf. If the access class in the configuration file is blank, then the access class for the user must also be blank. If the access class in the configuration file is not blank, then the access class for the user must either match the access class in the configuration file or the access class list for the user must be blank.



```
[Global]
Address=*:6222
AccessClass=SFTP
Banner=/etc/messageway/banner
MessageNameFormat=3
```

To control access to MessageWay, User Properties, Groups tab should list the access class, which is case-sensitive

Assigning Rights for Locations

Once you have assigned rights to your user, you must make sure that the user is able to access the necessary locations. To do so, you assign appropriate rights to the locations, which are called access lists, that determine who can do what to locations.

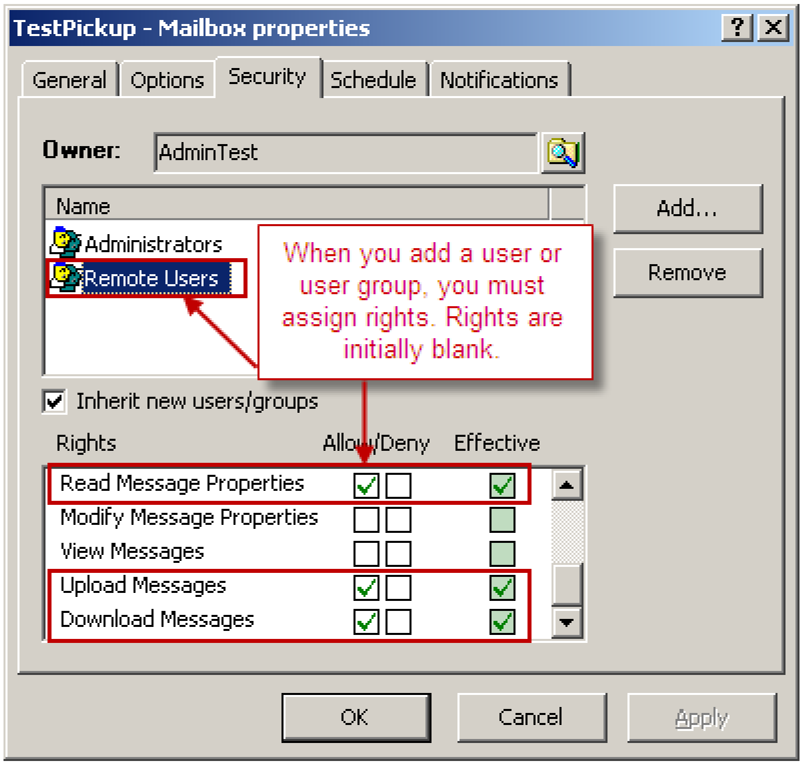
To create an access list, you add user groups or users to the **Names** box and specify the rights in the **Rights** box. You set these rights separately from the rights set for the user. When a user attempts to access a location, the rights of the location are compared with the rights of the user, and only those rights that match are allowed. The user must be a member of one of the listed groups or must be listed separately. For more information, refer to the topic ***Configuring User Security*** (on page 375).

A mailbox is a special type of location that allows users to pickup or collect messages. In the following example, the Remote Users group has been added to the Security page of the mailbox, TestPickUp, and we set the same rights for the mailbox as we set for the Remote Users user group, not all of which are currently visible.

Notice that we had to check the **Allow** boxes for the rights *Upload Messages* and *Download Messages*. This is because the Remote Users group was added to this specific mailbox rather than being inherited from its folder. That is, the Remote Users group is not listed on the **Security** tab of the **Folder** Properties window for the **Locations** folder, so its rights could not be inherited. Had Remote Users group been inherited from the **Locations** folder, this mailbox would have inherited the rights set at the folder level. Since they weren't inherited, we had to specifically set the rights for the mailbox.

Since the rights for our user match the rights for the mailbox, the user will be able to access messages in this mailbox.

IMPORTANT: For users to be able to access messages in locations other than their default mailbox, they must have access rights to those other locations.



Owner: AdminTest

Name
Administrators
Remote Users

When you add a user or user group, you must assign rights. Rights are initially blank.

☑ Inherit new users/groups

Rights	Allow	Deny	Effective
Read Message Properties	☑	□	☑
Modify Message Properties	□	□	□
View Messages	□	□	□
Upload Messages	☑	□	☑
Download Messages	☑	□	☑

Access List for TestPickup Mailbox (Mailbox Properties Window, Security Page)

Configuring a Secure or Non-Secure Connection to the Service Interface

To configure a secure or non-secure connection between the SFTP server and the MessageWay Service Interface (SI), you change the following parameters in the MSI section of the mwsftpd.conf file. The SI also has a configuration file, mwsi.conf, which defines the ports on which it listens. For more information about SI configuration, refer to the topic, ***Service Interface*** (on page 95).

The options in the mwsftpd.conf file are commented, so you should only have to comment the one you do not want to use, and uncomment the one you do want to use. Here are the parameters to select in the MSI section:

Parameter	Non-secure Value	Secure Value
Address=	*IPaddress*:**6280**	*IPaddress*:**6243**
Security=	**None**	**SSL** or **TLS**

Parameter	Non-secure Value	Secure Value
CertVerifyFile=	Ignored	Choose this to use the anonymous certificates installed with SI. **IMPORTANT:** Use either the CertVerifyFile or CertFingerprint parameter.
CertFingerprint=	Ignored	Choose this to use the fingerprint associated with the certificate installed with SI. **IMPORTANT:** Use either the CertVerifyFile or CertFingerprint parameter.

Configuring Public Key Authentication of the Client

By default, the MessageWay SFTP Server uses a MessageWay user ID and password for MessageWay to authenticate the user. Users, however, may prefer to use their public key for authentication. To accomplish this, the SFTP server authenticates the client user, and then passes its own credentials to be authenticated as a trusted agent to the MessageWay Service Interface (SI) together with those of the client.

NOTE: The SFTP server supports password and public key authentication. It does not support other types of authentication, including keyboard interactive.

To test this type of authentication, you must modify the configurations for SFTP Server (mwsftpd.conf) and SI (mwsi.conf) to support:

- Client certificate authentication in mwsftpd.conf and mwsi.conf
- Agent authentication in mwsftpd.conf and mwsi.conf
- Public key authentication in mwsftpd.conf

IMPORTANT: The following instructions assume that this is a new installation and that the configuration files have the most recent defaults and settings. If you have already configured mwsftpd.conf or mwsi.conf, you may have to add the appropriate lines to the configuration file. Update processes never overlay existing configuration files.

To Configure SFTP for Public Key Authentication

To configure SFTP to test public key authentication, you will add information to the MSI section to define the client certificate and to enable agent authentication. Then in the SSHD section, you will enable public key authentication.

1 To configure client certificates and agent authentication, in the MSI section, uncomment the following lines:

- ClientCertFile
- ClientKeyFile
- ClientKeyPassphrase

IMPORTANT: Specify the correct file names of the certificate and key files. You can use the test files are supplied with the install package for testing or you specify your own certificate and key file names.

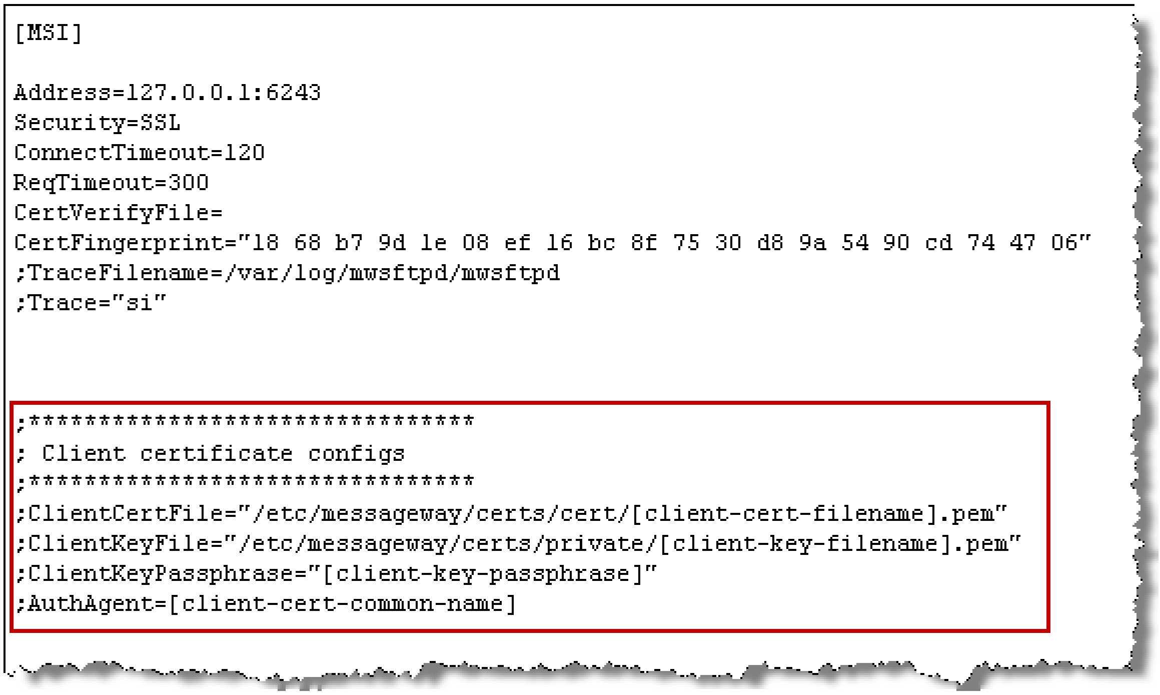
Also specify the passphrase and authorized agent with values that match the values in the test certificate.

2 To enable agent authentication, in the MSI section, uncomment the following line:

- AuthAgent

IMPORTANT: Specify the common name of the client certificate.

3 To use the test certificates provided, you should also change the address from 127.0.0.1 to *localhost* to match the Common Name in the certificates.



```
[MSI]

Address=127.0.0.1:6243
Security=SSL
ConnectTimeout=120
ReqTimeout=300
CertVerifyFile=
CertFingerprint="18 68 b7 9d 1e 08 ef 16 bc 8f 75 30 d8 9a 54 90 cd 74 47 06"
;TraceFilename=/var/log/mwsftpd/mwsftpd
;Trace="si"



;********************************
; Client certificate configs
;********************************
;ClientCertFile="/etc/messageway/certs/cert/[client-cert-filename].pem"
;ClientKeyFile="/etc/messageway/certs/private/[client-key-filename].pem"
;ClientKeyPassphrase="[client-key-passphrase]"
;AuthAgent=[client-cert-common-name]
```

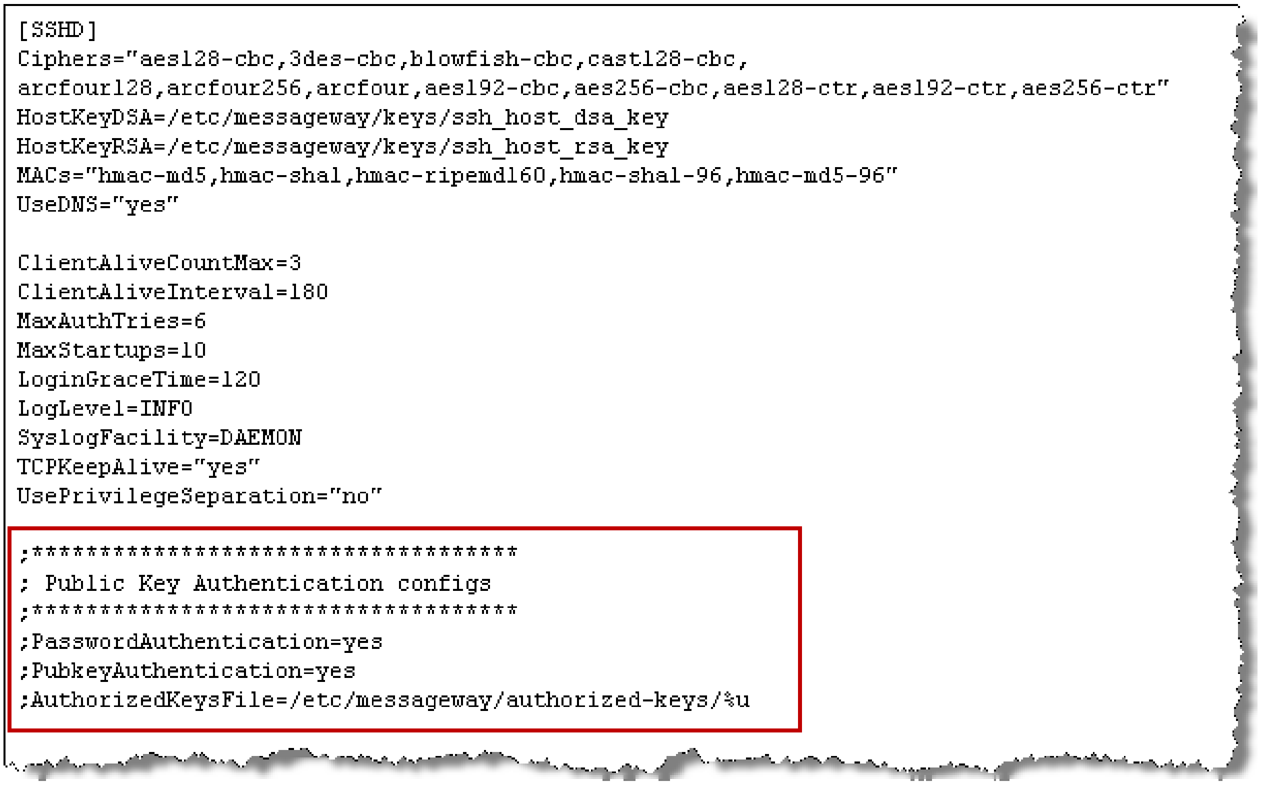
4 To enable public key authentication, in the SSHD section:

a) Comment the following line:

- PasswordAuthentication

b) Uncomment the following lines:

- PubkeyAuthentication
- AuthorizedKeysFile



```
[SSHD]
Ciphers="aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,
arcfour128,arcfour256,arcfour,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr"
HostKeyDSA=/etc/messageway/keys/ssh_host_dsa_key
HostKeyRSA=/etc/messageway/keys/ssh_host_rsa_key
MACs="hmac-md5,hmac-sha1,hmac-ripemd160,hmac-sha1-96,hmac-md5-96"
UseDNS="yes"

ClientAliveCountMax=3
ClientAliveInterval=180
MaxAuthTries=6
MaxStartups=10
LoginGraceTime=120
LogLevel=INFO
SyslogFacility=DAEMON
TCPKeepAlive="yes"
UsePrivilegeSeparation="no"

;************************************
; Public Key Authentication configs
;************************************
;PasswordAuthentication=yes
;PubkeyAuthentication=yes
;AuthorizedKeysFile=/etc/messageway/authorized-keys/%u
```

To Configure Service Interface for Public Key Authentication

To configure the Service Interface to test public key authentication, you will add information to force the Service Interface to request a client certificate and to then validate the certificate, if provided. Then you will specify the location of the agent file that contains all authorized agents and a list of authorized groups or users.

For more information about the use of the parameters for the CTX1 configuration, refer to the topic, ***Service Interface, Security Context Configurations Section*** (on page 99).

For more information about the use of the parameters for the L2HTTPS configuration, refer to the topic, ***Service Interface, HTTP Listener Configurations Section*** (on page 98).

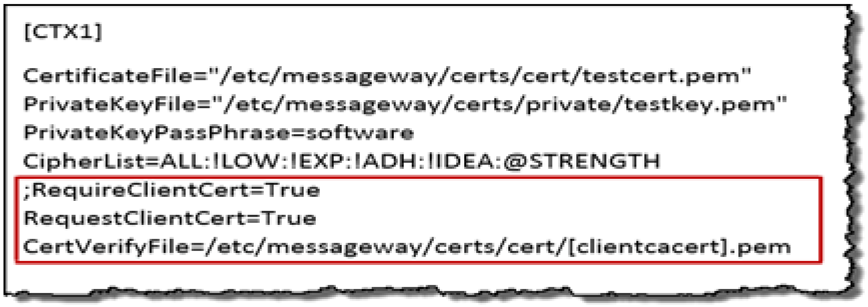
Proceed as follows:

1 To configure client certificates and agent authentication, in the CTX1 configuration of the Security Context Configurations section:

a) Uncomment RequestClientCert and ensure it is set to True.

NOTE: If you only want to allow public key authentication and not password, make use of RequireClientCert instead of RequestClientCert.

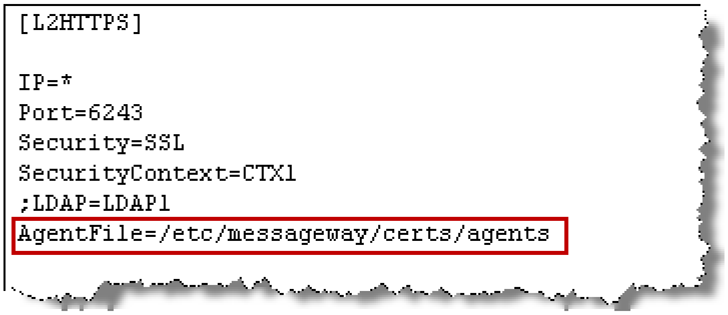
b) Uncomment the parameter CertVerifyFile, and type the name of your certificate bundle in place of *[clientcacert]*.



```
[CTX1]

CertificateFile="/etc/messageway/certs/cert/testcert.pem"
PrivateKeyFile="/etc/messageway/certs/private/testkey.pem"
PrivateKeyPassPhrase=software
CipherList=ALL:!LOW:!EXP:!ADH:!IDEA:@STRENGTH
;RequireClientCert=True
RequestClientCert=True
CertVerifyFile=/etc/messageway/certs/cert/[clientcacert].pem
```

2 To specify the location of the agent file, in the L2HTTP configuration of the HTTP Listeners Configurations section, uncomment the AgentFile parameter, and specify the location of the file.

CAUTION: The agents file may be used by multiple processes, including the SFTP Server and the AS2 Interface. You may have multiple agents files, but when one is used by multiple processes, don't move it without specifying the new location for all processes.



```
[L2HTTPS]

IP=*
Port=6243
Security=SSL
SecurityContext=CTX1
;LDAP=LDAP1
AgentFile=/etc/messageway/certs/agents
```

To Create the Agents File

You must create the agents file in the location specified in the parameter, AgentFile, in the mwsi.conf file.

By default, a sample file called agents.sample is installed in the following locations, depending on the operating system:

Operating System	Location of the Agents Sample File
UNIX or Linux	/etc/messageway/certs/agents.sample
Windows	\Users\MessageWayUser\AppData\Roaming\messageway\certs\agents.sample

The general rules for the agents file are as follows:

- Must list the AuthAgent value in the appropriate configuration file, such as mwas2.conf or mwsftpd.conf or mwftpd.conf if you are configuring anonymous user access
- Must list all groups and users allowed or denied connection for a given agent

The syntax rules for the agents file are as follows:

- Use Semi-colon (;) to comment a line
- Use separate lines for each AuthAgent and its users and groups list
    - AuthAgent must be first item on the line separated from list of users by at least one space or tab character
        - AuthAgent must match the common name (CN) used in the client certificate
        - Users and groups must be users or groups configured in MessageWay
    - Users and groups follow AuthAgent on the same line
        - Items in this list are separated by commas
        - Items may be in any order
        - Allowed or denied status of user overrides status of group
        - Allowed or denied status of group or user overrides asterisk (*)
        - Use an exclamation mark (!) to deny access to a user or group
        - Enclose group names in greater than (<) and less than (>) signs
        - Optionally use quotation marks (" ") around user names

The following table provides some examples for the user list:

User List Syntax	Description
!*user* - or - !"*user*"	Deny access to this user. This access overrides any access for a group to which the user belongs.
user - or - "*user*"	Allow access to this user. This access overrides any access for a group to which the user belongs.
!<*group***>**	Deny access to this group. Individual user access overrides group access.
<*group***>**	Allow access to this group. Individual user access overrides group access.
*	Allow all users. Individual user or group access overrides this access.

To create and configure the agents file, proceed as follows:

1 In Windows, using a text editor, create an empty file called **agents** (no extension) in the same location specified in the AgentFile parameter of the HTTP Listeners Configuration section in the MessageWay Service Interface configuration file, mwsi.conf.

2 On a new line in the agents file, type the following:

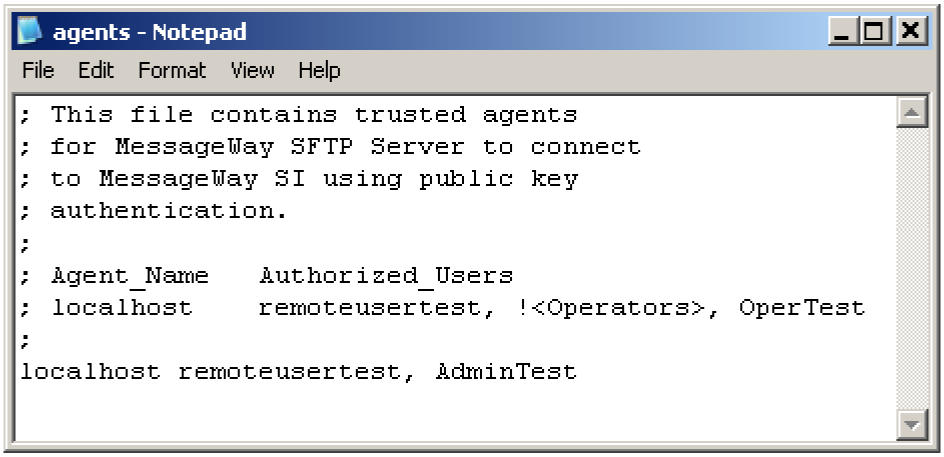
a) The name that matches the common name (CN) on the AS2 client certificate

b) At least one space or tab character

c) MessageWay users that will be allowed to send messages to MessageWay, with the user names separated by commas.

Following our example, type:

localhost remoteusertest, AdminTest



```
; This file contains trusted agents
; for MessageWay SFTP Server to connect
; to MessageWay SI using public key
; authentication.
;
; Agent_Name   Authorized_Users
; localhost    remoteusertest, !<Operators>, OperTest
;
localhost remoteusertest, AdminTest
```

To Copy Client's Public Key File

For each client that SFTP authenticates using a public key, you must copy the client's public key file to a MessageWay location, and name the file the same as the user ID that the client would use to log on to MessageWay.

1 From Windows, copy the client's public key file to the location specified in the SSHD section of the mwsftpd.conf file, typically **/etc/messageway/authorized-keys**.

2 Rename the test key file to the MessageWay user ID associated with the client, such as **RemoteUserTest**.

CAUTION: The user ID is case-sensitive here. When users log on through an SFTP client, they must specify the user ID with the appropriate case.

3 Repeat steps 1 and 2 for all clients who will connect to MessageWay through the MessageWay SFTP Server using a public key for authentication.

To Create A Public Key File for UNIX or Linux

To create public keys for testing, proceed as follows:

1 Logon to the system running the SFTP Client as user who will be running the SFTP Client, typically **mway**.

2 Go to the directory, /home/mway/.ssh.

3 Generate a key pair using the following command:

ssh-keygen -f id_rsa -t rsa

For example:

NOTE: Do NOT enter a passphrase when prompted unless you want to be prompted to enter the passphrase every time you run an SFTP Client)

[mway@SUN1 ~]$ **ssh-keygen -f id_rsa -t rsa**

Generating public/private rsa key pair.

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
fc:ec:37:59:17:a9:f6:a1:60:db:4e:95:09:5e:3f:33 mway@SUN1
```

The following two files will be created in the /home/mway/.ssh folder:

- id_rsa
- id_rsa.pub

4. Logon to the system where MessageWay is installed.
5. Copy the file, id_rsa.pub, created in step 3 into the folder:
   /etc/messageway/authorized-keys/
6. Rename the file to a valid MessageWay user ID, which you will use to start the SFTP client.

CAUTION: The user ID is case-sensitive here. When users log on through an SFTP client, they must specify the user ID with the appropriate case.

Configuring Anonymous Access

The MessageWay SFTP Perimeter Server may be configured to allow users to log on to MessageWay as anonymous. Proper configuration of MessageWay to do this requires the following:

- ***Define a MessageWay user called*** *anonymous* (on page 250)
- ***Configure the MessageWay SFTP server to allow anonymous access*** (on page 354)
- ***Configure the MessageWay Service Interface to allow anonymous access*** (on page 355)
- ***Configure the agents file to allow access to the client*** (on page 259)

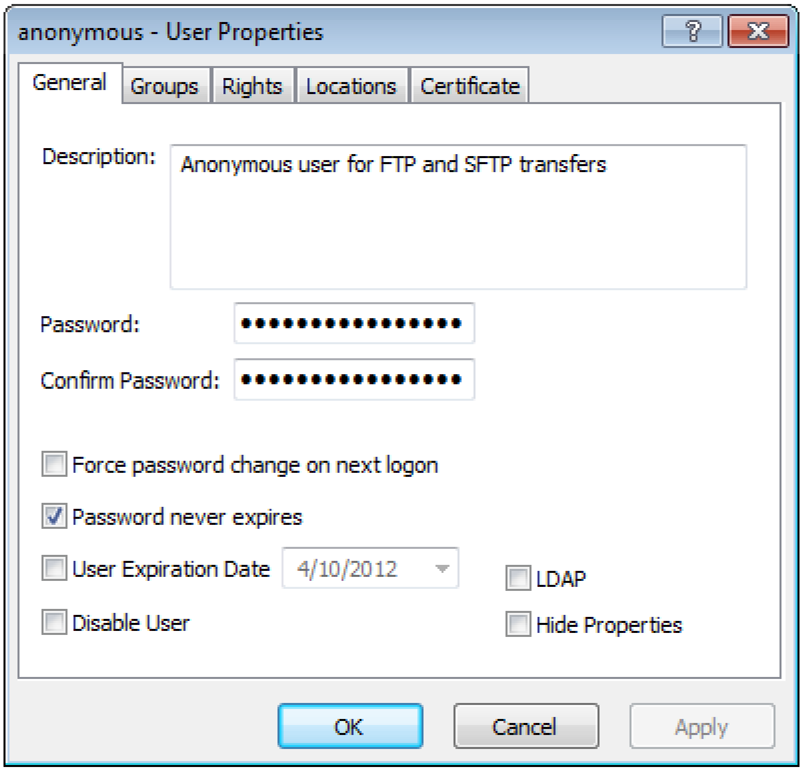
IMPORTANT: After you have finished these tasks, make sure you restart the perimeter server and the ***Service Interface*** (on page 103) so they will read the changed configuration files.

To Define an Anonymous MessageWay FTP or SFTP User

To configure an anonymous user who will access MessageWay from an FTP or SFTP client, proceed as follows:

1. Add a user called **anonymous**.
2. On the **General** page, type a description, a password and choose your password expiration policy.

NOTE: You must enter a password, but it is ignored during an FTP session.



Description: Anonymous user for FTP and SFTP transfers

Password: ••••••••••••••••

Confirm Password: ••••••••••••••••

□ Force password change on next logon

☑ Password never expires

□ User Expiration Date 4/10/2012

□ LDAP

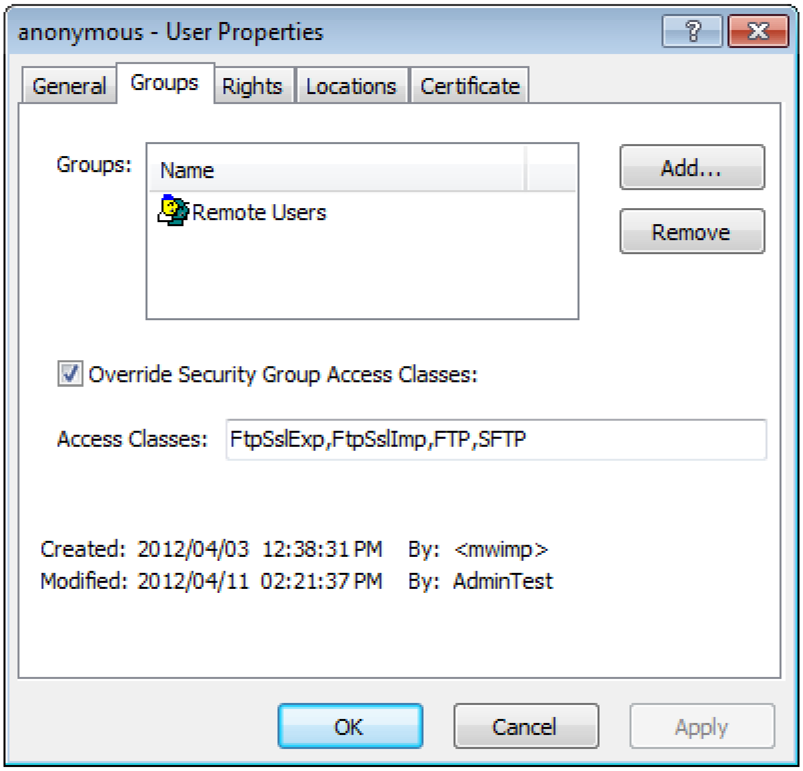
□ Disable User

□ Hide Properties

3 On the **Groups** page, add this user to the *Remote Users* group.

4 Check the Override Security Group Access Classes, and type the access class or classes that you support, separated by commas. They must match *exactly* what you have specified on the FTP server configuration file, mwftpd.conf or on the SFTP server configurations file, mwsftpd.conf.

CAUTION: Access class names are *case-sensitive*.



Groups:

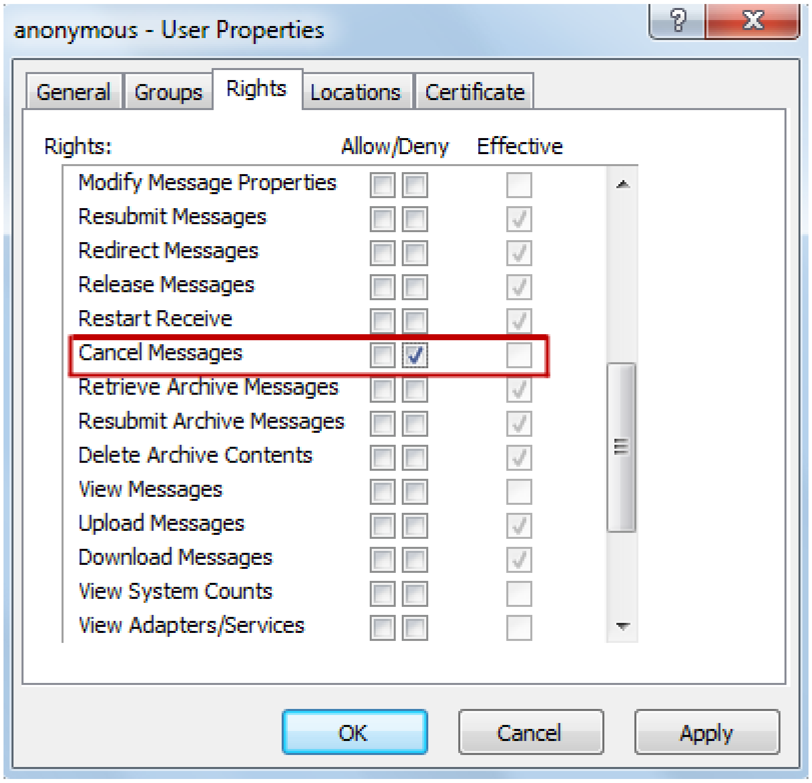
Name
Remote Users

☑ Override Security Group Access Classes:

Access Classes: FtpSslExp,FtpSslImp,FTP,SFTP

Created: 2012/04/03 12:38:31 PM By: <mwimp>
Modified: 2012/04/11 02:21:37 PM By: AdminTest

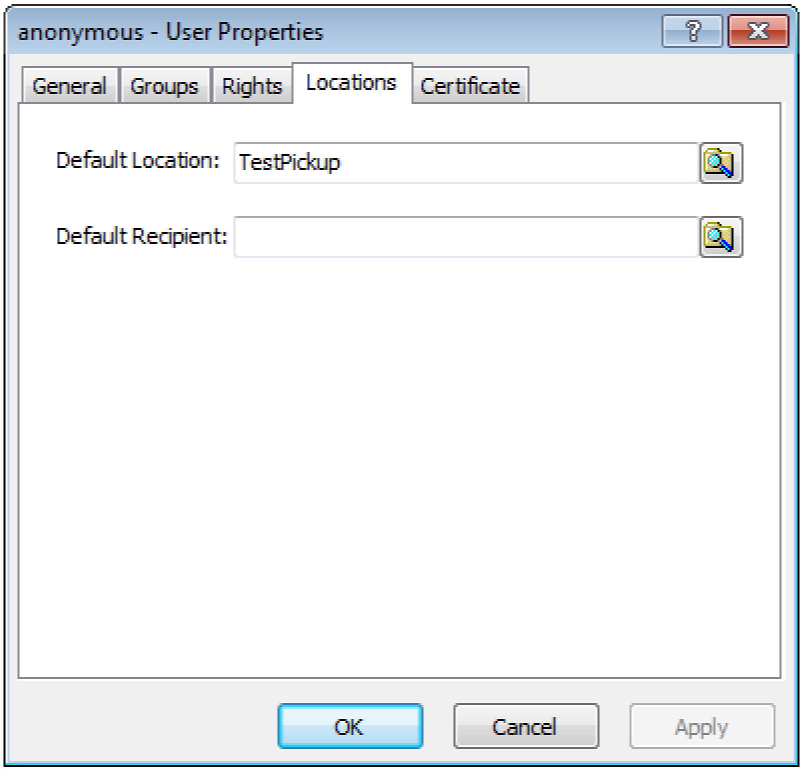
5 On the **Rights** page, appropriate rights will be inherited from the group *Remote Users*. You do not need to change anything, ***unless you have configured the group to be able to cancel messages*** (on page 241). If you do not want to give this privilege to anonymous users, you need to deny, **Cancel Messages**.



Rights:	Allow	Deny	Effective
Modify Message Properties	□	□	□
Resubmit Messages	□	□	☑
Redirect Messages	□	□	☑
Release Messages	□	□	☑
Restart Receive	□	□	☑
Cancel Messages	□	☑	□
Retrieve Archive Messages	□	□	☑
Resubmit Archive Messages	□	□	☑
Delete Archive Contents	□	□	☑
View Messages	□	□	□
Upload Messages	□	□	☑
Download Messages	□	□	☑
View System Counts	□	□	□
View Adapters/Services	□	□	□

6 On the **Locations** page, select a ***pickup mailbox*** (on page 237) for the default location and select an optional ***default recipient location*** (on page 236). The default recipient location is useful if all anonymous users will be sending files to a specific location, such as for translation, and they don't want to always specify the location in their PUT commands. Make sure you select or type the appropriate default location depending on whether it is in the Locations folder or the File System folder. For a description of the differences, refer to the topic ***Overview of Location Properties*** (on page 453).

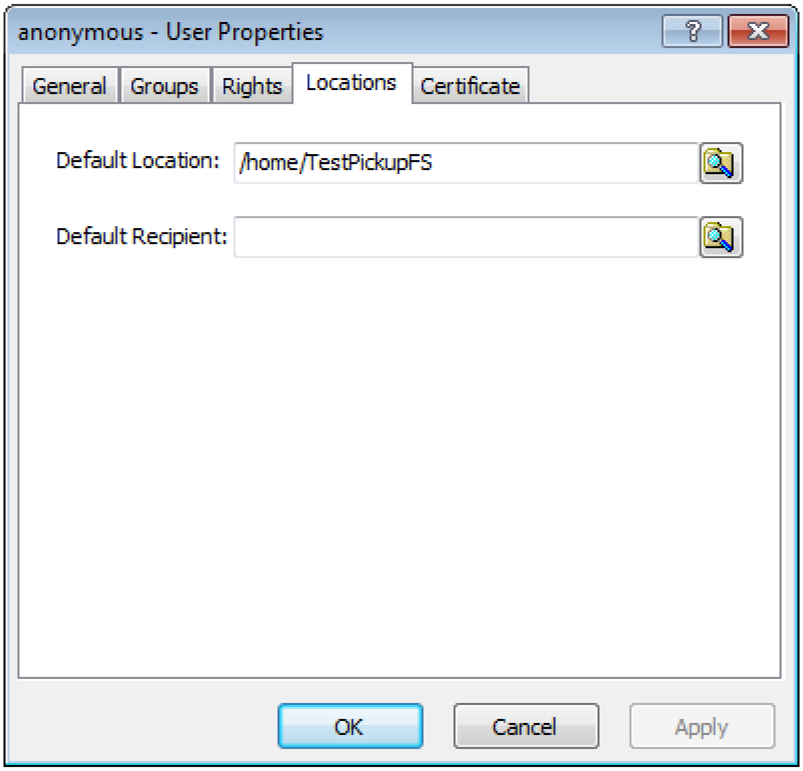
The following default location is in the Locations folder.



Default Location: TestPickup

Default Recipient:

This location is in the File System folder.



Default Location: /home/TestPickupFS

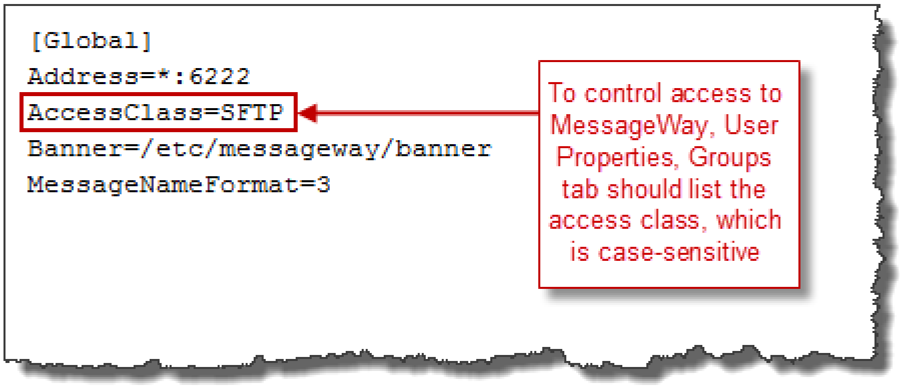
Default Recipient:

7 Click **OK**.

To Configure the SFTP Server for Anonymous Access

To configure the FTP server for anonymous access, you must make the following changes to the ***SFTP server configuration file*** (on page 321), mwsftpd.conf:

1 In the Global section, make sure the AccessClass parameter is assigned, typically SFTP:



```
[Global]
Address=*:6222
AccessClass=SFTP
Banner=/etc/messageway/banner
MessageNameFormat=3
```

To control access to MessageWay, User Properties, Groups tab should list the access class, which is case-sensitive

2 Anonymous access requires that the connection from the SFTP server to the Service Interface be SSL. There are two pre-configured MSI sections. Only one of the sections can be active at a time, so one is commented. The default is *without* SSL security. To configure the secure connection, in the MSI Section:

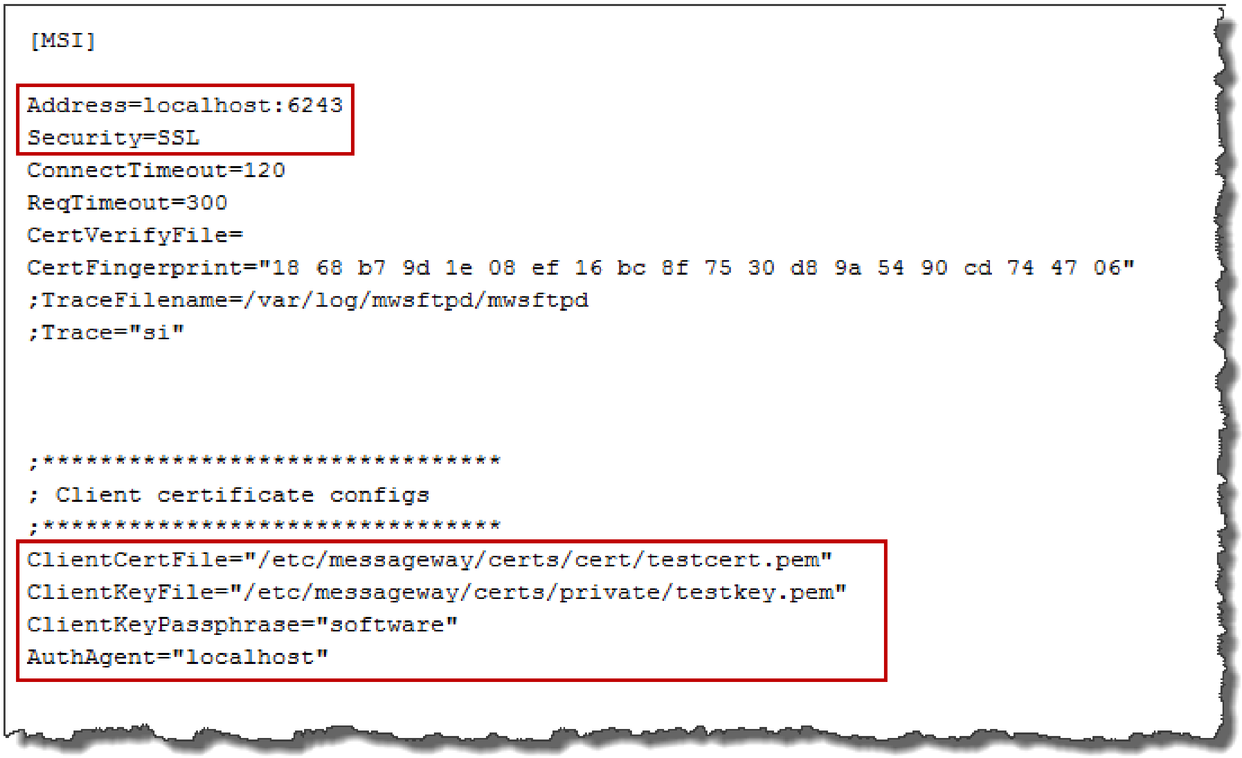
a) Comment all the lines for the first MSI section.

b) Uncomment the lines for the second MSI section, as shown here.

c) Review the following parameters, and make changes as required:

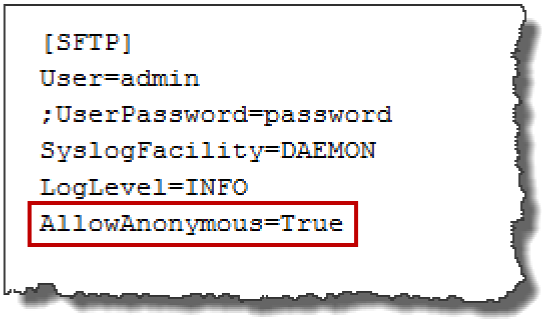
- **Address=localhost**
- Client certificate files are correct for your system, and for testing we will use the default test certificate files
- **ClientKeyPassphrase="software"**
- **AuthAgent="localhost"**

MessageWay uses a file, by default called *agents*, to specify who can connect to the service interface. The AuthAgent you specify here, must be configured in that file and must be the same as the *Address* name specified here.



```
[MSI]

Address=localhost:6243
Security=SSL
ConnectTimeout=120
ReqTimeout=300
CertVerifyFile=
CertFingerprint="18 68 b7 9d 1e 08 ef 16 bc 8f 75 30 d8 9a 54 90 cd 74 47 06"
;TraceFilename=/var/log/mwsftpd/mwsftpd
;Trace="si"



;********************************
; Client certificate configs
;********************************
ClientCertFile="/etc/messageway/certs/cert/testcert.pem"
ClientKeyFile="/etc/messageway/certs/private/testkey.pem"
ClientKeyPassphrase="software"
AuthAgent="localhost"
```

3 In the SFTP Section, set the AllowAnonymous parameter to **True**:



```
[SFTP]
User=admin
;UserPassword=password
SyslogFacility=DAEMON
LogLevel=INFO
AllowAnonymous=True
```

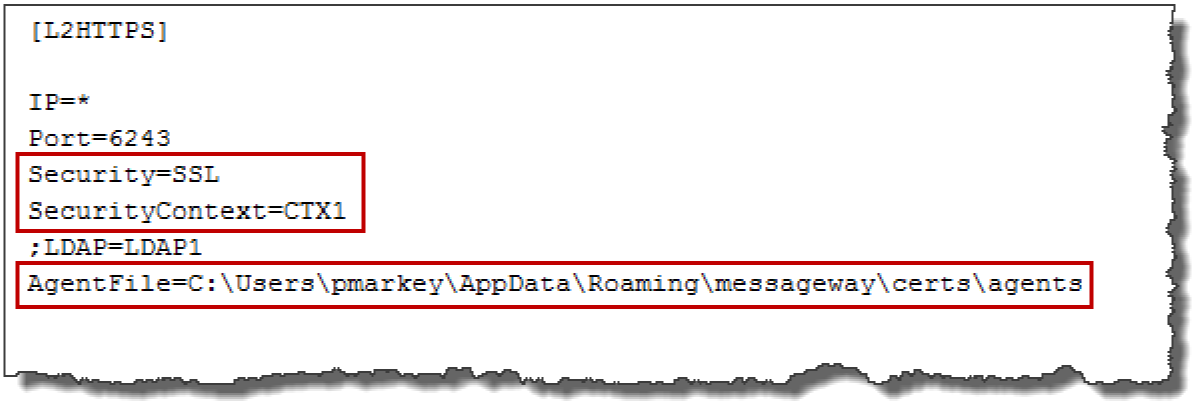
4 Save your changes.

5 ***Restart the SFTP perimeter server*** (on page 359) so that it will read the new configuration file.

To Configure the MessageWay Service Interface

The MessageWay Service Interface acts as a server to the MessageWay SFTP Perimeter Server when it attempts a connection to MessageWay. For connections that serve anonymous users, this must be SSL. To configure the ***MessageWay Service Interface configuration file, mwsi.conf*** (on page 95), to allow access to MessageWay for anonymous users, proceed as follows:

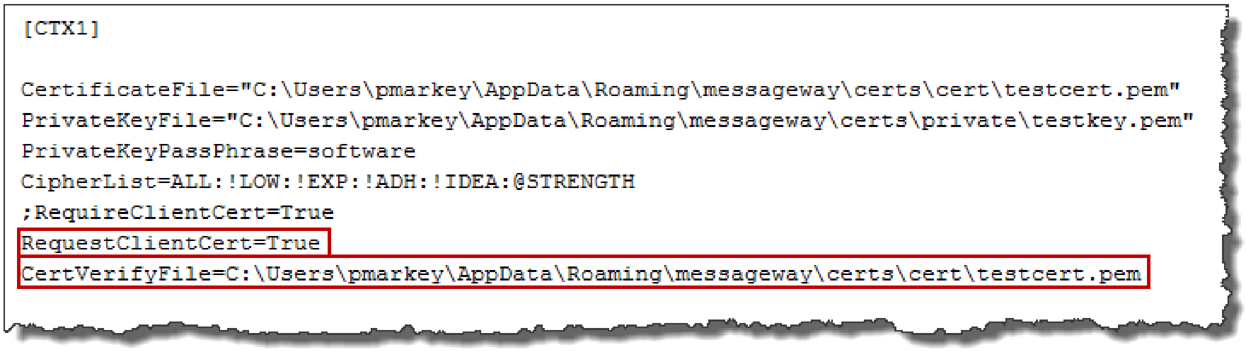
1 In the HTTP Listener Configurations Section, make sure the agents file is in the location specified. If not, you will need to change the location here to point to the correct location or ***create the file*** (on page 259).



```
[L2HTTPS]

IP=*
Port=6243
Security=SSL
SecurityContext=CTX1
;LDAP=LDAP1
AgentFile=C:\Users\pmarkey\AppData\Roaming\messageway\certs\agents
```

2 In the Security Context Configurations Section, review the [CTX1] configuration and change as necessary:

- Client certificates specify the correct location. You can leave these as is if you are using the default test certificates.
- Uncomment the RequestClientCert parameter, and set it to **True**.
- Uncomment the CertVerifyFile and specify the full path name of the certificate file to verify the connecting server.



```
[CTX1]

CertificateFile="C:\Users\pmarkey\AppData\Roaming\messageway\certs\cert\testcert.pem"
PrivateKeyFile="C:\Users\pmarkey\AppData\Roaming\messageway\certs\private\testkey.pem"
PrivateKeyPassPhrase=software
CipherList=ALL:!LOW:!EXP:!ADH:!IDEA:@STRENGTH
;RequireClientCert=True
RequestClientCert=True
CertVerifyFile=C:\Users\pmarkey\AppData\Roaming\messageway\certs\cert\testcert.pem
```

3 Save your changes.

Restart the Service Interface (on page 103), so that it will read the new configuration file.

Configuring the Agents File

To enable public key client authentication, the MessageWay Service Interface (SI) uses the agents file to authenticate MessageWay servers that present themselves as clients to SI and to authenticate the users they represent.

Syntax for the Agents File

You must create the agents file in the location specified in the parameter, AgentFile, in the mwsi.conf file.

By default, a sample file called agents.sample is installed in the following locations, depending on the operating system:

Operating System	Location of the Agents Sample File
UNIX or Linux	/etc/messageway/certs/agents.sample
Windows	\Users*MessageWayUser*\AppData\Roaming\messageway\certs\agents.sample

The general rules for the agents file are as follows:

- Must list the AuthAgent value in the appropriate configuration file, such as mwas2.conf or mwsftpd.conf or mwftpd.conf if you are configuring anonymous user access
- Must list all groups and users allowed or denied connection for a given agent

The syntax rules for the agents file are as follows:

- Use Semi-colon (;) to comment a line
- Use separate lines for each AuthAgent and its users and groups list
  - AuthAgent must be first item on the line separated from list of users by at least one space or tab character
    - AuthAgent must match the common name (CN) used in the client certificate
    - Users and groups must be users or groups configured in MessageWay
  - Users and groups follow AuthAgent on the same line
    - Items in this list are separated by commas
    - Items may be in any order
    - Allowed or denied status of user overrides status of group
    - Allowed or denied status of group or user overrides asterisk (*)
    - Use an exclamation mark (!) to deny access to a user or group
    - Enclose group names in greater than (<) and less than (>) signs
    - Optionally use quotation marks (" ") around user names

The following table provides some examples for the user list:

User List Syntax	Description
!*user* - or - !"*user*"	Deny access to this user. This access overrides any access for a group to which the user belongs.

User List Syntax	Description
user - or - **"***user***"**	Allow access to this user. This access overrides any access for a group to which the user belongs.
!<*group***>**	Deny access to this group. Individual user access overrides group access.
<*group***>**	Allow access to this group. Individual user access overrides group access.
*	Allow all users. Individual user or group access overrides this access.

To Create or Modify the Agents File

The default location of the agents file and the agents.sample file is as follows:

Operating System	Location of the Agents Sample File
UNIX or Linux	/etc/messageway/certs/agents.sample
Windows	\Users\MessageWayUser\AppData\Roaming\messageway\certs\agents.sample

Other processes also use the agents file, so it may already exist. If it doesn't exist or you want to create a new one, start with step 1, otherwise go to step 2.

1 In Windows, using a text editor, create an empty file called **agents** (no extension) in the same location specified in the AgentFile parameter of the HTTP Listeners Configuration section in the MessageWay Service Interface configuration file, ***mwsi.conf*** (on page 145).

CAUTION: When you save the file, make sure there is no extension attached to the end.

2 On a new line in the agents file, type the following:

a) The case-sensitive name that matches the common name (CN) on the SFTP client certificate.

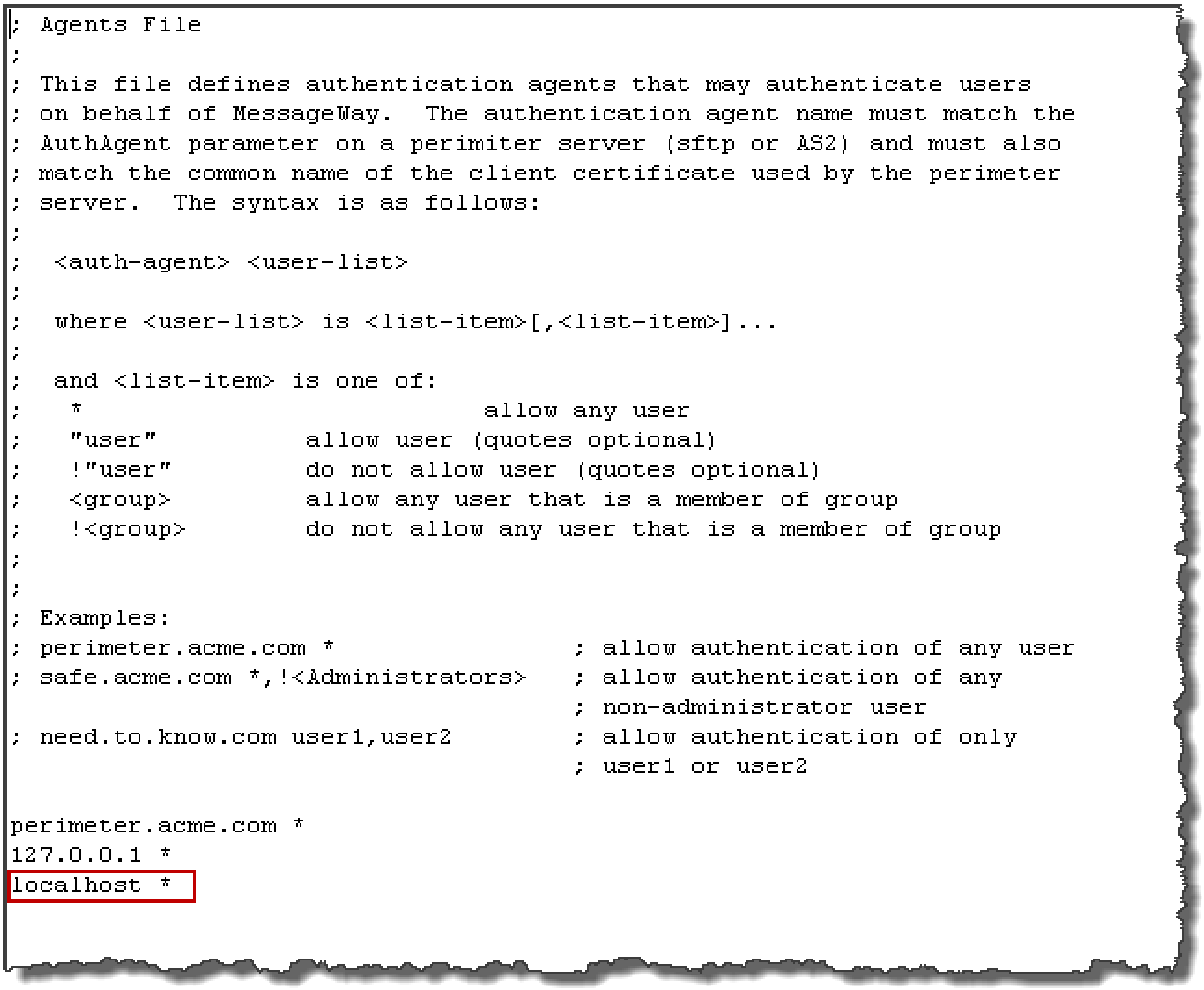
This name is also the AuthAgent value in the server configuration file.

b) At least one space or tab character.

c) MessageWay groups and users that will be allowed to send messages to MessageWay, with names separated by commas or an asterisk (*) for anyone.

Following our example, type:

localhost *



```
; Agents File
;
; This file defines authentication agents that may authenticate users
; on behalf of MessageWay.  The authentication agent name must match the
; AuthAgent parameter on a perimiter server (sftp or AS2) and must also
; match the common name of the client certificate used by the perimeter
; server.  The syntax is as follows:
;
;  <auth-agent> <user-list>
;
;  where <user-list> is <list-item>[,<list-item>]...
;
;  and <list-item> is one of:
;   *                           allow any user
;   "user"          allow user (quotes optional)
;   !"user"         do not allow user (quotes optional)
;   <group>         allow any user that is a member of group
;   !<group>        do not allow any user that is a member of group
;
;
; Examples:
; perimeter.acme.com *                 ; allow authentication of any user
; safe.acme.com *,!<Administrators>    ; allow authentication of any
                                       ; non-administrator user
; need.to.know.com user1,user2         ; allow authentication of only
                                       ; user1 or user2

perimeter.acme.com *
127.0.0.1 *
localhost *
```

NOTE: There may be other lines for agents and users in the file. Any MessageWay servers or interfaces that use public key authentication for input or that allow anonymous access to MessageWay must be listed as an agent.

Testing the SFTP Perimeter Server

To test the MessageWay SFTP Perimeter Server process from end to end, make sure you have completed the installation tasks, described in the topic, ***Basic Installation Tasks (SFTP Server)*** (on page 319).

When SFTP clients connect to the MessageWay SFTP Perimeter Server, they make a secure SSH connection to the SSH daemon. Then, the connection to MessageWay from the SFTP server may be configured as a secure connection. To review these connections, see the topic, ***Components and Processes of the SFTP Perimeter Server*** (on page 299).

NOTE: The SFTP server supports password and public key authentication. It does not support other types of authentication, including keyboard interactive.

The initial configuration is for a non-secure connection to MessageWay using password authentication. You can configure a secure connection to MessageWay.

- To configure a secure connection, refer to the topic, ***Configuring a Secure or Non-Secure Connection to SI*** (on page 342).
- To use public key authentication, which also requires a secure connection, refer to the topic, ***Configuring Public Key Authentication*** (on page 343).

To Start the SFTP Perimeter Server on UNIX or Linux

You start the MessageWay SFTP Perimeter Server with a startup script. The startup script, **mwsftpd**, has the options, **start**,**stop**,**restart** and **status**. Make sure you ***configure the server*** (on page 321) before you start it.

IMPORTANT: The script and the daemon process that the script starts and stops can be started only by the user, **root**. Check the system logs for errors if the server daemon process fails to start.

To start the SFTP server daemon, proceed as follows:

1. Log on as the user, **root**.

   NOTE: When running, MessageWay temporarily requires root access for the remote execution server, the SFTP proxy server and the FTP and SFTP perimeter servers. The FTP and SFTP perimeter servers require root access because they must listen on low ports (<1024), and both Linux and Solaris require root access to listen on low ports. Also, the SFTP perimeter server runs as root for the listener, but after a connection is accepted, it switches to the MessageWay user.

2. Go to the subdirectory where the script resides by typing:

   cd /etc/init.d

3. To start the server daemon process, type:

   ./mwsftpd start

   - or -

   To check the server status, type:

   ./mwsftpd status

   - or -

   To stop the server, type:

   ./mwsftpd stop

   - or -

   To restart the server, type:

   ./mwsftpd restart

NOTE: For Red Hat 7.x, MessageWay supports the systemctl utility, including automatically starting MessageWay when the application server is rebooted, and automatically starting MessageWay perimeter servers when the perimeter server is rebooted. The systemctl files are named *messageway.service*, *mwftpd.service*, *mwproxy.service*, *mwresd.service* and *mwsftpd.service*, and are located in **/usr/lib/systemd/system/**, with symbolic links being added in **/etc/systemd/system/multi-user.target.wants/**. See above systemctl files for more details.

IMPORTANT: For SUSE 10, 64-bit systems, if you use password authentication rather than public key authentication, you may need to enable password authentication in the SSH configuration file, typically /etc/sshd_config. If this is not enabled, and you attempt to use password authentication, you will get a 1113 error stating that the system has exhausted authentication methods.

To Start the SFTP Perimeter Server on Windows

From Windows, before you start the MessageWay SFTP Perimeter Server, you must first start Cygwin, which provides command-line access in a Linux type environment. If you have not yet installed Cygwin, refer to the topic, "To Install the SFTP Perimeter Server on Windows" *MessageWay Installation Guide*.

CAUTION: Before you proceed, make sure you do not have duplicate copies of cygwin1.dll installed on your server system. If you do, you will not be able to start syslogd or the SFTP server.

1 If you have not already done so, start the syslogd service as follows:

   From Windows Services, right-click **Cygwin syslogd**, and click **Start**.

   The status of the server should change to *Started*.

2 From Windows Services, right-click **MessageWay SFTP Server**, and click **Start**.

   The status of the server should change to *Started*.

Test the SFTP Connection

In this test, we will send and retrieve a message using the local address, localhost, and the MessageWay SFTP test port, 6222.

NOTE: This test connects the SFTP Server over a non-secure connection using password authentication. By default, SI authenticates users with a MessageWay user ID and password. To test a secure connection, refer to the topic, ***Configuring Secure or Non-Secure Connections to SI*** (on page 342). To have SI authenticate users with a public key, refer to the topic, ***Configuring Public Key Authentication*** (on page 343). Public key authentication requires a secure connection from the SFTP Server to SI.

If you have not already done so, start the following:

- MessageWay Manager (MessageWay Client)
- MessageWay Server (starts the Messaging Server, the Service Interface and the User Server)
- MessageWay SFTP Perimeter Server
- SFTP client

Once all processes are running, proceed as follows:

1 To start the SFTP client and connect to MessageWay:

- From a command line, type the following command:

  sftp -o Port=6222 remoteusertest@localhost

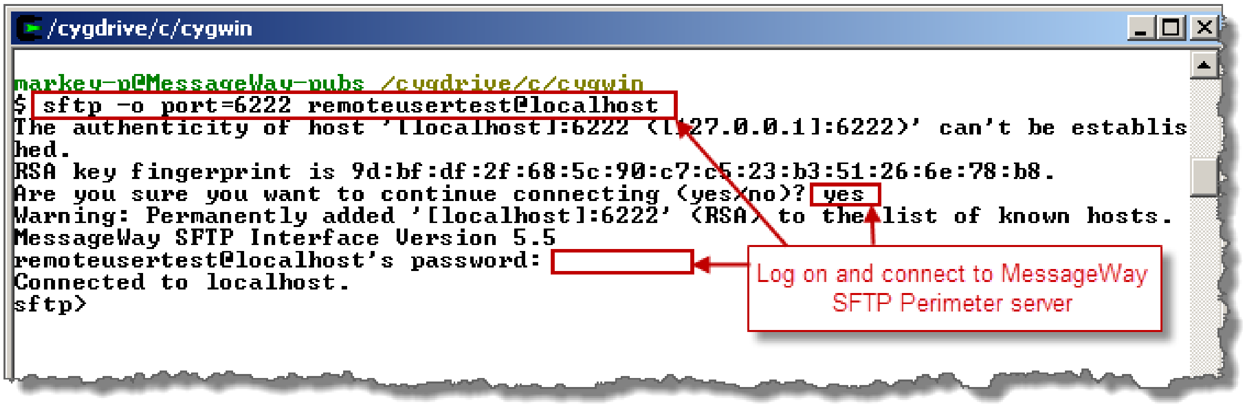
  - or -

- From a GUI SFTP client, such as WS_FTP Pro, enter the IP address, port and user ID in the connection information.

2 If you are using password authentication, which is the default, at the password prompt, type the password for the user ID, remoteusertest, which you should have created previously.

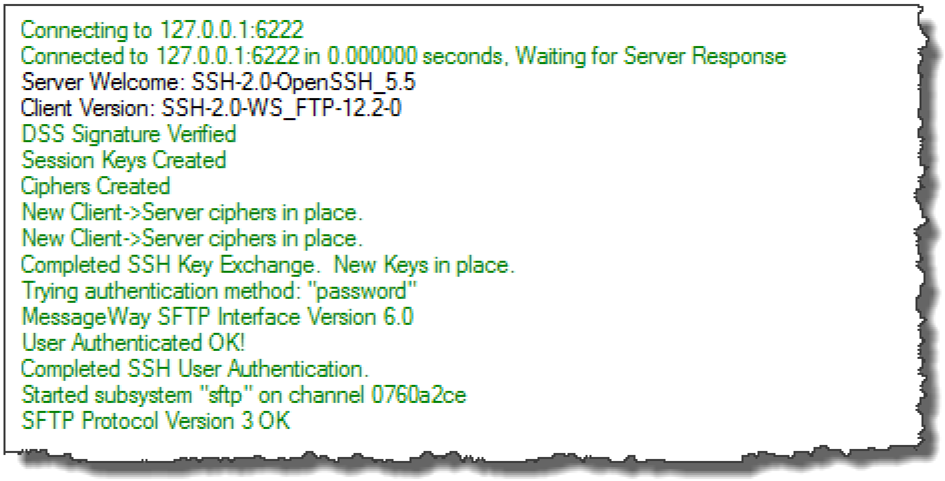
For instructions to add a user and mailbox for MessageWay, refer to the topic, ***Configuring MessageWay Users and Locations*** (on page 332). For instructions to specify the address and port for the server, refer to the topic, ***Configuring the SFTP Server Components*** (on page 320).

The client connects to your system using the localhost address, and points to the default mailbox for the user, TestPickup. The exchange looks something like one of these options, the first is from a command-line and the second is from WS_FTP Pro connection manager:



```
markey-p@MessageWay-pubs /cygdrive/c/cygwin
$ sftp -o port=6222 remoteusertest@localhost
The authenticity of host '[localhost]:6222 ([127.0.0.1]:6222)' can't be establis
hed.
RSA key fingerprint is 9d:bf:df:2f:68:5c:90:c7:c5:23:b3:51:26:6e:78:b8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:6222' (RSA) to the list of known hosts.
MessageWay SFTP Interface Version 5.5
remoteusertest@localhost's password:
Connected to localhost.
sftp>
```

Log on and connect to MessageWay SFTP Perimeter server



```
Connecting to 127.0.0.1:6222
Connected to 127.0.0.1:6222 in 0.000000 seconds, Waiting for Server Response
Server Welcome: SSH-2.0-OpenSSH_5.5
Client Version: SSH-2.0-WS_FTP-12.2-0
DSS Signature Verified
Session Keys Created
Ciphers Created
New Client->Server ciphers in place.
New Client->Server ciphers in place.
Completed SSH Key Exchange.  New Keys in place.
Trying authentication method: "password"
MessageWay SFTP Interface Version 6.0
User Authenticated OK!
Completed SSH User Authentication.
Started subsystem "sftp" on channel 0760a2ce
SFTP Protocol Version 3 OK
```

- or -

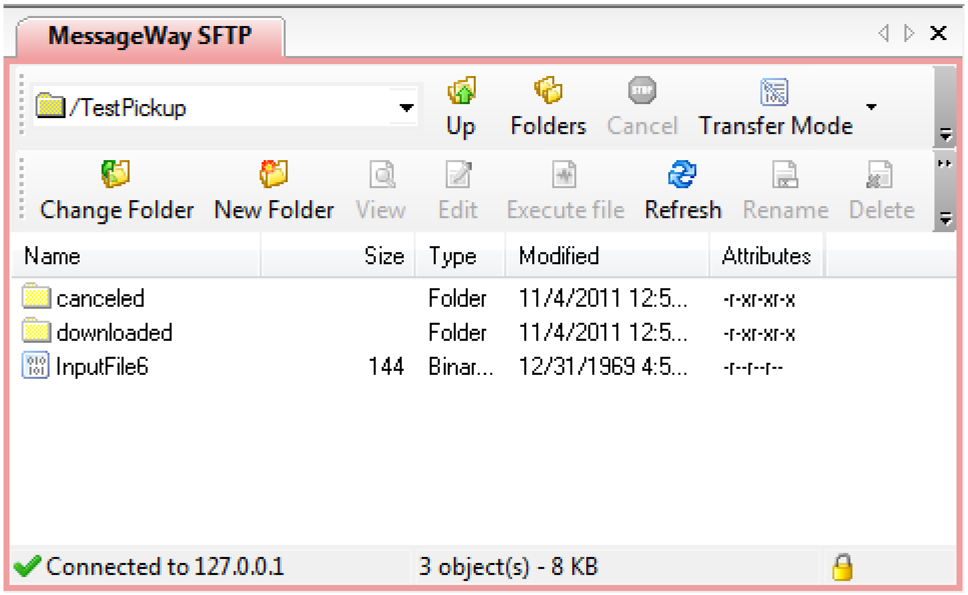
If you are using public key authentication, the password prompt does not appear.

3 From a command line, type **pwd** and then **ls -l**

- or -

From the GUI, view the working directory.

You should see your user's default mailbox, TestPickUp, something like this:



/TestPickup

Name	Size	Type	Modified	Attributes
canceled		Folder	11/4/2011 12:5...	-r-xr-xr-x
downloaded		Folder	11/4/2011 12:5...	-r-xr-xr-x
InputFile6	144	Binar...	12/31/1969 4:5...	-r--r--r--

✓ Connected to 127.0.0.1 3 object(s) - 8 KB

4 Identify a small file on your system and send it to the MessageWay mailbox, TestPickUp.

The user RemoteUserTest must have upload rights to the mailbox to which you are uploading the file, so for simplicity, we are uploading the file to the user's default mailbox, TestPickUp.

5 To view information about the message from the MessageWay Manager, in the MessageWay Explorer window:

a) In the left pane, select **Locations**.

b) In the right pane, right-click your mailbox, **TestPickUp**.

c) From the menu, select **Show Messages**.

d) Right-click on the most recent message.

e) From the menu, select **Properties**.

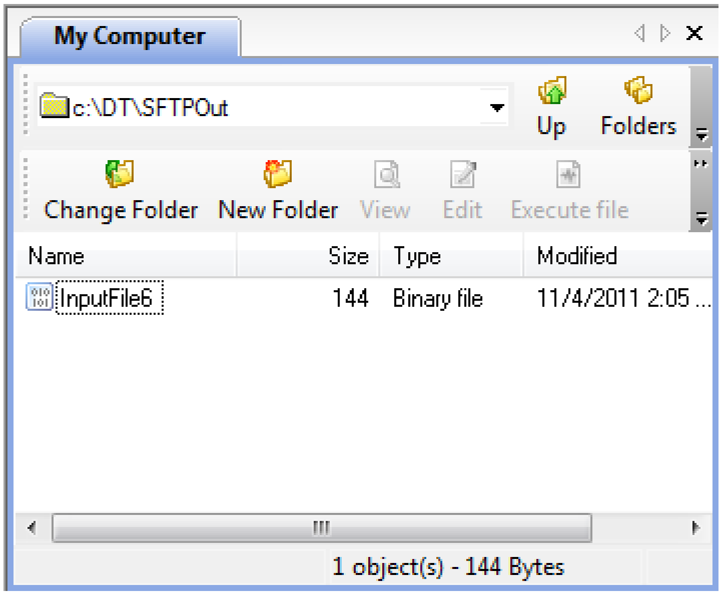
This message is now available for us to retrieve or download.

The connection may terminate while you check your message in MessageWay.

6 To reconnect to the SFTP Server and MessageWay from your SFTP Client, repeat step 1.

7 Retrieve your message from MessageWay.

You should see something like the following:



Name	Size	Type	Modified
InputFile6	144	Binary file	11/4/2011 2:05 ...

1 object(s) - 144 Bytes

Note that the file name is the result of the ***MessageNameFormat*** (on page 303) parameter we used on the ***mwsftpd.conf file*** (on page 322). In this case it is set to 3, which is filename, but it could be the message ID or a combination of message ID, filename or class ID.

Configuring the SFTP Proxy Server

The MessageWay SFTP Proxy Server provides secure access for the SFTP adapter from MessageWay to an external SFTP server for both input and output using Secure Shell 2 (SSH2). You install the SFTP proxy server separately. It is not part of the MessageWay SFTP Perimeter Server, which you install and configure separately. You can use the SFTP adapter with or without the proxy server.

This option uses the following components:

- MessageWay SFTP Adapter
- MessageWay SFTP Proxy Server

Licensing Requirements for the SFTP Proxy Server

The MessageWay SFTP Proxy Server is included as part of the license for the SFTP adapter and the SFTP perimeter server, although you install and configure them separately. For more information, contact MessageWay Technical Support.

Overview of the SFTP Proxy Server

Secure Shell (SSH) File Transfer Protocol (SFTP) is a way to move data securely from computer to computer. The SFTP adapter client accesses an SFTP server either using SFTP or SCP (UNIX/Linux only) protocol. For greater security, it may communicate with the external server via the MessageWay SFTP Proxy Server, which will establish the connection with the external server. Since SFTP does not provide security, it runs as a subsystem under SSH, which provides the authentication and security.

Components and Processes of the SFTP Adapter and Proxy Server

The main components of the SFTP adapter and proxy server system perform the following functions:

- The adapter makes a secure connection to either an SFTP server or the MessageWay proxy server, using either the SFTP or SCP protocol to download (input to MessageWay) or upload (output from MessageWay) data
- The proxy server, when used, establishes the connection to the SFTP server, and after a successful connection simply acts as a pass-through for all requests and data exchanged between the adapter client and the SFTP server

The following steps describe the typical process flow between the MessageWay SFTP Adapter client and the external SFTP server or the proxy server:

1. If using a proxy server:
   - At process initialization, the proxy server reads its configuration file, mwproxy.conf
   - Proxy server starts listening for incoming connections from the MessageWay SFTP Adapter.

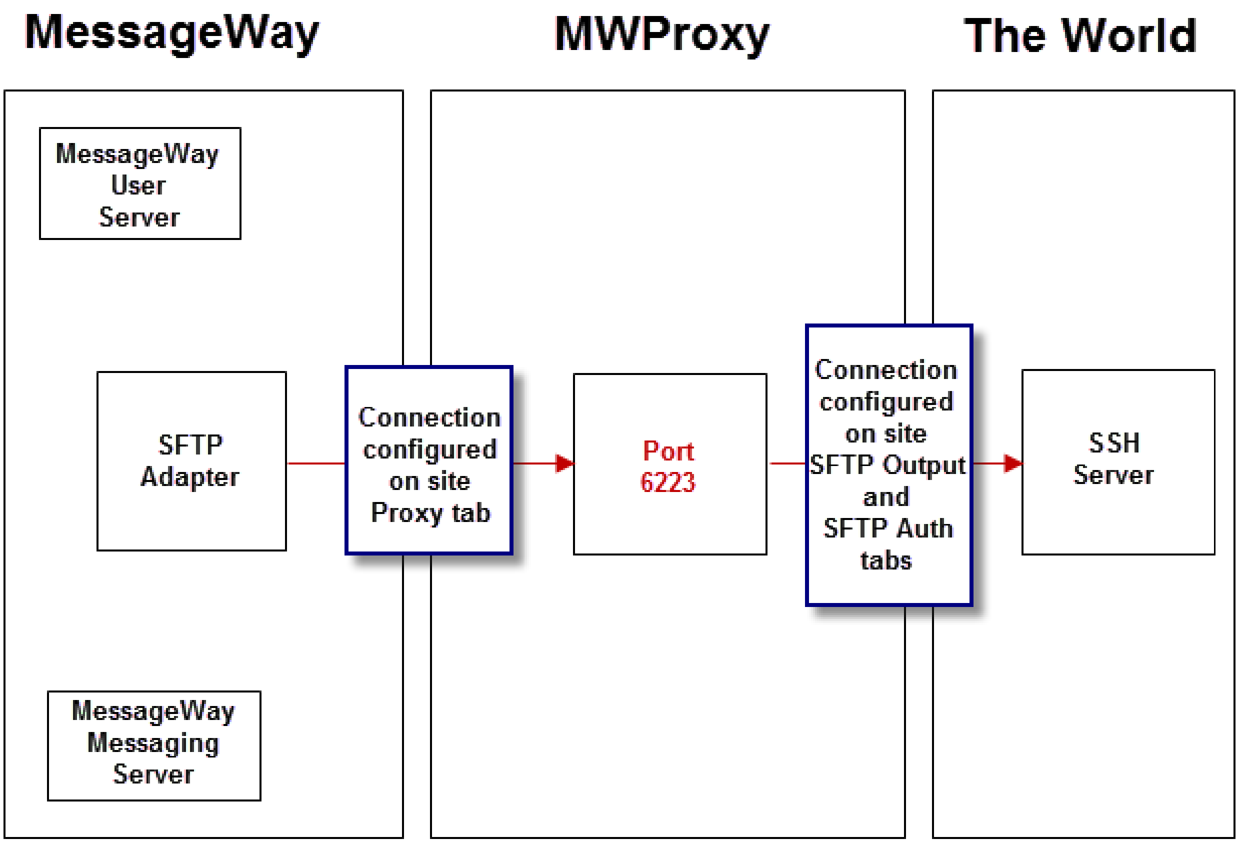
   NOTE: We suggest that you use TCP port 6223 for the proxy listening port.
2. SFTP adapter client issues connection request to an external SSH server or to the MessageWay proxy server
   - Default port to external server is 22
   - Default port to proxy server is 6223
3. SSH server processes connection request:

   If using proxy server:
   - Adapter and proxy server authenticate each other using the shared secret
   - Proxy processes connection request from adapter and establishes SSH connection with external server
   - Upon successful connection, proxy enters pass-through mode and passes traffic verbatim between the adapter and external server

   - or -

   If connecting directly to external server, adapter establishes SSH connection with external server
4. Once connected, adapter authenticates server using the server key fingerprint
5. Server authenticates adapter from the user ID and either a password or a public key exchange
6. Server uploads or downloads data using SFTP or SCP subsystem

The following diagram provides a high-level view of the communication process:


MessageWay
MWProxy
The World
MessageWay User Server
SFTP Adapter
Connection configured on site Proxy tab
Port 6223
Connection configured on site SFTP Output and SFTP Auth tabs
SSH Server
MessageWay Messaging Server

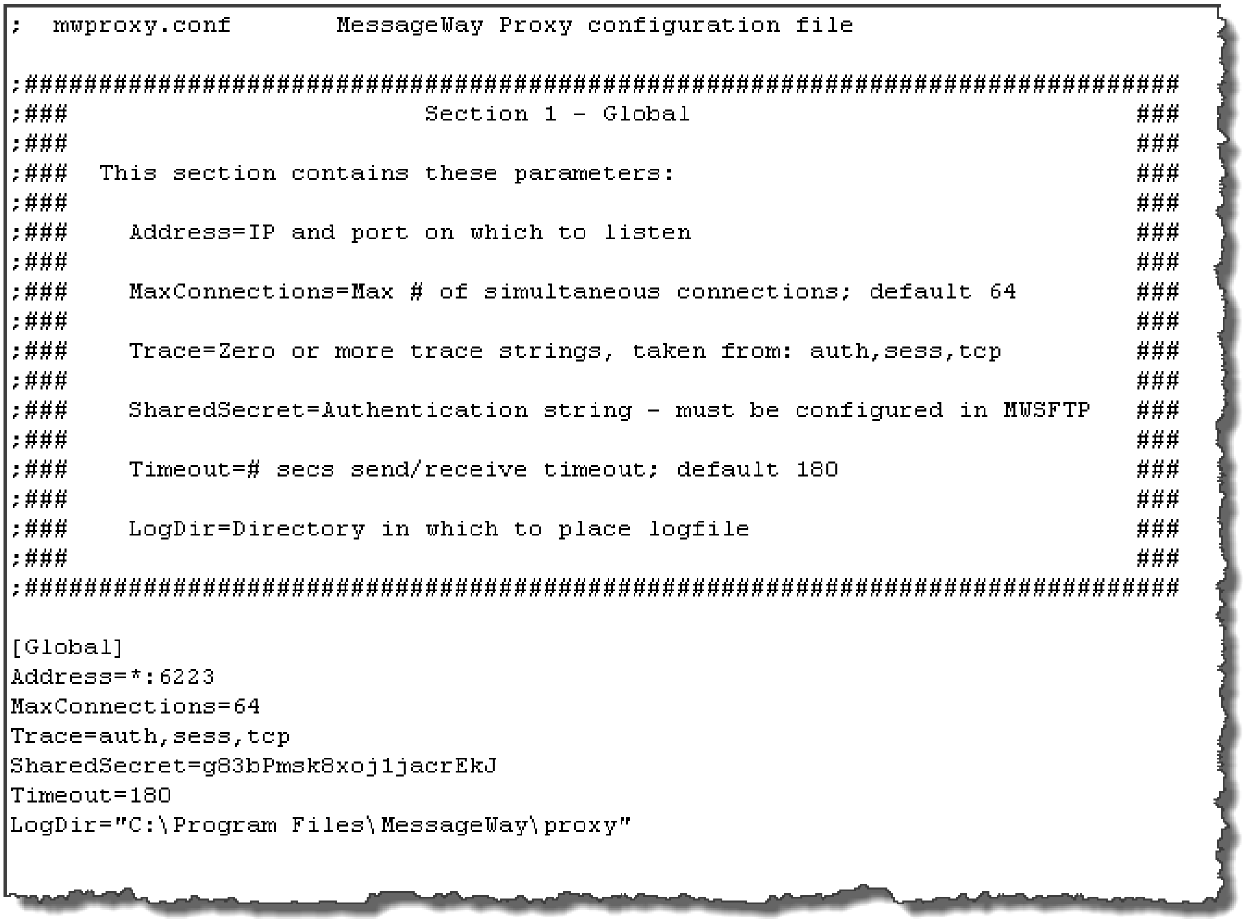
Configuring the SFTP Proxy Server Components

You set the parameters for the MessageWay SFTP Proxy Server in the configuration file, **mwproxy.conf**.

The following table shows the default location for the SFTP proxy server configuration file:

Operating System	Location of the SFTP Proxy Server Configuration File
UNIX or Linux	/etc/messageway/mwproxy.conf
Windows	\ProgramData\messageway\mwproxy.conf

TIP: When editing the configuration files, you can either use the UNIX/Linux editor, vi, from a command prompt or a text editor in Windows. You may need to convert the format from DOS to UNIX or UNIX to DOS, depending which system you choose. Programs to do this, dos2unix and unix2dos, are typically available free of charge from the Internet, if you don't already have them.



```
;  mwproxy.conf       MessageWay Proxy configuration file

;###############################################################################
;###                        Section 1 - Global                               ###
;###                                                                         ###
;###  This section contains these parameters:                                ###
;###                                                                         ###
;###    Address=IP and port on which to listen                               ###
;###                                                                         ###
;###    MaxConnections=Max # of simultaneous connections; default 64         ###
;###                                                                         ###
;###    Trace=Zero or more trace strings, taken from: auth,sess,tcp          ###
;###                                                                         ###
;###    SharedSecret=Authentication string - must be configured in MWSFTP    ###
;###                                                                         ###
;###    Timeout=# secs send/receive timeout; default 180                     ###
;###                                                                         ###
;###    LogDir=Directory in which to place logfile                           ###
;###                                                                         ###
;###############################################################################

[Global]
Address=*:6223
MaxConnections=64
Trace=auth,sess,tcp
SharedSecret=g83bPmsk8xoj1jacrEkJ
Timeout=180
LogDir="C:\Program Files\MessageWay\proxy"
```

The following table describes the purpose of each parameter for the proxy server.

Parameter	**Description**
Address	The IP address and port number where the proxy server should listen for client requests. Replace the IP address with an asterisk, *****, to listen on any IP address. We recommend that you use port **6223**.
MaxConnections	Maximum number of simultaneous connections. Default value is 64.
Trace	Optional parameter to trace the activity between the SFTP proxy server and the external SFTP server. Leave this blank to *not* log activity. To log activity, use any combination of the following values, separated by a comma when you use more than one: ▪ **auth** Log authentication details, but not shared secret ▪ **sess** Log accept, connect, disconnect and session statistics ▪ **tcp** Log all input and output bytes (very verbose)

Parameter	Description
SharedSecret	Arbitrary text string which must be configured identically for this proxy server and the SFTP adapter.
Timeout	Timeout of the TCP connection in seconds. Default value is 180.
LogDir	Name of the directory to which the trace file will be written. The environment variable, MWPROXY_LOGDIR, if it exists, overrides LogDir. The file name is the name of the server, typically MWPROXY, followed by *.log*.

Testing the SFTP Adapter and Proxy Server

To test the MessageWay SFTP Adapter and the MessageWay SFTP Proxy Server process from end to end, make sure you have completed the installation tasks described in the MessageWay Installation Guide.

If you have not already done so, start the following:

- MessageWay Manager (MessageWay Client)
- MessageWay Server (starts the Messaging Server, the Service Interface and the User Server)
- MessageWay SFTP Adapter

To Start the SFTP Proxy Server on UNIX or Linux

You start the SFTP Proxy Server with a startup script. The startup script, **mwproxy**, has the options, **start**,**stop**,**restart** and **status**. Make sure you ***configure the server*** (on page 366) before you start it.

IMPORTANT: The script and the proxy server process that the script starts and stops can be started only by the user, **root**. Check the system logs for errors if the server daemon process fails to start.

To start the SFTP Proxy Server, proceed as follows:

1 Log on as the user, **root**.

NOTE: When running, MessageWay temporarily requires root access for the remote execution server, the SFTP proxy server and the FTP and SFTP perimeter servers. The FTP and SFTP perimeter servers require root access because they must listen on low ports (<1024), and both Linux and Solaris require root access to listen on low ports. Also, the SFTP perimeter server runs as root for the listener, but after a connection is accepted, it switches to the MessageWay user.

2 Go to the subdirectory where the script resides by typing:

cd /etc/init.d

3 To start the server process, type:

./mwproxy start

- or -

To check the server status, type:

./mwproxy status

- or -

To stop the server, type:

./mwproxy stop

- or -

To restart the server, type:

./mwproxy restart

To Start the SFTP Proxy Server on Windows

To start the SFTP proxy server on Windows, proceed as follows:

1 From the **Start** menu, select **Programs|Administrative Tools|Computer Management**.

The Computer Manager window appears.

2 In the left pane, expand the folder **Services and Applications**, and click **Services**.

The Services window appears.

3 In the right pane, scroll to the service, **MessageWay SFTP Proxy Server**.

4 Right-click **MessageWay SFTP Proxy Server**, and select **Start** from the menu.

The Status column should display **Started**.

Test Uploading a Message to MessageWay Directly from the SFTP Server

To test the connection between the SFTP adapter client and an external SFTP server.

1 Make sure the external server is running and listening on the expected port, by default 22.

2 From the MessageWay Manager, start the SFTP adapter.

3 ***Configure an SFTP input location*** (on page 648) such as SFTPIn to *not* use the SFTP proxy server.

4 Place a test file in the external directory you identified in the URL field of the input location configuration, for example SFTPIn.

5 Right-click the input location, such as SFTPIn, and from the menu, select **Input Now**.

6 ***Find your input message*** (on page 735). One easy method is to find the location to which the message is to be delivered, for example AdminTest, right-click on that location and select **Show Messages**.

Test Uploading a Message Through the SFTP Proxy Server to an SFTP Server

To test the connection between the MessageWay SFTP Adapter through the SFTP Proxy Server to an external SFTP Server, proceed as follows:

1 Make sure the external SFTP server is running and listening on the expected port, by default 22.

2 Start the SFTP proxy server.

3 From the MessageWay Manager, start the SFTP adapter.

4 ***Configure an SFTP output location*** (on page 649) such as SFTPOut to ***use the SFTP proxy server*** (on page 650).

5 Find a test message in MessageWay and redirect it to your output location SFTPOut.

6 ***Find your output message*** (on page 735). One easy method is to find the location to which the message is to be delivered, SFTPOut, right-click on that location and select **Show Messages**.

Configuring Users and User and Object Security

User and object security controls access to MessageWay configurations and functions using:

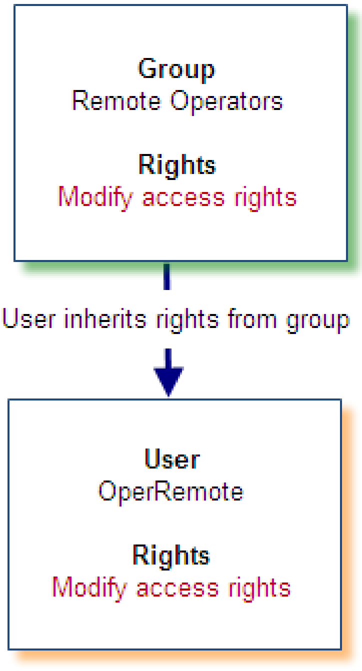
- General policies that are applied to all users control system access
- Configurations for individual users and user groups control what functions users are allowed to perform
- Configurations for folders and configurations for objects within the folders control which users have access to the configurations and what functions they may perform for the object

Overview of User and Object Security

MessageWay is installed with a single user, Administrator, with which you configure the rest of the system, including other users. The Administrator is the only user that has global rights and permissions that override all other configurations. Other users are controlled by user security configurations.

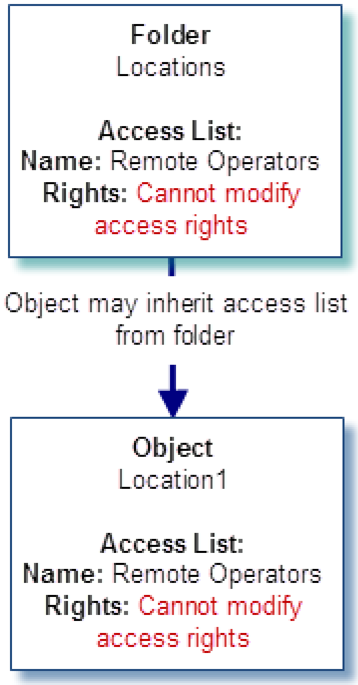
Once a user successfully logs on to MessageWay, the actions they perform are controlled by user security configurations. Object configurations specify which users can perform which actions for that object. User configurations specify what actions users can perform in general. The intersection of configurations for objects and users determines what tasks a user can perform on which objects at runtime.

Consider the configurations for users. To simplify applying security configurations, users may belong to groups. Security is applied to the group, and new users that are assigned to that group automatically inherit the rights of the group. This avoids having to assign the same rights to multiple users. These inherited rights may be overridden for a specific user. The following diagram shows a remote operator, OperRemote, that belongs to the user group, Remote Operators. There are many rights that this user inherits from the group, but the important one here is that OperRemote can modify access rights.



Security for Users Who Inherit Rights from Groups

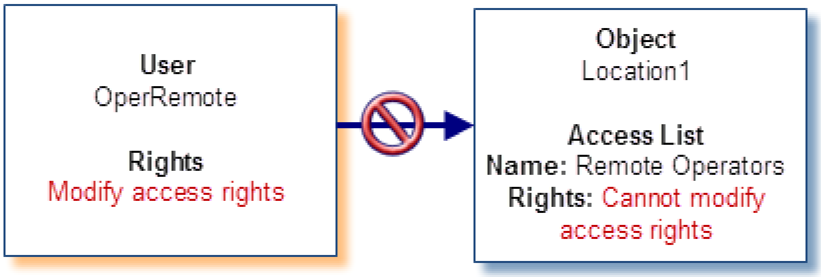
Objects, such as locations, have access lists, which they may inherit from their folders. An access list is a valid user or user group and specific rights assigned to it for this object. A user cannot access an object unless the user is on the access list or belongs to a group that is on the list. In the following diagram, the access list for the group Remote Operators is inherited from its folder, Locations. Here the group, Remote Operators, does not have the right to modify access rights for this folder or any of its contents.


Folder
Locations
Access List:
Name: Remote Operators
Rights: Cannot modify access rights
Object may inherit access list from folder
Object
Location1
Access List:
Name: Remote Operators
Rights: Cannot modify access rights

Security for Objects That Inherit Access Lists from Folders

Notice that the rights for objects are configured separately from the rights for users. Here, the effective rights for the user, OperRemote, includes *Modify Access Rights* while the effective rights for the object Location1 for the Group Remote Users, and thus OperRemote, includes *Cannot Modify Access Rights*. When a user attempts to perform an action on an object, the right to perform that action must be allowed for both the user and the object. Now when OperRemote attempts to change access rights for Location1, he will not be able to do so. As a user, OperRemote has the right to modify access rights in general, but the object Location1 does not give OperRemote the right.

IMPORTANT: Users may perform actions only when the rights for the user and the rights on the access list for the object are the same.



Common Rights for User and Object Required to Perform Tasks

This page intentionally blank.

Configuring User Security

This section describes how to control user access to MessageWay.

Configuring Policies for All Users

User security controls access to MessageWay configurations and functions. General security policies can be set for all users on the **User Policies** page of the User Folder Properties window.

IMPORTANT: You must restart MessageWay for changes to User Policies to take effect.

To configure policies for all users:

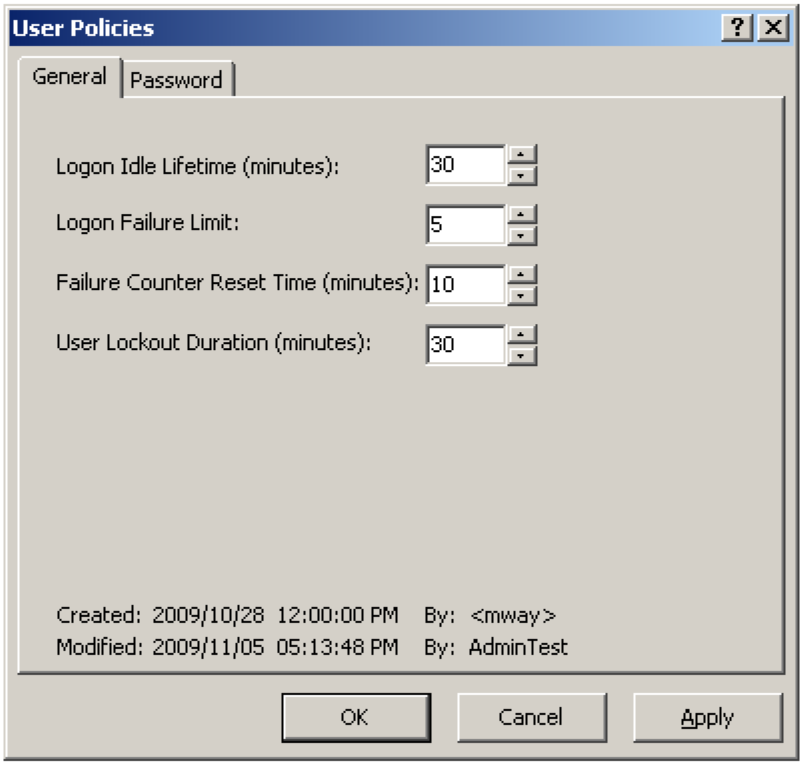
1 From the menu bar, select **File** and then **User Policies...**

- or -

From the task bar, click the Edit User Policies button, .

The User Policies window appears.

2 To change properties for logon idle lifetime and settings for brute force attacks, click the **General** tab.



Logon Idle Lifetime (minutes): 30

Logon Failure Limit: 5

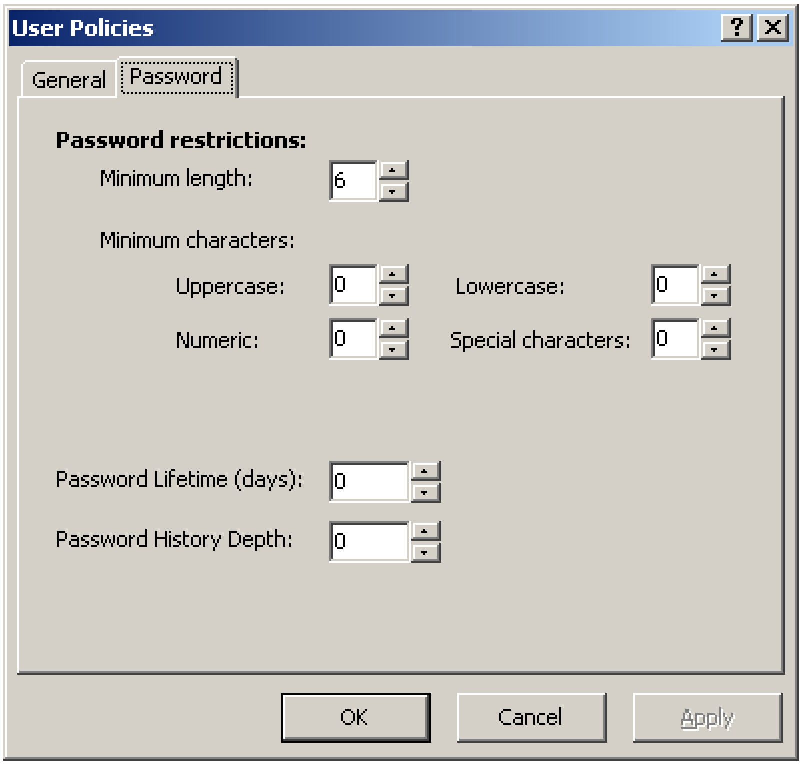
Failure Counter Reset Time (minutes): 10

User Lockout Duration (minutes): 30

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/05 05:13:48 PM By: AdminTest

3 To change properties for passwords, click the **Password** tab.



Password restrictions:

Minimum length: 6

Minimum characters:

Uppercase: 0 Lowercase: 0

Numeric: 0 Special characters: 0

Password Lifetime (days): 0

Password History Depth: 0

MessageWay enforces password policies when a user logs on or creates or modifies a password. The lockout policies are to mitigate a brute force attack from unknown sources trying to gain access to MessageWay. For more information about these fields, refer to the topic, ***User Policies Window*** (on page 1347) in the reference section.

Configuring User Groups

User groups allow you to configure a master set of rights for users. When you add a user to a group, the user inherits the rights of the group, which are then listed as the effective rights of the user. When you organize users and their group in folders, you can reduce the configuration tasks, because those users are automatically added to the group. For more information about this feature, refer to the topic, ***How to Create Folders for Users and User Groups*** (on page 389).

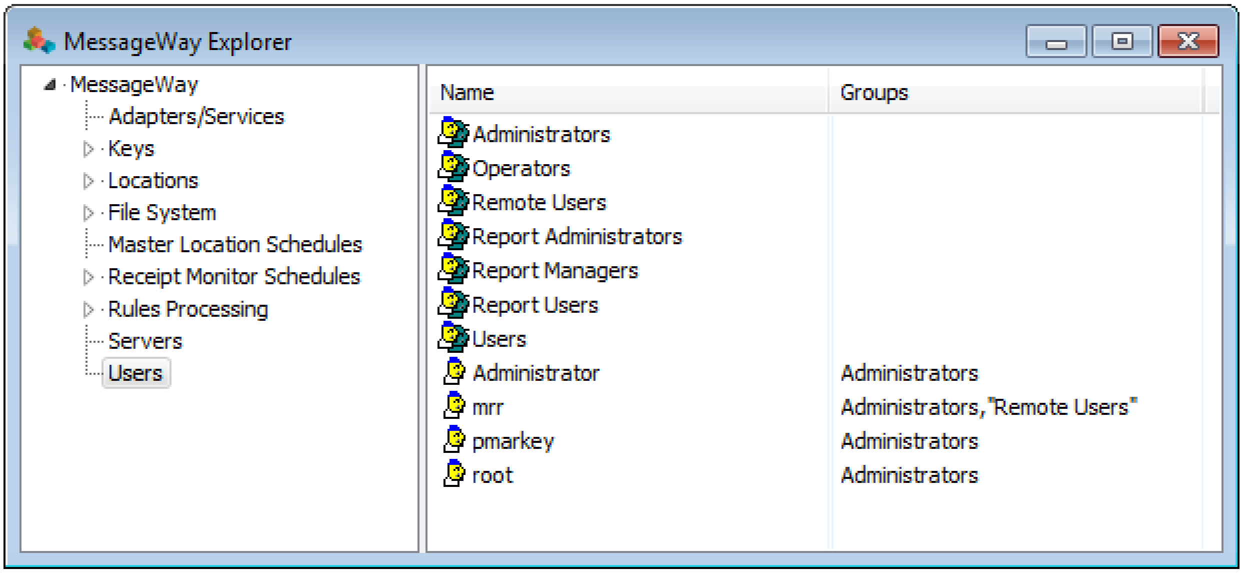
You access user groups from the right pane of MessageWay Explorer. Select a user group, and then click the **Properties** button on the task bar.

The icons distinguish between single users and groups, as follows:

Icon	Description
👤	Security properties for a single user
👥	Security properties for a group of users

When installed, MessageWay includes four pre-configured user groups:

- Administrators
- Operators
- Remote Users
- Users

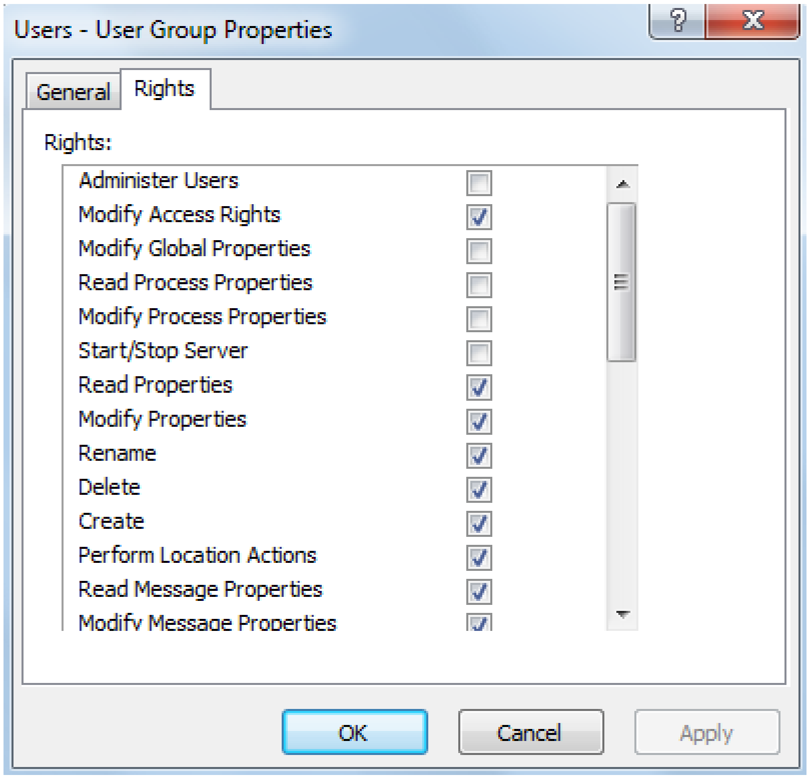


Name	Groups
Administrators	
Operators	
Remote Users	
Report Administrators	
Report Managers	
Report Users	
Users	
Administrator	Administrators
mrr	Administrators,"Remote Users"
pmarkey	Administrators
root	Administrators

You configure user groups on the **User Groups Properties** page. To create a user group, refer to the topic, ***How to Create User Groups*** (on page 378). To set the rights for a user group, you check or uncheck the boxes for the rights you think members of this group should have. These rights are preset for the pre-configured user groups, which you may modify to suit your needs. For more information about the rights for user groups, refer to the reference topic, ***Rights Page (User Group Properties)*** (on page 1338).

The boxes checked here will display in the Effective column on the **Rights** page of the User Properties window for each member of the group.When a user belongs to more than one group, the Effective column shows the combined rights granted by those groups.

IMPORTANT: Changes made to user or user group properties will take effect when the user logs on in a subsequent session.



Rights:

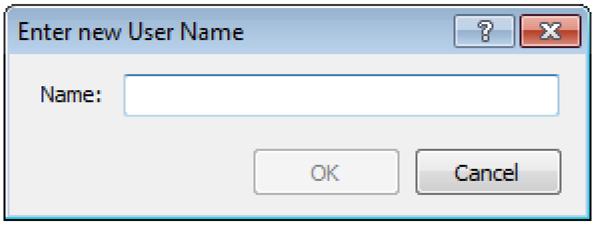
- Administer Users ☐
- Modify Access Rights ☑
- Modify Global Properties ☐
- Read Process Properties ☐
- Modify Process Properties ☐
- Start/Stop Server ☐
- Read Properties ☑
- Modify Properties ☑
- Rename ☑
- Delete ☑
- Create ☑
- Perform Location Actions ☑
- Read Message Properties ☑
- Modify Message Properties ☑

How to Create User Groups

1 From the left pane of MessageWay Explorer, select **Users** or some other sub-folder you have created.

2 On the right pane, right-click, and from the menu, select **Add User Group**.

The **Enter New User Group Name** dialog box appears.



3 Type a name for your user group, and select **OK**.

The User Group Properties window appears. For more information about this window, refer to the topic, ***User Group Properties Window*** (on page 1335).

4 On the **General** page:

- Type a description
- Optionally, assign ***access classes*** (on page 1337)

5 On the **Rights** page, left-click to check the tasks you want members of this group to perform. To check or clear all permissions at once, hold the **SHIFT** key and right-click one of the boxes.

6 Select **Apply** or **OK** to complete the process or **Cancel** to exit.

How to Add Users to a Group

1. Access the User Properties window for your user.
2. On the **Groups** tab, click **Add**.

   The **Select User Group** dialog box appears.
3. Select the user group you want to add from the list.
4. To complete the process, choose the **Select** button.

   The **Groups** tab appears with the added group.
5. To add more groups, repeat steps 2-4.
6. Click **Apply** or **OK** to complete the process.

Configuring Individual Users

The rights for a user determine which actions this user may perform. When the user attempts to perform an action, these rights together with the rights the user has for the object determine whether the request will be allowed or denied.

When users belong to one or more groups, they inherit the rights of the group or groups. These inherited, combined rights are the effective rights of the user. You may override inherited rights on the user configuration, which changes the effective rights.

You access user configurations from the right pane of MessageWay Explorer. Select a user, and then click the **Properties** button on the task bar.

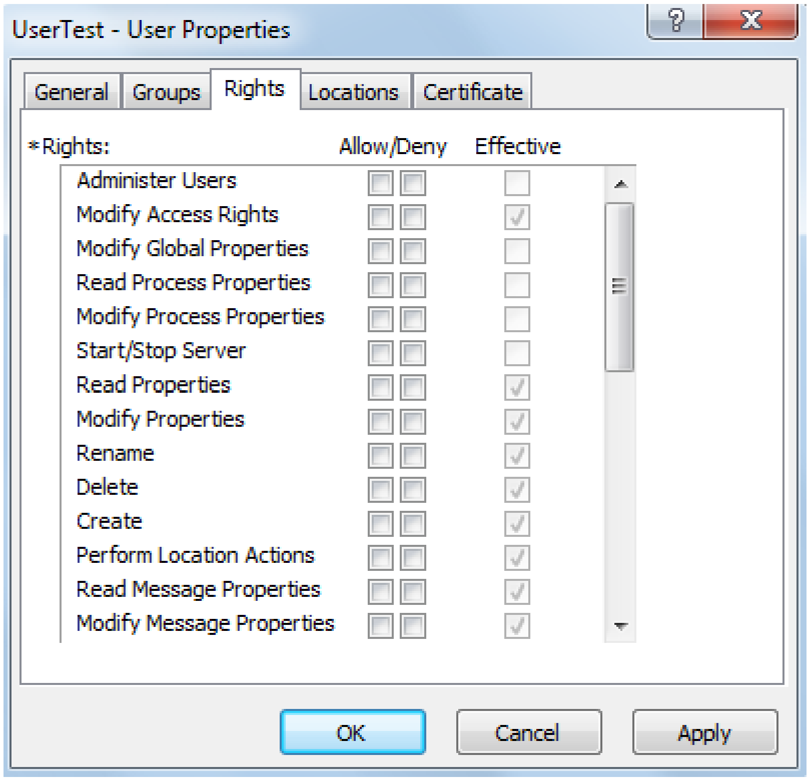
The icons distinguish between single users and groups, as follows:

Icon	Description
👤	Security properties for a single user
👥	Security properties for a group of users

When installed, MessageWay includes one pre-configured user, Administrator. You use Administrator to set your initial configurations. One of your first tasks should be to add a functional administrator, that you use to perform administrative tasks henceforth.

You configure users on the User Properties window. To create a user, refer to the topic, ***How to Create Users*** (on page 381). Remember that when the user belongs to one or more groups, the **Effective** column reflects the combined rights of the groups. For more information about what the specific rights mean, refer to the reference topic, ***Rights Page (User Properties)*** (on page 1358).

In the following example, UserTest has inherited rights from the group, Users, as shown in the Effective column.



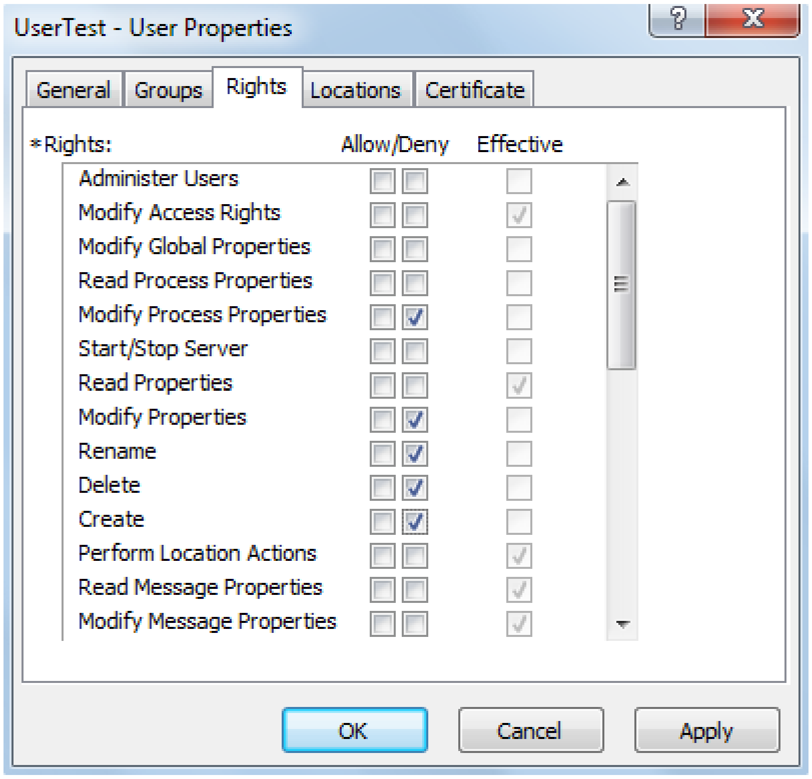
*Rights:	Allow/Deny		Effective
Administer Users	□	□	□
Modify Access Rights	□	□	☑
Modify Global Properties	□	□	□
Read Process Properties	□	□	□
Modify Process Properties	□	□	□
Start/Stop Server	□	□	□
Read Properties	□	□	☑
Modify Properties	□	□	☑
Rename	□	□	☑
Delete	□	□	☑
Create	□	□	☑
Perform Location Actions	□	□	☑
Read Message Properties	□	□	☑
Modify Message Properties	□	□	☑

Rights Inherited by the User Called UserTest (User Properties Window)

To set the rights for a user or override rights inherited from groups, you check or clear the boxes for the rights you think the user should have.

IMPORTANT: Changes made to user or user group properties will take effect when the user logs on in a subsequent session.

In the following example, we have removed the permissions, Modify Properties, Rename, Delete and Create, which affect folders, locations, rules processing profiles and other definitions associated with the ***MessageWay options*** (on page 893).



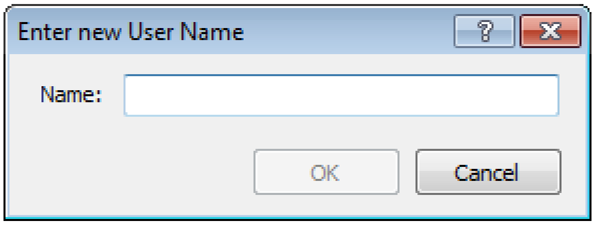
*Rights:	Allow/Deny		Effective
Administer Users	□	□	□
Modify Access Rights	□	□	☑
Modify Global Properties	□	□	□
Read Process Properties	□	□	□
Modify Process Properties	□	☑	□
Start/Stop Server	□	□	□
Read Properties	□	□	☑
Modify Properties	□	☑	□
Rename	□	☑	□
Delete	□	☑	□
Create	□	☑	□
Perform Location Actions	□	□	☑
Read Message Properties	□	□	☑
Modify Message Properties	□	□	☑

Override Inherited Rights for the User Called UserTest (User Properties Window)

How to Create Users

1. From the left pane of MessageWay Explorer, select **Users** or some other sub-folder you have created.
2. On the right pane, right-click, and from the menu select **Add User**.

   The **Enter New User Name** dialog box appears.

   Name:

3. Enter a name for your user, and select **OK**.

   The User Properties window appears. For more information about this window, refer to the topic, ***User Properties Window*** (on page 1351).

4. On the **General** tab, enter the following:
   - A brief description to identify this user.
   - In the **Password** field, a password with the minimum number of characters specified on the ***User Policies window*** (on page 1347).
5. On the **Groups** tab, perform these optional tasks:

- Select groups to which the user belongs. For instructions, refer to the topic, ***How to Add Users to a Group*** (on page 379).
- Check the box, **Override security group access classes**, to change or remove any access classes inherited from user groups.

6 On the **Rights** tab, change the permissions for the user as required.

For specific instructions, refer to the topic, ***How to Modify Rights for a User*** (on page 386).

7 Select **Apply** or **OK** to complete the process.

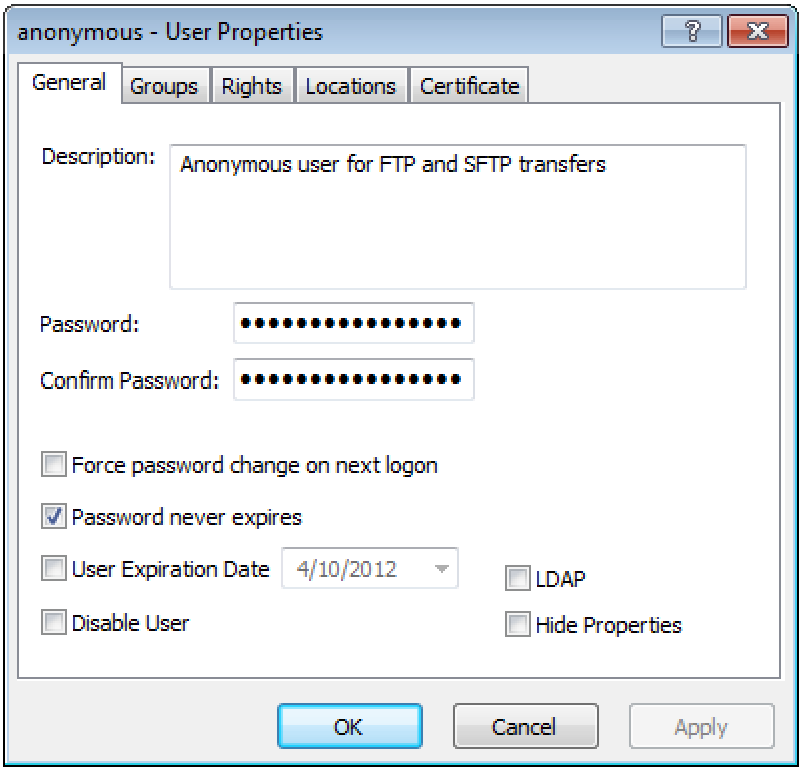
To Define an Anonymous MessageWay FTP or SFTP User

To configure an anonymous user who will access MessageWay from an FTP or SFTP client, proceed as follows:

1 Add a user called **anonymous**.

2 On the **General** page, type a description, a password and choose your password expiration policy.

NOTE: You must enter a password, but it is ignored during an FTP session.



Description: Anonymous user for FTP and SFTP transfers

Password: ••••••••••••••••

Confirm Password: ••••••••••••••••

□ Force password change on next logon

☑ Password never expires

□ User Expiration Date 4/10/2012

□ LDAP

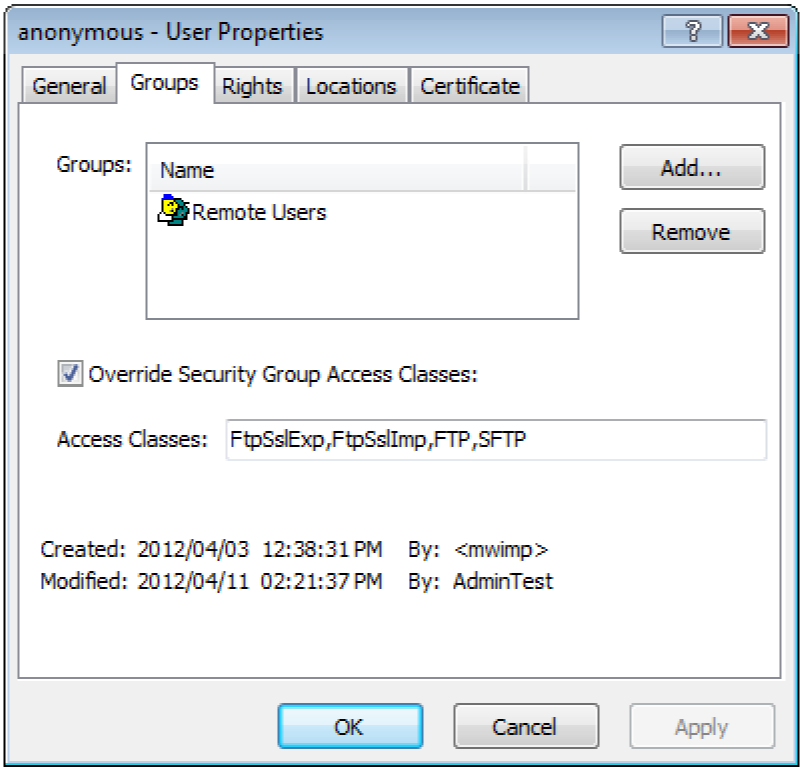
□ Disable User

□ Hide Properties

3 On the **Groups** page, add this user to the *Remote Users* group.

4 Check the Override Security Group Access Classes, and type the access class or classes that you support, separated by commas. They must match *exactly* what you have specified on the FTP server configuration file, mwftpd.conf or on the SFTP server configurations file, mwsftpd.conf.

CAUTION: Access class names are *case-sensitive*.



Groups:

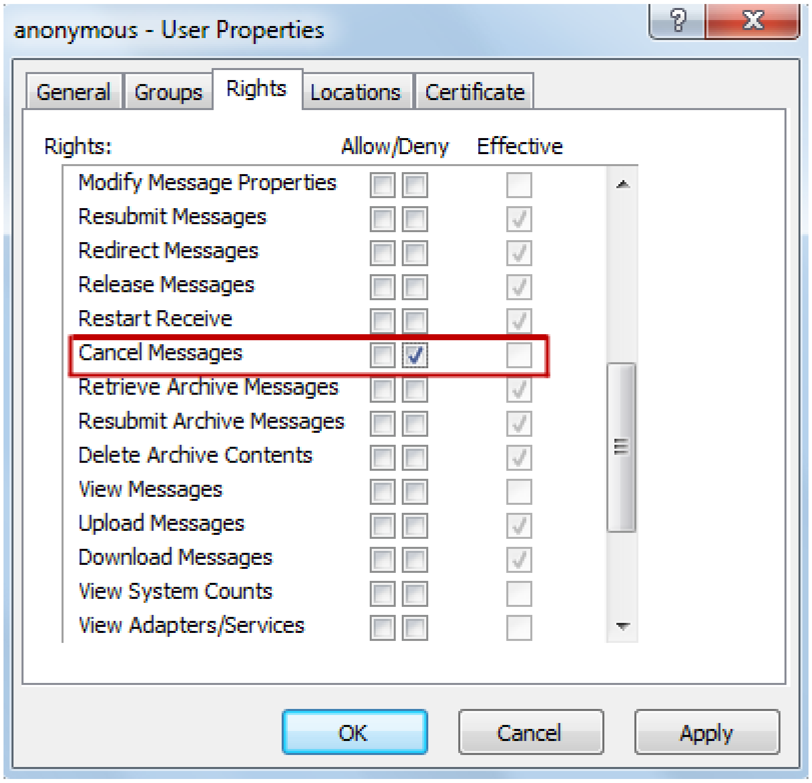
Name
Remote Users

☑ Override Security Group Access Classes:

Access Classes: FtpSslExp,FtpSslImp,FTP,SFTP

Created: 2012/04/03 12:38:31 PM By: <mwimp>
Modified: 2012/04/11 02:21:37 PM By: AdminTest

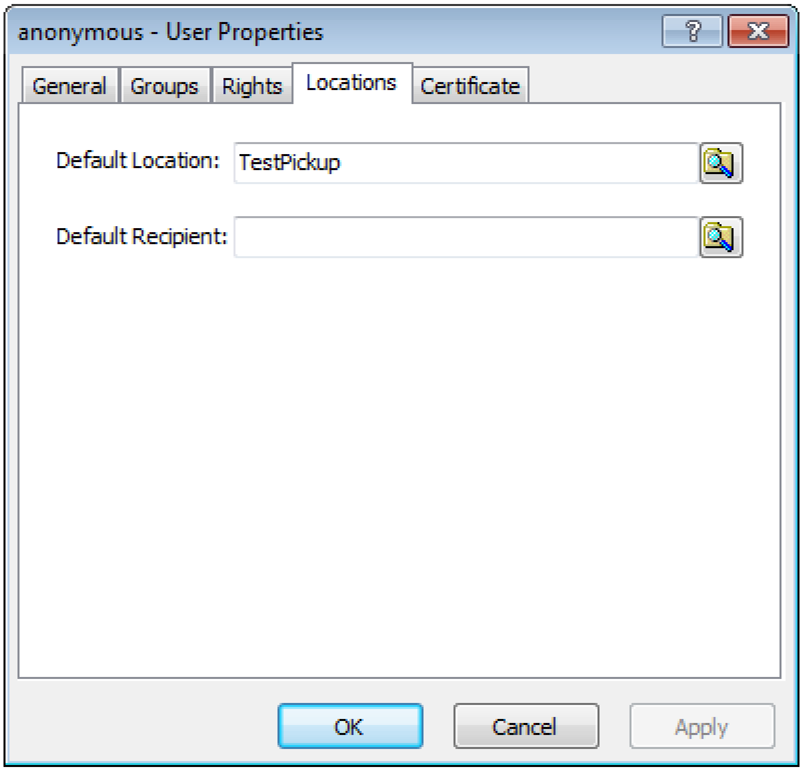
5 On the **Rights** page, appropriate rights will be inherited from the group *Remote Users*. You do not need to change anything, ***unless you have configured the group to be able to cancel messages*** (on page 241). If you do not want to give this privilege to anonymous users, you need to deny, **Cancel Messages**.



Rights:	Allow/Deny		Effective
Modify Message Properties	□	□	□
Resubmit Messages	□	□	☑
Redirect Messages	□	□	☑
Release Messages	□	□	☑
Restart Receive	□	□	☑
Cancel Messages	□	☑	□
Retrieve Archive Messages	□	□	☑
Resubmit Archive Messages	□	□	☑
Delete Archive Contents	□	□	☑
View Messages	□	□	□
Upload Messages	□	□	☑
Download Messages	□	□	☑
View System Counts	□	□	□
View Adapters/Services	□	□	□

6 On the **Locations** page, select a ***pickup mailbox*** (on page 237) for the default location and select an optional ***default recipient location*** (on page 236). The default recipient location is useful if all anonymous users will be sending files to a specific location, such as for translation, and they don't want to always specify the location in their PUT commands. Make sure you select or type the appropriate default location depending on whether it is in the Locations folder or the File System folder. For a description of the differences, refer to the topic ***Overview of Location Properties*** (on page 453).

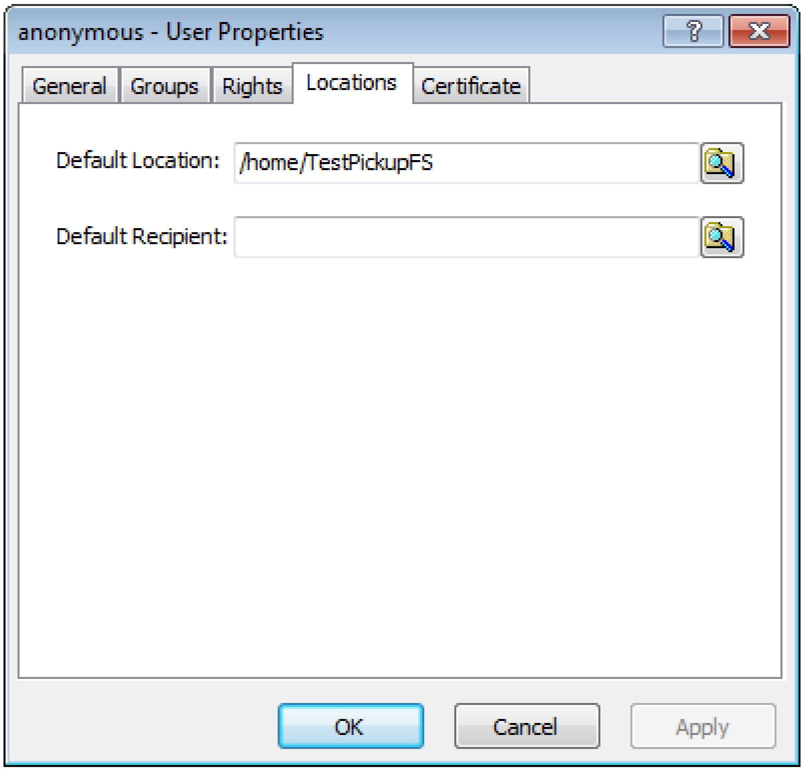
The following default location is in the Locations folder.



Default Location: TestPickup

Default Recipient:

This location is in the File System folder.



Default Location: /home/TestPickupFS

Default Recipient:

7 Click **OK**.

How to Control Logon to the MessageWay Manager

Administrators can control how users gain access to the MessageWay Manager at logon by:

- Forcing password changes
- Disabling the user, which denies access without deleting the configuration
- Unlocking users that have been locked out

To Force a User to Change a Password

NOTE: If an Administrator sets the **Force password change on next logon** option in User Properties, when the user next logs on using the MessageWay Manager, they will be prompted to change password. However, if the user logs onto via an MWFTPD perimeter server, the user will not see the change password prompt, but instead will see a "logon failed" message. In this case, an Administrator will need to reset the password or turn off the *force password change* option.

1 Open the User Properties window for the chosen user.

2 On the General tab, check the box **Force password change on next logon**.

- or -

Check the box **User Expiration Date**, and specify the date at which the password expires.

To Deny Access to a User

To deny access to a user without deleting the configuration, proceed as follows:

1 Open the User Properties window for the chosen user.

2 On the **General** tab, check the box, **Disable User**.

To Allow Access to a Locked-out User

To allow a user access that has been locked out, proceed as follows:

1 Open the User Properties window for the chosen user.

2 On the **General** tab, click the button **Unlock User**.

How to Modify Rights for a User

You can override the rights it has inherited from the groups to which it belongs, if any. To modify rights for a user, proceed as follows:

1 Access the appropriate User Properties window.

2 On the **Rights** tab, review the check marks in the **Effective** column, which is display-only.

The **Effective** column shows the combined rights of all groups listed on the **Groups** tab. When the user is not a member of any groups, this column will be blank.

3 To change the effective rights, right-click the **Allow** or **Deny** boxes as required.

The change appears in the **Effective** column. To check all boxes in a column select **SHIFT**, and right-click a box.

4 Select **Apply** or **OK** to complete the process or **Cancel** to exit.

How to Authenticate Users With LDAP

Users may access MessageWay either internally from the MessageWay Manager or externally, through a perimeter server, such as FTP, or SFTP or the Web Client. Users may be authenticated with one of these methods:

- MessageWay User ID and password
- Lightweight Directory Access Protocol (LDAP)

IMPORTANT: External users access MessageWay through one of the optional services, such as the FTP perimeter server or the SFTP perimeter server, or the Web Client. All external users must be authenticated as valid MessageWay users. LDAP must also be configured in the ***MessageWay Service Interface Configuration file*** (on page 98, on page 100), mwsi.conf, so MessageWay can communicate with the LDAP server.

To use LDAP authentication, you must define the same user ID in MessageWay and the LDAP server:

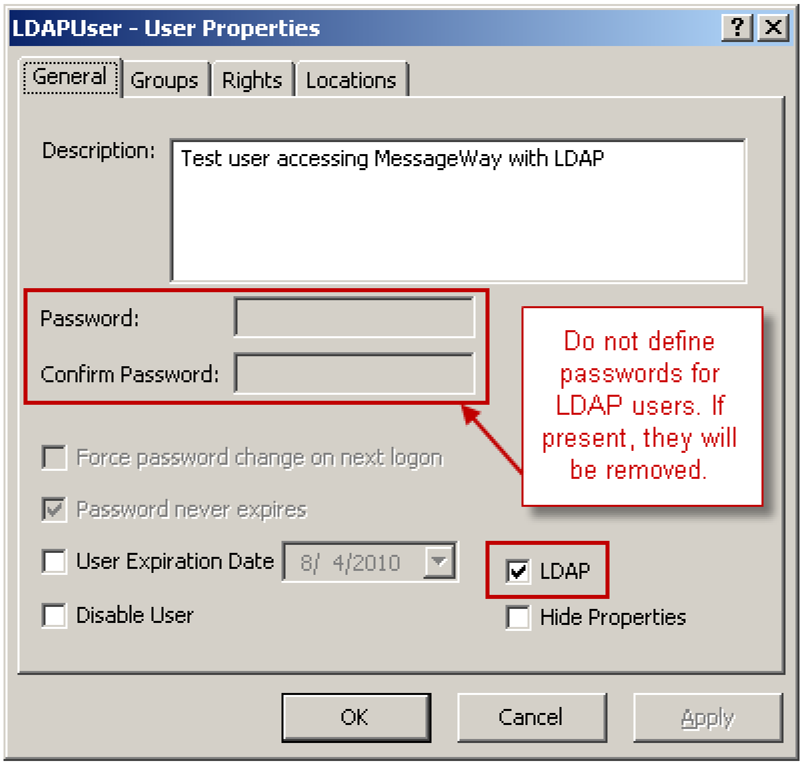
1 In MessageWay, ***create a MessageWay user*** (on page 381), but without a password.

If a user is already defined in LDAP, type the same user ID in the MessageWay Manager. For existing MessageWay users, go to step 2.

2 On the **General** page, check the box, **LDAP**.

The password fields are no longer available.

3 In the LDAP server, if the user is not already defined, add the same user ID that you created for MessageWay.



Description: Test user accessing MessageWay with LDAP

Password:

Confirm Password:

Do not define passwords for LDAP users. If present, they will be removed.

☐ Force password change on next logon

☑ Password never expires

☐ User Expiration Date 8/ 4/2010

☐ Disable User

☑ LDAP

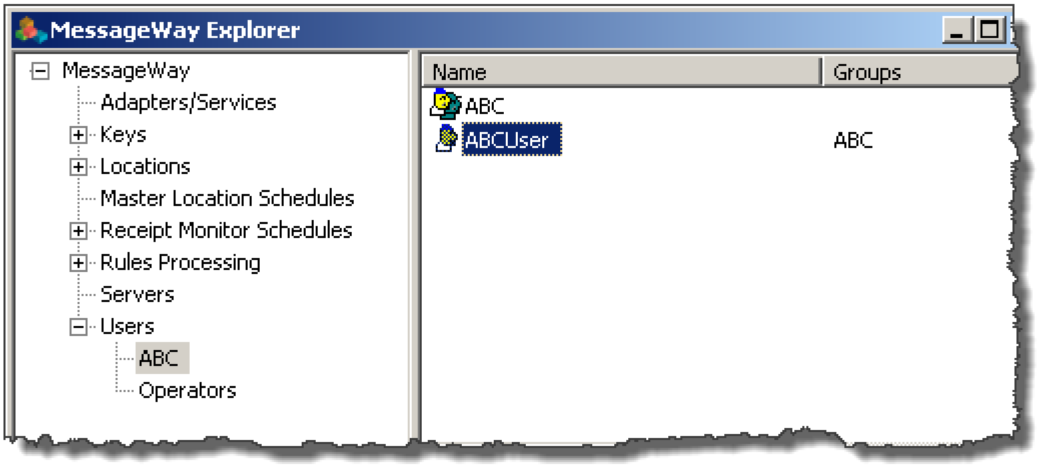
☐ Hide Properties

Configuring User Folders

When you need to configure many users for specific purposes, such as lines of business, you would create folders under the **Users** folder. The advantage is that when you add a user group to the folder with the same name as the folder, then all users that you add to the folder thereafter are automatically part of that group. As part of the group, they automatically inherit the security settings of the group.

TIP: Use this functionality when you create batches of users that must belong to the same user group.

In this example, we have ***added a folder*** (on page 389) called ABC. Within the ABC folder, we have ***added a user group*** (on page 378) called ABC. Then when we ***added the user*** (on page 381), ABCUser, it is automatically added to the group, ABC, and it inherits the rights from the group.



CAUTION: Do not create a folder with the name **Users**, because you will not be able to reference any users in the folder.

How to Create Folders for Users and User Groups

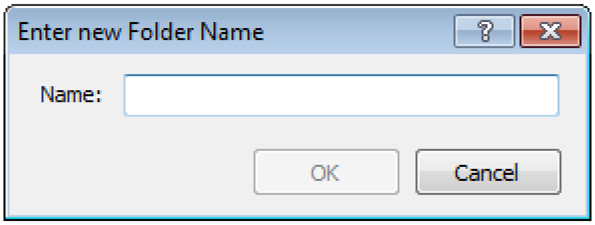
This procedure is an effective way to add many users to MessageWay who belong to the same group.

To organize your users and user groups you can create folders within the **Users** folder. When you add a user group to a sub-folder that has the same name as the group, each user you add to the folder will automatically be a member of this user group.

1 From the left pane of MessageWay Explorer, select **Users**.

2 On the right pane, right-click, and from the menu select **Add Folder**.

The **Enter New Folder Name** dialog box appears.



3 Enter a name for your folder that reflects your organizational needs, such as a line of business.

CAUTION: Do not create a folder with the name **Users**, because you will not be able to reference any users in the folder.

4 Click **OK** to complete the process or **Cancel** to exit.

The folder is added to the Users pane.

5 Within the folder, create a user group with the same name as the folder. Do not create the group outside of the folder and then move it to the folder. For instructions, refer to the topic, ***How to Create User Groups*** (on page 378).

6 Add users to the folder. For instructions, refer to the topic, ***How to Create Users*** (on page 381).

The group is automatically added to the user's **Group** page.

Controlling What Users Can See in the MessageWay Manager

You may need to control what a user sees in the MessageWay Manager.

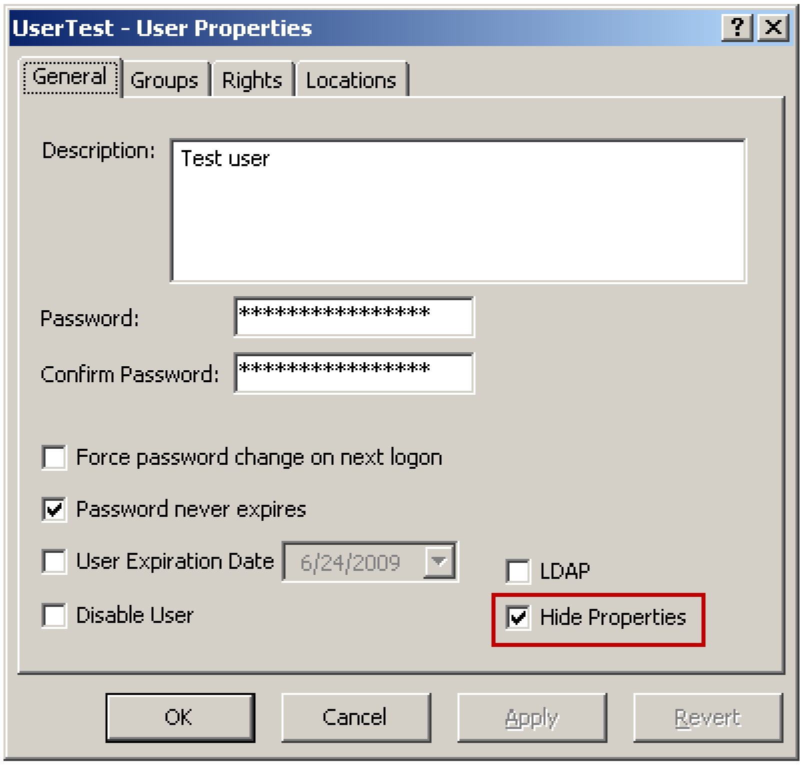
NOTE: These settings do not affect the owners of objects, who can always view and change the objects they own.

Access lists and ***user rights*** (on page 1358) determine what a user can do and see within the **Locations** folder. Users will not see a sub-folder within the **Locations** folder when they do not have access to the sub-folder.

TIP: To control which locations a user sees, all locations should be in sub-folders, whose access will be determined by access lists for the folder.

Some user rights and the **Hide Properties** ***setting*** (on page 1355) for a user also affect what a user can see in the Manager. The following table describes the options that control what users actually see in the Manager:

Option	Location	Description
Administer Users	User Properties window, **Rights** tab	When the box is clear, the **Users** folder is not visible.
View system counts	User Properties window, **Rights** tab	When the box is clear, users cannot see or access the system monitor or see message counts in the Adapter/Services monitor.
View Adapters/Services	User Properties window, **Rights** tab	When the box is clear, users cannot see the **Adapter/Service** folder or the list of adapters or services.
Hide Properties	User Properties window, **General** tab	▪ MessageWay Server option will not appear ▪ **Master Location Schedules** folder will not appear. ▪ **Receipt Monitor Schedules** folder will not appear ▪ **Rules Processing** folder will not appear ▪ No property windows will be accessible or visible, even if the user has explicit access to view properties



Description: Test user

Password: ****************

Confirm Password: ****************

□ Force password change on next logon

☑ Password never expires

□ User Expiration Date 6/24/2009

□ LDAP

□ Disable User

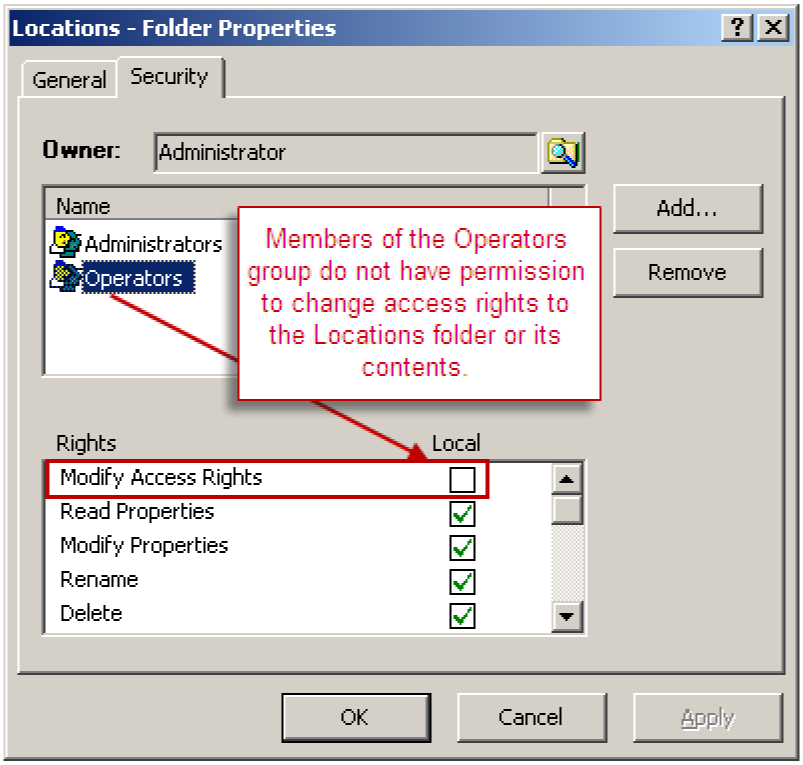
☑ Hide Properties

Hide Properties Option (User Properties Window, General Page)

Configuring Object Security

Access lists provide security for MessageWay root folders, their subfolders and objects other than users or user groups. To gain access to an object and perform functions, a user must have permission. Permissions are granted through access lists, which comprise a list of names of user groups and users and the specific rights granted to the names. The access list appears on the **Security** page of the object's window. For more information about the **Security** page for objects, refer to the topic, ***Security Page (Folder Properties)*** (on page 1026).

For example, assume we want to permit users in the Operators group access to locations. We will grant this permission at the highest level, at the root folder called **Locations**. To do this, we add the name of the user group to the **Locations** folder. In general, we don't want anyone that belongs to the group to be able to modify access rights to this folder or its contents. Our configuration appears in the following example.



Owner: Administrator

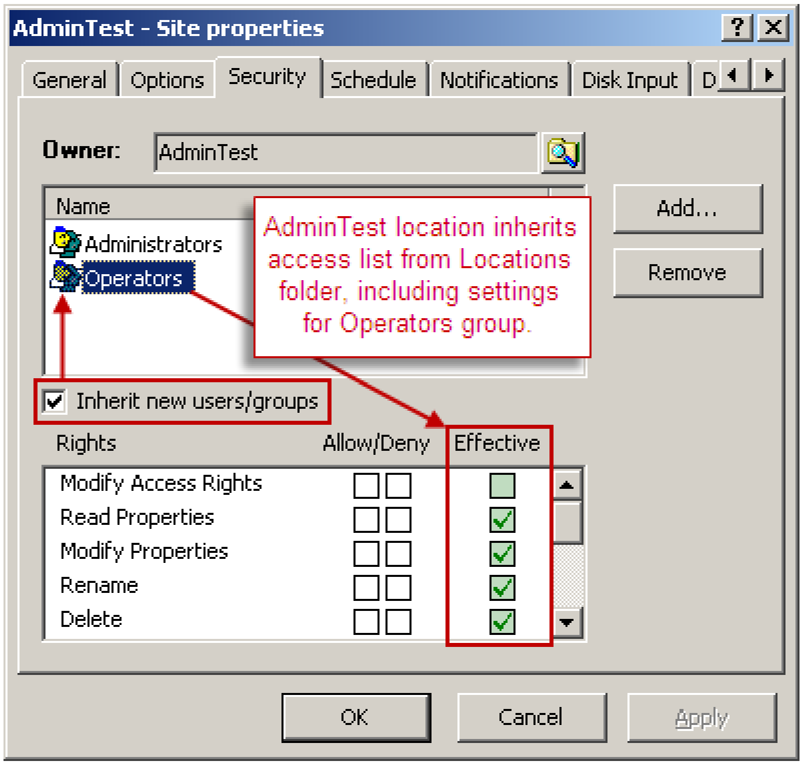
Name
Administrators
Operators

Members of the Operators group do not have permission to change access rights to the Locations folder or its contents.

Rights	Local
Modify Access Rights	□
Read Properties	☑
Modify Properties	☑
Rename	☑
Delete	☑

Access List for Locations Folder (Locations Folder Properties Window, Security Page)

Subfolders and locations within this folder inherit the access list from the **Locations** folder, when the **Inherit new users/groups** box is checked. In the following example, the **Effective** column displays the rights inherited from the **Locations** folder for the Operators user group.



Owner: AdminTest

Name
- Administrators
- Operators

AdminTest location inherits access list from Locations folder, including settings for Operators group.

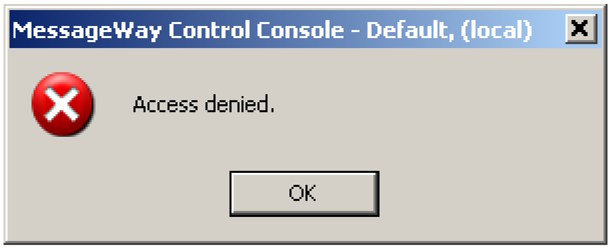
☑ Inherit new users/groups

Rights	Allow/Deny		Effective
Modify Access Rights	□	□	□
Read Properties	□	□	☑
Modify Properties	□	□	☑
Rename	□	□	☑
Delete	□	□	☑

Access List for AdminTest Site (Locations Folder Properties Window, Security Page)

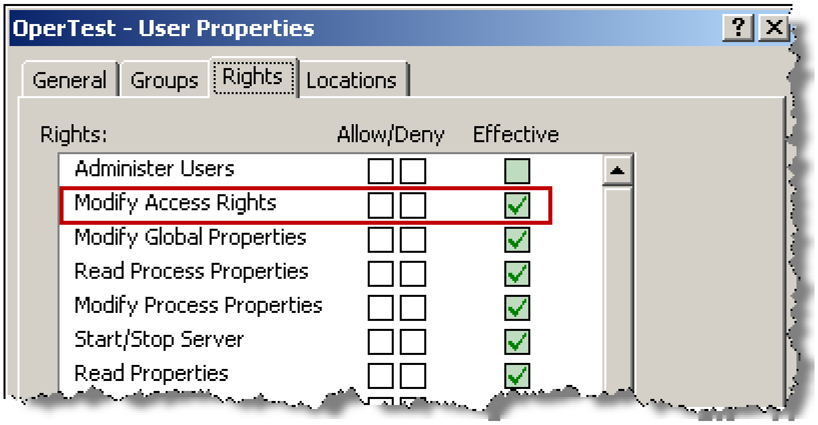
Now assume that a remote operator called OperTest wants to change the access rights for AdminTest. No matter what his user rights are, he will not be able to do so.

IMPORTANT: Attempts to access objects to which one does not have access, returns the message, **Access denied**.



Access denied.

The following example shows the **Rights** page for OperTest, who does have the general right to modify access rights, but he cannot change the access rights for locations.

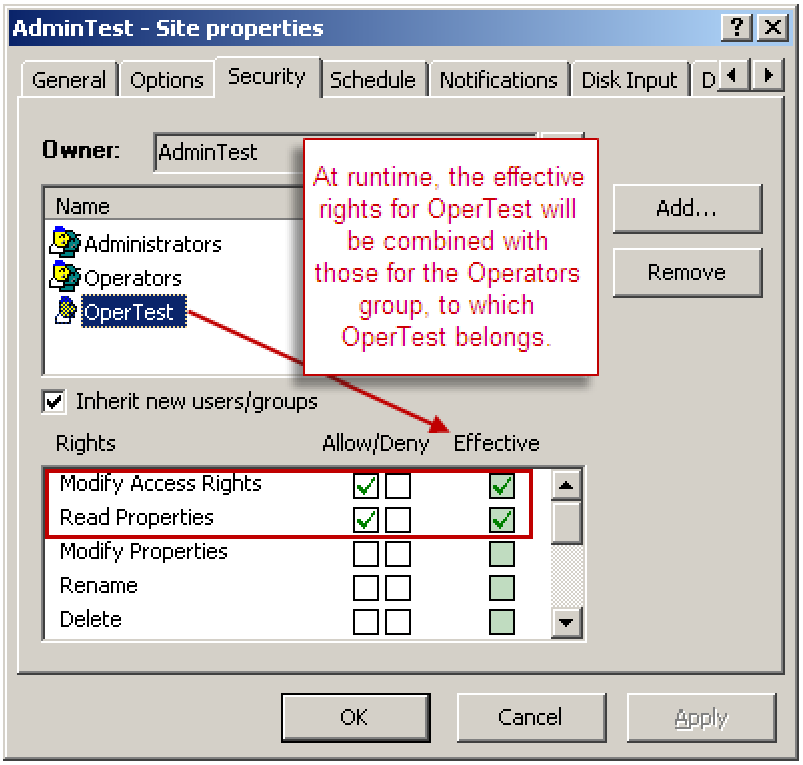


Rights:	Allow/Deny	Effective
Administer Users	□ □	□
Modify Access Rights	□ □	☑
Modify Global Properties	□ □	☑
Read Process Properties	□ □	☑
Modify Process Properties	□ □	☑
Start/Stop Server	□ □	☑
Read Properties	□ □	☑

Access List for OperTest (User Properties Window, Rights Page)

Now assume that you want only the user OperTest to be able to modify access rights only for the location, AdminTest. The best way to accomplish this is to add specific rights to the access list of the AdminTest location for the user. You could give permission to the entire Operators group. However, you can also add the user, OperTest, to the access list with permission to modify access rights.

The following example shows the OperTest user on the access list for the location, AdminTest, with permission to modify access rights. Now this user will have permission to modify access rights for only this location, because the rights in the user configuration and the object configuration allow it.



Owner: AdminTest

Name
Administrators
Operators
OperTest

At runtime, the effective rights for OperTest will be combined with those for the Operators group, to which OperTest belongs.

☑ Inherit new users/groups

Rights	Allow/Deny	Effective
Modify Access Rights	☑ □	☑
Read Properties	☑ □	☑
Modify Properties	□ □	□
Rename	□ □	□
Delete	□ □	□

Access List for AdminTest Location with User Override (AdminTest Site Properties Window, Security Page)

NOTE: When you add a user to an object's access list and the user belongs to another group on the list, the rights are combined at runtime to determine what the user may do for this object.

How to Add Users or Groups to a Security Access List

To add a user or group to the security list of a folder or other object:

1. Access the appropriate properties window.
2. On the **Security** page, select the **Add** button.

   The **Select User or User Group** dialog box appears.
3. Select the user or group you want to add from the list.
4. To complete the process, choose the **Select** button. To cancel, select the **Cancel** button.

   The **Security** page appears with the added user or group.
5. To view the current rights of the new user or group, select the name.

   The current rights appear in the **Effective** column.

How to Override Rights on a Security Access List

Whether rights are inherited from parent folders or you have added a new folder or user to the name list, you can change the current rights, assuming you have the rights to do so. When you are the owner of the object, you have the implicit right to maintain the configuration.

IMPORTANT: Access rights for users at runtime are the combined rights of all groups to which they belong that are listed in the box. Therefore, you cannot deny rights to users when the users are allowed the rights by a group.

1. Access the appropriate properties window. For instructions, see ***How to View Properties*** (on page 1214).
2. On the **Security** page, select the user or group whose access rights you want to override.

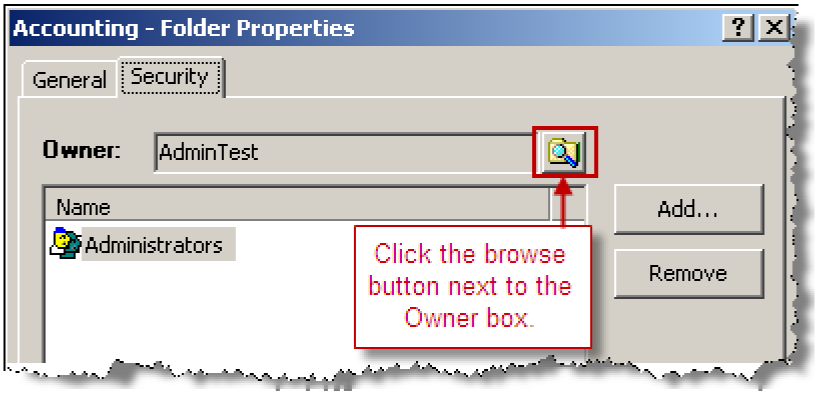
   The current rights appear in the **Effective** column.
3. To add rights, select one or more of the boxes under the **Allow** column. To check or clear all boxes at once, select **SHIFT** and the top box. Some rights depend on other rights. When you check a box, all required rights are also checked.
4. To delete rights, select one or more of the boxes under the **Deny** column. To check or uncheck all boxes at once, select **SHIFT** and the top box.

CAUTION: You cannot deny a right to an individual user for an object when that user belongs to a group on the access list that grants the group that right. For example, assume a user belonged to a group on an access list for an object that granted the right, Modify Properties. You cannot add that user to the access list and deny Modify Properties, because the user will be granted the right as part of the user group at runtime.

How to Transfer Ownership of an Object

The owner of an object, a configuration, has all rights to that object. There may be times that you may want another user to be responsible for the object. The current owner of an object or the super user of the system can transfer ownership of objects to another user, as follows:

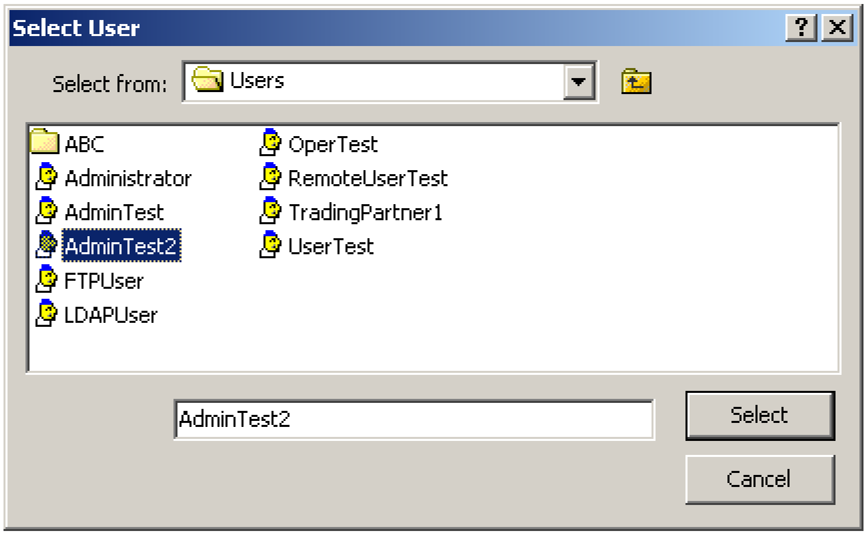
1. Log on to the MessageWay Manager as the owner of the object or as the super user.
2. For the object whose ownership you want to transfer, right-click the object and select **Properties**.
3. On the **Security** page, click the browse button next to the owner.



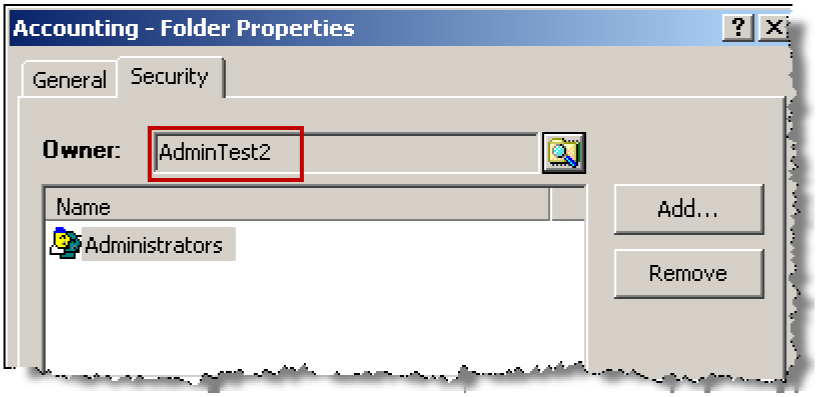
Click the browse button next to the Owner box.

The **Select User** dialog box appears.

4. Click the user to whom you want to transfer ownership, and click **Select**.



The new owner appears in the **Owner** box.



Owner: AdminTest2

Name
Administrators

This page intentionally blank.

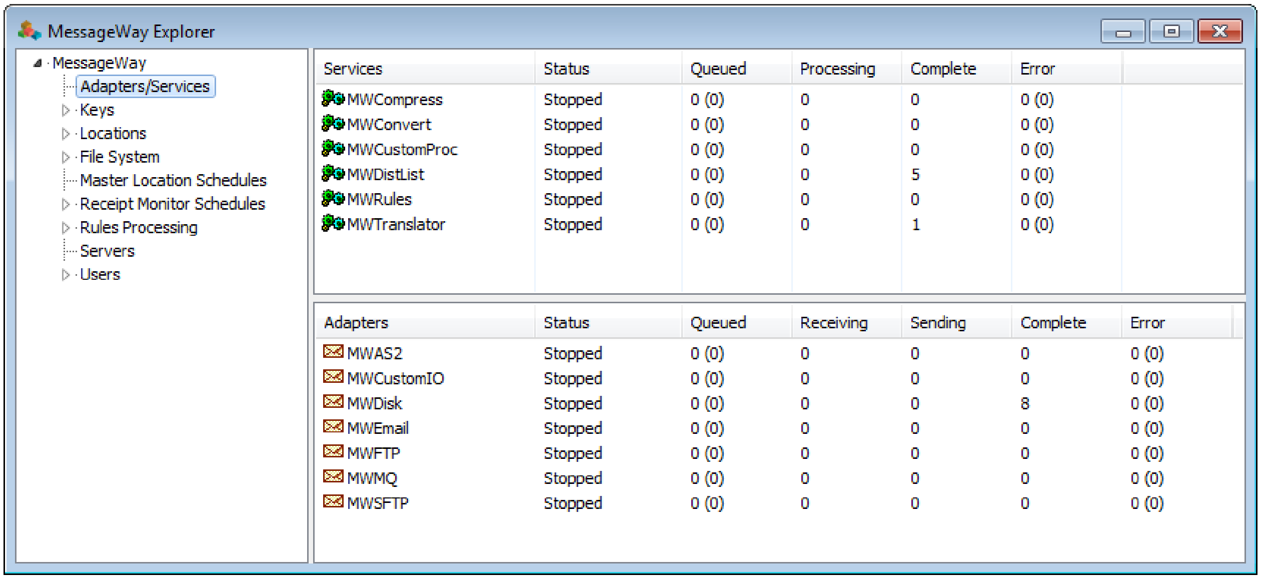
Configuring Adapters and Services

This section provides information about how to configure adapters and services, which provide entry and exit points for MessageWay and integrated processing services.

NOTE: Some adapters and services listed here are purchasable options and require additional licenses, as indicated for the adapter or service.

Overview of Adapter and Service Properties

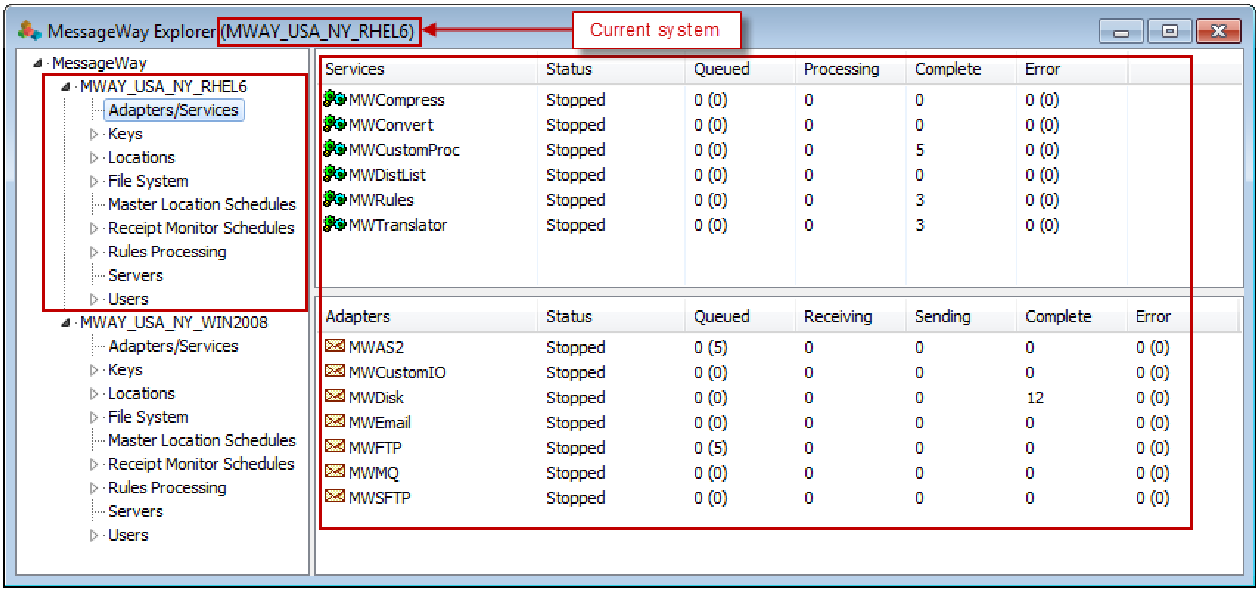
Adapters and services provide client services that move messages to and from the Message Store. MessageWay Explorer provides users with a list of all adapters and services for which the user has licenses. It shows the current status and statistics of all processing.



Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0	0	0 (0)
MWDistList	Stopped	0 (0)	0	5	0 (0)
MWRules	Stopped	0 (0)	0	0	0 (0)
MWTranslator	Stopped	0 (0)	0	1	0 (0)

Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWAS2	Stopped	0 (0)	0	0	0	0 (0)
MWCustomIO	Stopped	0 (0)	0	0	0	0 (0)
MWDisk	Stopped	0 (0)	0	0	8	0 (0)
MWEmail	Stopped	0 (0)	0	0	0	0 (0)
MWFTP	Stopped	0 (0)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

When you monitor a multi-system environment, you still only access and configure one system at a time. MessageWay Explorer lists all systems in the environment, but the current system name appears in the MessageWay Explorer title bar. Also all property windows show the system.



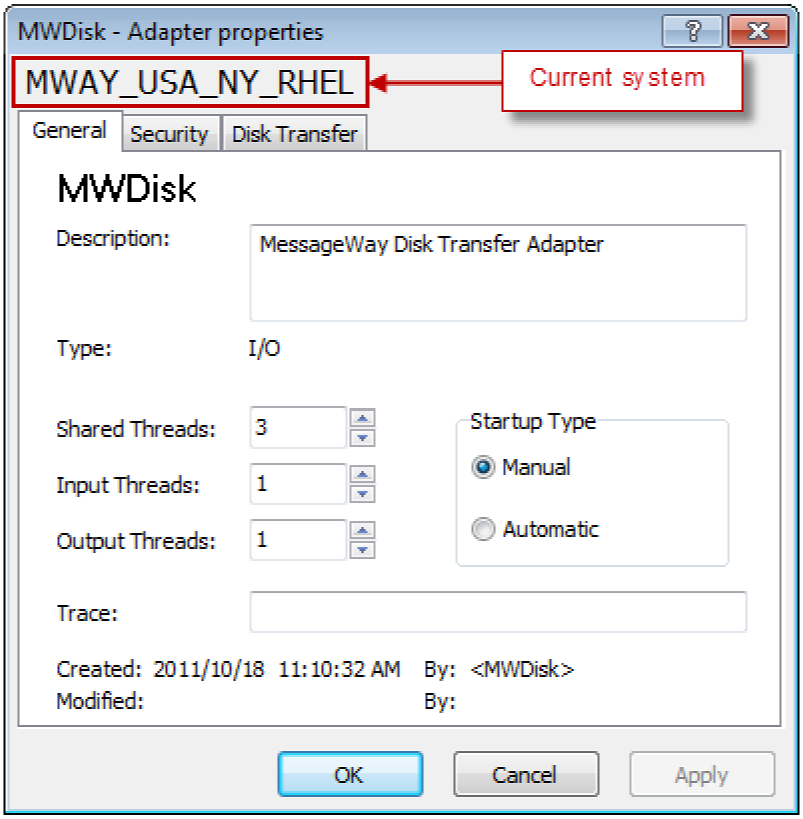
MessageWay Explorer (MWAY_USA_NY_RHEL6)

Current system

- MessageWay
  - MWAY_USA_NY_RHEL6
    - Adapters/Services
    - Keys
    - Locations
    - File System
    - Master Location Schedules
    - Receipt Monitor Schedules
    - Rules Processing
    - Servers
    - Users
  - MWAY_USA_NY_WIN2008
    - Adapters/Services
    - Keys
    - Locations
    - File System
    - Master Location Schedules
    - Receipt Monitor Schedules
    - Rules Processing
    - Servers
    - Users

Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0	5	0 (0)
MWDistList	Stopped	0 (0)	0	0	0 (0)
MWRules	Stopped	0 (0)	0	3	0 (0)
MWTranslator	Stopped	0 (0)	0	3	0 (0)

Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWAS2	Stopped	0 (5)	0	0	0	0 (0)
MWCustomIO	Stopped	0 (0)	0	0	0	0 (0)
MWDisk	Stopped	0 (0)	0	0	12	0 (0)
MWEmail	Stopped	0 (0)	0	0	0	0 (0)
MWFTP	Stopped	0 (5)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)



MWDisk - Adapter properties

MWAY_USA_NY_RHEL

Current system

MWDisk

Description: MessageWay Disk Transfer Adapter

Type: I/O

Shared Threads: 3

Input Threads: 1

Output Threads: 1

Startup Type
● Manual
○ Automatic

Trace:

Created: 2011/10/18 11:10:32 AM By: <MWDisk>
Modified: By:

Some adapters and services are part of base MessageWay and some are purchasable options, as shown in the following table:

Adapter or Service Status	Description	Name
Base Services	▪ Compression (zip, unzip) ▪ Custom Processing ▪ Distribution List ▪ Rules Processing	▪ MWCompress ▪ MWCustomProc ▪ MWDistList ▪ MWRules
Base Adapters	▪ Custom Input/Output ▪ Disk Transfer ▪ E-mail ▪ FTP ▪ SFTP	▪ MWCustomIO ▪ MWDisk ▪ MWEmail ▪ MWFTP ▪ MWSFTP
Optional Services	▪ Character Set Conversion ▪ Translation Service	▪ MWConvert ▪ MWTranslator
Optional Adapter	▪ Copy of any base adapter ▪ AS2 ▪ MQ ▪ AWS S3	▪ See, Base Adapters ▪ MWAS2 ▪ MWMQ ▪ MWAWSS3

▪

Function of Adapters and Services

Adapters provide the client interface to outside servers and control traffic to and from internal services. Adapters can typically perform both input (pull) and output (push) functions, depending on the communications protocol with which they are associated. The AS2 adapter, for example, is output only, because AS2 protocol only allows clients to push data to an AS2 server. Other protocols, such as FTP, allow clients to push and pull data from an FTP server.

Services provide internal processing for messages, such as compression, custom processing, distribution lists, character set conversion and rules processing. Optional services include translation.

Behavior of Adapters and Services

Adapter and service behavior varies depending on whether they are receiving input or sending output. Behavior is controlled by the locations associated with the adapter or service. The following table compares the behavior:

	Services	Adapters

	Services	Adapters
Input Behavior	Monitor locations configured to use that service: ▪ When a message appears in the location, service passes it to the process.	Monitor locations configured to use that adapter. Most adapters perform polling on a specified location. Users control the type of polling. ▪ When the location schedule is closed or the location is on hold, no polling occurs. ▪ When the schedule is open, the adapter polls to receive messages.
Output Behavior	Wait until all output has been generated before sending it to configured destination, which will be one or more locations. ▪ When processing completes successfully, the service attempts to deliver the messages. ▪ If there is a transaction failure during processing, all output generated to that point is deleted and nothing is sent. ▪ Links are maintained between the input, output, and reports for the transaction, which allows any entity to be queried in order to find all other related entities.	Send messages based on schedules associated with the location. ▪ When the schedule is open, the adapter attempts to deliver messages as soon as they appear in the destination location. ▪ For threshold release, messages are queued under a closed schedule until the threshold is met, and then the schedule opens, and all messages are sent at once.

Control of Adapters and Services

Users control adapters and services with two methods:

- Configurations
- Direct operator actions

This section discusses configurations. For operator actions, refer to the section ***Controlling Message Traffic*** (on page 701). Users may specify the following basic information for adapter or service configurations:

- Thread allocations to optimize processing
- Startup options: manual or automatic
- Trace parameters to debug problems
- Parameters specific to the adapter or service, such as:
  - Polling activity

- Default logon information for servers
- Default security options
- Default directories

Changing Location of Server Directory for Adapters and Services

MessageWay adapters and services has a subdirectory in the /messageway/server directory to support its functionality.

To change the location of the **Server** directory, add the following line to the MessageWay Server configuration file before the final </MessageWay> tag:

<ServerDir>*NewLocationOfServerDirectory***</ServerDir>**

For an example, refer to the topic, ***MessageWay Messaging Server Configuration File*** (on page 89).

Tracing Activity for Adapters and Services

This option specifies the type of activity to log to the MessageWay database for the adapter or service. Then you can filter and view the information online or send it to a file using the trace utility. Enter a list of types, separated by commas, that you want to use to appear in the trace log. The types available vary by adapter or service. You may also type an asterisk (*) to trace all activity. You can limit the log information further by location, message ID, user and/or IP address.

The trace utility, mwtrace, allows you to view trace information, online or from a disk file, and to delete trace records from the database. For information about how to use the trace utility, in the Troubleshooting section, refer to the topic, ***Tracing Communications Activity*** (on page 877).

Another utility, ***mwlogdump*** (on page 841), allows you to copy audit and event log information from the database to a syslog or csv format, which also includes trace information for adapters and services.

CAUTION: The trace process may have a significant impact on performance, especially when you use the asterisk * to trace everything, and particularly for the MessageWay User Server, mwuser. Except for the MessageWay Messaging Server, tracing starts as soon as you enter your trace options and click **Apply** or **OK**. When you have finished debugging, clear the field of all text to turn off the trace. If there is an asterisk in a trace field of core or other active servers when MessageWay starts, you risk overwhelming your system with trace activity.

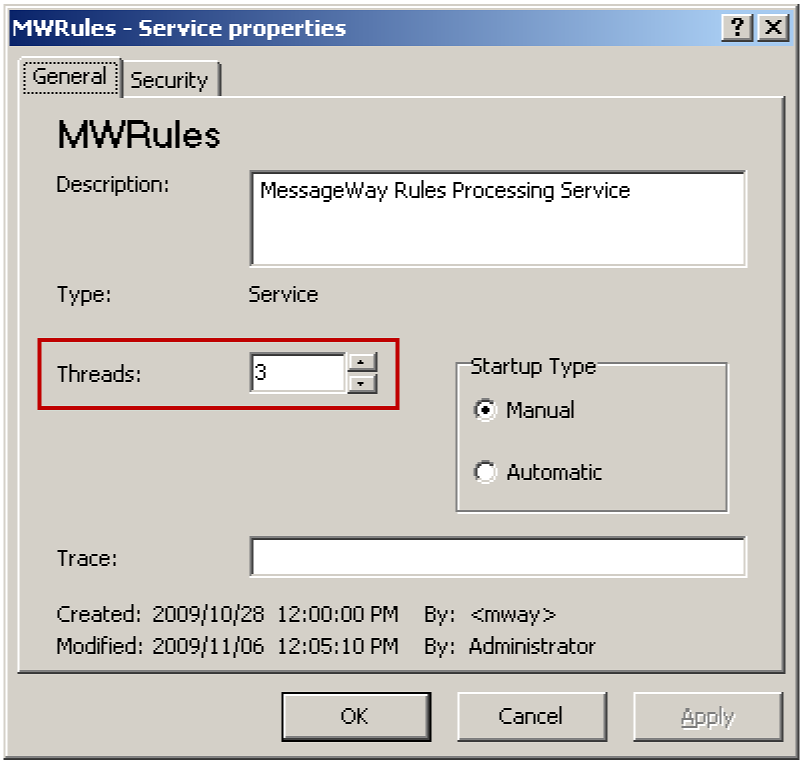
Configuring Threads for Adapters and Services

Adapters and services process messages in locations based on priority. Threads are allocated by the operating system based on assigned priority, in order of first-in, first-out (FIFO). Users may control worker threads assigned to the adapter or service by changing the thread assignments on the **General** page of the properties window. All adapters and services have one thread dedicated to moving the highest priority messages, those with priority 5. This reserved thread is not included in the thread count displayed on the properties window.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Examples of Thread Settings for Adapters and Services

For services, users may manipulate the total number of threads. The operating system controls when the threads are allocated for input or output functions. The following example shows the default settings for the Rules Processing service.



MWRules - Service properties

MWRules

Description: MessageWay Rules Processing Service

Type: Service

Threads: 3

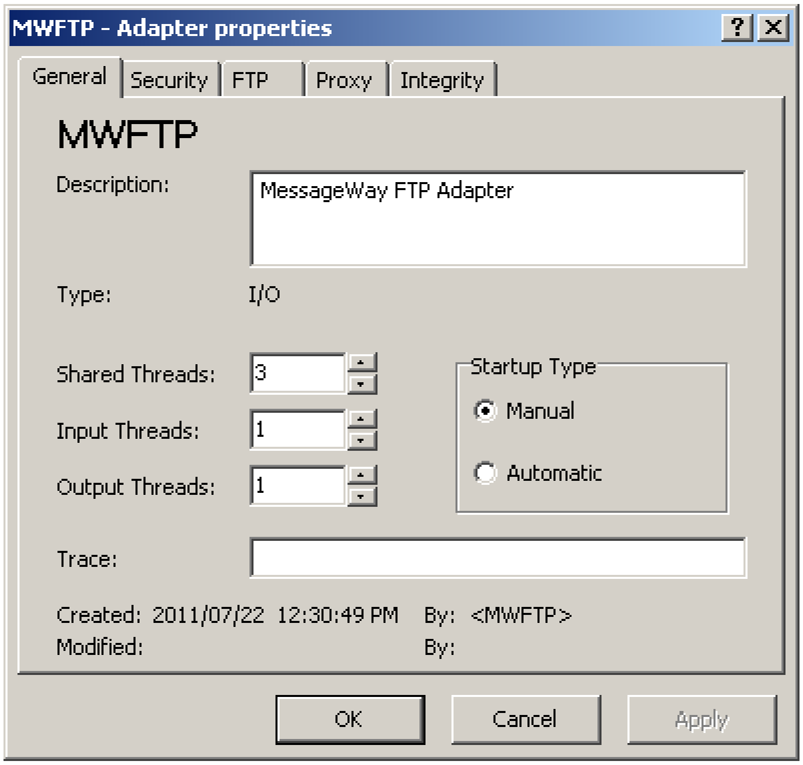
Startup Type: ● Manual ○ Automatic

Trace:

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/06 12:05:10 PM By: Administrator

Assigning Threads to a Service (Service Properties Window)

For adapters, users may choose the number of threads allocated for either input or output (Shared Threads). Users may also specify the threads to be reserved for input (Input Threads) and for output functions (Output Threads). Threads not specifically reserved will be allocated by MessageWay. The following example shows the default settings for the FTP adapter.



MWFTP

Description: MessageWay FTP Adapter

Type: I/O

Shared Threads: 3

Input Threads: 1

Output Threads: 1

Startup Type
● Manual
○ Automatic

Trace:

Created: 2011/07/22 12:30:49 PM By: <MWFTP>
Modified: By:

Assigning Threads to an Adapter (Adapter Properties Window)

Recommendations for Thread Settings of Adapters and Services

Users must test thread allocations in their own environment to optimize the use of resources. Allocated threads consume system resources, so users must test carefully. Resources that may affect thread assignment include:

- Available disk space
- Available memory
- Number of processors for multi-processor system
- Other applications that are running and vying for resources

The more processors you have, the more threads you may assign. Typically, low numbers of threads are best for throughput to process small numbers of large files and high numbers of threads are best for availability to process large numbers of small files.

IMPORTANT: One thread is reserved by MessageWay to process messages with the highest priority (5). This thread is not included in the shared threads count.

We recommend the following thread assignment for services, which is also the default assignment:

- Assign 3 worker threads as a starting point for basic systems

We recommend the following thread assignments for adapters, which are also the default assignments:

- Assign 3 worker threads to Shared Threads.
- When adapters process input and output data, users should assign at least 1 thread each to Input Threads and Output Threads. This provides a means for both kinds of messages to be moved. Assigning no threads to either input or output threads allows users to control the direction of processing and to avoid wasting system resources.

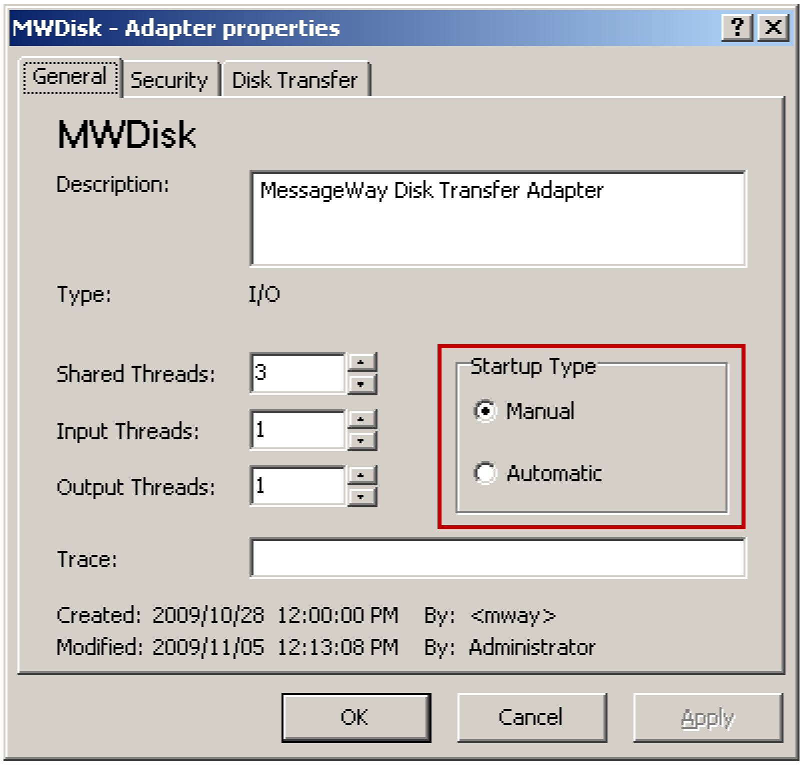
Configuring Adapters and Services for Startup

Users may control whether adapters or services should be started when MessageWay starts or by an operator.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Examples of Startup Type Settings for Adapters and Services

The startup type for all adapters and services is set to manual during installation. Since startup options are the same for both adapters and services, the following example of the Disk Transfer adapter applies to services as well.



MWDisk

Description: MessageWay Disk Transfer Adapter

Type: I/O

Shared Threads: 3

Input Threads: 1

Output Threads: 1

Startup Type

● Manual

○ Automatic

Trace:

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/05 12:13:08 PM By: Administrator

Specifying Startup Type for an Adapter or Service (Adapter Properties Window)

Recommendations for Startup Type Settings of Adapters and Services

Typically, when you start the MessageWay Server, you want to automatically start all adapters and services you need for processing. We recommend the following settings:

- *Automatic* for all adapters and services whose function you will use on a daily basis
- *Manual* for any adapter and service functions you never use or use on exception
- *Manual* to isolate specific adapters or services for testing or trouble-shooting

How to Start Adapters and Services Automatically

You may start MessageWay adapters and services from the MessageWay Manager or have them start automatically when you start the MessageWay server.

To start MessageWay adapters and services automatically, proceed as follows:

1 Start MessageWay for:
   - ***UNIX/Linux*** (on page 29)
   - ***Windows*** (on page 32)

2 From MessageWay Explorer in the left pane, expand the MessageWay folder and click **Adapters/Services**.

The list of installed adapters and services appears in the right pane.

3 Select one of them in the right pane, and then click the **Properties** button on the toolbar.

The Adapter or Services Properties window appears.

4 From the **General** page, select **Startup Type|Automatic**, and then select **OK**.

5 Repeat steps 2-4 for each of the remaining adapters or services.

The next time you start the MessageWay Server, it will also start the ones you have selected to start automatically.

Configuring the AS2 Adapter

To allow MessageWay to send messages to an AS2 server through the AS2 Interface, you must configure the properties of the AS2 adapter.

1 From the MessageWay Manager, in the left pane of MessageWay Explorer, click **Adapters/Services**.

2 In the right pane, double click **MWAS2**.

The Adapter Properties window appears.

3 Type or select the information as follows:

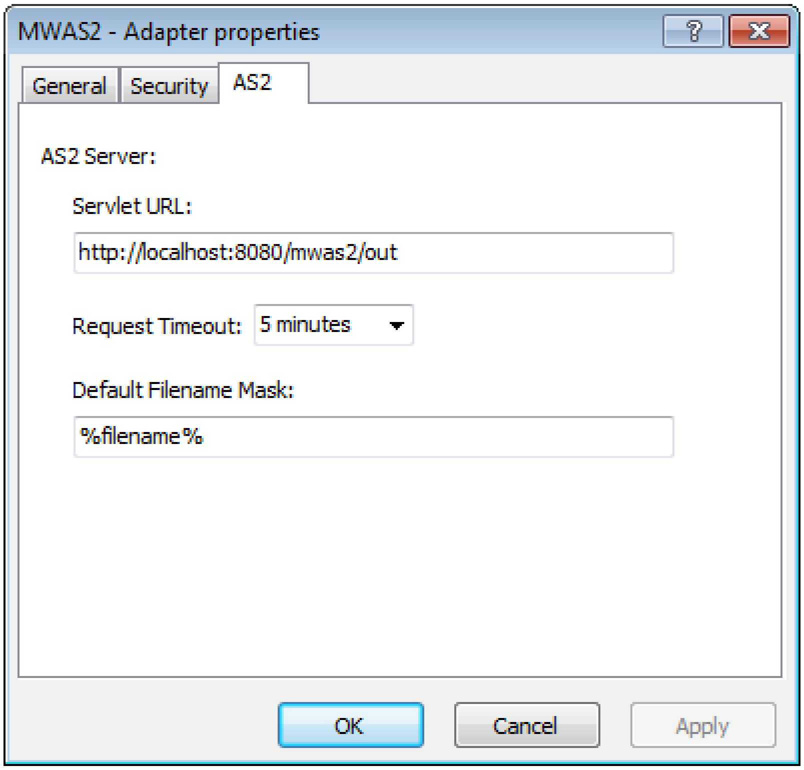
Servlet URL — This required field identifies the location of the outbound servlet. The values are case-sensitive. Type the Web address of the AS2 outbound servlet. For example, if the servlet is on the same system as the AS2 adapter, you might type, http://localhost:8080/mwas2/out. If the servlet is on a different machine than the AS2 adapter, you might type, http://192.168.0.4:8080/mwas2/out.

Request Timeout — Select or type the amount of time in seconds, minutes or hours to allow the AS2 outbound processing cycle to complete. This is a default value for AS2 sites, which users can override by selecting a Request Timeout value for a site.

Default FilenameMask — This is a template to create a file name for the output file. For new installations, the default mask is **%filebase%[%msgid%].%fileext%**. This mask generates unique names using the MessageWay message ID, which is enclosed in square brackets, [ ]. This avoids sending files that might be rejected because the file name already exists at the remote location. To change this default mask, use any combination of constants and MessageWay tokens. You may override this default for a specific location. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name.

4 Click **Apply** or **OK** to save your changes.

Here is an example of the configurations on an **AS2** page for a connection to an AS2 outbound servlet that is on the same Windows system as the AS2 adapter:



AS2 Server:

Servlet URL: http://localhost:8080/mwas2/out

Request Timeout: 5 minutes

Default Filename Mask: %filename%

NOTE: The MessageWay AS2 server and the AS2 adapter require a license from Progress. For more information, contact MessageWay Technical Support.

Configuring the Compression Service

There are no special configurations required for the Compression service.

The MessageWay Compression service compresses (zips) and uncompresses (unzips) files. It supports the PKWARE zip file format using the DEFLATE compression algorithm (RFC 1951) and the GZIP file format (RFC1952).

Most services specify their own routing, but the Compression service does not, although you can specify a mask to create a file name. Therefore, the output must be sent from a compression service location to a location whose adapter or service does provide routing, such as service locations like Distribution List, Translator, or Rules Processing or any of the I/O sites, which use adapters.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Configuring the Conversion Service

There are no special configurations required for the Conversion service.

Most services specify their own routing, but the Conversion service does not. Therefore, the output must be sent from a conversion service location to a location whose adapter or service does provide routing, such as service locations like Distribution List, Translator, or Rules Processing or any of the I/O sites, which use adapters.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

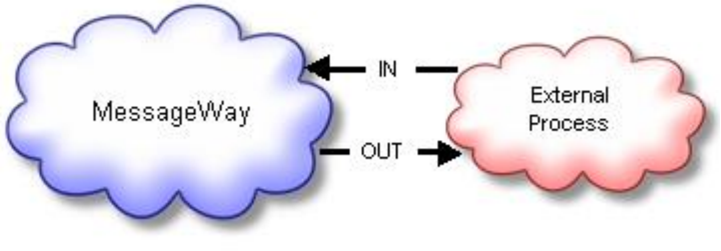
Configuring the Custom IO Adapter

The MessageWay Custom I/O Adapter is a generic adapter that executes user-defined programs or scripts to do one of the following:

- Transfer messages to MessageWay
- Transfer messages from MessageWay
- Send a trigger message to start an external process

Users may send messages to and from MessageWay or simply start an external process by running a shell script or an executable program. Valid scripting languages include those that are installed on and supported by the operating system.

The concepts of in and out as seen in the default subdirectories and the replaceable parameters, are relative to MessageWay. The terms *in* and *input* refer to messages transferred to MessageWay from the external process, and *out* and *output* refer to messages transferred from MessageWay to the external process.



This service includes the following configurable entities:

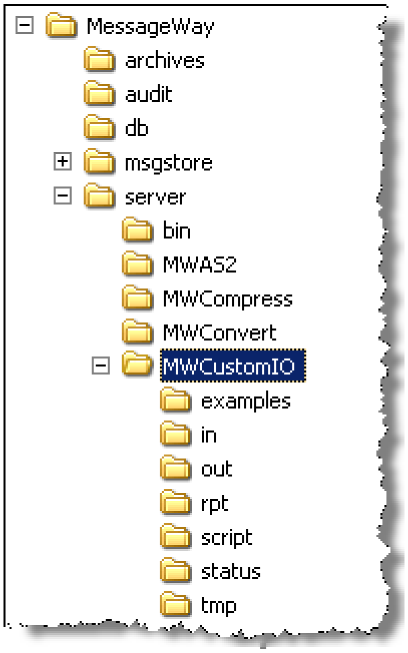
- Custom I/O Adapter
- Custom I/O locations, created by users

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Understanding the Default Subdirectories (Custom IO Adapter)

Within the /MessageWay/server directory, the install process creates a directory structure for the MWCustomIO subdirectory with default locations for passing files to and from MessageWay.

On Windows, the structure looks like this:



```
⊟ MessageWay
     archives
     audit
     db
  ⊞  msgstore
  ⊟  server
        bin
        MWAS2
        MWCompress
        MWConvert
     ⊟  MWCustomIO
           examples
           in
           out
           rpt
           script
           status
           tmp
```

The following table explains how the adapter uses these subdirectories. Note that the directories used for temporary storage will typically never have anything in them because MessageWay deletes the files when it successfully completes its processing. Files might remain in the subdirectory when a process aborts.

Directory	Use
examples	Directory that contains the sample scripts to show how to use the replaceable parameters and return statuses
in	Directory for temporary storage of files loaded into MessageWay
out	Directory for the temporary storage of output , notification and acknowledgment files created by the external process to be returned to MessageWay

Directory	Use
script	Default directory for script files referenced in the Command field.
status	Directory for the temporary storage of status files.
tmp	Directory for the temporary storage of scripts configured within the **Script** box, after the parameters have been resolved and before successful completion of the script

Configuring a Custom I/O Adapter

The Custom I/O Adapter identifies the input polling interval for its sites and the default directory for script files.

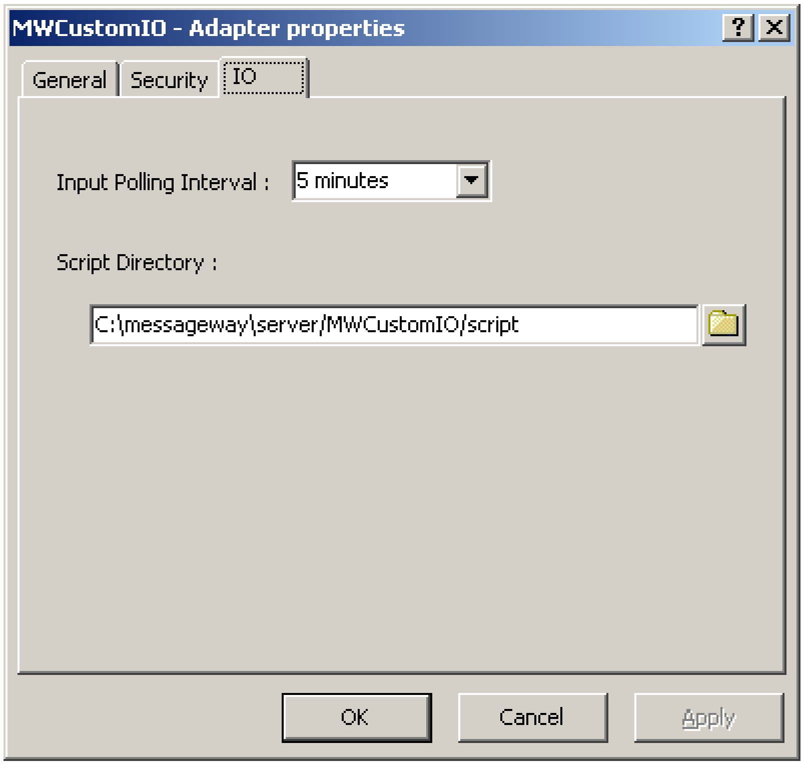
Output scripts are activated when a message is delivered to a site that uses the Custom I/O Adapter.

Input scripts are activated by one of two types of events:

- Polling configured for the adapter
- Triggers sent by the MessageWay Server, initiated by one of the following:
  - Service Interface
  - **Input Now** command

The script information appears on the **Input** or **Output** tab of the Site Properties window. The events cause the adapter to run commands or scripts it finds on any of the custom I/O sites. When the script is specified in the **Command** box, the adapter searches the Script subdirectory shown on this **IO** tab. Note that this differs from the way polling works for other adapters, which poll sites for messages to transfer into MessageWay, rather than for scripts to run.

IMPORTANT: To avoid complications with mapped drives, always use the full Universal Naming Convention (UNC) directory name. A Windows service should not directly access local or network resources through mapped drive letters. MessageWay servers, which includes MWTranslator, run as Windows services.

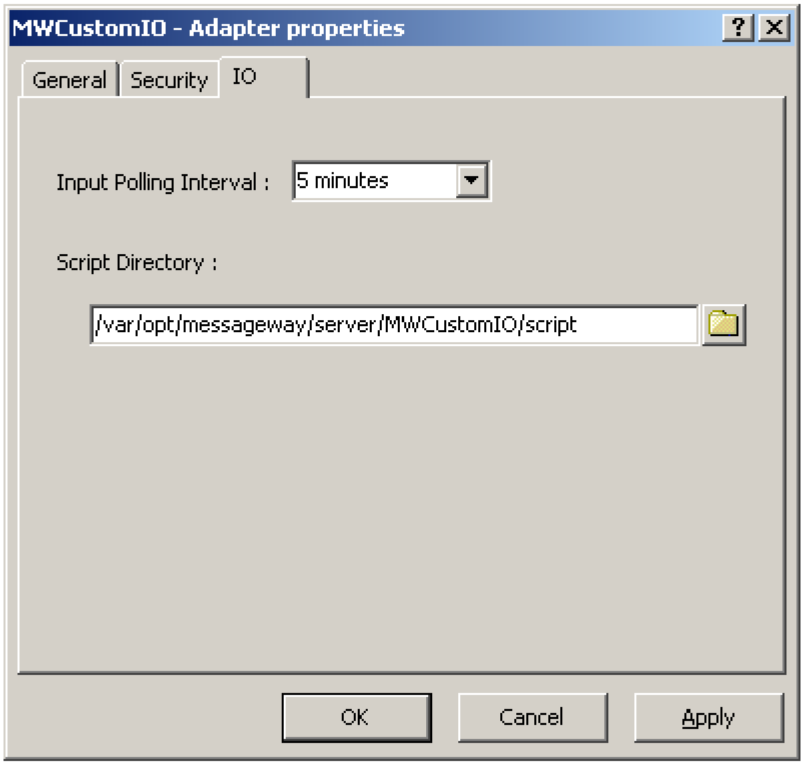


Input Polling Interval : 5 minutes

Script Directory :

C:\messageway\server/MWCustomIO/script

IO Page, Windows (Adapter Properties Window)



Input Polling Interval : 5 minutes

Script Directory :

/var/opt/messageway/server/MWCustomIO/script

IO Page, UNIX/Linux (Adapter Properties Window)

IMPORTANT: To make changes in adapter configurations take effect, you must stop and restart the adapter. To assure that all message traffic has been sent before the adapter is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

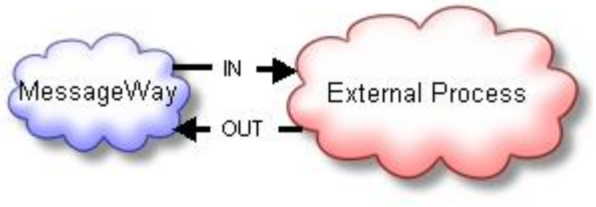
For basic information about MessageWay adapters or services, refer to the section, ***Configuring Adapters and Services*** (on page 399). For generic information to configure a MessageWay adapter or service, refer to the sections in “MessageWay Manager Reference” for the ***Adapter or Service Properties window*** (on page 925). For most adapters or services, the last page of each window is specific to configurations required to transfer messages.

Configuring the Custom Processing Service

The MessageWay Custom Processing Service allows users to send messages from MessageWay to an external process, start the process and receive files back from the process. The external process typically manipulates the information and returns one or more related messages. However, the input message might simply be a trigger to run the process, which may not return any files.

The service runs a shell script, such as a batch file, or an executable program that is configured for a custom processing location. Valid scripting languages include those that are installed on and supported by the operating system. The scripts may reside in MessageWay or outside of MessageWay. Certain events will initiate the script or command.

The concepts of in and out as seen in the default subdirectories and the replaceable parameters, are relative to the external process. The terms *in* and *input* refer to messages transferred from MessageWay to the external process, and *out* and *output* refer to messages transferred from the external process to MessageWay.



This service includes the following configurable entities:

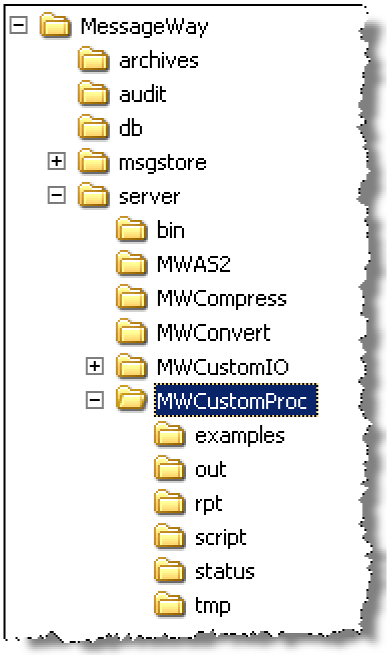
- Custom Processing Service
- Custom Processing service locations, created by users

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Understanding the Default Subdirectories

Within the /MessageWay/server directory, the install process creates a directory structure for the MWCustomProc subdirectory with default locations for passing files to and from MessageWay.

On Windows, the structure looks like this:



The following table explains how the service uses these subdirectories. Note that the directories used for temporary storage will typically never have anything in them, because MessageWay deletes the files when it successfully completes its processing. Files will remain in a subdirectory when a process aborts.

Directory	Use
examples	Directory that contains the sample scripts to show how to use the replaceable parameters and return statuses
out	Directory for the temporary storage of output , notification and acknowledgment files created by the external process to be returned to MessageWay
rpt	Directory for the temporary storage for report files created by the external process to be returned to MessageWay
script	Default directory for external script files referenced in the Command field
status	Directory for the temporary storage for status files to be returned to MessageWay
tmp	Directory for the temporary storage for scripts configured within the Script box, after the parameters have been resolved and before successful completion of the script

Configuring a Custom Processing Service

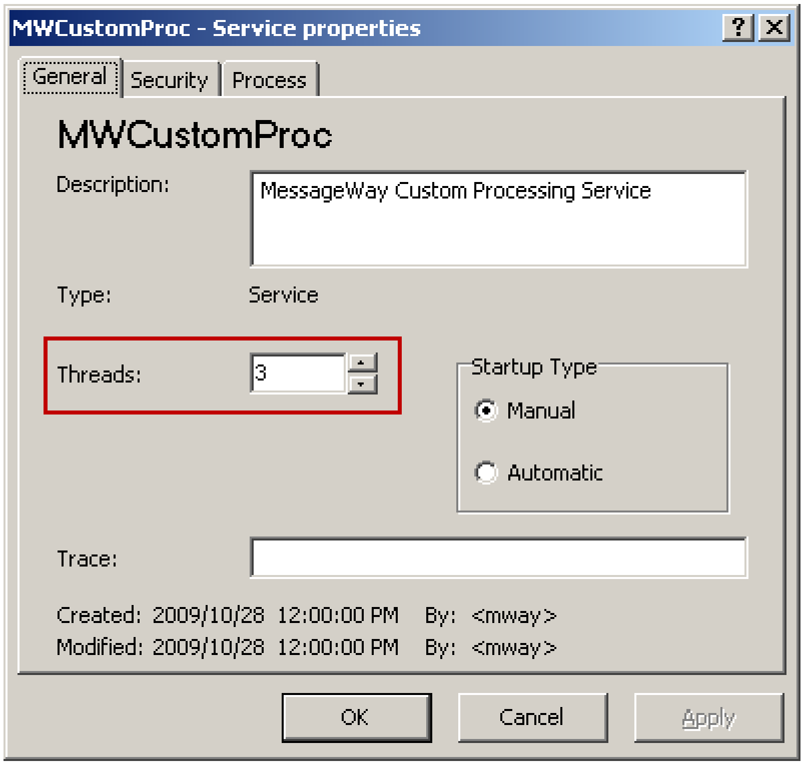
This service performs these basic functions, which are determined by the configurations on the custom processing service location:

- Send a data message to an external process, which will process the data and typically return files to MessageWay

  - or -
- Start an external process when a trigger message is sent to the service location, which may return files or not, but, typically, the file name of the trigger message is not passed to the external process

  - and -
- Upload files created by the external process to MessageWay

IMPORTANT: When using trigger messages to start a script specified for Custom Processing service locations, the number of threads must be greater than 1, because trigger messages are assigned a default priority of 5. Other messages should not compete with this priority and there must be a reserved thread available for these messages so they will always appear in the queue. Otherwise, the trigger messages may not be added to the queue and, therefore, not be processed.



MWCustomProc

Description: MessageWay Custom Processing Service

Type: Service

Threads: 3

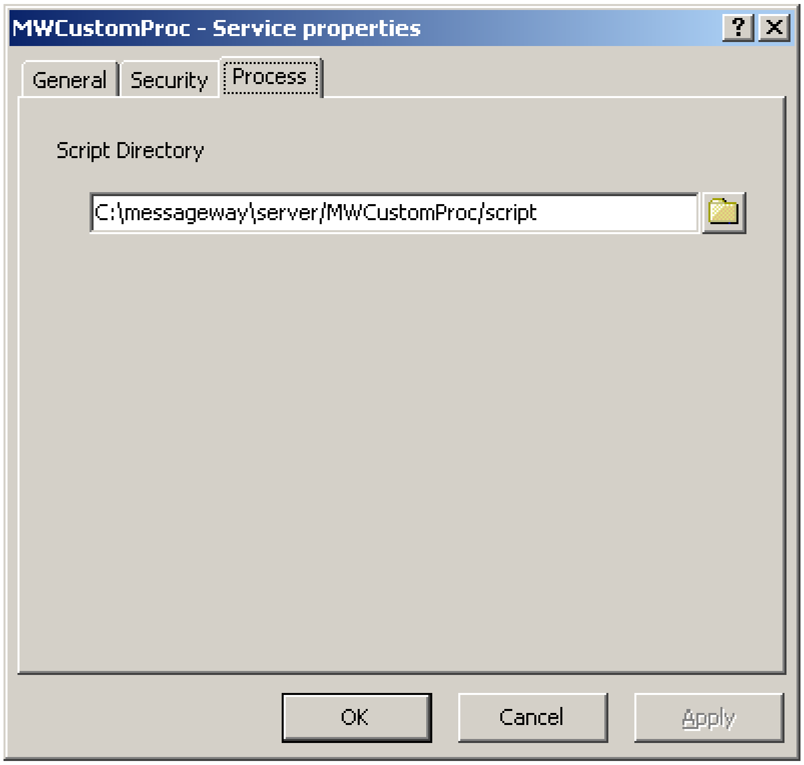
Startup Type
● Manual
○ Automatic

Trace:

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/10/28 12:00:00 PM By: <mway>

An external process may be a script or an external command. Scripts may be stored internally in MessageWay or externally. The Custom Processing Service configuration specifies the default directory for external script files. These files are called from the custom processing service location. The name of the script file appears in the **Command** box on the **Process** tab of the custom processing service location properties window.The directory for the script files appears on the **Process** tab of the Service Properties window.

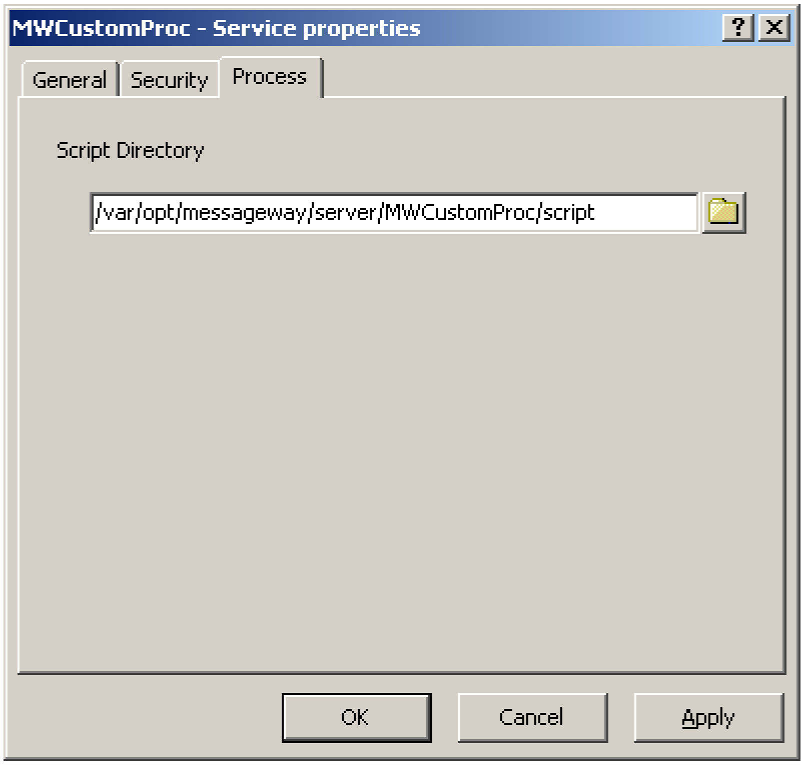
IMPORTANT: To avoid complications with mapped drives, always use the full Universal Naming Convention (UNC) directory name. A Windows service should not directly access local or network resources through mapped drive letters. MessageWay servers, which includes MWTranslator, run as Windows services.



Script Directory

C:\messageway\server/MWCustomProc/script

Process Page, Windows (Service Properties Window)



Script Directory

/var/opt/messageway/server/MWCustomProc/script

Process Page, UNIX/Linux (Service Properties Window)

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

For basic information about MessageWay adapters or services, refer to the section, ***Configuring Adapters and Services*** (on page 399). For generic information to configure a MessageWay adapter or service, refer to the sections in “MessageWay Manager Reference” for the ***Adapter or Service Properties window*** (on page 925). For most adapters or services, the last page of each window is specific to configurations required to transfer messages.

Configuring the Disk Transfer Adapter

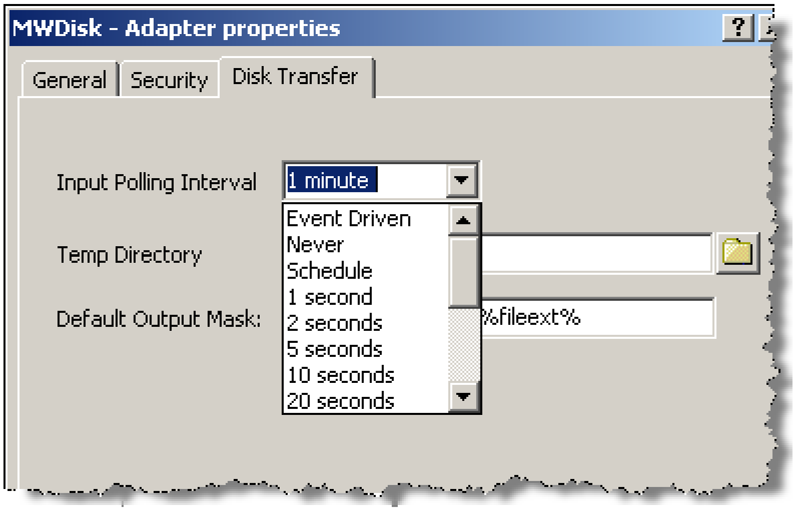
The Disk Transfer Adapter monitors a disk location for input files that it can move to the MessageWay Message Store. Users may change the setting for the adapter to poll for input messages. The disk location to be monitored for input and the disk location to which the adapter writes output data are specified on the site configurations. In one cycle, the adapter polls all locations specified in all site configurations associated with it and moves them to the Message Store.

Users may select an option from the Input Polling Interval drop-down menu or they may enter a value. Refer to the online help for this field for the syntax to enter a different value.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Example of Options for a Disk Transfer Adapter

The **Disk Transfer** page of the Adapter Properties window allows users to specify the polling option this adapter will use to transfer input data from disk to the Message Store. The adapter polls locations specified on Disk Transfer sites only when the schedules for the sites are open and a site is not on hold.



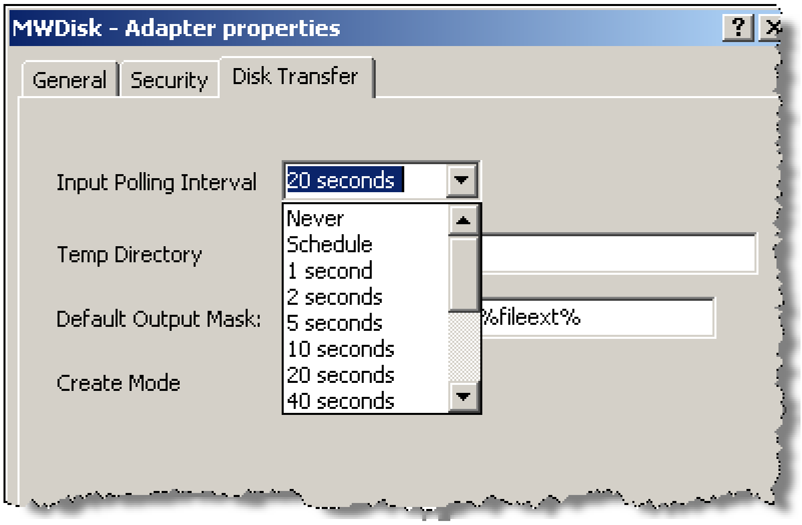
Input Polling Interval: 1 minute

Temp Directory:

Default Output Mask: %fileext%

Specifying Input Polling Interval for a Disk Transfer Adapter on Windows (Adapter Properties Window, Windows)

Note that *Event Driven* polling is not available for remote environments, such as those running on UNIX or Linux.



Input Polling Interval: 20 seconds

Temp Directory

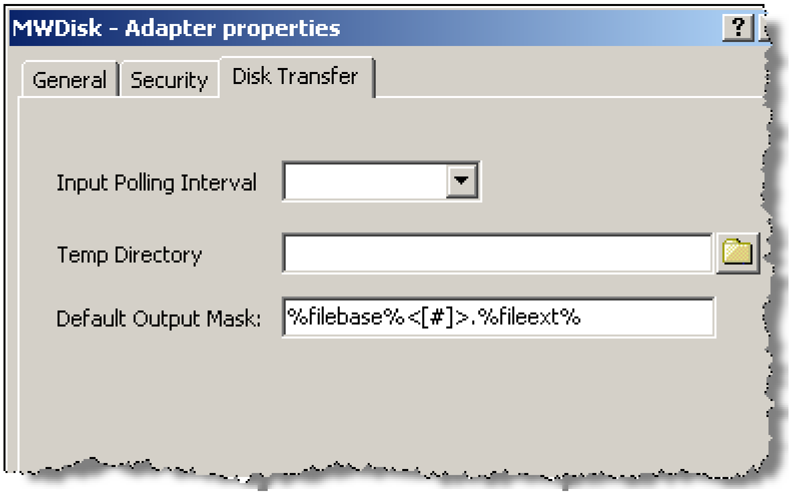
Default Output Mask: %fileext%

Create Mode

Specifying Input Polling Interval for a Disk Transfer Adapter on UNIX/Linux (Adapter Properties Window)

The **Temp Directory** and **Default Output Mask** ensure that a file will be delivered and complete.

CAUTION: Make sure you have a value in the **Default Output Mask** field. The install process provides a value, but if a user subsequently clears the field, messages may fail delivery attempts.



Input Polling Interval

Temp Directory

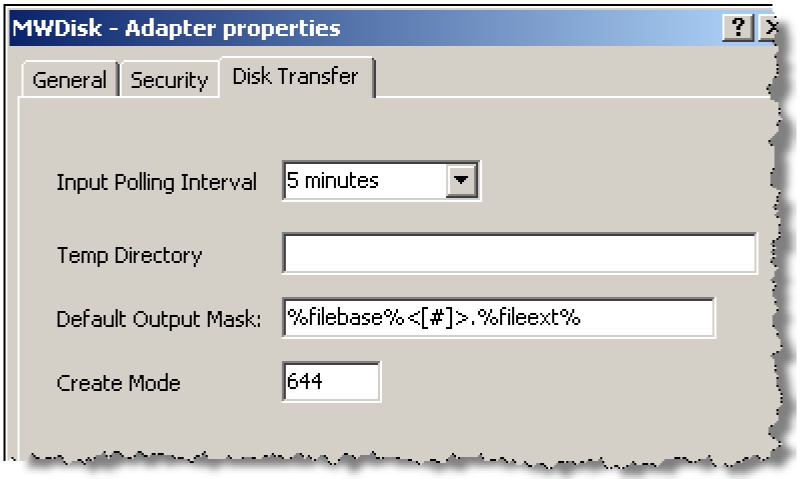
Default Output Mask: %filebase%<[#]>.%fileext%

Specifying Default Output Mask for a Disk Transfer Adapter on Windows (Adapter Properties Window)

The **Create Mode** option is only available for UNIX/Linux systems. Type a 3-digit numeric value to set the default file permissions when MessageWay creates a file. You may override these settings in the properties for a disk transfer site.

Each digit may be from 0 to 7, representing permissions, from left to right, for owner/user, group, and all other users. To set the rights for each entity, add the total of the values assigned to each right, where, 4 = read (r), 2 = write (w), 1 = execute (x) and 0 = none (-). For example, 644 would give read and write

(4+2=6) permissions to the owner/user, for example *mway*, and 4 would give read permissions to the group and others.



Input Polling Interval: 5 minutes

Temp Directory:

Default Output Mask: %filebase%<[#]>.%fileext%

Create Mode: 644

Specifying Default Output Mask for a Disk Transfer Adapter on UNIX/Linux (Adapter Properties Window)

For more information about these fields, refer to the topic, ***Disk Transfer Page (Adapter Properties)*** (on page 948).

Recommendations for Polling Options of a Disk Transfer Adapter

We recommend the default setting of Event Driven that is assigned during installation for local disks. When the file is on a network disk, you must specify a polling delay. Note that polling occurs only when the schedule for a Disk Transfer site is open. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

The following table shows users the effects of the various options:

Polling Option	Effect
Event Driven (local disks only)	Messages are transferred as soon as they appear on disk. Not available for a remote MessageWay Manager, such as for UNIX or Linux systems.
Never	The adapter does not process input messages. This may be overridden by setting polling for a specific location.
Time	Specifies the amount of time between attempts to transfer data from disk.

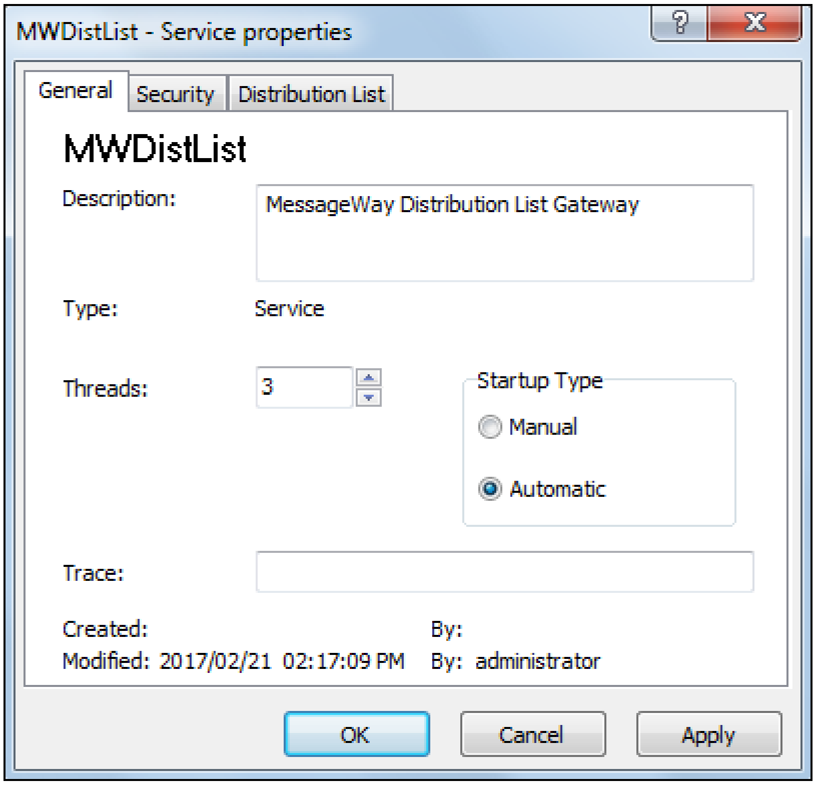
IMPORTANT: When you are using Disk Transfer to poll a location other than a LAN, make sure you allow enough time for the polling to occur without flooding the destination location with requests.

The Disk Transfer Adapter may poll remote locations on Windows Servers within the local network. Polling remote locations is not supported for UNIX or Linux.

Configuring the Distribution List Service

There is one special parameter to configure for the Distribution List Service, which can be found on the Distribution List tab.   See below for further details.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.



MWDistList - Service properties

MWDistList

Description: MessageWay Distribution List Gateway

Type: Service

Threads: 3

Startup Type
○ Manual
● Automatic

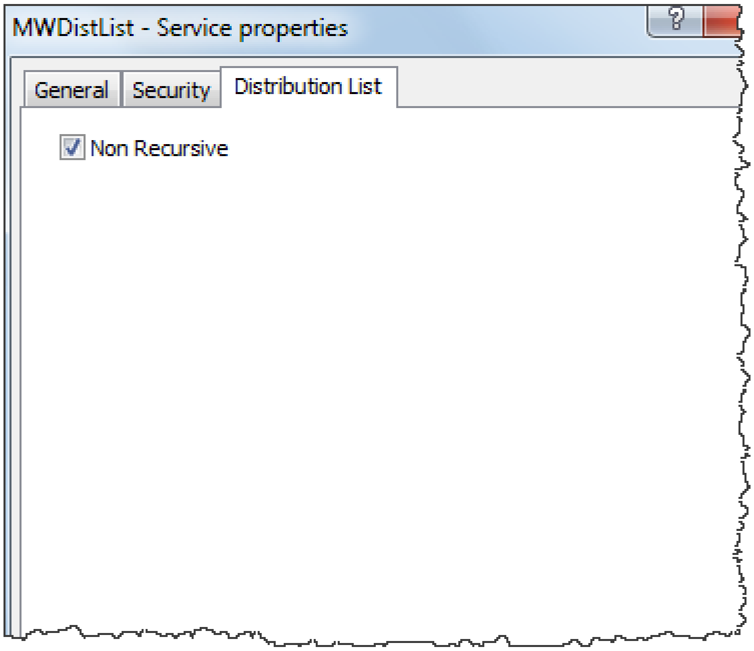
Trace:

Created: By:
Modified: 2017/02/21 02:17:09 PM By: administrator

Distribution List Service (Service Properties Window)

Example of Options for a Distribution List Service

The **Distribution List** tab of the Service properties window allows users to specify whether to use Non Recursive or not. This selection affects all Distribution List locations, and cannot be overridden on a location by location basis. When this box is checked, Distribution Lists will NOT evaluate recipients, but will instead create message aliases for all recipients, even those associated with another Distribution List. This will allow nested Distribution Lists to all be referenced in a 'Get Related' command, as well as any 'On Hold' or 'Closed' Distribution List status to be honored. Default is 'Recursive', and you must restart the Service for changes to take effect.



☑ Non Recursive

Specifying Non Recursive for a Distribution List Service (Service Properties Window)

Configuring the E-mail Adapter

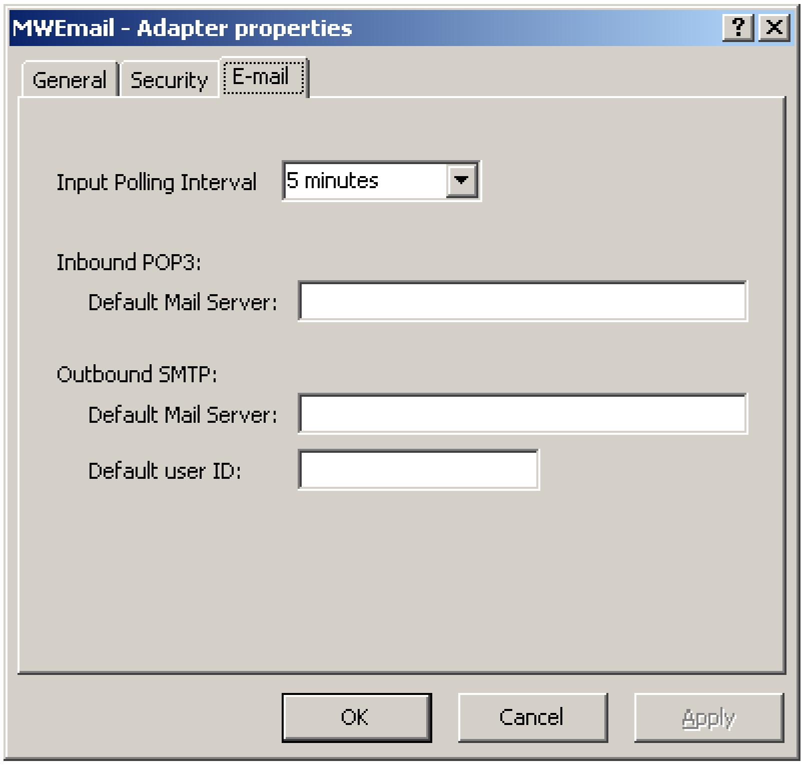
The E-mail Adapter is an e-mail client that contacts an e-mail server. Users may change the setting for the adapter to poll for input e-mail messages. Configurations to log on to the e-mail server and the e-mail addresses for receiving and sending messages are specified on the site configurations. In one cycle, the adapter polls all locations specified in all E-mail sites. It does not poll a site when its schedule is closed or when the site is on hold.

Users may select an option from the Input Polling Interval drop-down menu or they may enter a value. Refer to the topic ***Polling Interval*** (on page 957) for the syntax to enter a different value.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Example of Polling Options for an E-mail Adapter

The **E-mail** page of the Adapter Properties window allows users to specify the polling option the adapter client uses to transfer messages from a POP3 server to the Message Store, and to transfer messages from the Message Store to an SMTP server. The POP3 and SMTP fields will be used as defaults when you create locations that use this E-mail adapter.



Input Polling Interval: 5 minutes

Inbound POP3:

Default Mail Server:

Outbound SMTP:

Default Mail Server:

Default user ID:

Specifying Polling Interval and Logon for an E-mail Adapter (Adapter Properties Window)

Recommendations for Polling Options of an E-mail Adapter

We recommend the default setting of 5 minutes that is assigned during installation. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

The following table shows users the effects of the options:

Polling Option	Effect
Never	The adapter will not process input messages
Time	Specifies the amount of time between attempts to transfer data from disk.

IMPORTANT: When you are using E-mail to poll a location other than a LAN, make sure you allow enough time for the polling to occur without flooding the destination location with requests. The default of 5 minutes is probably a minimum amount of time for polling over the Internet, for example. Constant polling using any time less than five minutes might be viewed as an attack. One-second polling is only useful for testing on a local LAN.

The remaining fields are used to log on to an e-mail server and are also used as default values when configuring an e-mail adapter.

Configuring the File Transfer Protocol (FTP) Adapter

The File Transfer Protocol (FTP) adapter is an FTP SSL-enabled client. Users may change the setting for the adapter to poll for input messages and, optionally, specify the default location for the server security certificates. Users may also configure the adapter to communicate with an FTP perimeter server acting as a proxy, rather than directly with an external FTP server. In addition, users may check the integrity of data by performing hash calculations and comparing those with similar calculations from the server.

In one cycle, the adapter polls all locations configured for FTP input. It does not poll a location when its schedule is closed or when the location is on hold.

Users may select an option from the Input Polling Interval drop-down menu or they may enter a value. Refer to the topic, ***Polling Interval (Adapter Properties, FTP)*** (on page 959), for the syntax to enter a different value. For SSL connections, users must specify the location of the certificates. To specify a location for the server certificates, refer to the topic, ***Certificate Repository.*** (on page 963)

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

The FTP adapter performs the following basic steps:

1 At the polling interval, the adapter proceeds as follows:

a) Polling thread connects to the remote FTP server

b) Logs on to the server

c) Issues an NLST command

d) Logs off

e) Builds an internal queue that contains the list of file names returned by NLST.

2 One worker thread exists for each input thread configured in the FTP adapter, and those worker threads constantly monitor the internal queue.

3 When a worker thread finds a message in the internal queue, it does the following:

a) Logs on to the remote FTP server

b) Changes directory to the location specified in the input location configuration

c) Accesses the first non-busy file name from the internal queue

d) Marks the file name in the queue as busy

e) Issues a GET (retrieve) command for that file

f) Upon successful retrieval, the adapter:

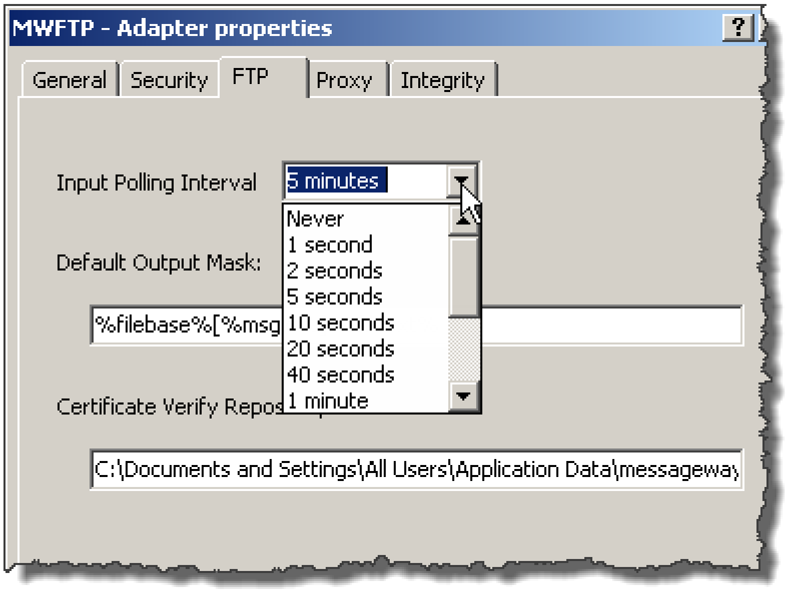
1. Optionally deletes the file from the remote server
2. Deletes the file name from the queue
3. Closes the connection

4 For additional files in the queue, repeat steps 1-3.

Example of Options for an FTP Adapter

The **FTP** page of the Adapter Properties window provides some basic default settings.

The **Input Polling Interval** field controls when the adapter attempts to connect to a remote FTP server to transfer messages to the MessageWay. The **Default Output Mask** field provides a default value for output file names, which may be overridden by a location configuration. The **Certificate Verify Repository** field provides the location for certificate bundles that are used during secure transfers. The location on disk shown here is the default location on Windows where test certificates are stored during installation. This test location varies depending on the operating system where MessageWay runs. You may store you certificate bundles elsewhere.



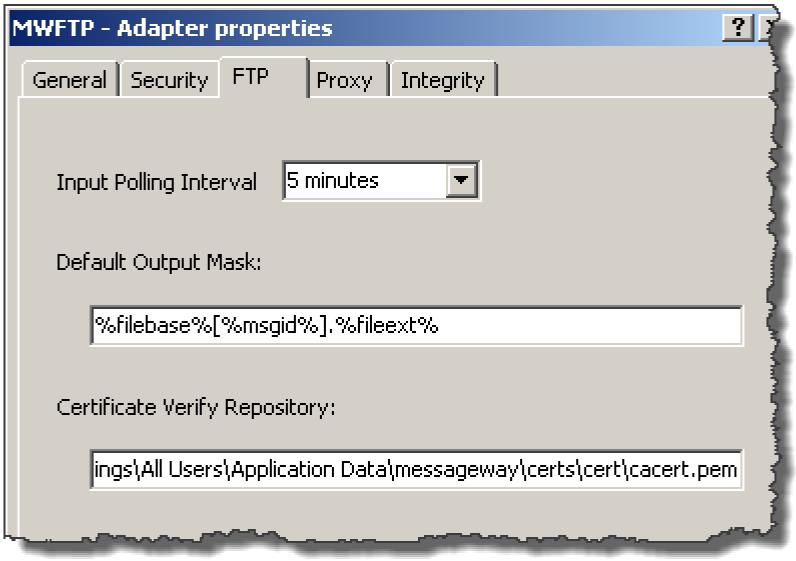
MWFTP - Adapter properties

Input Polling Interval: 5 minutes

Default Output Mask: %filebase%[%msg

Certificate Verify Repos

C:\Documents and Settings\All Users\Application Data\messageway



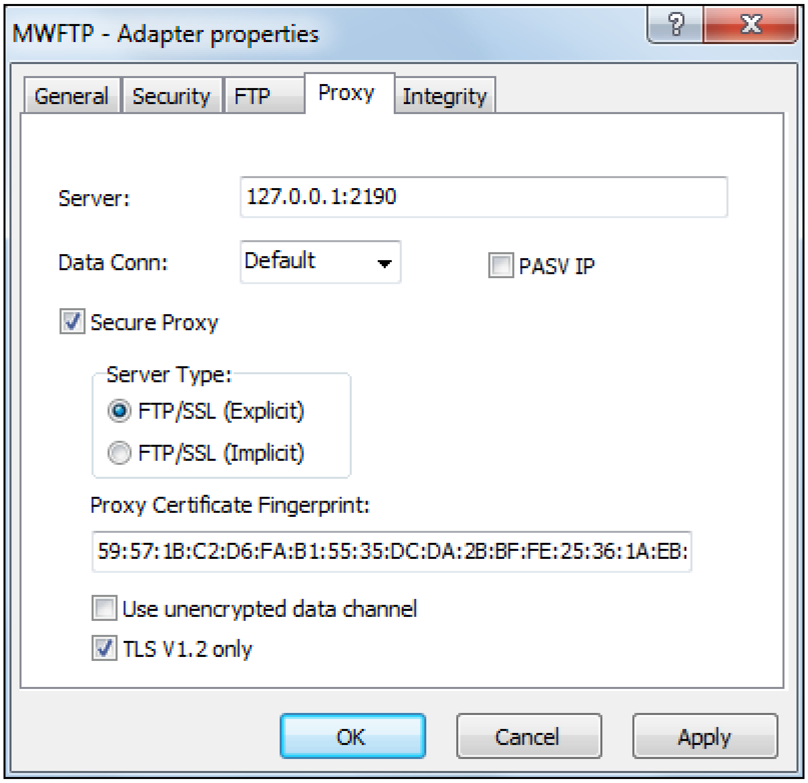
Input Polling Interval: 5 minutes

Default Output Mask: %filebase%[%msgid%].%fileext%

Certificate Verify Repository: ings\All Users\Application Data\messageway\certs\cert\cacert.pem

CAUTION: Make sure you have a value in the **Default Output Mask** field. The install process provides a value, but if a user subsequently clears the field, messages may fail delivery attempts.

You may also configure this adapter to communicate through the MessageWay FTP Perimeter Server, by completing the values on the **Proxy** page. These are default values for the FTP sites, which may override the settings. When the FTP perimeter server acts as a proxy for the adapter, it makes the connection to the external FTP server, which provides additional security for the adapter. The connection between the adapter and proxy server may also use SSL.



Server: 127.0.0.1:2190

Data Conn: Default

□ PASV IP

☑ Secure Proxy

Server Type:

● FTP/SSL (Explicit)

○ FTP/SSL (Implicit)

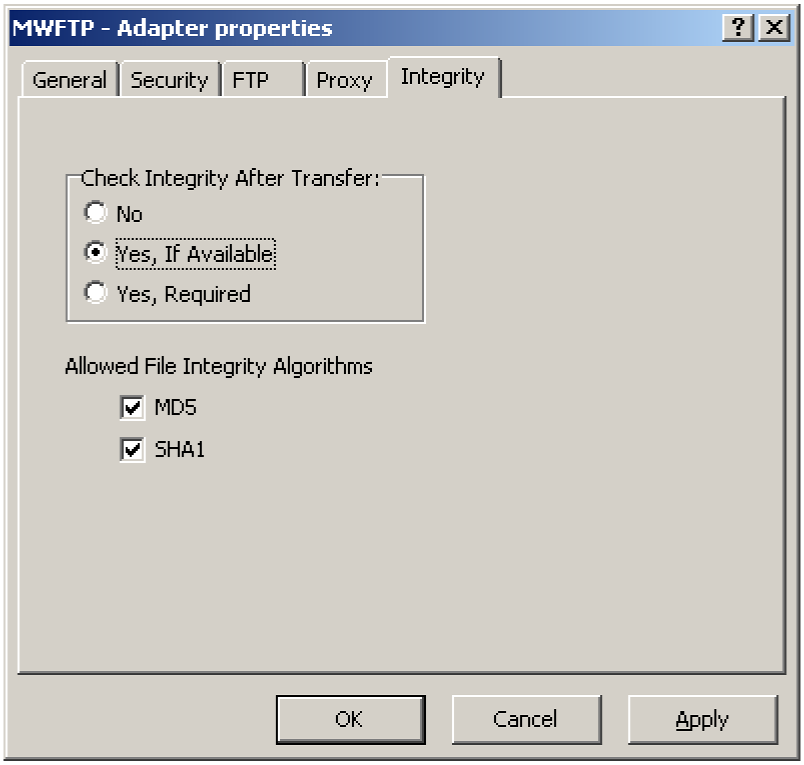
Proxy Certificate Fingerprint:

59:57:1B:C2:D6:FA:B1:55:35:DC:DA:2B:BF:FE:25:36:1A:EB:

□ Use unencrypted data channel

☑ TLS V1.2 only

As an option to enforce guaranteed delivery, users may also configure the adapter to perform hash calculations and compare them with hash values provided by the FTP server with which it communicates. The values for such integrity checks are on the **Integrity** page and provide default values for the FTP sites. Individual FTP sites may override these settings. Integrity checks work with all other FTP configurations, including input, output, SSL and proxy options.



Check Integrity After Transfer:
○ No
● Yes, If Available
○ Yes, Required

Allowed File Integrity Algorithms
☑ MD5
☑ SHA1

Recommendations for Polling Options of an FTP Adapter

We recommend the default setting of 5 minutes that is assigned during installation. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

The following table shows users the effects of the options:

Polling Option	Effect
Never	The adapter will not process input messages
Time	Specifies the amount of time between attempts to transfer data from an FTP server. This interval should include enough time to allow the system to connect to the FTP server.

IMPORTANT: When you are using FTP to poll a location other than a LAN, make sure you allow enough time for the polling to occur without flooding the destination location with requests. The default of 5 minutes is probably a minimum amount of time for polling over the Internet, for example. Constant polling using any time less than five minutes might be viewed as an attack. One-second polling is only useful for testing on a local LAN.

Recommendations for Integrity Checking for an FTP Adapter

If supported by the FTP server, MessageWay can perform a file integrity check on all transferred files. As part of the last step of the transfer, both the FTP client and the FTP server perform a cryptographic hash of the transferred file. If the values agree, both sides *know* that the file transferred is identical to the original.

This feature detects data modification so connection hijacking attacks (when an attacker reads, inserts, or modifies files in transit) can be detected in file transfers.

Although the result of an integrity check will vary depending on whether the check is optional (*Yes, If Allowed*) or required (*Yes*, *Required*), the basic file integrity check process is as follows:

- MessageWay FTP sites must be configured to support file transfer integrity, and:
  - On the **FTP Input** or **FTP Output** tabs, *Transfer Mode* must be set to **Binary**
  - On the **Integrity** tab, for *Yes, Required*, the *Append to file* options are *not* allowed on the **FTP Output** tab. If the append option and integrity are both invoked, an error occurs, and the user must disable one or the other. Append is not compatible with Integrity checks. If the **Append to** box is checked and integrity checking is mandatory, the transfer will fail, and an error will be logged to the error log and placed on the **Error** tab of the Message Properties window. If the **Append to** box is checked and integrity checking is optional, integrity will be ignored, the transfer will proceed, and a warning will appear on the **Misc** tab of the Message Properties window.

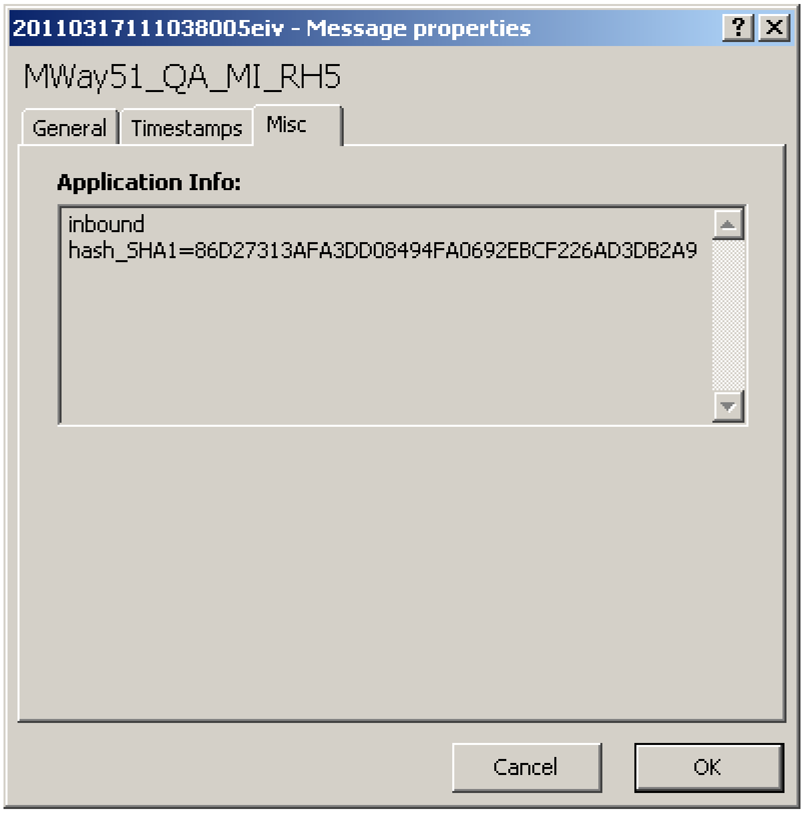
1 When integrity is enabled for an FTP site, MessageWay will check the integrity of the file as requested.

   a) First it will query the server about the algorithms that are selected. Moving from the strongest to the weakest, MessageWay will issue a FEAT command to the server to see if the server supports the algorithm.

   b) If the server returns an error, usually "500 command not supported", MessageWay will try the next algorithm.

   c) When it finds an algorithm that the server supports, MessageWay performs a hash calculation of the data using that algorithm and compares the results with the hash results of the same data returned from the server.

2 When the integrity check succeeds, the algorithm used and the hash value appear on the **Misc** tab of the Message Properties window.



Application Info:

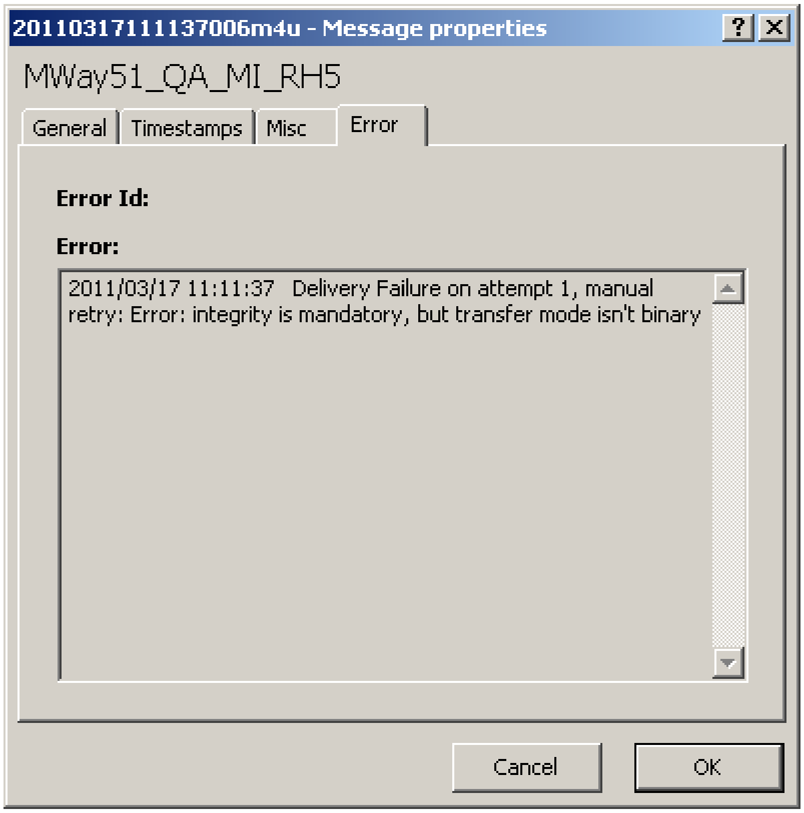
```
inbound
hash_SHA1=86D27313AFA3DD08494FA0692EBCF226AD3DB2A9
```

3 When the integrity check fails:

a) For optional integrity checks, if no file integrity algorithms on the list are supported by the server, then processing proceeds without an integrity check.

b) For required integrity checks, the message is marked with a state of *Error*, and error information appears on the **Error** tab of the Message Properties window, which may result from any of the following situations:

- Transfer mode is *not* binary for either input or output
- Both the Append to option on the FTP Output tab and integrity checking option on the Integrity tab are selected
- FTP server does *not* support integrity checks
- FTP server does *not* support any of the selected file integrity algorithms
- Hash values are *not* the same



Error Id:

Error:

2011/03/17 11:11:37 Delivery Failure on attempt 1, manual retry: Error: integrity is mandatory, but transfer mode isn't binary

IMPORTANT: The algorithm strength affects the time it takes to verify file integrity. The stronger the algorithm, the longer the transfer verification usually takes.

Configuring the MQ Adapter

CAUTION: Before you install the MQ adapter, you must first install the IBM WebSphere MQ Client, version 6, 7 or 9. For more information, refer to the appropriate IBM site.

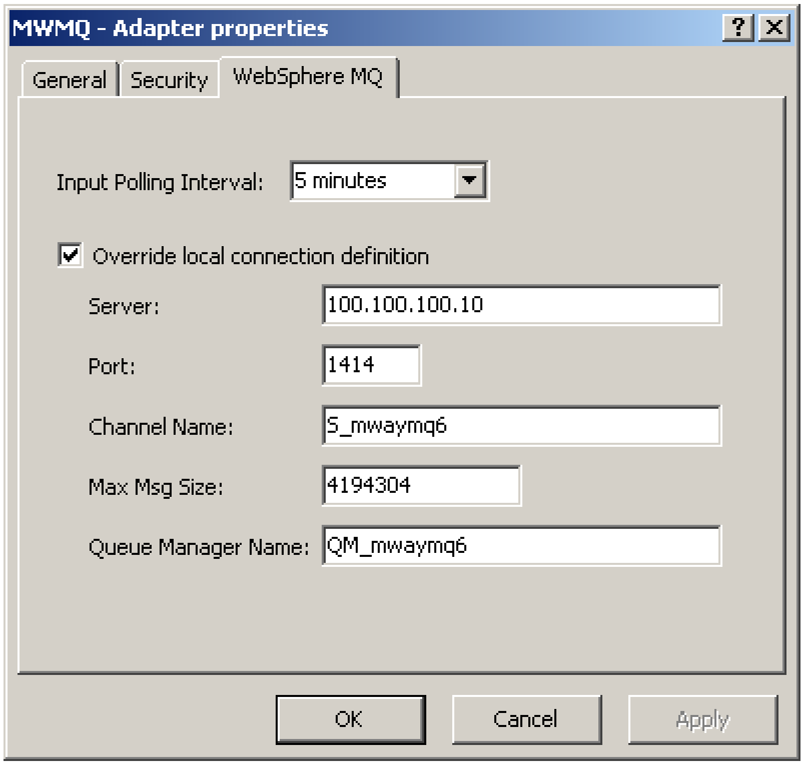
NOTE: The MessageWay MQ Adapter requires a license from Progress. You must have a license in order to start the adapter. For more information, contact MessageWay Technical Support.

The MessageWay MQ Adapter allows users to exchange files with IBM WebSphere MessageQueue (MQ), version 6, 7 or 9 over a TCP/IP connection. This feature uses the MQ client libraries, which you must install separately. Users should be familiar with the MQ client and MQ Manager software. For more information about the installation of the MQ client and WebSphere MQ, refer to the IBM site for WebSphere MQ Client for version 6, 7 or 9.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Examples of Options for an MQ Adapter

The **WebSphere MQ** page of the Adapter Properties window allows users to specify the polling option this adapter will use to transfer data over a TCP/IP connection between MessageWay and the MQ queue manager. The adapter polls locations specified on MQ sites only when the schedules for the sites are open and a site is not on hold.


MWMQ - Adapter properties

Input Polling Interval: 5 minutes

☑ Override local connection definition

Server: 100.100.100.10

Port: 1414

Channel Name: S_mwaymq6

Max Msg Size: 4194304

Queue Manager Name: QM_mwaymq6

Some default connection information is supplied by the adapter. You must determine the additional information based on how you have configured the MQ server. Such information should be available from those who support the MQ Manager. To override or add configurations:

1 Check the box **Override local connection definition**.
2 Type the IP address or name of the server.
3 To override the default, type the port number where the listener detects incoming connections. The default TCP/IP port for MQ is 1414.
4 Type the name of the channel that will handle this traffic between the MQ client and the MQ queue manager.
5 If necessary, type the maximum message size in bytes allowed for the MQ adapter. The default value for the adapter is 4 MB (4194304 bytes). The actual maximum message size that is allowed will be the

lower of the configured queue manager value, the configured queue value, the configured server connection value and this adapter value.

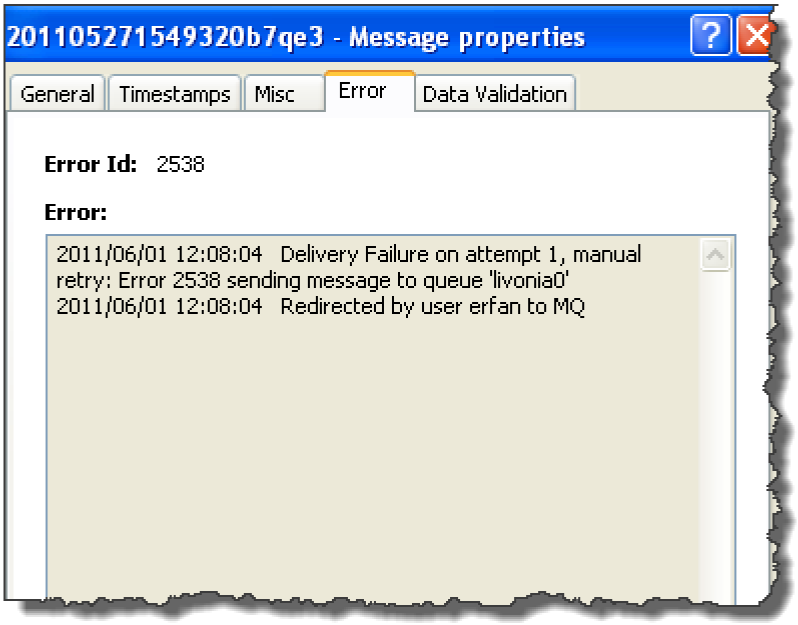
6 Type the name of the queue manager. If there is only one queue manager, you can leave this blank to default.

For more information about these fields, refer to the topic, ***MQ, WebSphere MQ Page (Adapter Properties)*** (on page 969).

Troubleshooting MQ Adapter Errors

Unlike most other adapters in MessageWay, many of the errors from MQ activity are defined by the WebSphere MQ application itself.

When you receive an error during an MQ transmission, the **Error** tab on the Message Properties window displays the error number and a brief message about the error, as shown in the following example.



Error Id: 2538

Error:

2011/06/01 12:08:04 Delivery Failure on attempt 1, manual retry: Error 2538 sending message to queue 'livonia0'
2011/06/01 12:08:04 Redirected by user erfan to MQ

To troubleshoot MQ adapter errors:

1 Display a list of messages with MQ adapter errors.

2 Double click the message in question.

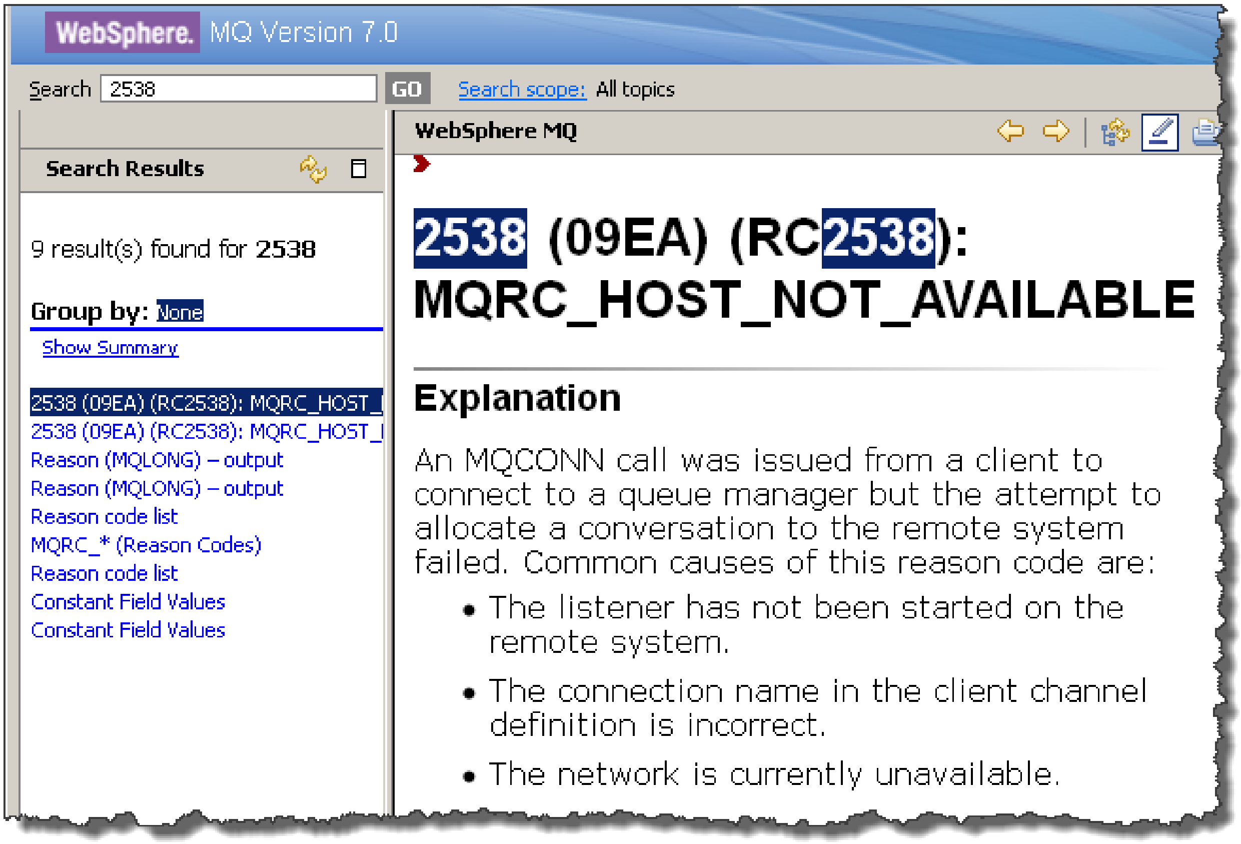
The Message Properties window appears.

3 From the Error tab, determine if the error is from MessageWay or WebSphere MQ.

4 For MessageWay errors, search for the error in the MessageWay Manager online help

- or -

For WebSphere MQ errors, access the WebSphere MQ site and search for the reason code, as in this example:



Search: 2538

9 result(s) found for 2538

2538 (09EA) (RC2538): MQRC_HOST_
2538 (09EA) (RC2538): MQRC_HOST_
Reason (MQLONG) – output
Reason (MQLONG) – output
Reason code list
MQRC_* (Reason Codes)
Reason code list
Constant Field Values
Constant Field Values

2538 (09EA) (RC2538): MQRC_HOST_NOT_AVAILABLE

Explanation

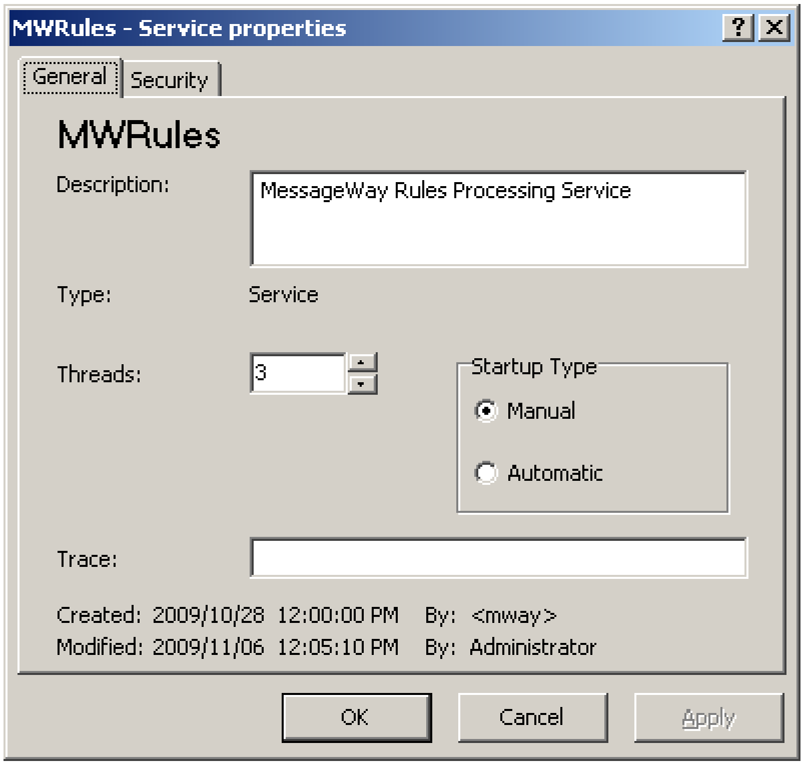
An MQCONN call was issued from a client to connect to a queue manager but the attempt to allocate a conversation to the remote system failed. Common causes of this reason code are:

- The listener has not been started on the remote system.
- The connection name in the client channel definition is incorrect.
- The network is currently unavailable.

Configuring the Rules Processing Service

There are no special parameters to configure for the Rules Processing Service, so there is no rules tab.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.



MWRules

Description: MessageWay Rules Processing Service

Type: Service

Threads: 3

Startup Type
● Manual
○ Automatic

Trace:

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/06 12:05:10 PM By: Administrator

Configuring the SFTP Adapter

NOTE: The MessageWay SFTP Adapter is included as part of the license for the SFTP Proxy Server and the SFTP perimeter server, although you install and configure them separately. For more information, contact MessageWay Technical Support.

The SFTP adapter is an SSH-enabled client that uses either SFTP or SCP (UNIX/Linux only) protocol. Users may change the setting for the adapter to poll for input messages, specify a default mask to create file names for output files, specify a default create mode for output files, and specify default ciphers, KEX algorithms and HMACs for establishing SSH connections. Users may also configure the adapter to communicate with the MessageWay SFTP Proxy Server, rather than directly with an external SFTP server.

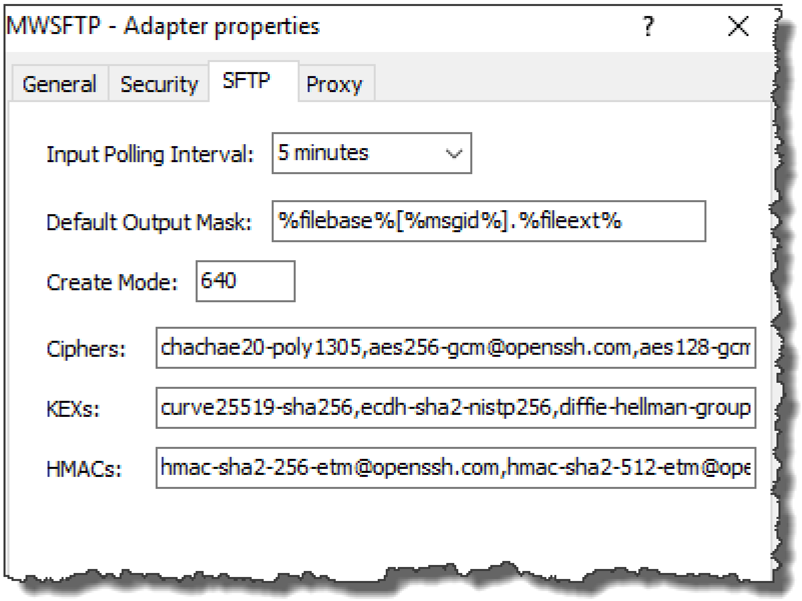
In one cycle, the adapter polls all locations configured for SFTP input. It does not poll a location when its schedule is closed or when the location is on hold.

Users may select an option from the Input Polling Interval drop-down menu or they may enter a value. Refer to the topic, ***Polling Interval*** (on page 972), for the syntax to enter a different value.

Example of Options for an SFTP Adapter

The **SFTP** page of the Adapter Properties window allows users to specify the polling option the adapter uses to transfer messages to and from an external SFTP server using this SFTP client.

You can specify a default polling interval, a default output mask, a default create mode, and default ciphers, KEX algorithms and HMACs. For reference information, refer to the reference topic, ***SFTP Page (Adapter Properties)*** (on page 971).



MWSFTP - Adapter properties

Input Polling Interval: 5 minutes

Default Output Mask: %filebase%[%msgid%].%fileext%

Create Mode: 640

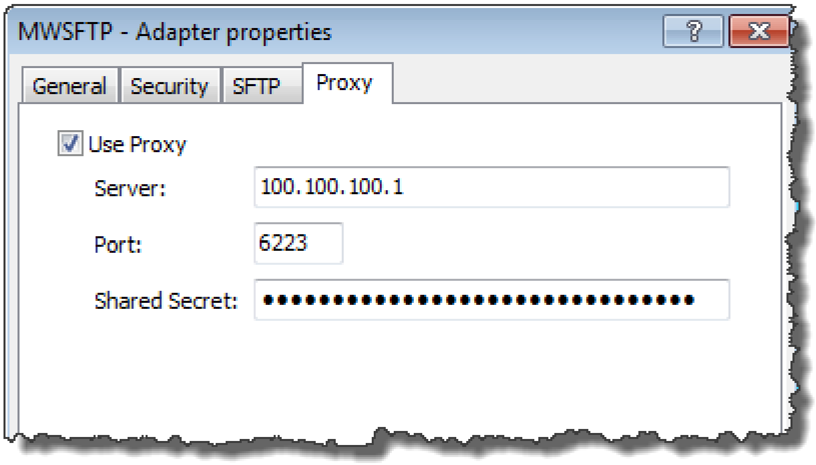
Ciphers: chachae20-poly1305,aes256-gcm@openssh.com,aes128-gcm

KEXs: curve25519-sha256,ecdh-sha2-nistp256,diffie-hellman-group

HMACs: hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@ope

CAUTION: Make sure you have a value in the **Default Output Mask** field. The install process provides a value, but if a user subsequently clears the field, messages may fail delivery attempts.

You may also configure this adapter to communicate with the MessageWay SFTP Proxy Server, by completing the values on the **Proxy** page to provide default values for the SFTP sites. Individual SFTP sites may override these settings. For reference information, refer to the reference topic, ***SFTP, Proxy Page (Adapter Properties)*** (on page 973).



MWSFTP - Adapter properties

☑ Use Proxy

Server: 100.100.100.1

Port: 6223

Shared Secret: ••••••••••••••••••••••••••••••••

Recommendations for Polling Options of an SFTP Adapter

We recommend the default setting of 5 minutes that is assigned during installation. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

The following table shows users the effects of the options:

Polling Option	Effect
Never	The adapter will not process input messages
Time	Specifies the amount of time between attempts to transfer data from an SFTP server. This interval should include enough time to allow the system to connect to the SFTP server.

IMPORTANT: When you are using SFTP to poll a location other than a LAN, make sure you allow enough time for the polling to occur without flooding the destination location with requests. The default of 5 minutes is probably a minimum amount of time for polling over the Internet, for example. Constant polling using any time less than five minutes might be viewed as an attack. One-second polling is only useful for testing on a local LAN.

Using an SFTP Proxy Server

The MessageWay SFTP Adapter communicates with an SFTP server, either directly or through the SFTP proxy server. The MessageWay SFTP Adapter and the MessageWay SFTP Proxy Server perform mutual authentication using a shared secret. You can configure the adapter to use the proxy server as a default for all locations. Then, if necessary, you can override that configuration for specific locations.

IMPORTANT: You must first install the MessageWay SFTP Proxy Server and the MessageWay SFTP Adapter. For instructions, refer to the MessageWay Installation Guide.

To configure the SFTP adapter to use the SFTP proxy server, proceed as follows:

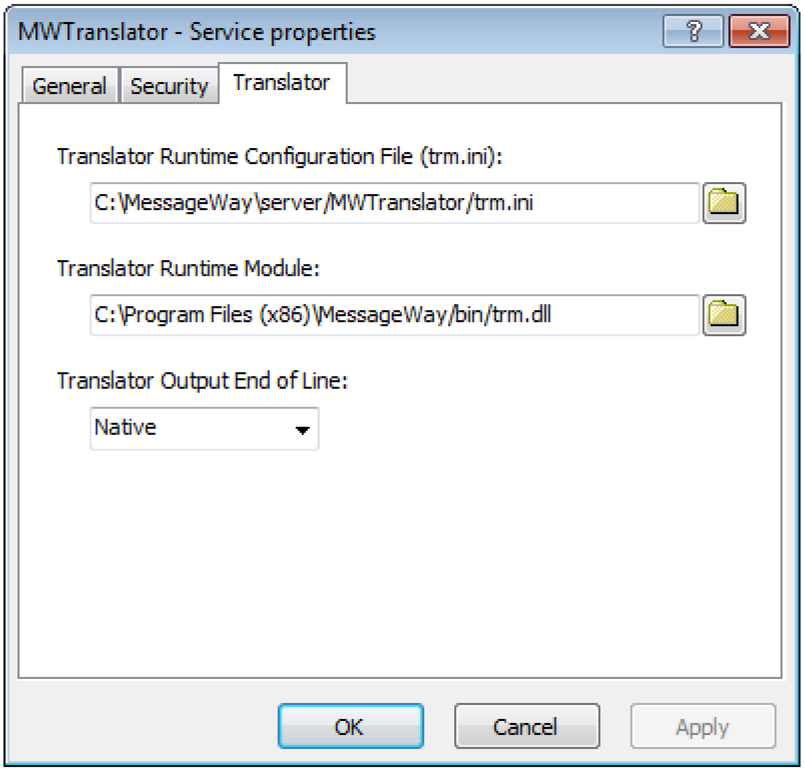
1. Using a text editor, ***modify the configurations file*** (on page 366) for the proxy server, mwproxy.conf, as needed.
2. Copy the value for the SharedSecret parameter from mwproxy.conf.
3. From the MessageWay Manager, view the **Proxy** tab of the SFTP adapter properties window.
4. Check the **Proxy** box.
5. In the **Shared Secret** box, paste the value you copied from the configuration file.
6. In the **Server** box, type the IP address of the proxy server.
7. In the **Port** box, type the port on which the proxy server listens, such as **6223**.
8. Click **Apply** or **OK** to save your configurations.

Configuring the Translation Service

NOTE: The MWTranslator service requires a license from Progress. You must have a license in order to start the service. Contact MessageWay Technical Support for more information.

The MWTranslator Service controls the Translator Runtime Module (TRM). When you start or stop the MWTranslator, it starts or stops the TRM. The **Translator** page provides flexibility to users when testing. Users may change the following additional settings for the MessageWay Translation service:

- Location of the Translator Runtime configuration file (trm.ini)
- Location of the Translator Runtime Module (TRM) (trm.dll for Windows and trm.so for UNIX/Linux)
- Translator Output End-of-Line specifies the format to use for text mode output from the translator (allows for differences between default settings of previous MessageWay releases)
  - Native (default, and matches 4.2 behavior)
  - CR/LF
  - NL
  - Unchanged (matches 5.0 behavior to use NL in place of CR/LF)



Translator Runtime Configuration File (trm.ini): C:\MessageWay\server/MWTranslator/trm.ini

Translator Runtime Module: C:\Program Files (x86)\MessageWay/bin/trm.dll

Translator Output End of Line: Native

The TRM provides translation services. The configuration file contains the information that the TRM requires in order to process the input data, including where the other configuration files are located and the method of generating control references.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

For basic information about MessageWay adapters or services, refer to the section, ***Configuring Adapters and Services*** (on page 399). For generic information to configure a MessageWay adapter or service, refer to the sections in “MessageWay Manager Reference” for the ***Adapter or Service Properties window*** (on page 925). For most adapters or services, the last page of each window is specific to configurations required to transfer messages.

The default locations assigned during installation are recommended for production environments. They vary depending on the operating system.

The default locations for MWTranslator on a Windows system are as follows:

File	Default Location
MWTranslator Configuration	..\MessageWay\server\MWTranslator\trm.ini
Translator Runtime Module	..\Program Files\MessageWay\bin\trm.dll

The default locations for MWTranslator on a UNIX/Linux system are as follows:

File	Default Location
MWTranslator Configuration	../var/opt/messageway/server/MWTranslator/trm.ini
Translator Runtime Module	../opt/messageway/bin/trm.so

Users may need to change the assignment, typically for testing purposes.

This page intentionally blank.

Configuring Remote Access Environments

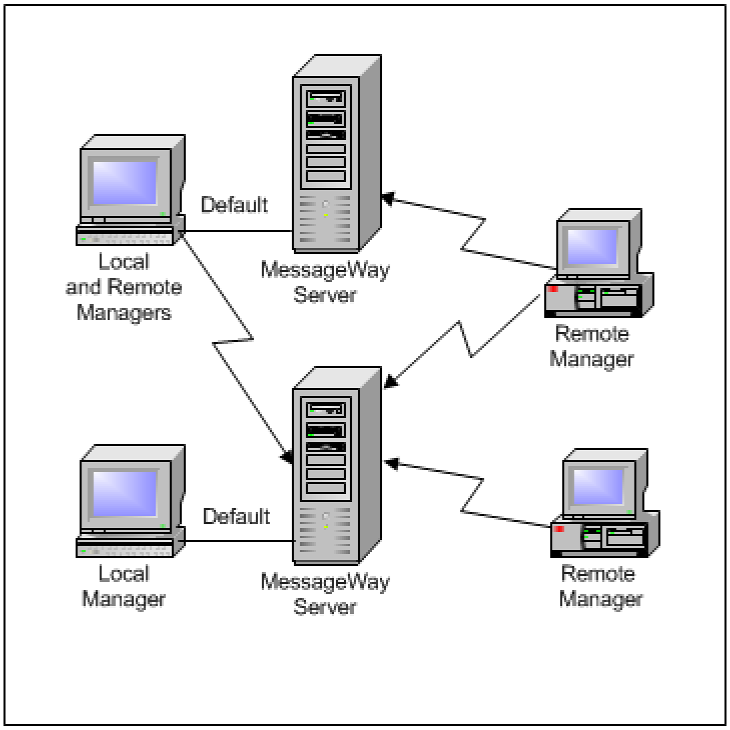
This information explains how users configure a system to access a remote MessageWay environment by creating environments for one or more systems.

Overview of Remote Access

There is only one MessageWay Server per machine. The server and all of its components and database configurations constitute a MessageWay system. The MessageWay Server Properties configurations apply to this single system. However, users may create an environment that includes multiple systems, a multi-system environment.

Users access an environment using the MessageWay Manager within the same local area network (LAN) or wide area network (WAN). The initial environment installed with MessageWay is called Default. When users create additional environments, they create an environment name and can include up to 4 MessageWay systems.

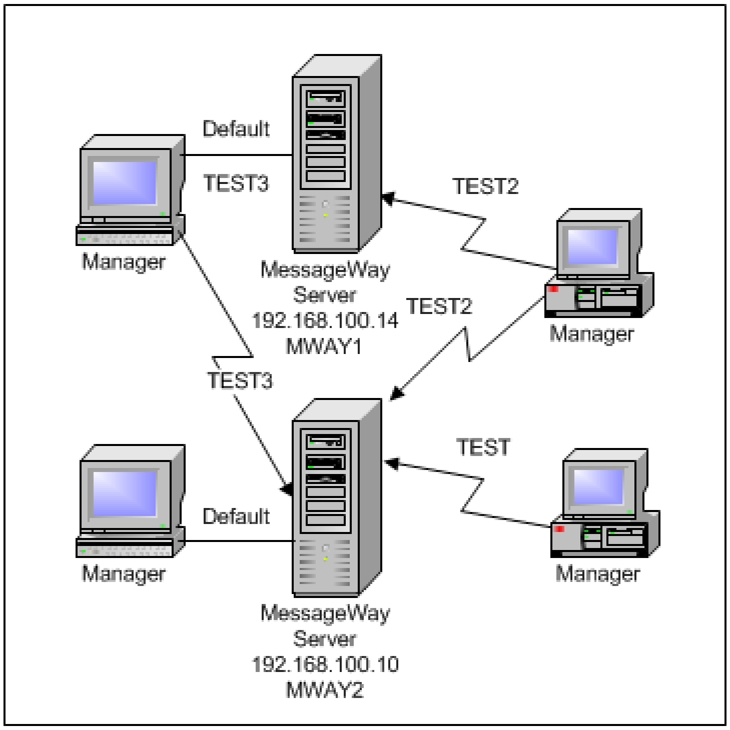
Users select the MessageWay environment that they want to access, and configure an environment with its own Connection Options.



Understanding Environments

Each instance of the MessageWay Manager connects to one server environment at a time, which the user names. Each environment includes up to 4 systems, which the user also names. The configurations for each system determine the type of connection. In the following figure, there are default environments, and user-named environments called TEST, TEST2 and TEST3, each representing a different server or servers and their database environments. In the following example, notice that the environment names vary, though they point to the same system (Default and TEST3).

The current environment and server appear in the title bar, as shown here for TEST, mway-pm. The remote user named the environment TEST, which points to the mway-pm server.



Creating and Selecting Environments

Remote users must first add an environment to their list that points to the MessageWay Server to which they want to connect.

IMPORTANT: Before users can do anything, they must be connected to the remote system, such as being logged on the local area network (LAN), wide area network (WAN), or over the Internet, typically using a Virtual Private Network (VPN).

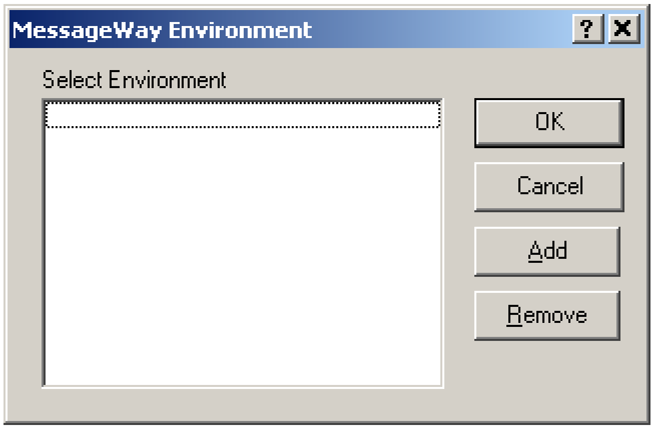
Required Security Access

Users must have a valid user ID and password to log on to the remote MessageWay system. For more information, contact your system administrator.

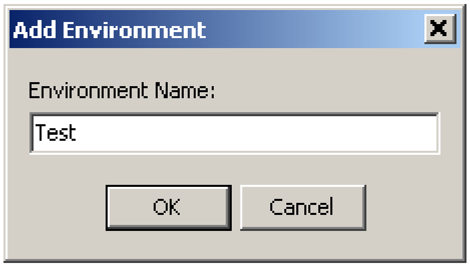
How to Create an Environment

1 From the MessageWay Manager, click the **Select Environment** button .

The **MessageWay Environment** dialog box appears. When the server is not on the same system as the Manager, the **Select Environment** list will initially be blank.

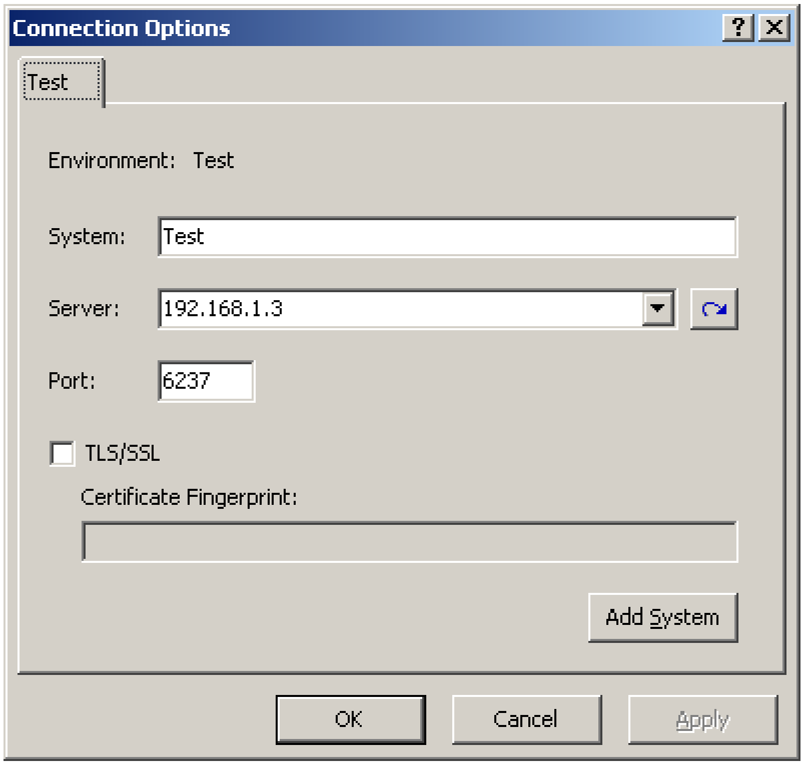


2 Click the **Add** button, and when the **Add Environment** dialog box appears, type a name for the remote environment, and click **OK**.



Environment Name: Test

The Connection Options window appears for an environment named what you created with a system of the same name.



Environment: Test

System: Test

Server: 192.168.1.3

Port: 6237

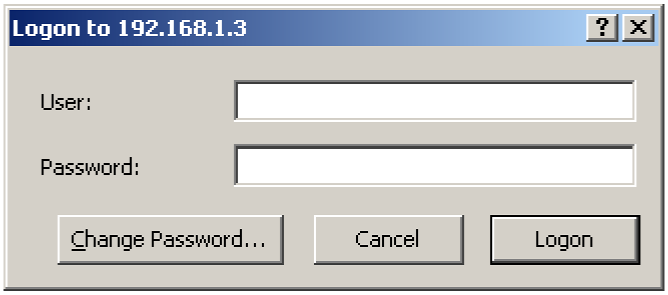
□ TLS/SSL

Certificate Fingerprint:

NOTE: For specific information about the fields on the Connection Options window, refer to the reference topic, ***Connection Options Window*** (on page 976).

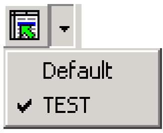
3 Click **OK**.

4 Once a user has completed these tasks, the Manager points to the remote environment, and, if the Manager has been able to connect to the MessageWay database on the remote system, a logon window appears to allow the user to log on to the MessageWay system.



Switching Environments

Once environments are added to the list of a MessageWay Manager, users may switch among environments. This is very useful for testing and general management.



1 To select an environment, click the **Select Environment** drop-down list button , which displays a list of defined environments.

When the user selects an environment, the title bar reflects the change, displaying the name of the environment, TEST, the name of the server and its IP address.

2 If necessary, log on to the remote system.

Users must log on to a remote system the first time they access it during their session, but not thereafter.

How to Add Multiple Systems to an Environment

You can add up to four systems to an environment to do the following:

- Monitor combined statistics from all systems in the Systems Monitor
- Configure and operate multiple systems individually without switching environments

After you create an environment, you can add more systems to the environment from the Connection Options window, as follows:

1 From the MessageWay Manager, select the environment, for example Test.

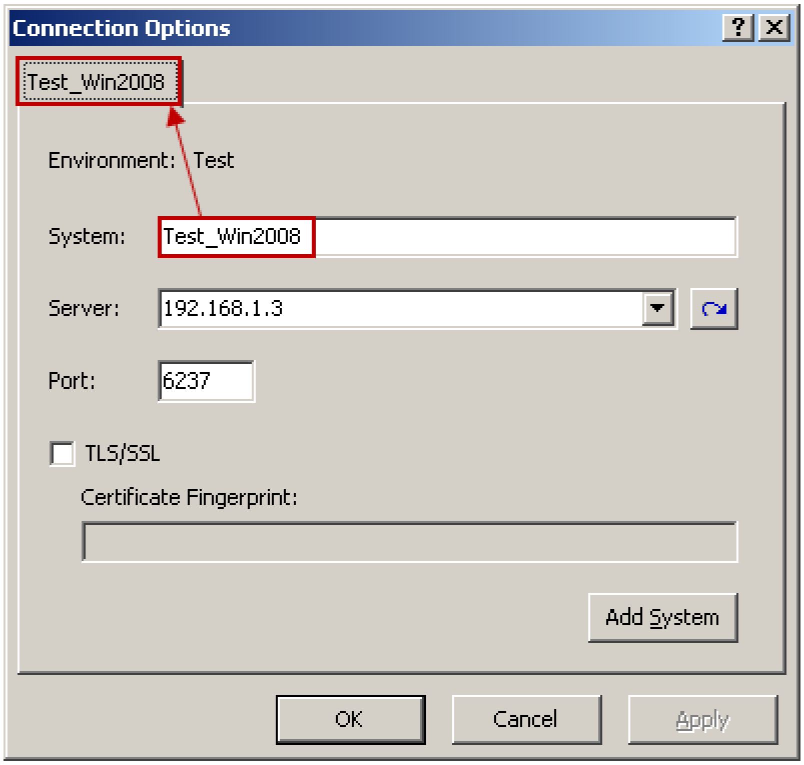
2 From the MessageWay Manager task bar, click the **Connection Options** button, .

The Connection Options window appears for an environment named what you created with a system of the same name.

NOTE: For specific information about the fields on the Connection Options window, refer to the reference topic, ***Connection Options Window*** (on page 976).

3 In the **System** box, type a name to represent the first system in the environment.

CAUTION: There is a known limitation on the *combined* number of characters that you can enter for names of multiple systems, which is 59. When you exceed the limitation in the second system, you will not be able to delete the first system and the manager locks when to try to do so.

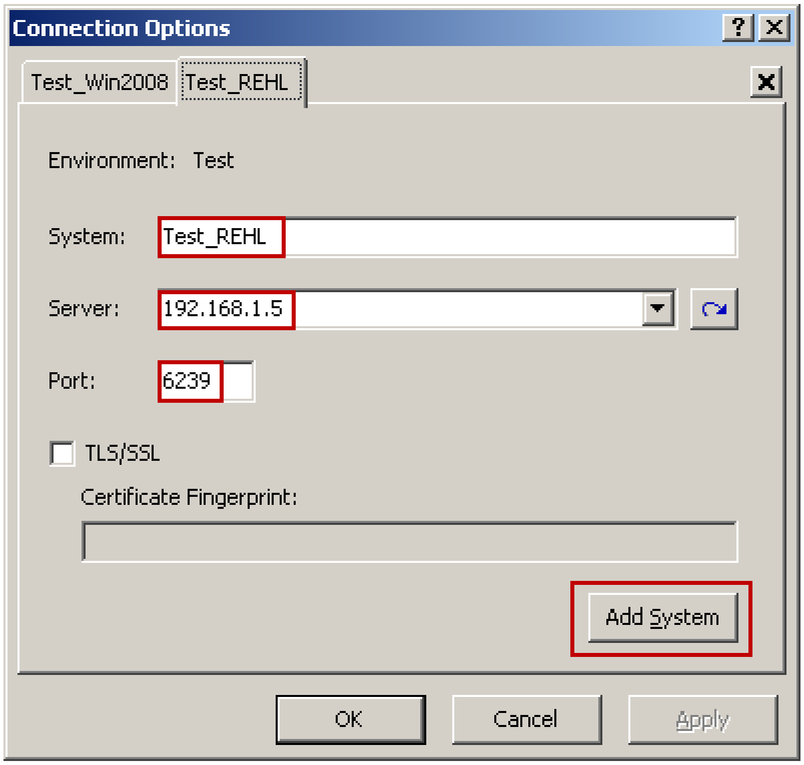


4 To add a second system to the environment, click the **Add System** button.

A second tab appears with a default system name, System2.

5 Type the name of the second system, the server and the port.

The system name appears on the tab.



Environment: Test

System: Test_REHL

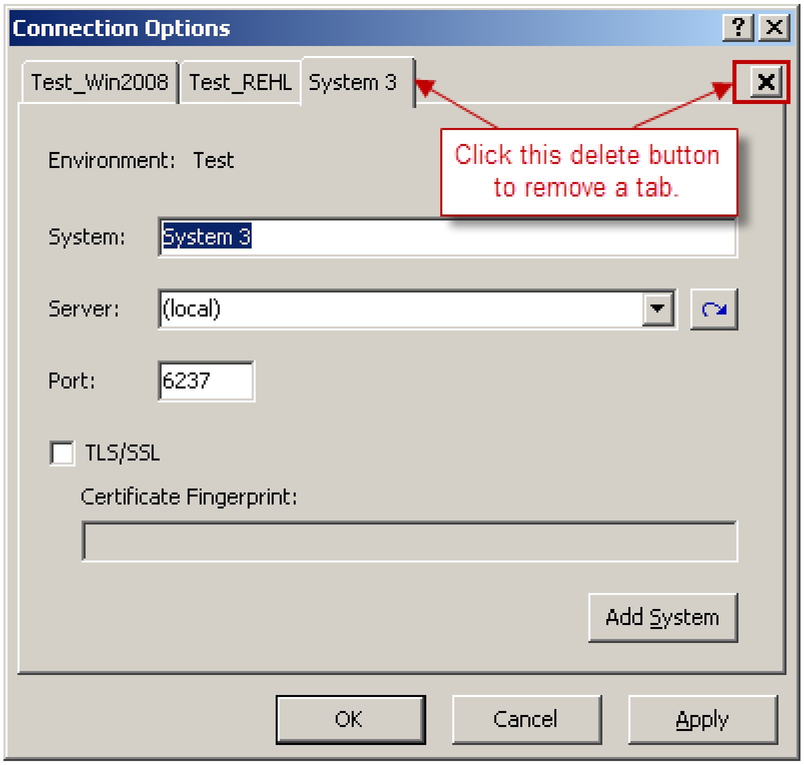
Server: 192.168.1.5

Port: 6239

☐ TLS/SSL

Certificate Fingerprint:

To remove a tab, select the tab and click the delete button, ☒, to the right of the tabs.



Click this delete button to remove a tab.

Environment: Test

System: System 3

Server: (local)

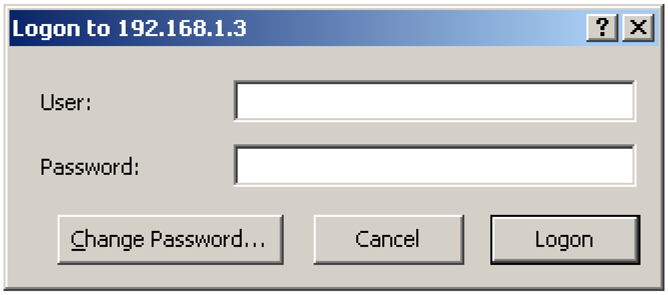
Port: 6237

☐ TLS/SSL

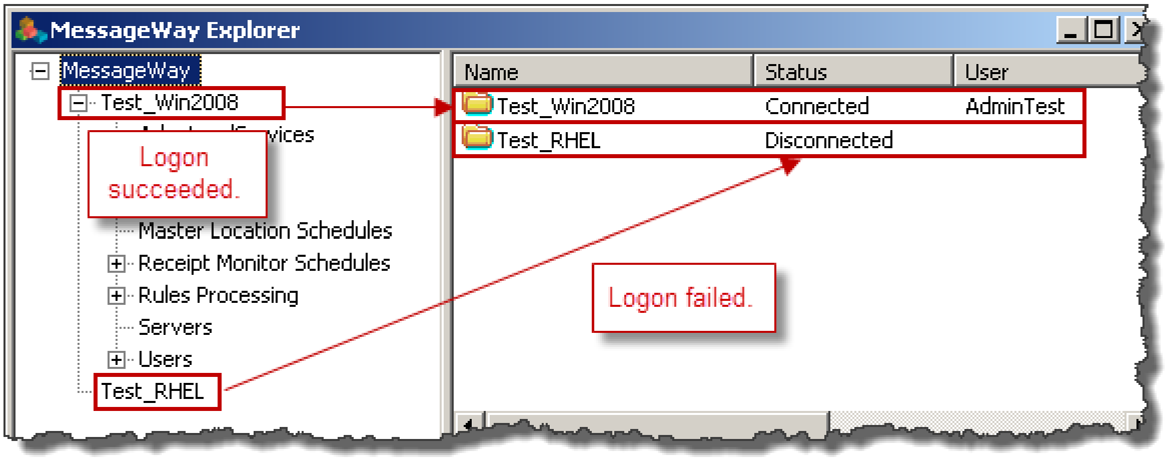
Certificate Fingerprint:

6 Click **OK**.

7 Once a user has completed these tasks, the MessageWay Manager points to the remote environment, and, if the Manager has been able to connect to the MessageWay database on the remote system, a logon window appears to allow the user to log on to each system.



8 The MessageWay Explorer window appears to show whether the logon succeeded, status will be *Connected*, or failed, status will be *Disconnected*.



Name	Status	User
Test_Win2008	Connected	AdminTest
Test_RHEL	Disconnected	

Logon succeeded.

Logon failed.

This page intentionally blank.

Configuring Locations

This section explains how to configure locations by setting their properties. Some types of locations are associated with adapters or services that are purchasable options and require additional licenses, as indicated for the location type.

There are two systems to create locations. One system is under the *Locations* folder and the other is under the *File System* folder. They are similar in their configuration options and requirements, but they differ in the way information is presented to remote users. The Locations folder provides a view for all remote users that shows messages based on the status of the message. The File System folder is only for remote FTP and SFTP clients whose users prefer a typical hierarchical directory structure that they can view and maintain themselves. These two systems operate independently in MessageWay and the location and messages in the two folders are separate. You can move locations and messages between the Locations and File Systems folders, if the message and location names meet the requirements of the destination folder.

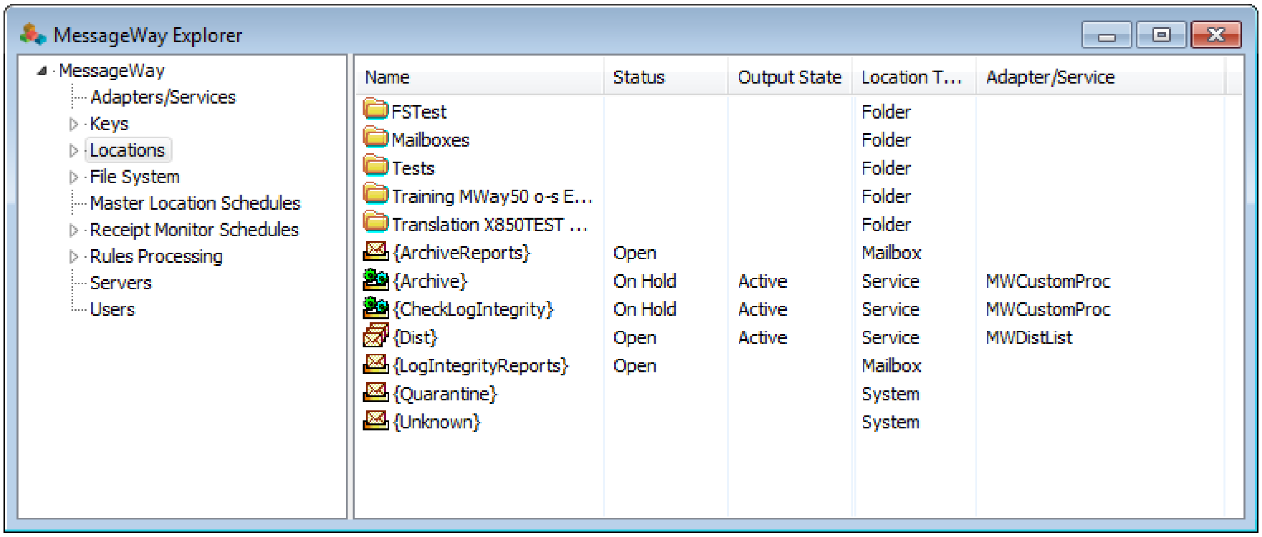
Overview of Location Properties

Locations specify the configurations to transfer messages to and from the Message Store based on sender and recipient requirements. MessageWay Explorer provides users with a list of all configured locations and their current status.

There are two ways for remote clients using the FTP and SFTP perimeter servers to view their messages: the normal MessageWay view and a new hierarchical, directory type view. To support both client views, locations have been separated into a *Locations* folder and a *File System* folder. Locations created under one folder are independent of the other folder, and they have different characteristics. Which system the client views depends on the value in *Default Location* for the user. When the default location for a user starts with a forward slash /, the remote client views the File System directory structure, otherwise it views the Locations structure.

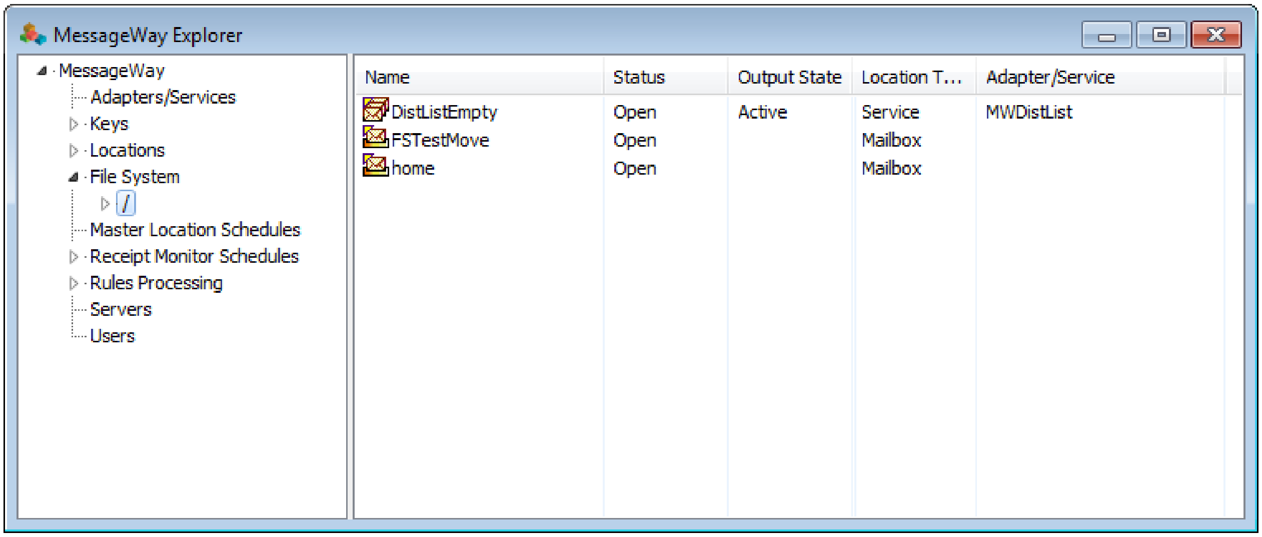
The characteristics of the two folders also varies when viewed from MessageWay Manager. Here is a sample view from MessageWay Manager of the contents of the Locations folder. Notice that in addition to locations it contains folders, such as *Tests*, as well as system locations, such as *{Unknown}*. Remote users have no ability to create folders or locations, only send and collect messages. You control the content of the Locations folder only from MessageWay Manager.

NOTE: When remote users access MessageWay, for example from FTP or SFTP client software, they will view messages within a predefined directory structure, which is their default mailbox as the highest directory with two subdirectories *Downloaded* and *Canceled*.



Name	Status	Output State	Location T...	Adapter/Service
FSTest			Folder	
Mailboxes			Folder	
Tests			Folder	
Training MWay50 o-s E...			Folder	
Translation X850TEST ...			Folder	
{ArchiveReports}	Open		Mailbox	
{Archive}	On Hold	Active	Service	MWCustomProc
{CheckLogIntegrity}	On Hold	Active	Service	MWCustomProc
{Dist}	Open	Active	Service	MWDistList
{LogIntegrityReports}	Open		Mailbox	
{Quarantine}			System	
{Unknown}			System	

Here is sample view from MessageWay Manager of the contents of the File System folder. The first level of the directory or root is signified by a forward slash (/). Note that a directory such as the root contains service locations and mailboxes, but no folders nor any system locations or sites (locations for adapters). Remember that the File System folder is primarily for remote FTP and SFTP clients as an alternative way to view their messages as if they were looking at a more traditional hierarchical directory structure. Remote users can build and maintain the directory structure themselves. When necessary, you can control the content of the File System folder from MessageWay Manager.

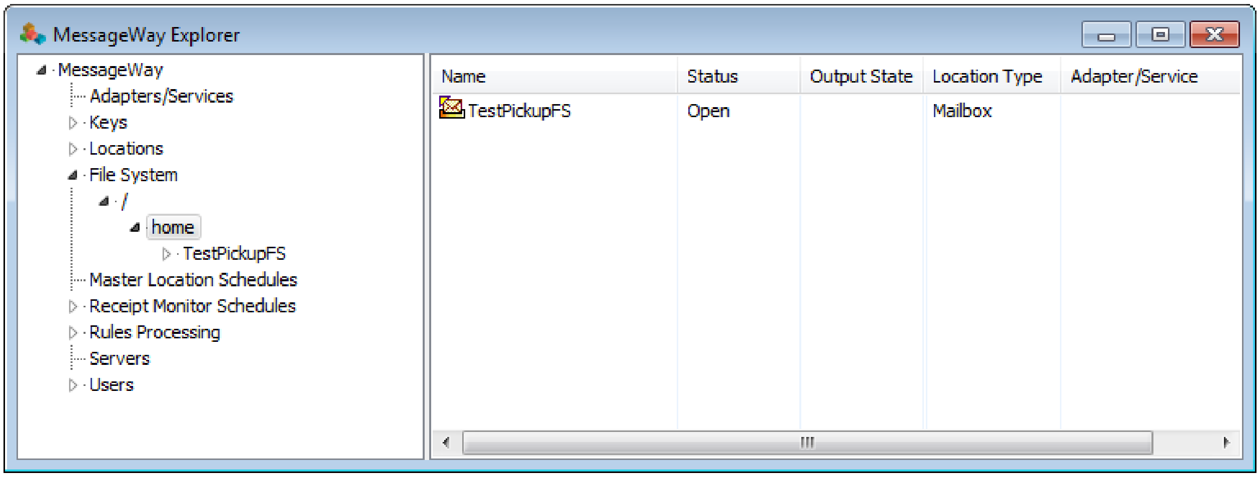


Name	Status	Output State	Location T...	Adapter/Service
DistListEmpty	Open	Active	Service	MWDistList
FSTestMove	Open		Mailbox	
home	Open		Mailbox	

Also note that for the File System folder, the left pane displays the directory structure and the right pane displays the locations within the selected directory. In this view, the *Home* subdirectory contains locations in the right pane with the same names as its subdirectories in the left pane. For example, *FS_Tests* is both the name of a mailbox and the name of a subdirectory. This is because the location functions as both a location and a container node in the directory structure. The name of a location is actually the full path name of the node in the directory where it resides.

NOTE: When you double-click a location in the right pane, the default action is *Explore*, which expands the directory in the left pane, and displays the next level of locations/subdirectories in the right pane. This contrasts with the default action of *Properties* under the Locations folder, which displays the location properties window. To view the properties of a location under File System, you must right-click the location and select **Properties**.

When FTP and SFTP clients access MessageWay, they will view messages within a directory structure as shown in the left pane of MessageWay Explorer.



Name	Status	Output State	Location Type	Adapter/Service
TestPickupFS	Open		Mailbox	

The following table compares the systems.

	Original Location (Locations Folder)	**Hierarchical Location (File System Folder)**
Location structure	Allows manager users to create multiple levels of folders to manage locations. These folders are only visible from MessageWay Manager. Folders are not visible to remote clients, and are not used during MessageWay processing. Manager users can create folders only for original locations, not File System locations	Allows FTP and SFTP clients to view messages within a file system type structure with sub-directories. When manager users create a location, a Directory is added automatically under the root folder /. The directory has the same name as the location. When remote users add a directory under their default location, they actually create a new pickup mailbox with the same name as the directory. The directory is only a representation of the location hierarchy, since locations here are also containers.
Inherited rights	Rights may be inherited from parent folders	Rights may be inherited from parent locations

	Original Location **(Locations Folder)**	**Hierarchical Location** **(File System Folder)**
Location names	Requires unique names throughout the Locations folder	Allows the same location names to be used at various places in the structure, though the name must be unique within a directory
Location type	Supports all location types: sites (for adapters); service locations; mailboxes	Supports only service locations and mailboxes
Naming restrictions	Requires name to begin with alphanumeric character. Maximum of 256 characters, and *cannot* contain any of the following characters: **\ / : * ? " < > | ! & ( ) ` ' ; ,**	Requires name to begin with alphanumeric character. Maximum of 256 characters, not including directory path, and *cannot* contain any of the following characters: **\ / : * ? " < > | ! & ( ) ` ' ; ,** **IMPORTANT:** File name cannot be the same as the name of a sub-location
Message naming conventions	Allows users to upload duplicate file names	Allows user to upload duplicate file names, but the first file will be canceled. Remote users can rename files or move them to another location to which they have access, if the target name does not already exist and if the file name is not the same as the name of the location where it is moved
Actions on messages	Allows remote users to access messages until they are removed from the Message Store. Users can access messages from pseudo-directories, *Canceled* or *Downloaded,* based on the status of the message. Manager users can resubmit or redirect messages from MessageWay Manager depending on the message status	Allows remote users to only access available messages in mailboxes or possibly messages queued to a service location and to which they have access. Messages with statuses such as canceled or complete (downloaded) are not visible. Manager users cannot resubmit messages. They can only redirect messages from MessageWay Manager

Status of Locations

Locations have several settings that affect how they receive or deliver messages. The status appears on the General page of the location (Site, Service Location, or Mailbox) Properties window and on MessageWay Explorer. It is a combination of three settings on the location properties window:

- State (active or on hold), on General page
- Schedule (open or closed), on Schedule page
- Threshold Release (works with a closed schedule), on Schedule page

When the state of the location is active, the state of the schedule controls delivery. However, a location on hold overrides the schedule. The following table shows the status associated with a location and what it means:

Status	Description	Schedule and Location States
On Hold	The location is not available to send or receive messages. This overrides the schedule.	Schedule: open or closed Location: on hold
Open	The location is currently available to send or receive messages.	Schedule: open Location: active
Closed	The location is not currently available to send or receive messages.	Schedule: closed Location: active
Threshold: *nn*	The location schedule is controlled by threshold release rules. The *nn* is the number of messages that must accumulate before the schedule is opened and messages are delivered.	Schedule: closed, uses threshold release Location: active

Output State of Service Locations

Service locations have a state, active or on hold, as do sites.

Service locations are associated with services that produce outputs, so they also have a state for the output. Users may allow the outputs to be delivered automatically, which is the default, or place the outputs on hold.

- When the output state is *active*, messages are automatically delivered from the service location.
- When the output state is *on hold*, messages are queued to the destination location until users release the hold.

Types of Locations

Locations may be associated with an adapter or service that automatically performs the transfer of its messages based on the location configurations. Locations associated with adapters may be configured to send messages only, to receive messages only, or to both send and receive messages. The locations associated with services are used for messages that require processing, such as services provided by Rules Processing, Distribution List, Compression, Conversion and Translator services.

Two types of locations are not associated with adapters or services: system mailboxes and pickup mailboxes. For example, the system mailbox {Unknown} stores messages that cannot be delivered. Pickup mailboxes allow users to collect messages, for example through the MessageWay FTP Perimeter Server, the SFTP Perimeter Server or the MessageWay Web Client.

There are some locations that are created and preconfigured during the install process, and their names appear between braces: {ArchiveMaintenance}, {ArchiveReports}, {ArchiveRetrieve}, {Archive}, {CheckLogIntegrity}, {Dist}, {LogIntegrityReports}, {Quarantine}, {RetrievedMessages} and {Unknown}. The following table describes their use:

System Locations	**Description**
{ArchiveMaintenance}	Custom Processing service location that runs the archive maintenance program on a schedule configured to produce a trigger.
{ArchiveReports}	Pickup type mailbox that receives the reports generated by the archive/delete program, archive maintenance program and archive retrieve program.
{ArchiveRetrieve}	Custom Processing service location that runs the archive retrieve program.
{Archive}	Custom Processing service location that runs the archive program on a schedule configured to produce a trigger.
{CheckLogIntegrity}	Custom Processing service location that runs the tamper detection program for audit log records on a schedule, and writes reports to the {LogIntegrityReports} location.
{Dist}	Distribution List service location to handle multiple, comma-separated recipients. To create dynamic distribution lists, use a recipient of **{Dist}:loca,locb** then the {Dist} location creates an ad hoc distribution list using the recipients, loca,locb. If you send just a comma-separated list of recipients, then MessageWay adds the *{Dist}:* to the front.
{LogIntegrityReports}	Pickup type mailbox that receives the reports generated by the audit log tamper detection program.
{Quarantine}	System mailbox that receives messages that cannot be delivered because the message failed the antivirus scan, or the message could not be scanned.
{RetrievedMessages}	Pickup type mailbox that receives messages that have been retrieved from archive.
{Unknown}	System mailbox that receives messages that cannot be delivered. **NOTE:** Some processes such as Custom Processing and Custom IO use a default recipient of UNKNOWN. If the location called UNKNOWN does not exist, it will be forwarded to the system mailbox {Unknown}. This may also be true for MessageWay Translation Service, if users have specified UNKNOWN as a default routing address.

The configuration windows for locations are named by their location category: service location, site or mailbox. The location type provides further distinctions. The following table shows the type associated with a location, the category to which it belongs and what it means. Note that locations in the File System folder only support mailboxes or service locations.

Location Type	Location Category	Description
Folder	N/A	This is a folder to organize locations. It has no affect on processing. All location names must be unique, whether they are in a group or not.
Service	Service location	This location is associated with a service, such as MWRules or MWTranslator, that receives and processes input messages and delivers output to various locations. When in the File System folder, a service location also functions as a container/directory node.
Input	Site	This location is associated with an adapter and is configured to automatically transfer messages into MessageWay.
Output	Site	This location is associated with an adapter and is configured to automatically transfer messages from MessageWay.
I/O	Site	This location is associated with an adapter and is configured to automatically transfer messages both to and from MessageWay.
System	Mailbox	The system mailboxes, called {Unknown} and {Quarantine}, this latter is created when you use the option Content Validation to check for viruses), are created by the system during installation. They are not associated with any adapter or service. {Unknown} contains messages in error when they cannot be delivered, for example, when the destination location does not exist. {Quarantine} contains messages that have failed validation, and are believed to contain a virus, or that are incomplete, for example, when the validation server is unavailable.
Mailbox	Mailbox	This mailbox is not associated with an adapter or service. It holds messages until they are picked up or collected by an external user through a supported interface, such as the Web Client or MessageWay FTP Perimeter Server. When in the File System folder, a mailbox also functions as a container/directory node.

Locations are associated with one adapter or service at a time or no adapter. The icons show the function of the location entities. The following icons are used in the Locations folder.

Icon	Location Function (Locations Folder)
⚙	Service location (Compression, Conversion, Custom Processing, Rules Processing, Translator)

Icon	Location Function (Locations Folder)
✉	Service location (Distribution List)
📥	Sites and mailboxes (system mailboxes and pickup mailboxes)
📁	Folder to organize locations

The next icons are used in the File System folder. Note the arrow in the upper left corner.

Icon	Location Function
⚙	Service location (Compression, Conversion, Custom Processing, Rules Processing, Translator)
✉	Service location (Distribution List)
📥	Mailboxes (pickup mailboxes)

Control of Locations

Users control locations with various methods:

- Configurations
- Direct operator actions
- Remote access via FTP or SFTP (File System locations only) to create pickup mailboxes (default settings only)

This section discusses configurations. Operator actions are discussed in the section ***Controlling Message Traffic*** (on page 701). Users may specify the following basic information for location configurations:

- (Locations folder) User folder within which locations may be optionally defined to improve organization
- Adapter (Locations folder only) or service that will automatically send messages to or from this location
- Delivery or processing priority for messages sent to this destination location
- Retention days before archive and/or delete for messages sent to this destination location
- Retry attempts and intervals when the initial delivery attempt fails
- Which users may perform which tasks
- Delivery options based on schedules or threshold release
- When and where to send notification reports
- Parameters specific to the adapter or service location
- Thread group functionality - parallel or serial processing
- Message storage capability - database (with encryption/compression) or disk
- Check for duplication of messages

Adding Locations and Folders to the Locations Folder

Users may add locations and folders to organize the locations in the Locations folder. Users may configure folders to which they will add locations using either drag-and-drop or creating locations directly within the folder.

IMPORTANT: Locations defined inside and outside folders are all considered to be at the same level, and their names must be unique. If you have a large number of folders, use the *Find Locations* function to search for a particular one.

How to Create a Location in the Locations Folder

Users may create any type of location except a system mailbox, which is created during installation. To create a location, proceed as follows:

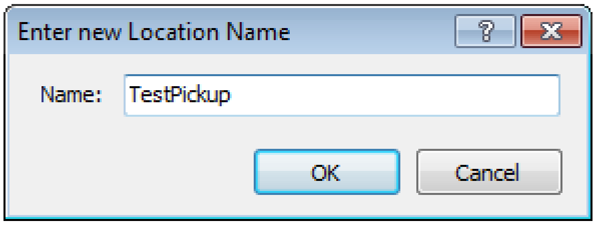
1. From the left pane of MessageWay Explorer, select **Locations**.
2. Right-click the mouse.

   - or -

   Select the **Locations** menu.
3. Select **Add Location**.

   The **Enter New Location Name** dialog box appears.

4 Enter a unique name for the location. The name is *not* case sensitive and it must not exist, even within a folder. A location name has a maximum length of 256 characters and must not contain any of the following characters: **\ / : * ? " < > | ! & ( ) ` ' ;** , nor be only one period (**.**) or two periods (**..**).



Name: TestPickup

5 Click **OK**.

The General page of the properties window appears. You should complete this page and others as described later in this section, based on your requirements and instructions for any tabs specific to the type of location. Mailboxes only have default tabs.

How to Create a Location Folder

You may create a location folder directly within the **Locations** folder or within a subfolder. Folder names must be unique whether they are within other folders or not and are *not* case-sensitive. You may add existing locations to a folder using drag-and-drop, or you may create new locations directly within the folder. Remember that whether locations are in a folder or not, all location names must be unique.

To create a location folder, proceed as follows:

1 From MessageWay Explorer, from the left pane select **Locations**.

2 Right-click the mouse.

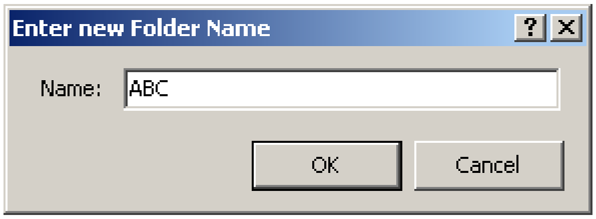
- or -

Select the **Locations** menu.

3 Select **Add Location**.

The **Enter New Folder Name** dialog box appears.

4 Type a unique name for the folder. The name is not case-sensitive and it must not exist.



Name: ABC

5 Select **OK**.

MessageWay Explorer appears with the new folder listed.

6 To add a location to a folder, do one or more of the following:

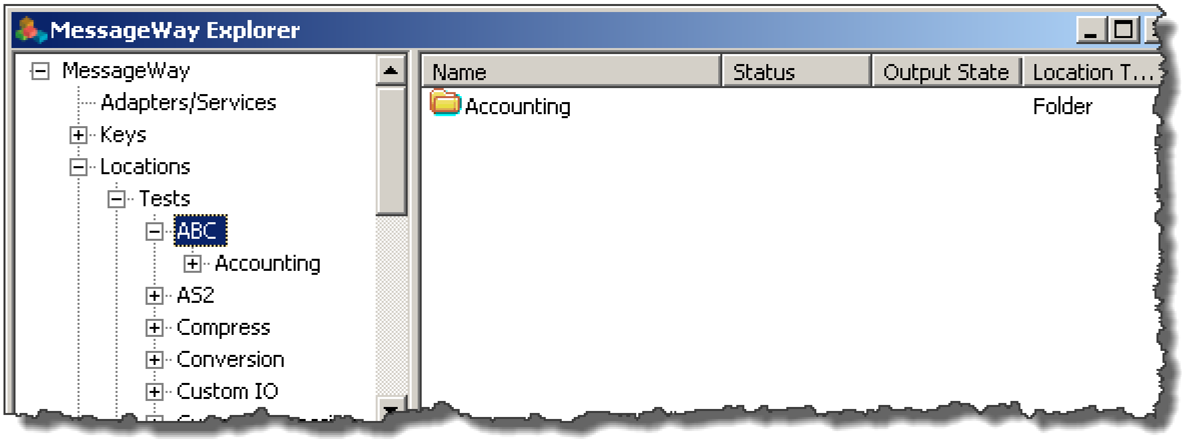
- Drag-and-drop existing locations into the new folder.

  - or -

- Select the folder, and then follow the instructions in the topic ***How to Create a Location*** (on page 461).

7 Press **F5** to update the window information.

Folders appear in the list of locations and may be embedded in other folders. The following example of MessageWay Explorer shows the folder *Accounting*, embedded within the folder *ABC*, which is embedded with the folder *Tests*.

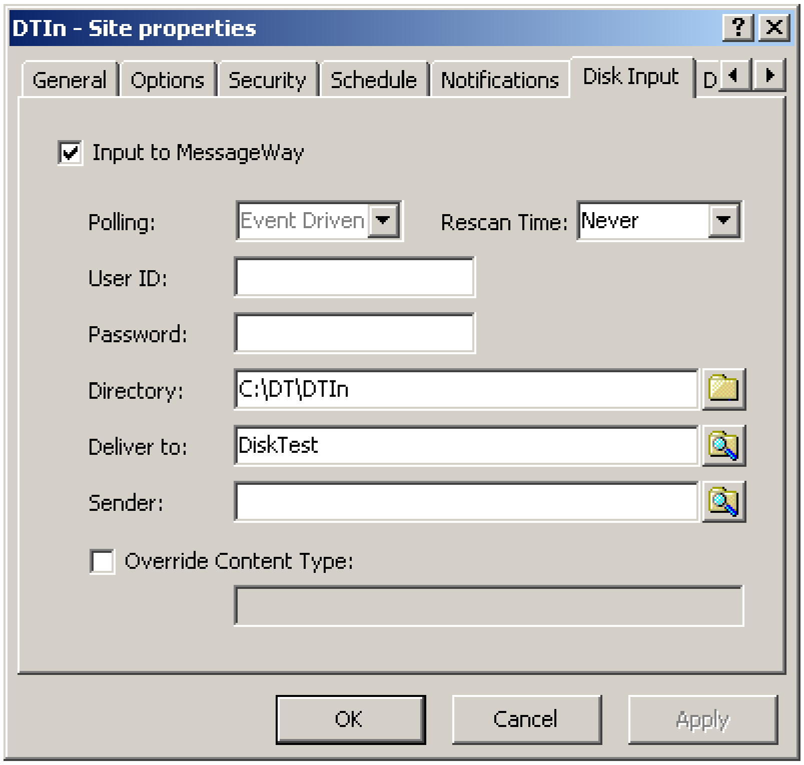


Name	Status	Output State	Location T...
Accounting			Folder

Recommendations for Sites (I/O Locations)

When you create locations that use an adapter, which are called sites, such as Disk Transfer, FTP or E-mail, you should create separate sites for input and output. Configuring separate sites allows you to control the messaging traffic separately. You can have separate schedules for input and output. You can also put sites for input on hold without affecting output, and you can limit input polling without affecting output. Similarly, you can put output sites on hold without affecting receipt of input messages.

In the following example configurations, there is one Disk Transfer site configured for input and another configured for output.



DTIn - Site properties

☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

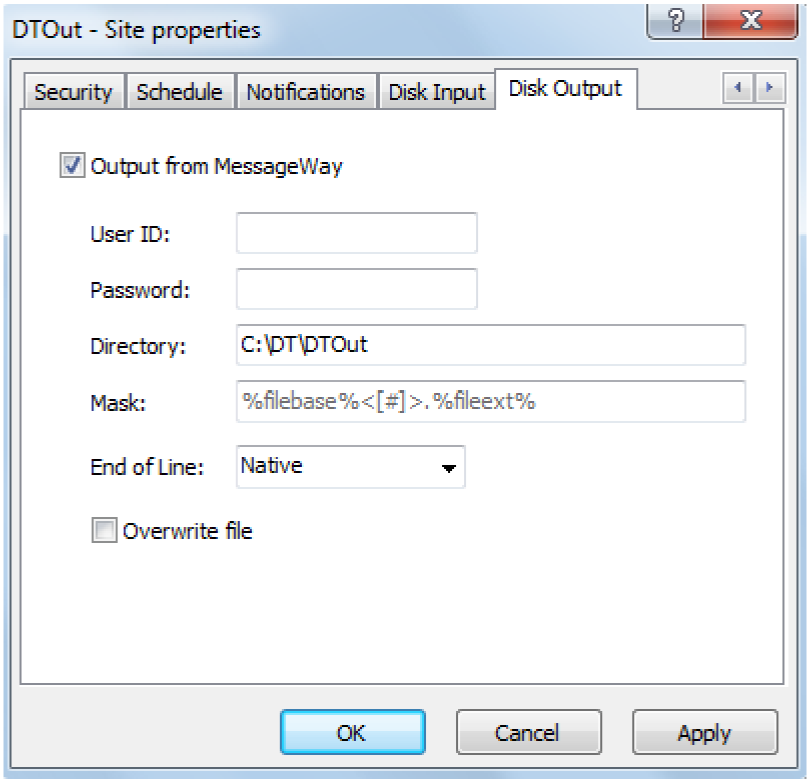
Password:

Directory: C:\DT\DTIn

Deliver to: DiskTest

Sender:

☐ Override Content Type:



DTOut - Site properties

☑ Output from MessageWay

User ID:

Password:

Directory: C:\DT\DTOut

Mask: %filebase%<[#]>.%fileext%

End of Line: Native

☐ Overwrite file

Adding Locations to the File System Folder

Within the File System folder, you can create a limited set of location types: service locations or mailboxes. You cannot create sites, which are locations associated with an adapter, such as Disk Transfer, nor can you create folders. When you create a location in the File System folder, the name of the locations also becomes a node or subdirectory in the tree structure. The properties of the subdirectory are actually the properties of the location of the same name.

NOTE: When remote users create directories, they actually create pickup mailbox locations within their default location (home directory), which is defined on the Locations tab of the User Properties window.

To create a location in the File System folder, proceed as follows:

1 From the left pane of MessageWay Explorer, expand the *File System* folder and click the root directory, **/**.

2 In the right pane, right-click the mouse.

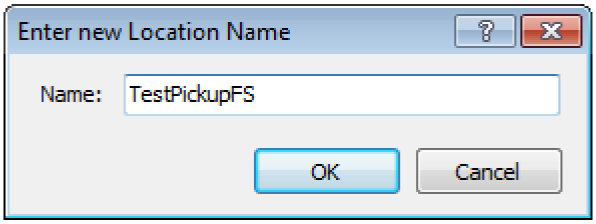
- or -

Select the **Locations** menu.

3 Select **Add Location**.

The **Enter New Location Name** dialog box appears.

4 Enter a unique name for the location. The name is not case sensitive. A location name has a maximum length of 256 characters and must not contain any of the following characters: **\ / : * ? " < > | ! & ( ) ` ' ; ,** nor be only one period (**.**) or two periods (**..**).

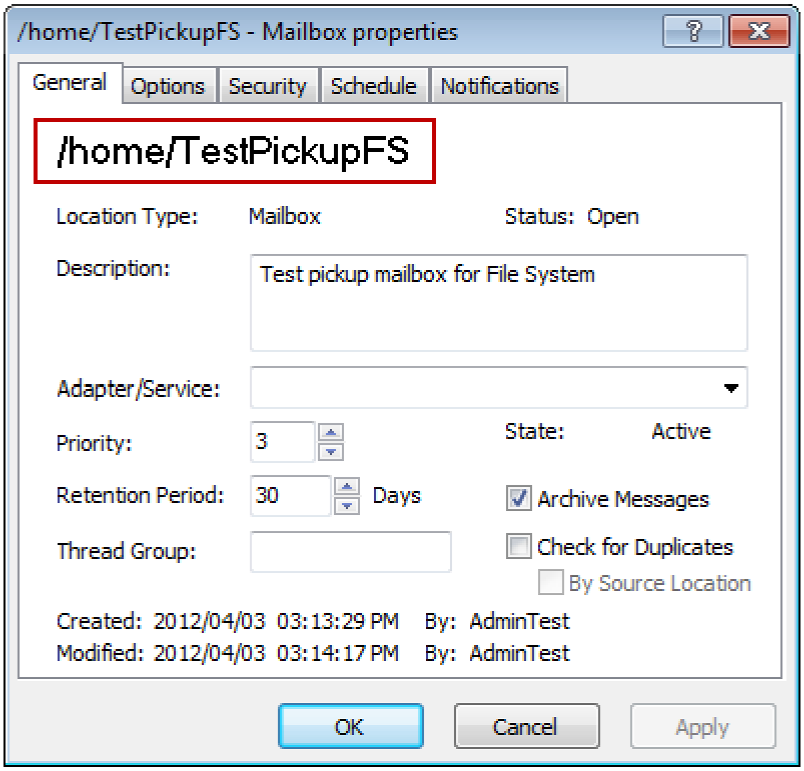


Name: TestPickupFS

5 Click **OK**.

The General page of the properties window appears. You should complete this page and others as described later in this section, based on your requirements and instructions for any tabs specific to the type of service location. Mailboxes only have default tabs. Note that the Inherit property on the Security tab refers to the container for the location, which for File System locations is its parent location (directory).

Also, MessageWay adds a new node to the directory path with the same name as the location. The name of the location becomes the full path name, for example */home/TestPickupFS*.



/home/TestPickupFS - Mailbox properties

/home/TestPickupFS

Location Type: Mailbox

Status: Open

Description: Test pickup mailbox for File System

Adapter/Service:

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

□ Check for Duplicates

□ By Source Location

Created: 2012/04/03 03:13:29 PM By: AdminTest

Modified: 2012/04/03 03:14:17 PM By: AdminTest

Moving Locations Between Locations and File System Folders

When you move locations between Locations and File System folders:

- Location must *not* exist in the target folder
- Effective rights will be maintained
  - If the access list for the location is the same, there will be no changes to the Security tab properties, including the Inherit flag.

  - or -

  - If the access list for the location is different (because it inherits different access lists from the folder in which it will reside), the following changes are made to the Security tab:
    - Inherit box will be cleared
    - *Allowed* rights will be set to the current *Effective* rights
    - *Denied* rights will be set to inverse of *Allowed* rights

Other behavior varies depending on the direction of the move.

- *From File System to Locations*,
  - Source location cannot have any child locations (sub-directories)
- *From Locations to File System*
  - Source location must be mailbox or service location, not a site (location for adapter)
  - Source location cannot have any messages associated with it

To move a location between Locations and File System folders, you can use cut-and-paste or drag-and-drop.

1. In the left pane of MessageWay Explorer, navigate to the location you want to move.
2. Select the location, and then

   a) Drag the location to its desired place.

   - or -

   b) Right-click and select **Cut** from the menu, and then put you cursor in the new place, right-click and select **Paste**.

Specifying General Properties for Locations

On the General page of the location (Site, Service Location, Mailbox) Properties window, users must specify different types of general parameters for different location types, such as adapter/service, priority, retention period, thread group, archive and check for duplicates.

Associating a Location with an Adapter or Service

When users add a location, they typically associate it with an adapter or service, so messages may be processed automatically. What they select determines, in part, the type assigned to the location. The location type is not specified for an adapter or service until users complete a page specific to the adapter or service, which appears when one is selected.

Sites are easier to understand and messages are easier to manage when the site is configured for either input or output, but not both. When a site is configured for both input and output, schedules control both polling for input and message delivery, which occur only when the schedule is open. Separate sites allow you to limit polling for input without blocking message delivery. Conversely, they allow you to limit message delivery, such as when you use Threshold Release, without stopping input polling. Separate sites also allow you to put locations on hold, which will affect only input or output.

When users do not associate a location with an adapter or service, that location by default is a mailbox that retains messages for external users to pick up. A pickup mailbox is required as a default mailbox for any user that accesses MessageWay through the MessageWay Service Interface, even when they do not use the mailbox to collect messages, as is the case for ***AS2*** (on page 114) users. Pickup mailboxes also allow users to collect their messages through such options as the ***FTP Server*** (on page 185), or the ***SFTP Server*** (on page 298) or the Web Client, rather than having MessageWay automatically deliver their messages.

The Location Type is specified on the General page of the properties window and shown on MessageWay Explorer. There are base adapters and services delivered with MessageWay as well as options that users may add. The base selections are listed in the following table:

BaseAdapter/Service	Description
Compression service	Compresses (zips) and uncompresses (unzips) message content, supporting both zip and gzip formats
Custom IO adapter	Provides I/O interface between MessageWay and external applications
Custom Processing service	Provides service interface between MessageWay and external applications
Disk Transfer adapter	Provides input from and output to disk locations on the local network
Distribution List service	Delivers messages to multiple recipient locations simultaneously
E-mail adapter	Provides e-mail POP3 and SMTP client services
FTP adapter	Provides File Transfer Protocol (FTP) client services and encryption and decryption services using Transport Layer Security (TLS) and Secure Socket Layer (SSL)
Rules Processing service	Routes messages based on various properties or content of the message
SFTP adapter	Provides SFTP client using SSH or SCP (Linux only) protocol to connect to an SFTP server.

The optional selections are listed in the following table:

Option	Description
Additional instances of adapters and services	▪ You may have more than one instance of an adapter or service.
AS2 Interface	▪ Provides support for the AS2 protocol. Includes both an AS2 adapter to send messages from MessageWay to an external AS2 server and an AS2 server that controls message delivery to and from MessageWay over HTTP or HTTPS.
AWS S3 adapter	▪ Provides support for storing and retrieving any amount of data on Amazon Web Services (AWS) using Simple Storage Service (S3). **NOTE:** This option is documented separately in the document *MessageWay MWAWSS3 User's Guide and Reference*.
Convert adapter	▪ Provides character conversion based on character set (code page).
MQ adapter	▪ Provides connection through an IBM WebSphere client to a WebSphere manager.

Option	Description
Translation service	▪ Provides translation between different formats, typically between proprietary and EDI standards. ▪ Provides routing with or without translation. ▪ Provides additional logging and reconciliation services to manage acknowledgments

For more information about optional adapters or services in MessageWay, refer to ***Options*** (on page 893).

Selecting a Priority

Priorities are only applicable for auto-delivery. They are assigned to messages based on the destination location configuration.

MessageWay applies the following rules:

- Valid priorities are from 1 (lowest) to 5 (highest)
- Default priority is 3
- The adapter or service associated with this location will deliver higher priority messages first
- Output messages created by a service have the same priority as the input message delivered to the service location, except:
  - ***When an operator manually changes the priority*** (on page 729)

    - or -
  - ***When a rules profile for a rules processing location applies a different priority*** (on page 631)
- When an outbound message already has a priority assigned, then the new priority will be the higher of the assigned or the default priority
- Changes to the priority field take effect for messages that are not currently being processed or transferred. However, changes will be applied to any future output messages generated by service locations, such as Rules Processing.

Selecting a Retention Period

The retention period indicates the number of days that must pass before a message whose status is Complete or Error is available for archiving or deletion. Users may configure a destination location to archive messages automatically, or they may manually select messages to archive or delete. Users must run the Archive/Delete program separately to archive and/or delete the messages. Until that time they remain in the Message Store with a status of Complete or Error. The default Retention Period is 30 days. For more information about how MessageWay archives messages, refer to the topic, ***Maintaining Message Information*** (on page 783).

Identifying Duplicate Messages

Users may configure any location that is capable of delivering messages to check for duplicate messages before attempting delivery. This applies to locations other than an input sites, pickup mailboxes or the system mailbox, {Unknown}.

Basically, any message that has been resent to the same location in MessageWay might be a duplicate. Two messages are defined as duplicates when they have all the characteristics explained in the following table. If any characteristic is not true, then the messages are not considered duplicates.

Duplicate Criteria	Explanation
Different Original Message IDs	Messages with different Original Message IDs as shown on the Message Properties window, have been sent to MessageWay separately and each has been assigned a unique Original Message ID. Messages resent with the Resubmit command will have the same Original Message IDs, so they will not be considered duplicates.
Same destination location	The destination location is the same for both messages. Messages resent with the **Redirect** command will probably have different locations, so they would not be considered duplicates.
Duplicate data content	The content of the two messages has been compared and they contain exactly the same data.
Same source location	When **By Source Location** is checked, the source location of the messages must be the same.

The following table shows some examples of messages that would not be considered duplicates and why. Note that with distribution lists, since they may contain location groups, duplicate location entries are eliminated before the duplicate message criteria are applied.

Message Action	Different Original Message ID	Same Location	Same Content
Messages sent to a distribution list	No (all messages have same original message ID)	Possibly	Yes
Resubmitted	No (resubmitted messages retain the original message ID)	Yes	Yes
Redirected	No (redirected messages retain the original message ID)	No	Yes
Retranslated	Yes	Yes	No (assuming data change, e.g. control reference, timestamp.)

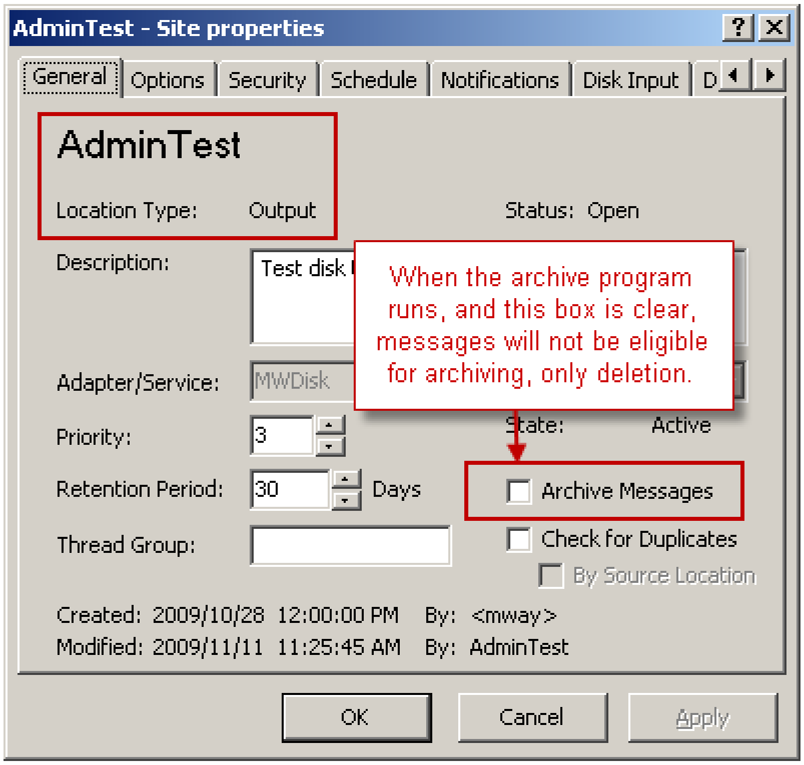
NOTE: For the optional service, MWTranslator, when a message is retranslated, if the content of the output data is exactly the same as another message, the output messages will be considered duplicates.

Specifying Archiving

To archive messages sent to a location, check the **Archive Messages** box. When the archive program runs, messages will be archived based on various conditions.

MessageWay first determines which messages are to be archived, and then after archiving eligible messages, it deletes those messages eligible for deletion.

CAUTION: When the archive program runs, if the destination location has the **Archive Messages** box *unchecked*, all messages queued to that site will be eligible for deletion, not archiving, whether or not they were originally marked for archive.



AdminTest - Site properties

AdminTest

Location Type: Output

Status: Open

Description: Test disk

Adapter/Service: MWDisk

Priority: 3

State: Active

Retention Period: 30 Days

Thread Group:

□ Archive Messages

□ Check for Duplicates

□ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 11:25:45 AM By: AdminTest

When the archive program runs, and this box is clear, messages will not be eligible for archiving, only deletion.

NOTE: Linked messages have a unique Message ID but the same Original Message ID, and thus share the same content file. Linked messages typically result from the **Resubmit Message** or **Redirect Message** commands, or services that do not change the data, such as Rules Processing or Distribution List. The content file may be archived multiple times, if linked messages remain from one archive run to another.

Messages are eligible for archiving based on the following criteria:

- State of the message is *Complete*

  - and -

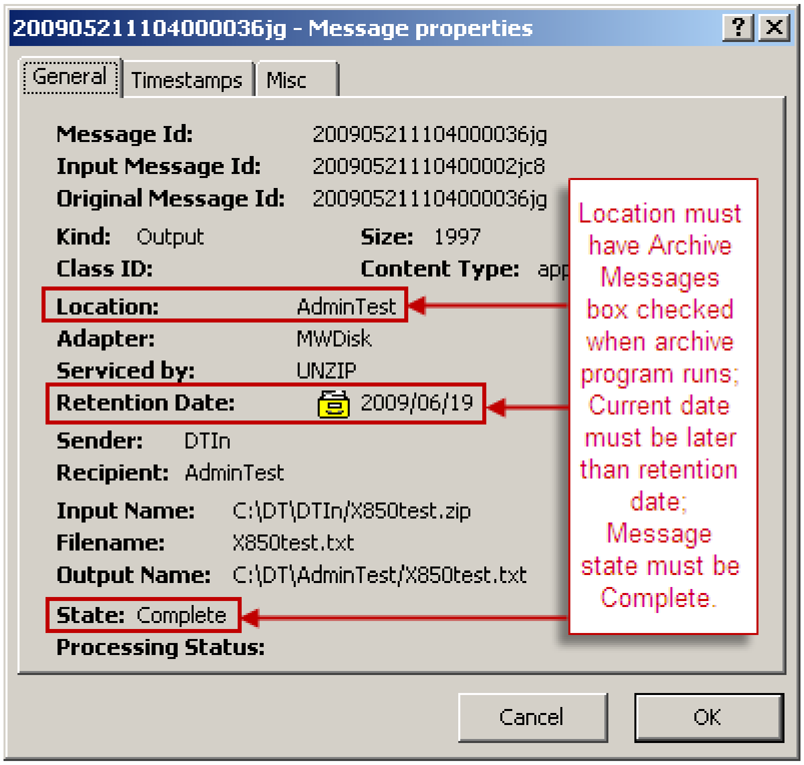
- Retention date for the message (Message Properties window, **General** tab) is less than the current system date

  - and -

- **Archive Messages** box is checked for the location (Site, Service Location, Mailbox) properties window, **General** tab) when the archive program runs

  - and -

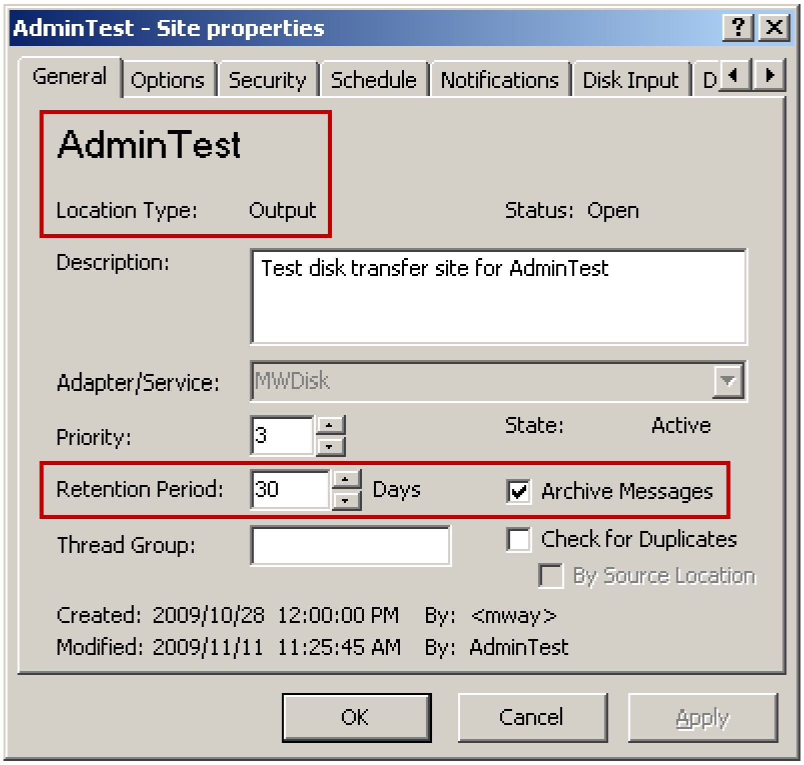
- For MWTranslator that uses document reconciliation, no part of the message (interchange, functional group, document) has a status of *Awaiting Ack*



200905211104000036jg - Message properties

Message Id: 200905211104000036jg
Input Message Id: 200905211110400002jc8
Original Message Id: 200905211104000036jg
Kind: Output **Size:** 1997
Class ID: **Content Type:** app
Location: AdminTest
Adapter: MWDisk
Serviced by: UNZIP
Retention Date: 2009/06/19
Sender: DTIn
Recipient: AdminTest
Input Name: C:\DT\DTIn/X850test.zip
Filename: X850test.txt
Output Name: C:\DT\AdminTest/X850test.txt
State: Complete
Processing Status:

Location must have Archive Messages box checked when archive program runs; Current date must be later than retention date; Message state must be Complete.



AdminTest - Site properties

AdminTest

Location Type: Output

Status: Open

Description: Test disk transfer site for AdminTest

Adapter/Service: MWDisk

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

☐ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 11:25:45 AM By: AdminTest

Messages will be deleted after archiving when:

- A message has been properly archived and has no other constraints

  - or -

- All ***linked messages*** (on page 748) have been archived or deleted

NOTE: The content file is deleted from the Message Store only when the last linked message is archived or deleted.

- or -

For MWTranslator that uses document reconciliation, no part of the message is awaiting an acknowledgment

Specifying a Thread Group to Enforce Serial Processing

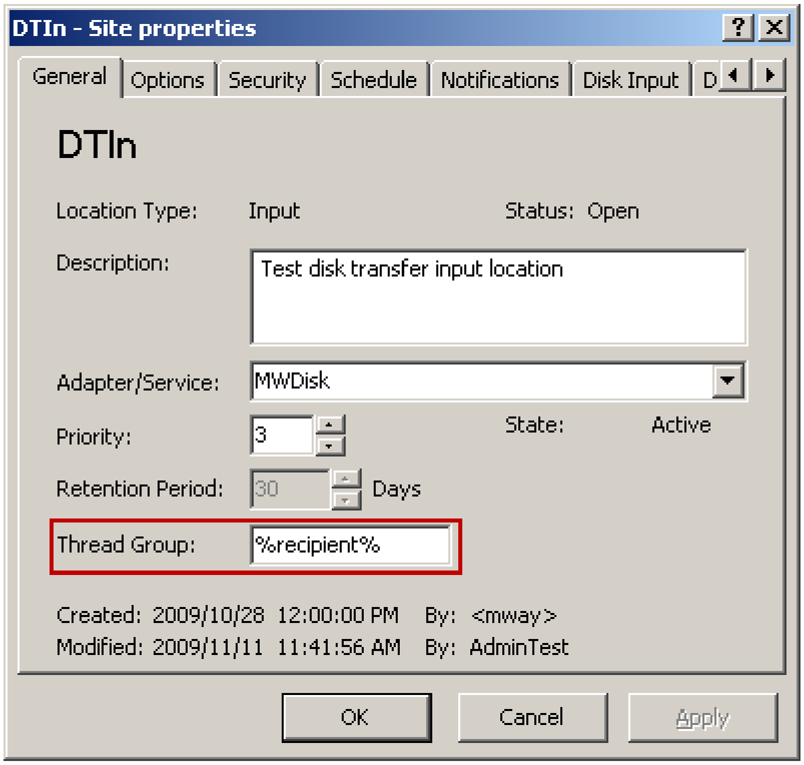
By default, MessageWay adapters and services are multi-threaded. At times, users may need to enforce sequential processing. To do this, you assign a thread group to one or more locations.

To enforce sequential processing of messages, type the name of a thread group, using any MessageWay tokens as necessary to uniquely identify the group. Some useful tokens might be: %sender%, %recipient%, %classid%, %filename%, %inputname%, %outputname%, %contenttype%, %filebase% or %fileext%.

Some MessageWay services or external sites may require serial processing, such as a translation location that has to process an original purchase order before it processes a purchase order change or an FTP site that allows only one logon per user. Adapters and services typically process input and output messages using parallel processing with multiple threads. In order to force serial processing of input or output messages, you may configure a thread group for the location. The thread group is assigned at runtime, when a message is available for receipt or delivery. It processes messages in the queue sequentially until no more messages are available. Multiple locations may share a thread group.

NOTE: Thread groups for Custom IO sites and Email sites are only valid for output, since Custom IO and Email adapters receive messages as they are detected.

In the following example, any messages input from the following location will be assigned to a thread group of the name of the recipient on the **Disk Input** tab. All messages queued to this thread group will be processed sequentially.



DTIn

Location Type: Input Status: Open

Description: Test disk transfer input location

Adapter/Service: MWDisk

Priority: 3 State: Active

Retention Period: 30 Days

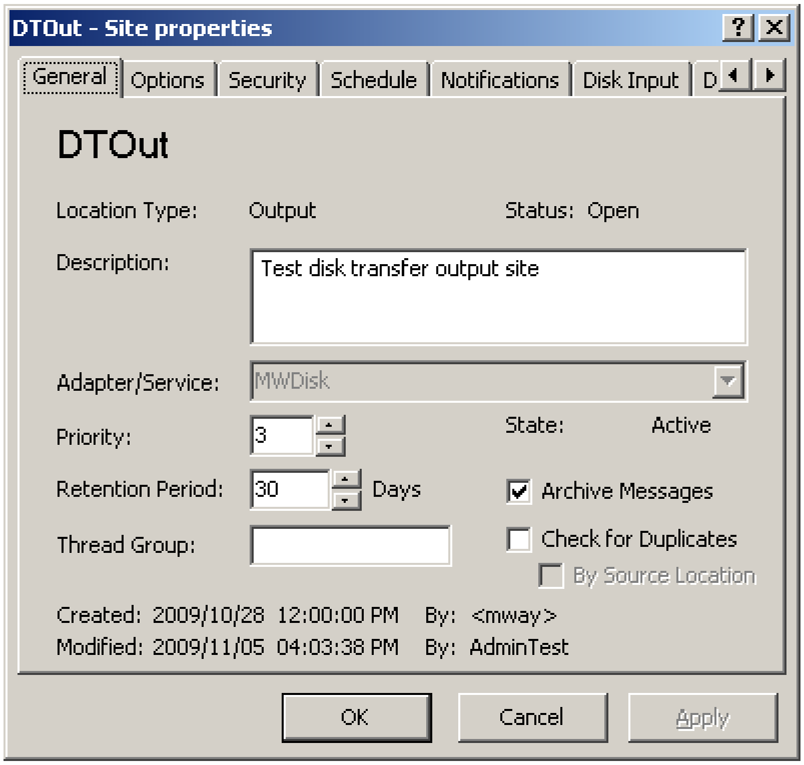
Thread Group: %recipient%

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/11 11:41:56 AM By: AdminTest

Examples of General Properties for Locations

The following screens show examples of configurations for various location types. Not all locations require the same configurations, as you can see.

This is an example of an output site, where you may configure any of the items discussed here.



DTOut

Location Type: Output

Status: Open

Description: Test disk transfer output site

Adapter/Service: MWDisk

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

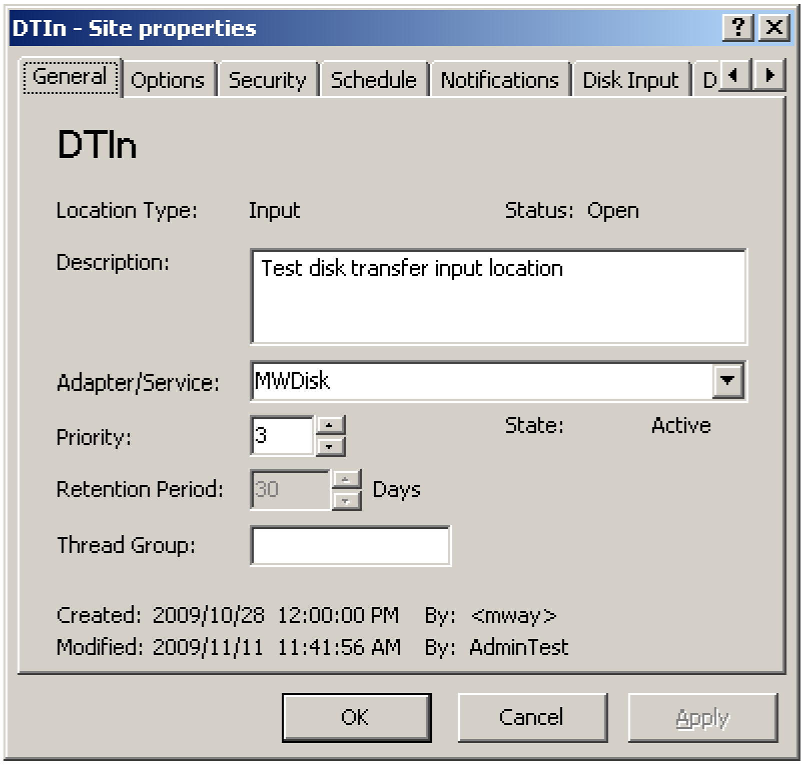
☐ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/05 04:03:38 PM By: AdminTest

Example of an Output Site (General Page, Site Properties Window)

The following window shows an example of an input site. Note that you may not configure the retention period, because input messages are actually associated with the destination location, and governed by its retention period.



DTIn

Location Type: Input

Status: Open

Description: Test disk transfer input location

Adapter/Service: MWDisk

Priority: 3

State: Active

Retention Period: 30 Days

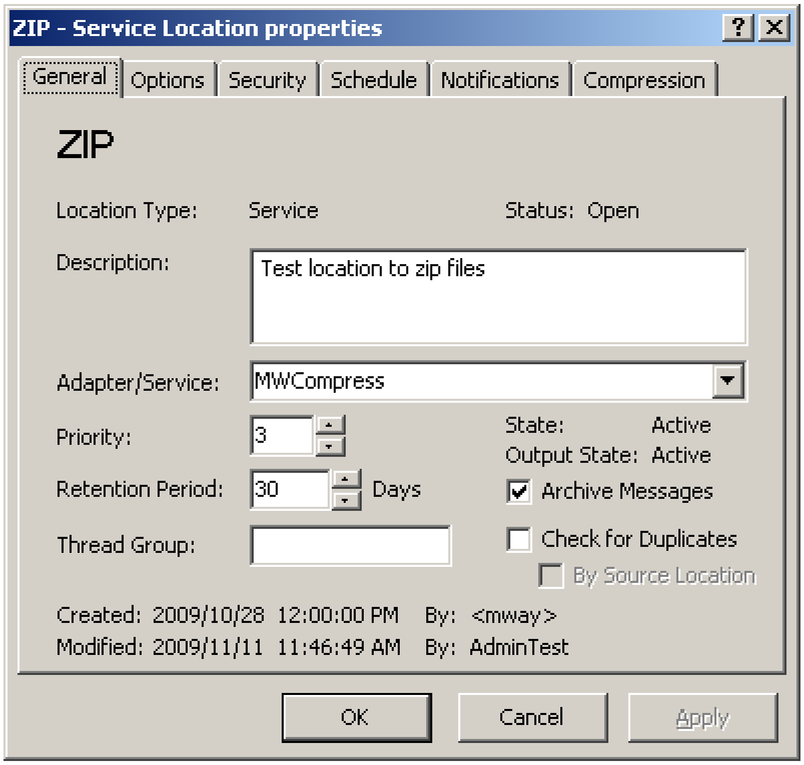
Thread Group:

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 11:41:56 AM By: AdminTest

Example of an Input Site (General Page, Site Properties Window)

This is an example of a service location.



ZIP

Location Type: Service

Status: Open

Description: Test location to zip files

Adapter/Service: MWCompress

Priority: 3

State: Active

Output State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

☐ By Source Location

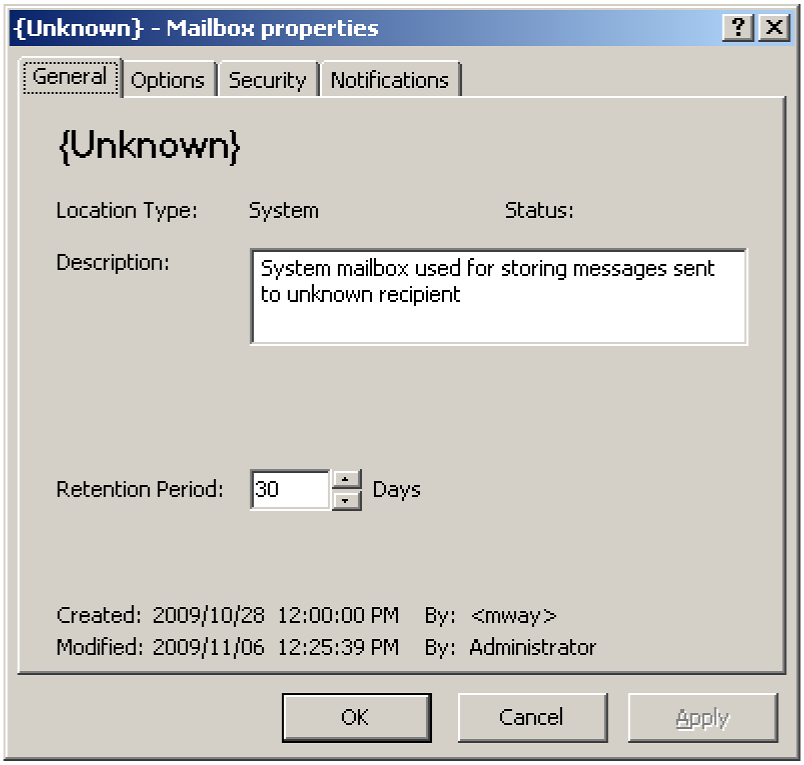
Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 11:46:49 AM By: AdminTest

Example of a Processing Service Location Type (General Page, Service Location Properties Window)

The following window shows an example of the system mailbox, {Unknown}. Users may not add this type of location. It is not associated with an adapter or service, since it is never used to deliver messages. Users may, however, set the retention period.

IMPORTANT: All messages in the {Unknown} mailbox will be archived by default when the retention period passes.



{Unknown}

Location Type: System Status:

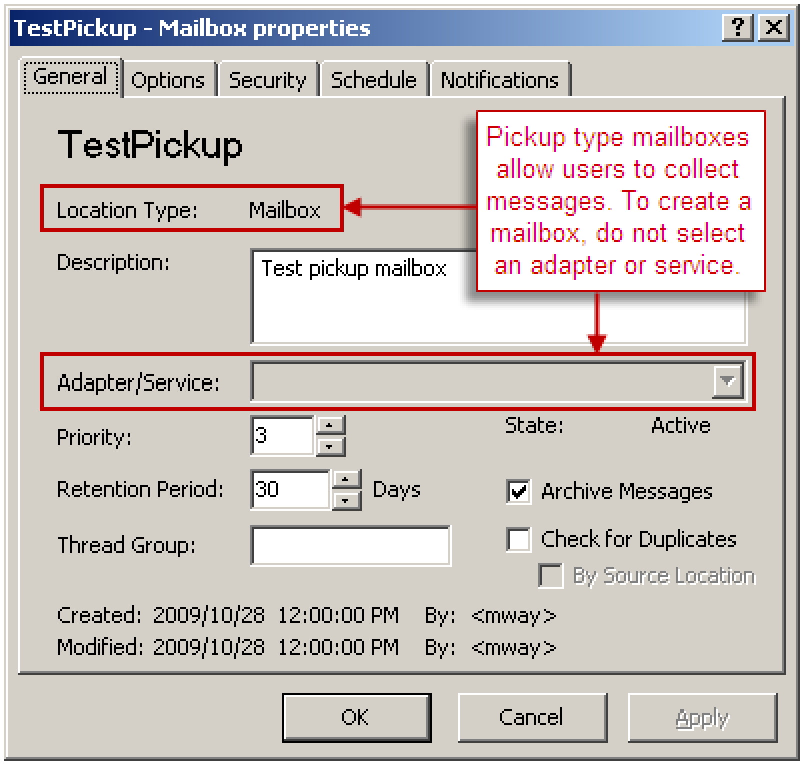
Description: System mailbox used for storing messages sent to unknown recipient

Retention Period: 30 Days

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/06 12:25:39 PM By: Administrator

Example of the System Mailbox (General Page, Mailbox Properties Window)

This is an example of a pickup type mailbox. A pickup mailbox is required as a default mailbox for any user that accesses MessageWay through the MessageWay Service Interface, even when they do not use the mailbox to collect messages, as is the case for ***AS2*** (on page 114) users. Users may pick up messages through options such as the ***FTP Server*** (on page 185), or the ***SFTP Server*** (on page 298) or the Web Client.



TestPickup

Location Type: Mailbox

Description: Test pickup mailbox

Adapter/Service:

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

□ Check for Duplicates

□ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/10/28 12:00:00 PM By: <mway>

Pickup type mailboxes allow users to collect messages. To create a mailbox, do not select an adapter or service.

Example of a Pickup Mailbox (General Page, Mailbox Properties Window)

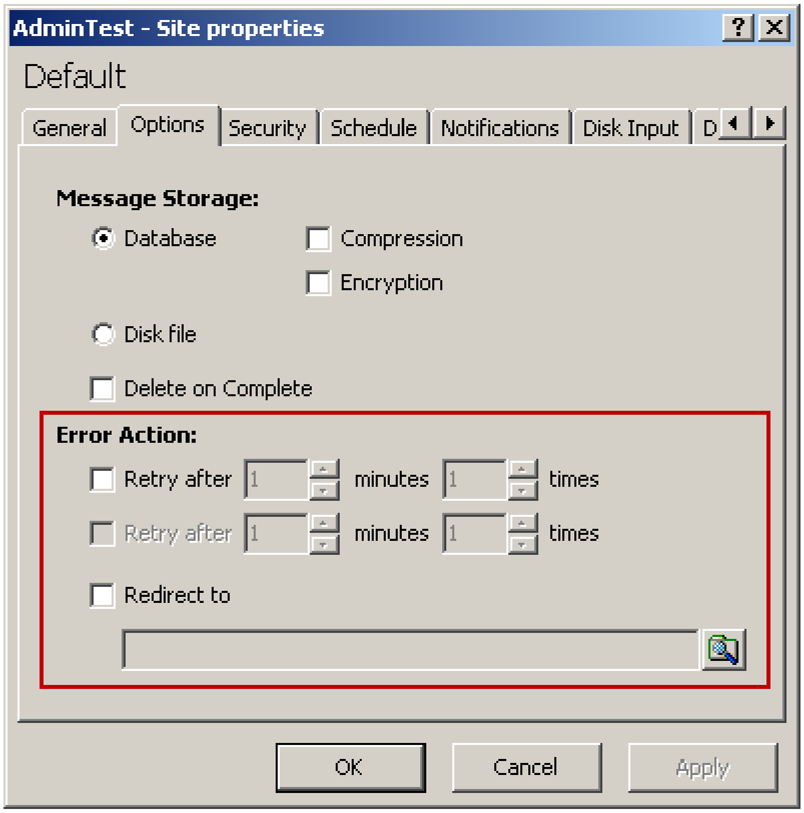
Specifying Options for Locations

Users may specify different content storage options, including compression and encryption, and retry strategies on the **Options** page of a location properties window.

Specifying Retry Parameters

For a location, users may create up to two retry options with an option to redirect the message to another location. They may enter the number of retries that the system will attempt when the initial delivery has failed. They may also set the time between attempts. The default for retry attempts is none (0). To invoke retries, users must check at least one of the Retry after boxes. To redirect the message, without retries or after the retries have failed, users must also check the Redirect to box.

IMPORTANT: For input locations, users should specify an Error Action. For input messages that go to an error state because they are not properly received, MessageWay will only attempt to input the message again when an error action is configured for the input location or when the adapter is restarted.



Message Storage:

● Database □ Compression

□ Encryption

○ Disk file

□ Delete on Complete

Error Action:

□ Retry after 1 minutes 1 times

□ Retry after 1 minutes 1 times

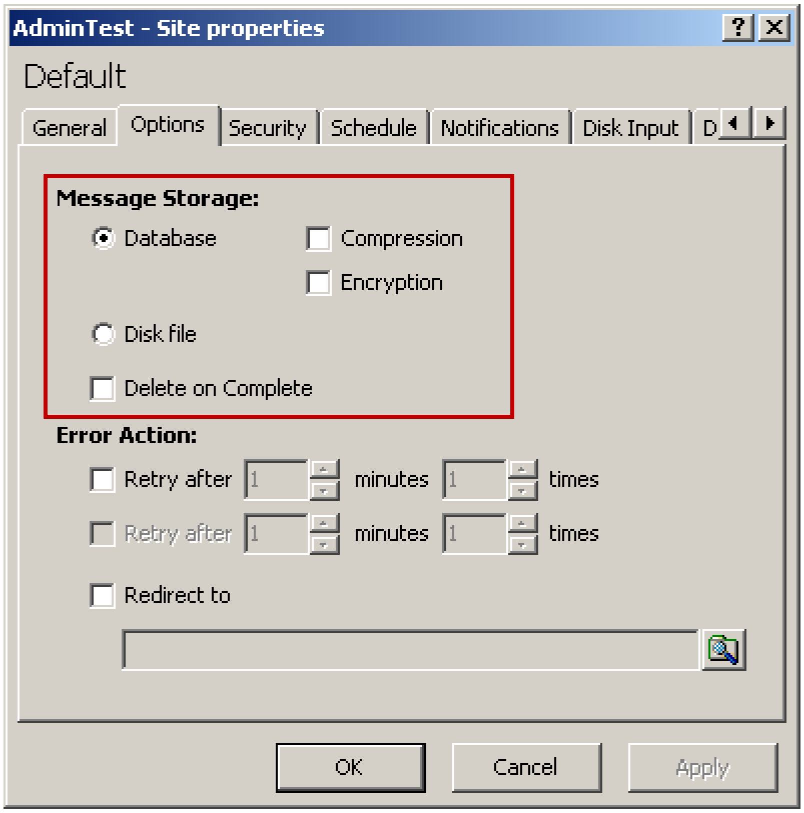
□ Redirect to

Specifying Where to Store Message Content

By default, message content is stored on disk.

Users may also choose to store the message content in the MessageWay database, with options to compress and/or encrypt the content. Data is encrypted using the Advanced Encryption Standard (AES).

NOTE: To be able to access the Encryption option, users must first ***add a master key*** (on page 834), using the mwadmin utility.



AdminTest - Site properties

Default

General | Options | Security | Schedule | Notifications | Disk Input | D

Message Storage:

- ● Database
- □ Compression
- □ Encryption
- ○ Disk file
- □ Delete on Complete

Error Action:

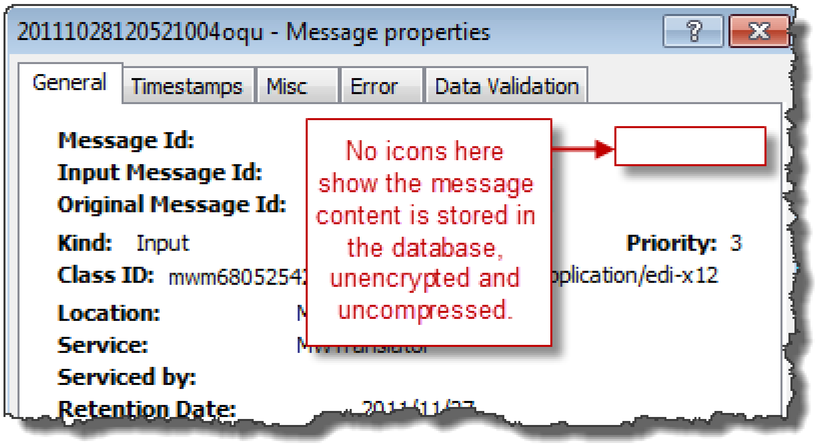
- □ Retry after 1 minutes 1 times
- □ Retry after 1 minutes 1 times
- □ Redirect to

Icons on the Message Properties window represent where and how the message content is stored or whether it was deleted after successful delivery. The representative icons appear as follows:

Icon	Storage Option
None	SQL database, no encryption, no compression
🔑	SQL database, Encrypted
🗜	SQL database, Compressed
💾	Disk
✗	Deleted from Message Store after successful delivery

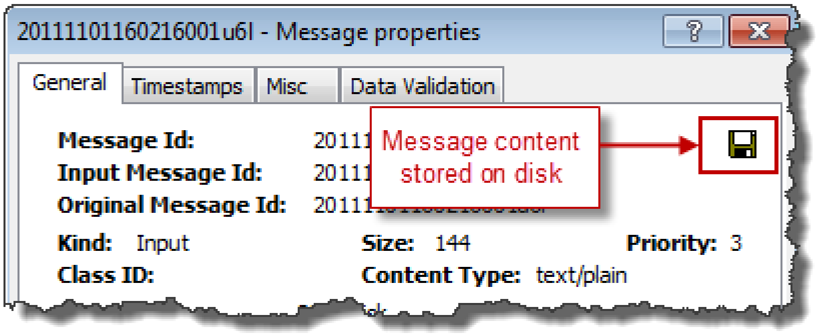
IMPORTANT: When you send messages to a distribution list for delivery to multiple locations, the storage option on the Distribution List Service Location is what determines how a message is stored, not the option on the final destination location. This is because the message is stored once, and the final destination locations point back to the original message sent to the distribution list.

The icons appear to the right of the Message ID. No icons indicate that the message is stored in the database, not encrypted and not compressed. The following figures show some examples.



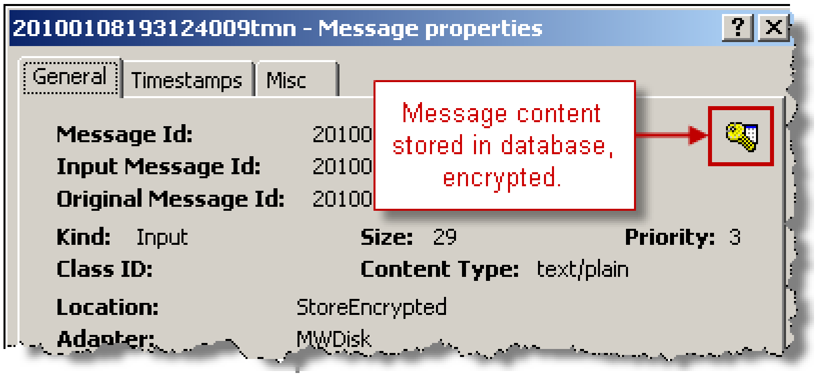
Message Id:
Input Message Id:
Original Message Id:
Kind: Input
Priority: 3
Class ID: mwm6805254
pplication/edi-x12
Location: M
Service: MWTranslator
Serviced by:
Retention Date: 2011/11/27

No icons here show the message content is stored in the database, unencrypted and uncompressed.



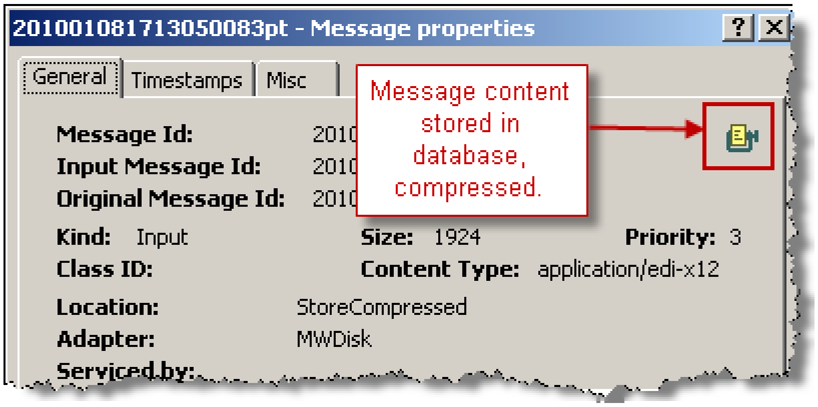
Message Id: 20111
Input Message Id: 20111
Original Message Id: 20111
Kind: Input
Size: 144
Priority: 3
Class ID:
Content Type: text/plain

Message content stored on disk



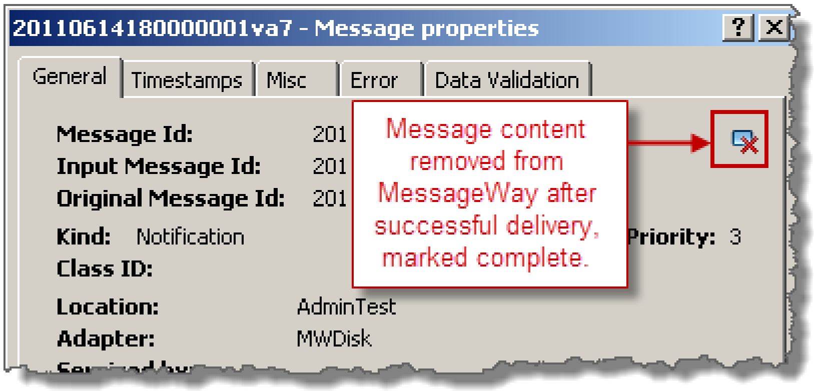
Message Id: 20100
Input Message Id: 20100
Original Message Id: 20100
Kind: Input
Size: 29
Priority: 3
Class ID:
Content Type: text/plain
Location: StoreEncrypted
Adapter: MWDisk

Message content stored in database, encrypted.



Message Id: 2010
Input Message Id: 2010
Original Message Id: 2010
Kind: Input
Size: 1924
Priority: 3
Class ID:
Content Type: application/edi-x12
Location: StoreCompressed
Adapter: MWDisk
Serviced by:

Message content stored in database, compressed.



Message Id: 201
Input Message Id: 201
Original Message Id: 201
Kind: Notification
Class ID:
Location: AdminTest
Adapter: MWDisk

Message content removed from MessageWay after successful delivery, marked complete.

CAUTION (UNIX/Linux): For MessageWay systems configured to encrypt data content in the database, if you run the archive process from a custom processing service location, as we do from the {Archive} location, instead of from the command line, you must have a ***passphrase file*** (on page 835). To initiate the archive process, the encryption password must be saved as a file, because this process cannot be prompted for the password.

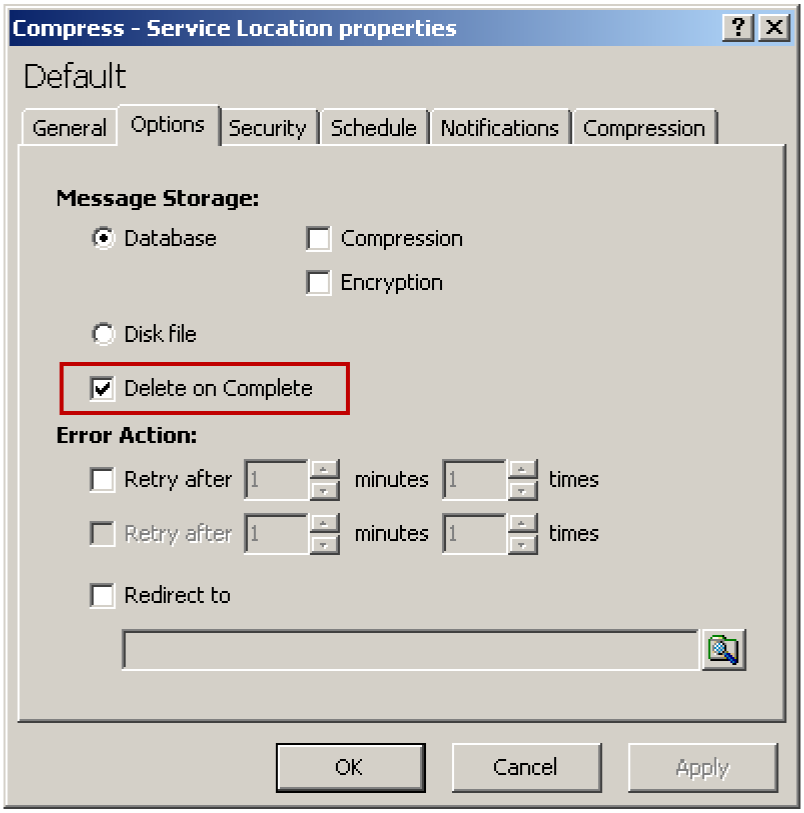
Deleting Content from the Message Store After Successful Delivery

Users may configure MessageWay to remove the content of a message from the message store immediately upon successful delivery of a message, without waiting for the archive process to remove it.

In the following example, a file is picked up from a disk location, DTIn, and then delivered to a compression service location, Compress. Finally, the compressed file is delivered to a disk location, DTOut. We will remove the content of the output from Compress when it is successfully delivered to DTOut. To configure and test this scenario, proceed as follows:

1 ***Create a location*** (on page 461) called Compress, and associate it with the Compress service.

2 On the **Options** page of the Compress service location properties window, check the box **Delete on Complete**.



Compress - Service Location properties

Default

Message Storage:

● Database □ Compression

□ Encryption

○ Disk file

☑ Delete on Complete

Error Action:

□ Retry after 1 minutes 1 times

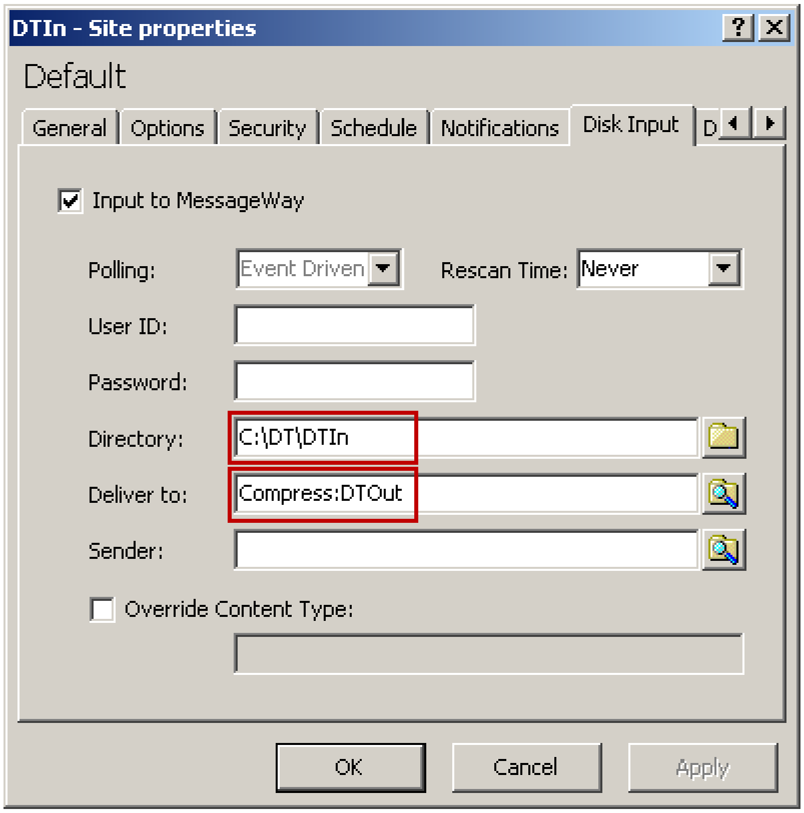
□ Retry after 1 minutes 1 times

□ Redirect to

3 Create a disk input location called DTIn, and on the **Disk Input** page:

a) Create and specify the input directory location where you will put the test file

b) ***Specify the compound address*** (on page 657) to send the file first to the compress service location and then to the disk output location



☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

Password:

Directory: C:\DT\DTIn

Deliver to: Compress:DTOut

Sender:

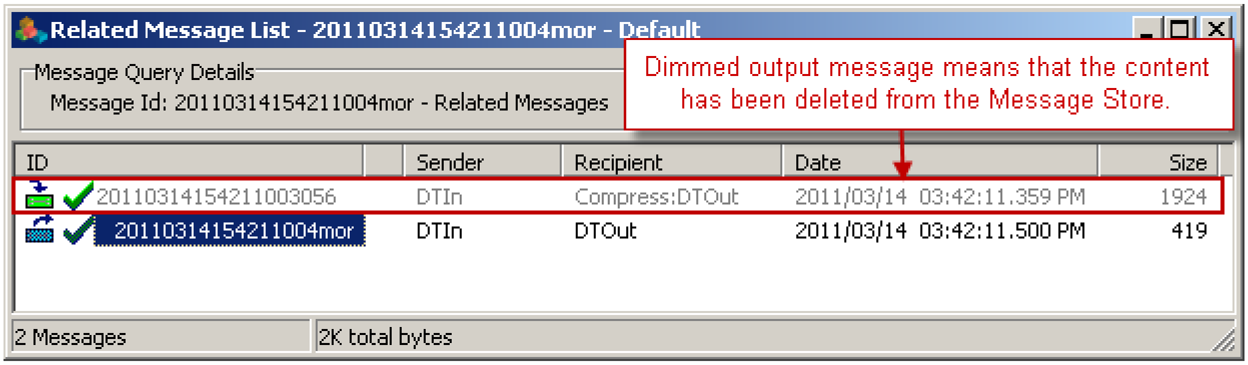
□ Override Content Type:

4 Create a disk output location called DTOut, and if necessary, create the output directory on disk.

5 Make sure the disk adapter and compress service are running.

6 Create or copy a small file for testing, and put it in the input directory.

7 From the MessageWay Manager, ***find the completed message*** (on page 735), and right-click and select **Get Related** from the pop-up menu. Notice that the output file from the Compress location is dimmed, which indicates that the content file has been deleted from the Message Store.



Message Id: 20110314154211004mor - Related Messages

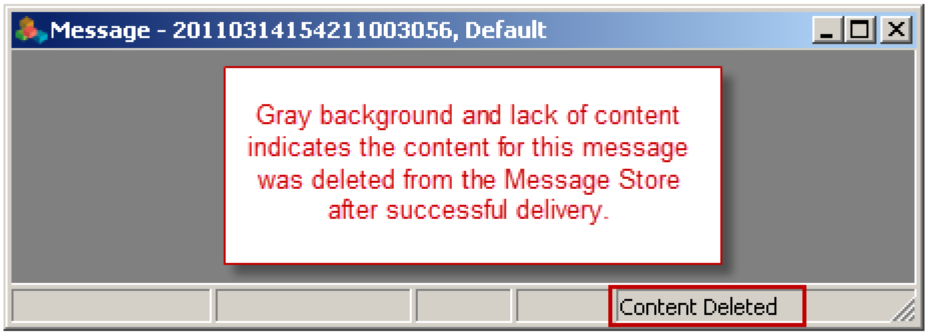
Dimmed output message means that the content has been deleted from the Message Store.

ID	Sender	Recipient	Date	Size
20110314154211003056	DTIn	Compress:DTOut	2011/03/14 03:42:11.359 PM	1924
20110314154211004mor	DTIn	DTOut	2011/03/14 03:42:11.500 PM	419

2 Messages

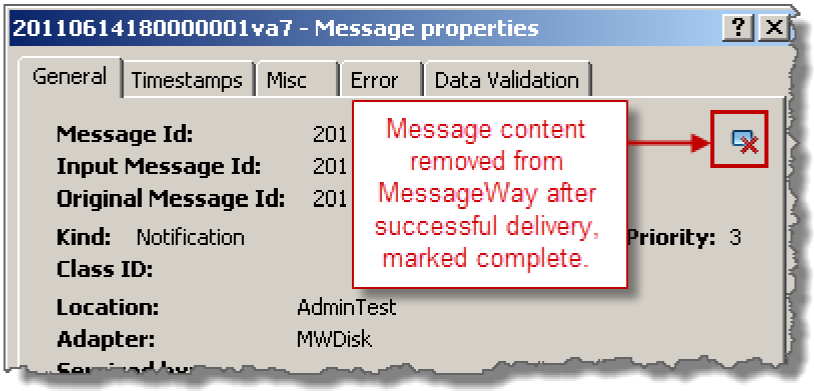
2K total bytes

8 From the Related Message List window, double-click the dimmed message to display the message content window. Notice that it is gray and the message in the bottom right corner says *Content Deleted*.



Gray background and lack of content indicates the content for this message was deleted from the Message Store after successful delivery.

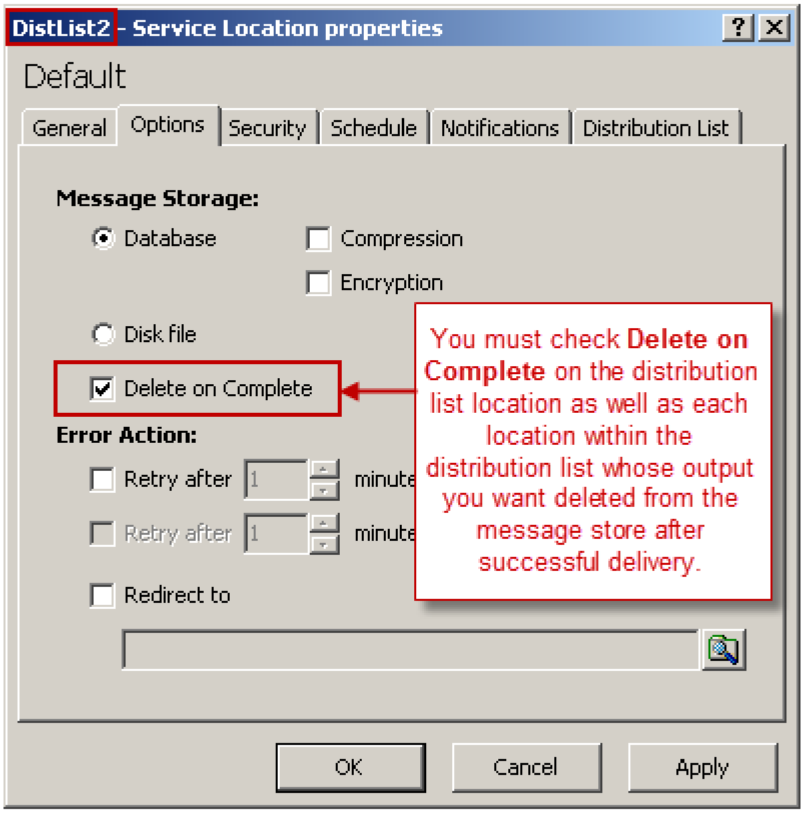
9 From the Related Message List window, right-click the output message, and select **Properties**. On the **General** page of the Message Properties window, notice the icon in the upper right corner indicates that the content of the message has been deleted.



Message Id: 201
Input Message Id: 201
Original Message Id: 201
Kind: Notification
Priority: 3
Class ID:
Location: AdminTest
Adapter: MWDisk

Message content removed from MessageWay after successful delivery, marked complete.

CAUTION: To use Delete on Complete (DOC) with a distribution list, all configurations associated with that distribution list must also have DOC set, including the distribution list itself. And if you are using dynamic distribution lists, which are locations separated by commas, the system location {Dist} must also have DOC set. Also, during runtime, all messages must be marked *Complete* or *Canceled*. If any message *does not* have a status of *Complete* or *Canceled* or one of the location configurations *does not* have DOC configured, *no* message will be deleted.



Message Storage:

● Database

□ Compression

□ Encryption

○ Disk file

☑ Delete on Complete

Error Action:

□ Retry after 1 minute

□ Retry after 1 minute

□ Redirect to

You must check **Delete on Complete** on the distribution list location as well as each location within the distribution list whose output you want deleted from the message store after successful delivery.

Specifying Security for Locations

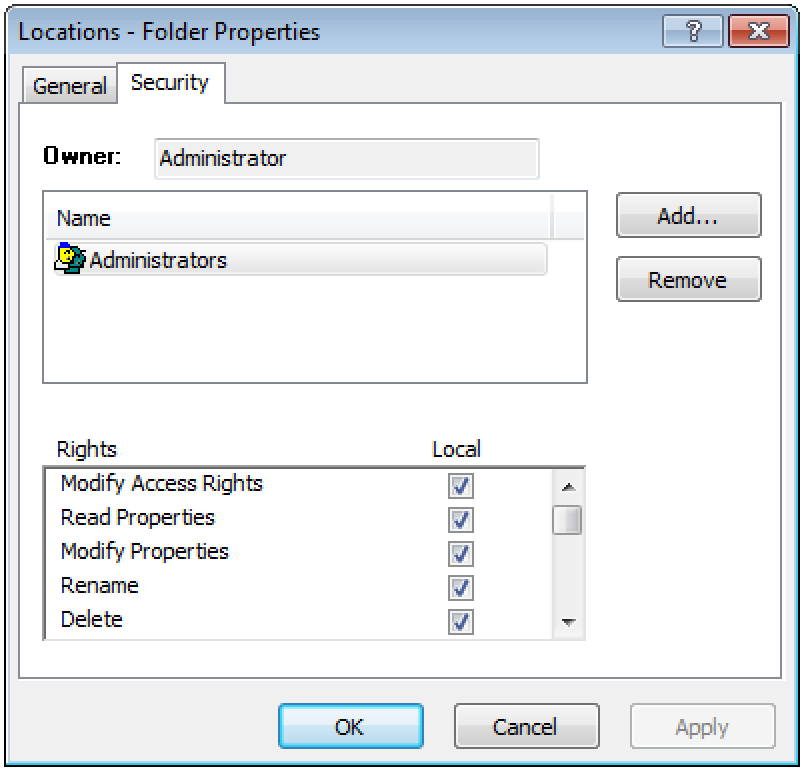
Users must specify which users or user groups have access to this location and which tasks they are allowed to perform.

Configuring Security for Folders

Locations may inherit some security settings from their system folder, **Locations** or **File System**, depending on where they are defined. For all system folders, the Administrators group with full rights is on the access list. For locations defined in the Locations folder, users may create other levels of folders within this system folder to organize their locations. For locations defined in the File System folder, users may create parent directories by creating locations beneath locations.

The **Security** page of the Folder Properties window shows the owner of the folder, which users or user groups are allowed access to the folder and its contents and what actions these users or user groups may perform. An access list controls access to this folder. The access list consists of a list of users or user groups and the rights that each one has. Objects directly beneath the folder or directory may inherit its access list.

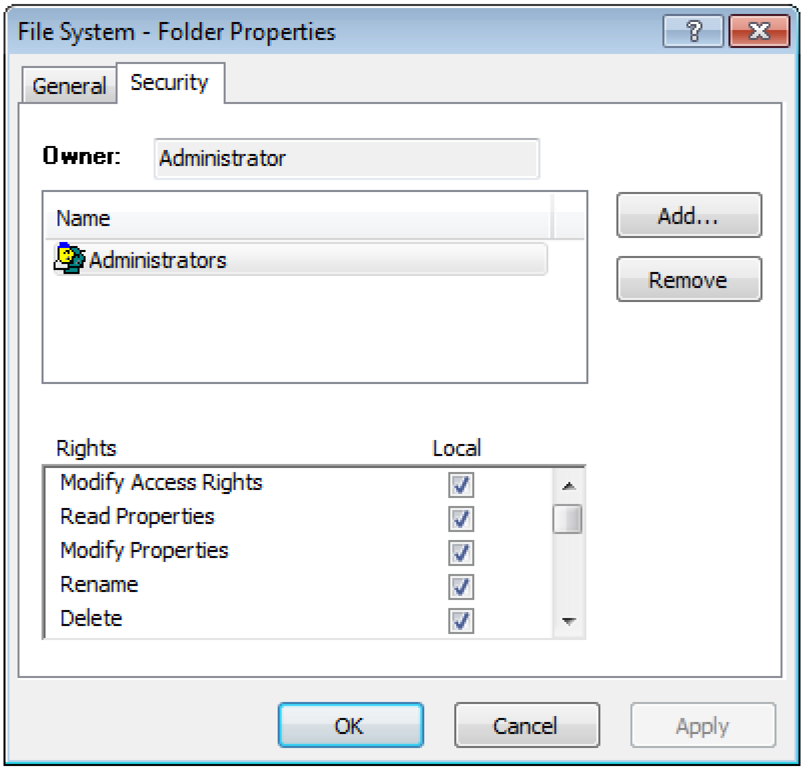
Different folders have different rights. For more information about the rights for a specific folder, refer to the topic, ***Rights (Folder Properties)*** (on page 1029). By default, when users create new folders or directories, the Administrators group with full rights is on the access list.



Owner: Administrator

Name
Administrators

Rights	Local
Modify Access Rights	☑
Read Properties	☑
Modify Properties	☑
Rename	☑
Delete	☑



Owner: Administrator

Name
Administrators

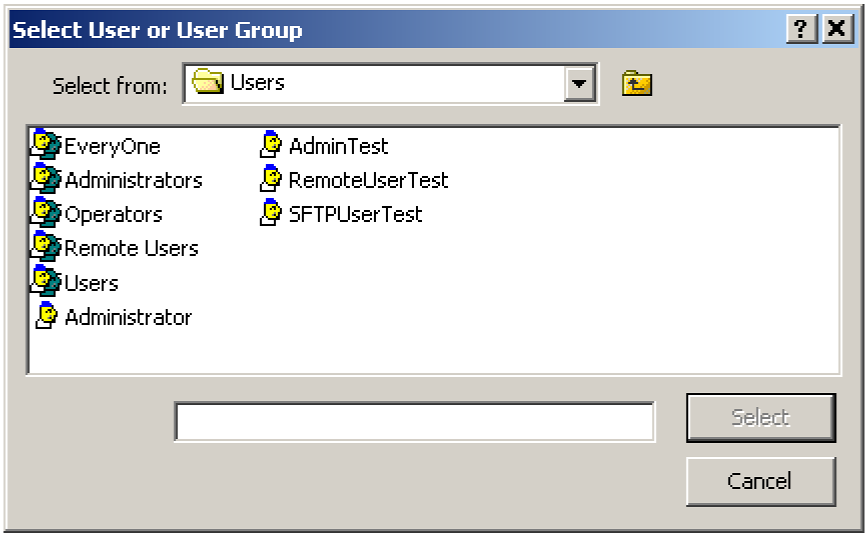
Rights	Local
Modify Access Rights	☑
Read Properties	☑
Modify Properties	☑
Rename	☑
Delete	☑

NOTE: These instructions only apply to folders in the Locations folder.

To give a user or user group access to a new folder:

1. Within the **Locations** folder, ***create a new folder*** (on page 462).
2. Double click the new folder, and on the **Security** page, click the **Add** button.

   The Select User or User Group window appears.



Select from: Users

EveryOne
Administrators
Operators
Remote Users
Users
Administrator
AdminTest
RemoteUserTest
SFTPUserTest

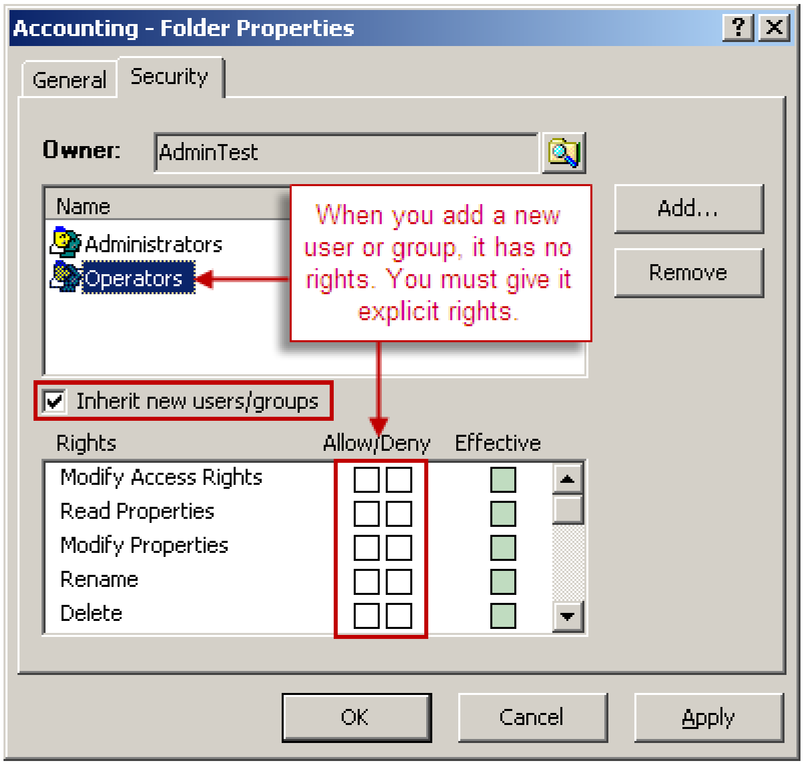
3. Select a group or user from the list, and click the **Select** button.

- or -

Type the name of a group or user in the box, and click the **Select** button.

NOTE: The EveryOne group is on the selection list, but not on the list under the Users folder, unless someone has added it manually. This group is only available for access lists. Add this group to the list to grant access rights to all users. All users are implicitly members of the EveryOne user group. As a result, when EveryOne is added to an access list, the associated rights are granted to all users.

The Folder Properties window appears.



Owner: AdminTest

When you add a new user or group, it has no rights. You must give it explicit rights.

☑ Inherit new users/groups

Rights	Allow/Deny		Effective
Modify Access Rights	□	□	🟩
Read Properties	□	□	🟩
Modify Properties	□	□	🟩
Rename	□	□	🟩
Delete	□	□	🟩

IMPORTANT: For folders created by users, the box, **Inherit new users/groups**, is checked by default. If you do not want to inherit the security settings from higher folders, clear this box. Initially, there are no rights defined for the user or group added to the access list.

4 To specify rights for the user or user group on the access list, click the user or group you just added.

5 In the **Rights** box, click the **Allow** or **Deny** box to set the appropriate rights. For specific information about rights for folders, refer to the topic, ***Rights (Folder Properties)*** (on page 1029).

6 Click **Apply** or **OK**.

Configuring Security for Locations

Security for locations depends on who has access to do what. Although rights can be applied directly for users and user groups, rights can also be inherited. Containers hold objects and have security properties that can be inherited by locations in the containers. What functions as a container is different in the Locations folder and the File System folder.

For locations In the Locations folder, the containers are folders. Location security properties may be inherited from parent folders.

In the FIle System folder, the containers are the locations themselves, because they play a dual role: they are both locations and a node in a directory. Location properties may be inherited from parent locations.

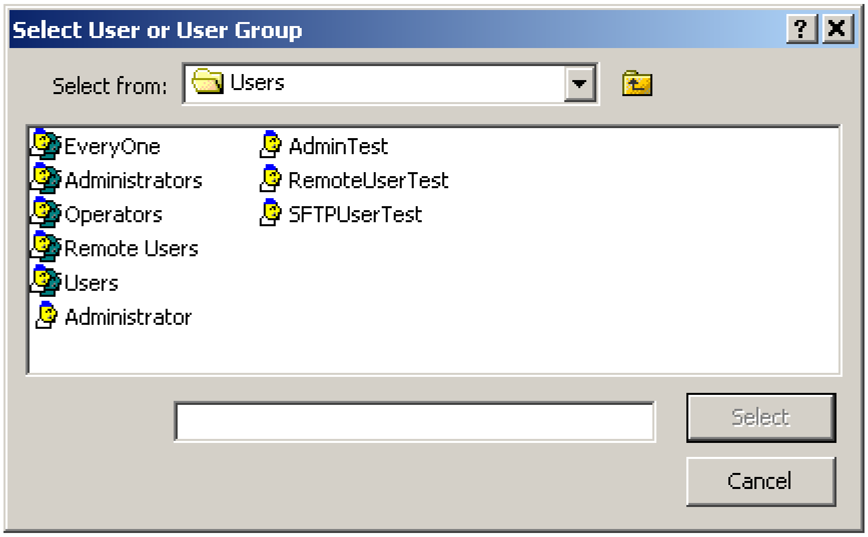
To Give a User or User Group Access to a Location in the Locations Folder

Locations may be created directly under the system folder, **Locations**, or within one or more levels of user folders within the **Locations** folder. These folders have access lists and rights settings. Folders created by users may inherit rights from higher folders.

You give locations access to MessageWay users by adding them or a user security group to which they belong to the access list. To create a location, refer to the topic, ***How to Create a Location*** (on page 461). To configure security for the location, proceed as follows:

1 On the **Security** page of the location properties window, click **Add**.

The Select User or User Group window appears.



2 Select a group or user from the list, and click the **Select** button.

- or -

Type the name of a group or user in the box, and click the **Select** button.

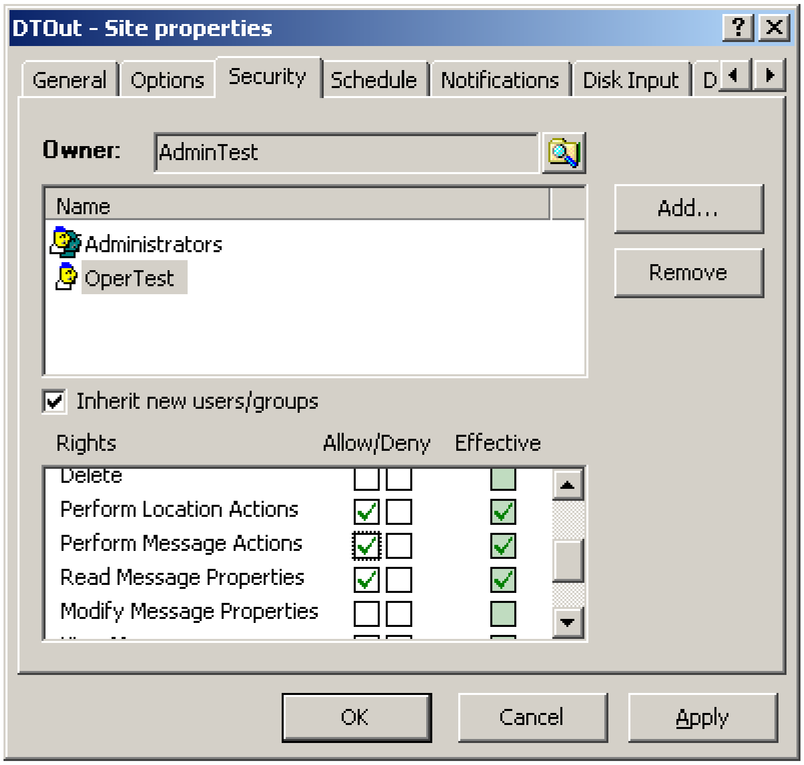
NOTE: The EveryOne group is on the selection list, but not on the list under the Users folder, unless someone has added it manually. This group is only available for access lists. Add this group to the list to grant access rights to all users. All users are implicitly members of the EveryOne user group. As a result, when EveryOne is added to an access list, the associated rights are granted to all users.

The Location Properties window appears.

IMPORTANT: For folders created by users, the box, **Inherit new users/groups**, is checked by default. If you do not want to inherit the security settings from higher folders, uncheck this box. Initially, there are no rights defined for the user or group when someone adds it to the access list.

3 To specify rights for the user or user group on the access list, click the user or group you just added.

4 In the **Rights** box, click the **Allow** or **Deny** box to set the appropriate rights. For specific information about rights for folders, refer to the topic, ***Rights (Folder Properties)*** (on page 1029).



Owner: AdminTest

Name
Administrators
OperTest

☑ Inherit new users/groups

Rights	Allow	Deny	Effective
Delete	□	□	□
Perform Location Actions	☑	□	☑
Perform Message Actions	☑	□	☑
Read Message Properties	☑	□	☑
Modify Message Properties	□	□	□

5 Click **Apply** or **OK**.

To Give a User or User Group Access to a Location in the File System Folder

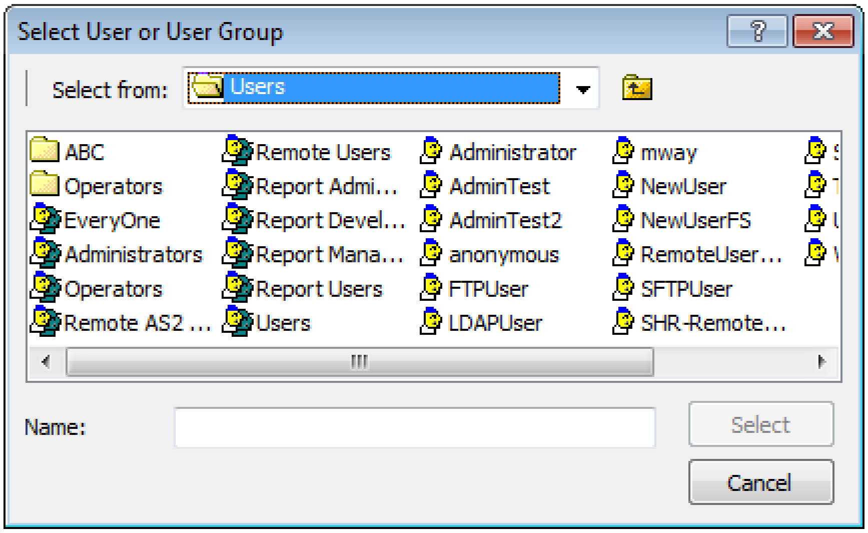
To give a user or user group access to a File System location:

1 Within the **File System** folder, ***create a new location*** (on page 465).

2 In the right pane, right-click the new folder, and select **Properties**.

3 On the **Security** page, click the **Add** button.

The Select User or User Group window appears.



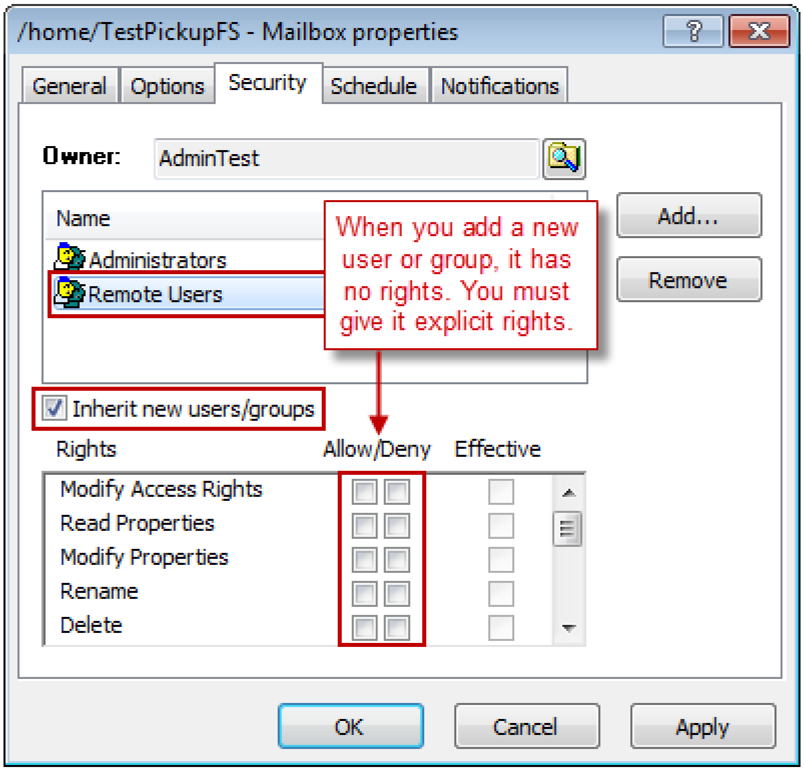
4 Select a group or user from the list, and click the **Select** button.

- or -

Type the name of a group or user in the box, and click the **Select** button.

NOTE: The EveryOne group is on the selection list, but not on the list under the Users folder, unless someone has added it manually. This group is only available for access lists. Add this group to the list to grant access rights to all users. All users are implicitly members of the EveryOne user group. As a result, when EveryOne is added to an access list, the associated rights are granted to all users.

The Mailbox or Service Location Properties window appears.



/home/TestPickupFS - Mailbox properties

Owner: AdminTest

Name
- Administrators
- Remote Users

When you add a new user or group, it has no rights. You must give it explicit rights.

☑ Inherit new users/groups

Rights	Allow/Deny	Effective
Modify Access Rights	□ □	□
Read Properties	□ □	□
Modify Properties	□ □	□
Rename	□ □	□
Delete	□ □	□

IMPORTANT: For folders created by users, the box, **Inherit new users/groups**, is checked by default. If you do not want to inherit the security settings from higher locations (directory), clear this box. Initially, there are no rights defined for the user or group added to the access list.

5 To specify rights for the user or user group on the access list, click the user or group you just added.

6 In the **Rights** box, click the **Allow** or **Deny** box to set the appropriate rights. For specific information about rights for folders, refer to the topic, ***Rights (Folder Properties)*** (on page 1029).

7 Click **Apply** or **OK**.

Specifying Scheduling Strategies

Users may specify a scheduling strategy using the **Schedule** page of the location properties window. Schedules affect both polling for input and automatic delivery of output. We recommend, therefore, to avoid conflict of schedules for input and output, that users create locations for either input or output, but not both.

System and pickup mailboxes do not use schedules, because they are never used to poll for input or deliver output messages. Schedules apply only to locations that use input polling or automatic delivery of output, which are sites and service locations.

The basic types of schedule strategies are as follows:

Schedule Option	Description
Always open	No constraints on when messages may be received or delivered
Always closed	Messages may be received or delivered only when opened by another process, such as: ▪ Threshold release ▪ Input Now command ▪ Execute Now command
Schedule	Input and output controlled by time/date windows
Location	Local schedule that applies only to this location
Master	Schedule that may be shared by multiple locations
Threshold Release	Batches received messages during a closed schedule and delivers them when the schedule opens.

Configuring Threshold Release

Users may need to accumulate messages in a location before MessageWay attempts delivery. This is called threshold release. Users configure threshold release on the **Schedule** tab of the location properties window. Threshold release works by opening a closed schedule when a certain number of messages have accumulated in the location. If the state of the schedule is open, then threshold release will have no effect, because messages will not accumulate.

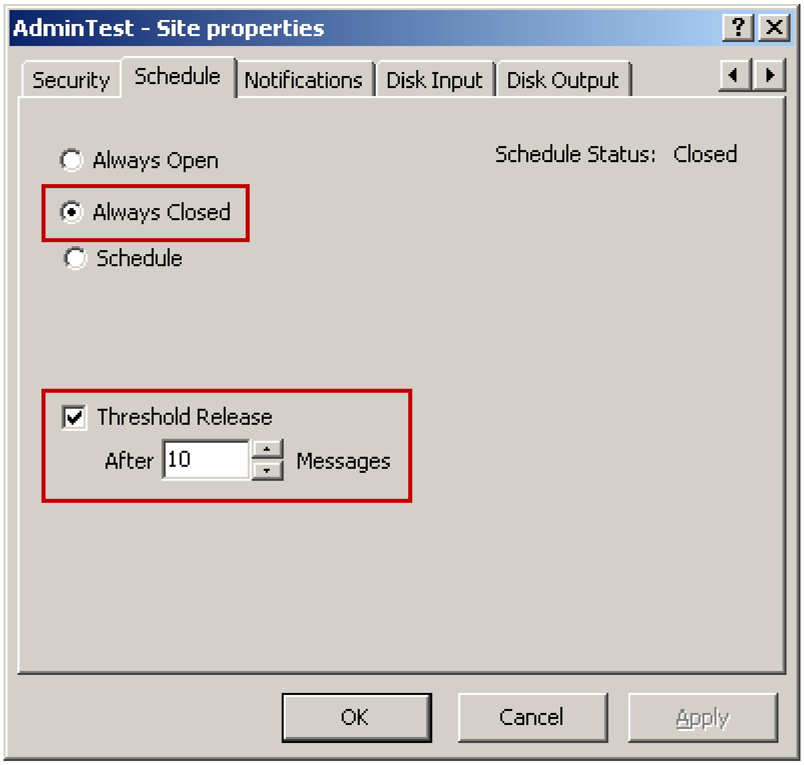
To use threshold release, from the **Schedule** page of the location properties window, proceed as follows:

1. Select **Always Closed**

   - or -

   Select **Schedule**

2 Check **Threshold Release**, and type or select a number of messages, such that when this many accumulate in the location, they will be released to the adapter or service for delivery.



○ Always Open

Schedule Status: Closed

● Always Closed

○ Schedule

☑ Threshold Release

After 10 Messages

3 Click **OK** or **Apply** to save the changes.

Configuring Master Schedules for Locations

Master schedules allow users to create a schedule that can be used by mulitple locations. First, you create a master schedule in the Master Location Schedules folder, and then you link it to any location capable of polling or auto-delivery, such as sites and service locations.

To Create a Master Schedule

1 In the left pane of MessageWay Explorer, select **Master Location Schedules**.

2 In the right pane, right-click and select **Add Schedule** from the menu.

3 In the **Enter New Master Schedule Name** dialog box, type the name of your schedule.

The schedule window appears.

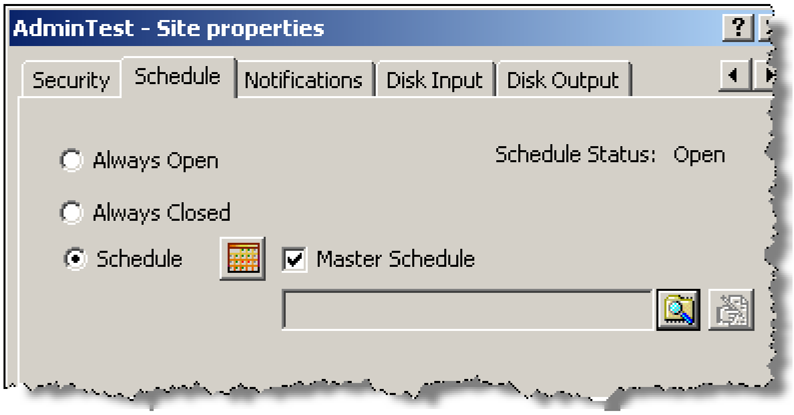
4 ***Add items to the schedule.*** (on page 499)

To Use a Master Schedule for a Location

To link a master schedule to a location, proceed as follows:

1 From the location window, click the **Schedule** tab.

2 Select **Schedule**, and check the **Master Schedule** box.



AdminTest - Site properties

○ Always Open

○ Always Closed

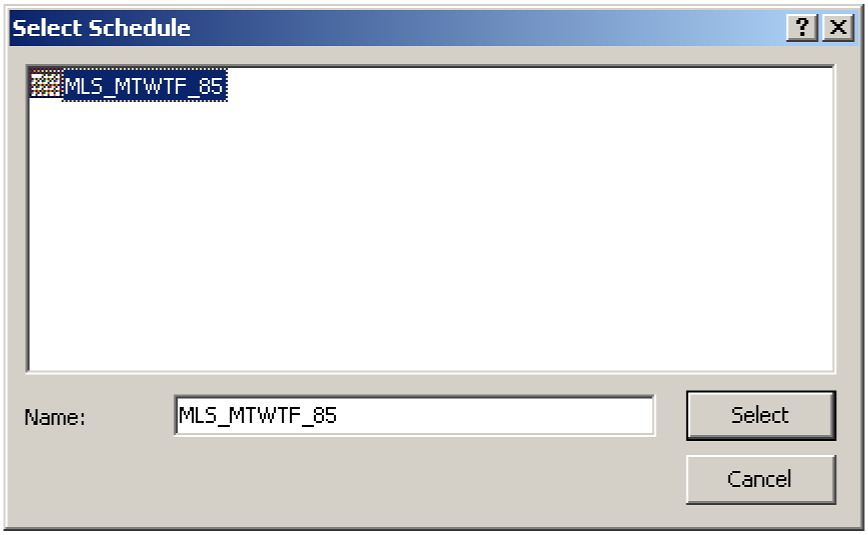
● Schedule ☑ Master Schedule

Schedule Status: Open

3 Click the **Select Master Location Schedule** button, .

The **Select Schedule** dialog box appears.

4 From the list, select the schedule you want, and click the **Select** button.

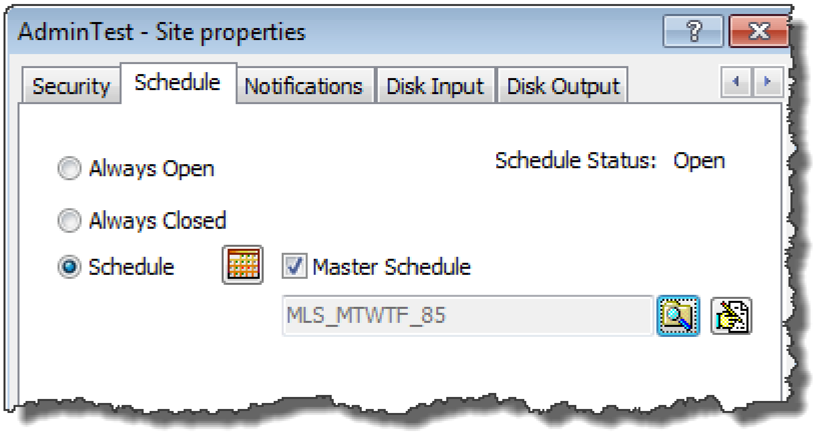


Select Schedule

MLS_MTWTF_85

Name: MLS_MTWTF_85

5 The master schedule name appears in the schedule box.



AdminTest - Site properties

○ Always Open

○ Always Closed

● Schedule ☑ Master Schedule

MLS_MTWTF_85

Schedule Status: Open

6 To view the master schedule, click the **View Master Schedule** button, . The schedule appears with all items dimmed, since you cannot change the master schedule from here.

7 ***To use this master schedule as a template to create a local schedule*** (on page 498), click the **Customize Schedule** button, .

Configuring Local Schedules for Locations

Local schedules allow users to create a schedule for a location that has specific requirements. Users create schedules by adding schedule items. They can also use a master schedule as a starting point, and modify the items to create a local schedule.

To Create a Local Schedule

1 In the left pane of MessageWay Explorer, select **Locations**.

2 In the right pane, double-click a location for which you want to create a schedule.

The location window appears.

3 On the **Schedule** tab, click **Schedule**.

The schedule window appears.

4 ***Add items to the schedule*** (on page 499).

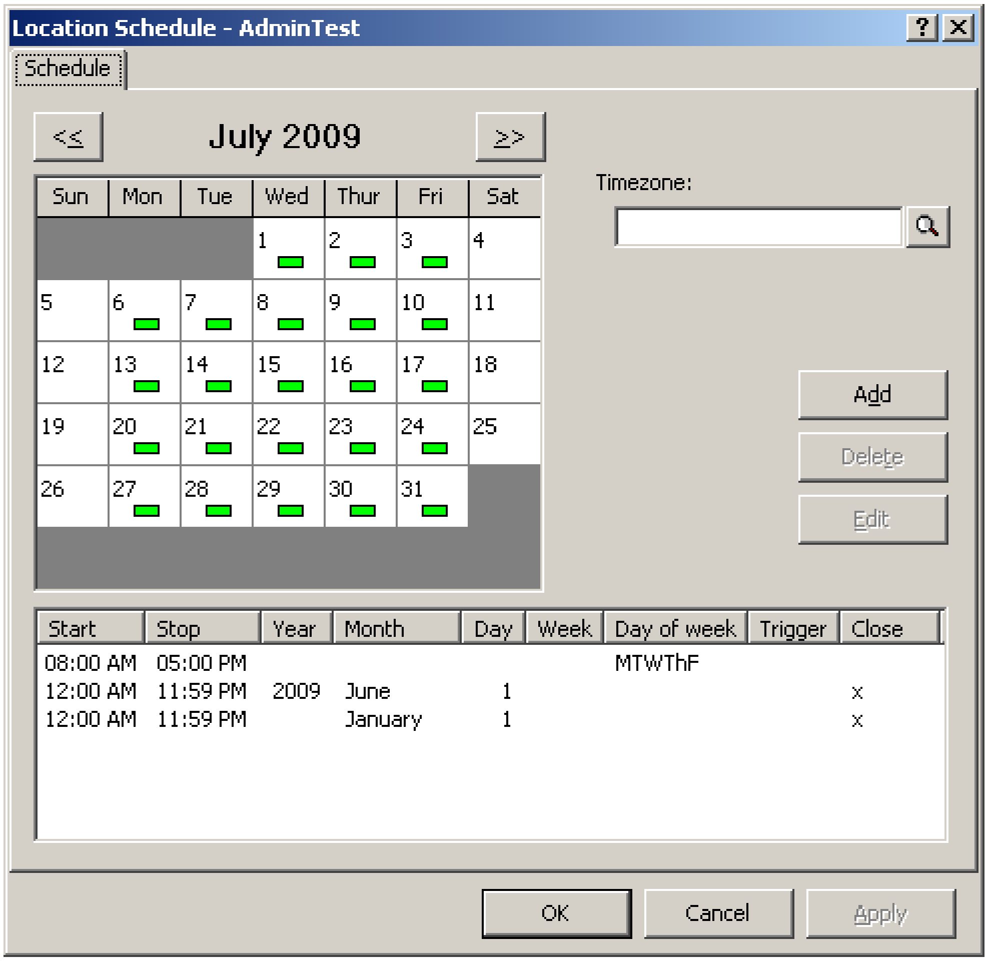
To Create a Local Schedule from a Master Schedule

To create a local schedule starting from a master schedule, proceed as follows:

1 From the location window, click the **Schedule** tab.

2 Select **Schedule**, and click the **Customize Schedule** button, .

The schedule window appears with the items from the master schedule.



Sun	Mon	Tue	Wed	Thur	Fri	Sat
			1 🟩	2 🟩	3 🟩	4
5	6 🟩	7 🟩	8 🟩	9 🟩	10 🟩	11
12	13 🟩	14 🟩	15 🟩	16 🟩	17 🟩	18
19	20 🟩	21 🟩	22 🟩	23 🟩	24 🟩	25
26	27 🟩	28 🟩	29 🟩	30 🟩	31 🟩	

Start	Stop	Year	Month	Day	Week	Day of week	Trigger	Close
08:00 AM	05:00 PM					MTWThF		
12:00 AM	11:59 PM	2009	June	1				x
12:00 AM	11:59 PM		January	1				x

3 ***Configure schedule item*** (on page 499) as required.

4 Click **OK** or **Apply** to save changes.

Configuring Schedule Items

Whether you create a master location schedule to be shared by various locations or a local schedule specific to a location, you use the same procedures to create and maintain schedule items.

To Create a Schedule Item

To create a schedule item for a master or local schedule:

1 From the schedule window, on the **Schedule** tab, click **Add**.

The Add Schedule Item window appears.

2 For **Schedule Type**, click the down arrow, and from the menu select **Daily**, **Weekly**, **Monthly**, **Yearly** or **Absolute**.

3 Type or select the date and time the period starts.

4 Type or select the date and time the period ends, which by default creates an open window.

- or -

To initiate an event at the start date and time period rather than open or close the schedule for a period of time:

a) ***Check the* Trigger *box*** (on page 1276).

The end date and time options are dimmed.

b) ***Select an event from the drop-down menu*** (on page 1276).

5 To close the window for the period and override any settings that have created an open window, check **Force Closed**.

6 Click **Add** to add the item to the schedule.

The item appears in the **Schedule** list, and a rectangular bar appears in the calendar as a visual aid.

7 To add another schedule item to the schedule, repeat the previous steps.

To Edit a Schedule Item

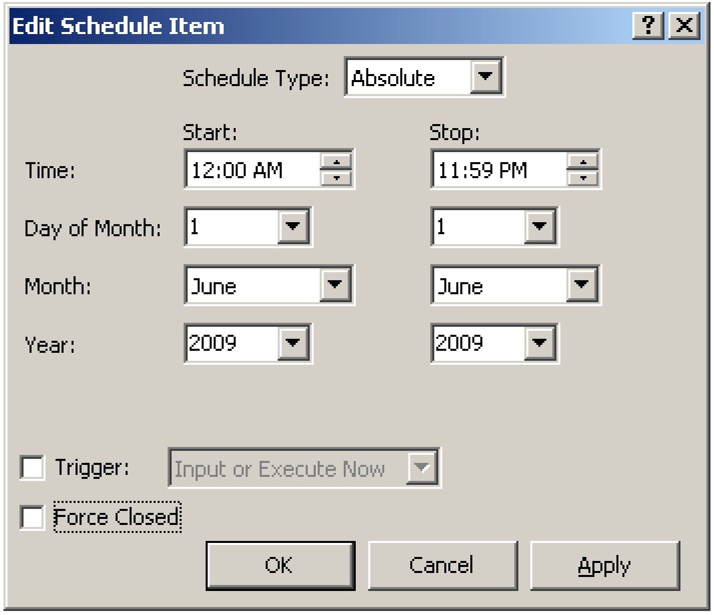
You may edit one schedule item from the list.

1 From the list, select the schedule item you want to edit, and click the **Edit** button.

The Edit Schedule Item window appears with the current settings.

2 Change the settings as required.

When you make changes, the **Apply** button becomes active.



Schedule Type: Absolute

	Start:	Stop:
Time:	12:00 AM	11:59 PM
Day of Month:	1	1
Month:	June	June
Year:	2009	2009

□ Trigger: Input or Execute Now

□ Force Closed

3 Click the **OK** button to save the changes and close the window.

The schedule window appears.

To Delete Schedule Items

To delete one or more schedule items from the list, proceed as follows:

1. From the **Schedule** list, select one or more schedule items you want to delete.
2. Click the **Delete** button, and when a confirmation dialog box appears, click **OK** to confirm the delete.

Specifying Notification Strategies

The **Notifications** page of the location properties window allows users to specify whether to create a notification message, under what circumstances, and the location to which it should be sent. Notification reports are short text messages identifying the event that occurred. Notice that the events that you can select to generate a notification report vary depending on whether the location is a site, associated with an adapter, or a service location, associated with a service.

Options for Notifications for Locations

Click the **Create Notification Reports 1** or **2** check box and choose events to request that a notification be sent to the specified location when the event occurs. Users may configure up to two notification options, typically to send different types to different locations.

Select any of the notification events for which you want to send a notification report. The options for the various types of locations are listed in the following table:

Location Type	**Valid Notification Events**
Input	Receipt Receipt Failure **NOTE:** For pickup mailboxes, receipt notifications should be set on the default location of the sender.
Output or Mailbox	Arrival Delivery Non-Delivery Notification Failure Duplicate Receipt **NOTE:** For pickup mailboxes, arrival notifications should be set on the default location of the recipient.
System Mailbox	Arrival Receipt Failure Notification Failure Duplicate Receipt

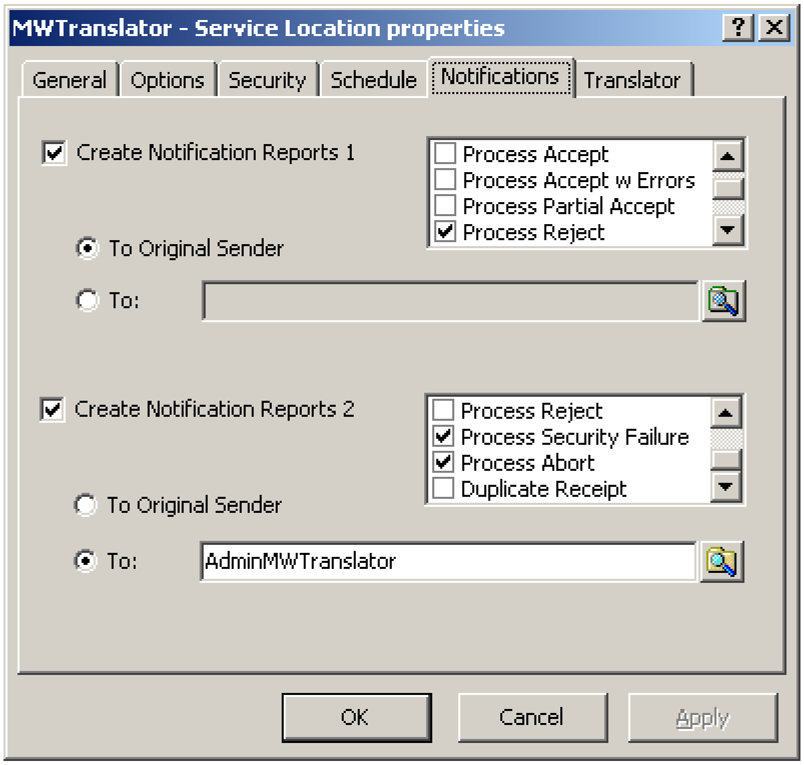
Location Type	Valid Notification Events
I/O	Receipt Receipt Failure Arrival Delivery Non-Delivery Notification Failure Duplicate Receipt
Service	Receipt Receipt Failure Arrival Process Accept Process Accept w(ith) Errors Process Partial Accept Process Reject Process Security Failure Process Abort Duplicate Receipt

Select **To Original Sender** to send the report of the selected event(s) to the original sending location or address. MessageWay determines this original sender. This is not the original sender as determined by MWTranslator to return acknowledgments.

Select **To** and type or select a location name to which the notification reports will be sent for the selected event(s). When the location does not exist, the report is sent to the **{Unknown}** system mailbox.

Examples of Notification Configurations

The following example shows notifications configured for the service location, MWTranslator. Note that different types of reports may be sent to different locations.



☑ Create Notification Reports 1

□ Process Accept
□ Process Accept w Errors
□ Process Partial Accept
☑ Process Reject

● To Original Sender

○ To:

☑ Create Notification Reports 2

□ Process Reject
☑ Process Security Failure
☑ Process Abort
□ Duplicate Receipt

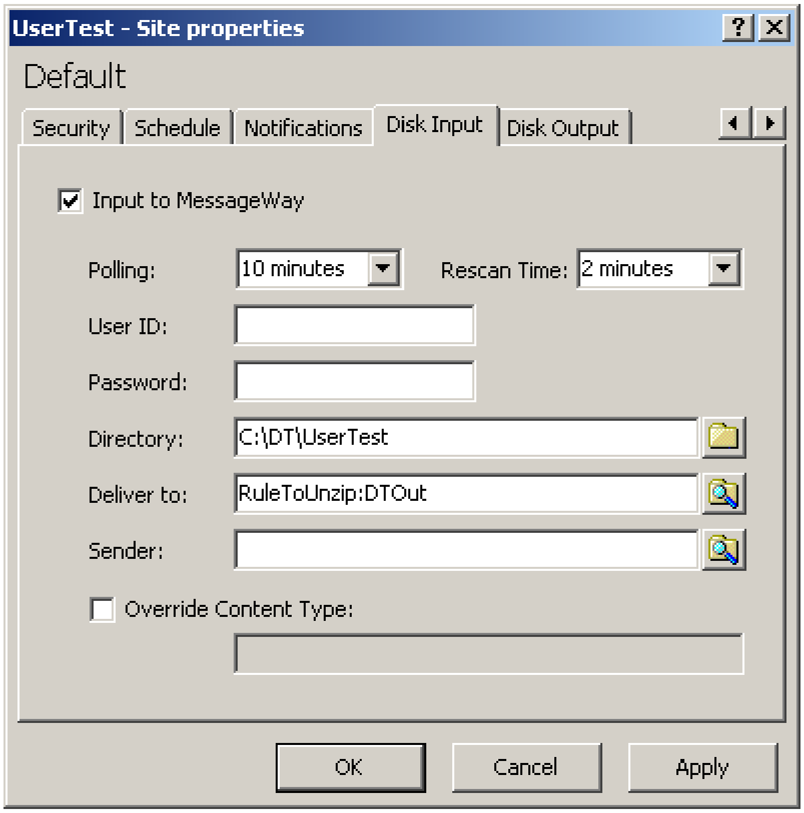
○ To Original Sender

● To: AdminMWTranslator

Examples of Notifications Configured for the MWTranslator service location (Notifications Page, Service Location Properties Window)

The following set of examples shows a notification should be created when the process rejects the message, and the resulting notification report should be returned to the original sender, so the site must support both input and output. This is one example of where a site would be configured for input and output.

In this scenario, the input site, UserTest, sends a message to the service location, RuleToUnZip, to determine where to route the message. The UserTest site must be configured for both input and output. The input configuration allows the Disk Transfer Adapter to poll for messages in the specified location. The output configuration allows it to send the returned notification to a different disk location. Compression service locations, such as UNZIP, do not have routing capability, so the input page uses a compound address to route the output when it has been unzipped. .



UserTest - Site properties

Default

☑ Input to MessageWay

Polling: 10 minutes

Rescan Time: 2 minutes

User ID:

Password:

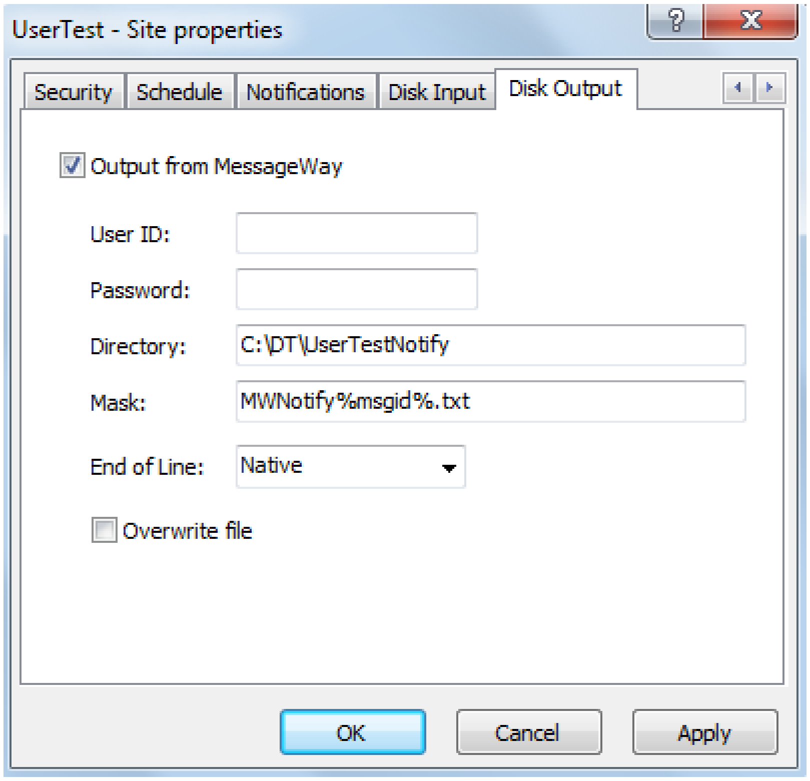
Directory: C:\DT\UserTest

Deliver to: RuleToUnzip:DTOut

Sender:

□ Override Content Type:

Example of I/O Site to Send Message and Receive Notification (Disk Input Page, Site Properties Window)



☑ Output from MessageWay

User ID:

Password:

Directory: C:\DT\UserTestNotify

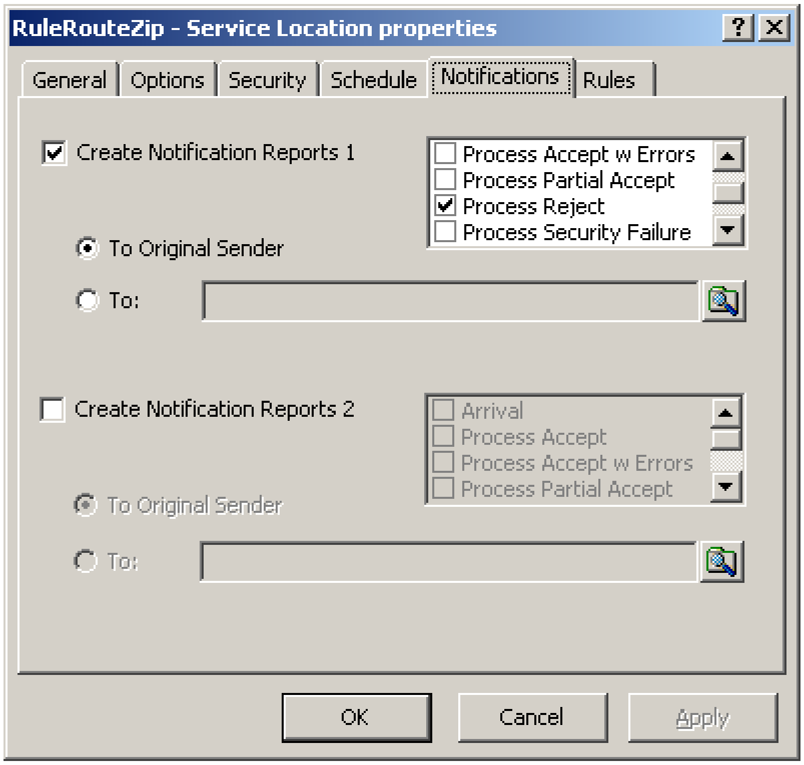
Mask: MWNotify%msgid%.txt

End of Line: Native

□ Overwrite file

Example of I/O Site to Send Message and Receive Notification (Disk Output Page, Site Properties Window)

The Rules Processing Service associated with this service location, uses the rules processing profile listed on the **Rules** page to determine how to route the message. When one of the rules rejects the message, the service generates a notification report, which it sends back to the original sender, UserTest, as specified on the **Notifications** page of the RulesRouteZip service location configuration.



☑ Create Notification Reports 1

☐ Process Accept w Errors
☐ Process Partial Accept
☑ Process Reject
☐ Process Security Failure

● To Original Sender
○ To:

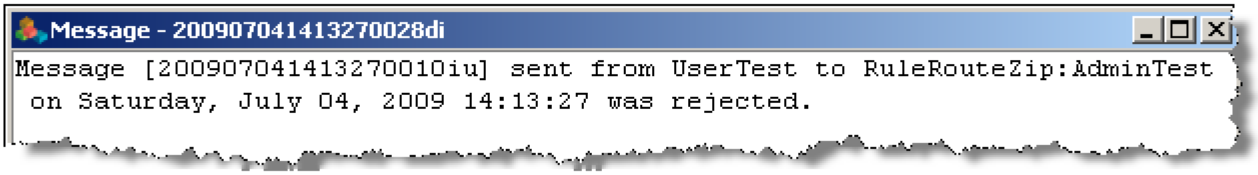
☐ Create Notification Reports 2

☐ Arrival
☐ Process Accept
☐ Process Accept w Errors
☐ Process Partial Accept

● To Original Sender
○ To:

Examples of Notifications Configured for a Rules Processing Service Location (Notifications Page, Service Location Properties Window)

The process rule only routes the message when it identifies it as a zipped file. In this case, the message was not zipped, so the service rejected the message, and sent a notification to the sender. When you review the messages for the original sender location, UserTest, you find the notification report shown here.



```
Message [20090704141327001Oiu] sent from UserTest to RuleRouteZip:AdminTest
 on Saturday, July 04, 2009 14:13:27 was rejected.
```

Example of Notification Report

Configuring an AS2 Site

An AS2 site is for outbound messages only, because AS2 is a push protocol, so you only use the AS2 adapter to send AS2 messages, not collect them.

NOTE: The MessageWay AS2 server and the AS2 adapter require a license from Progress. For more information, contact MessageWay Technical Support.

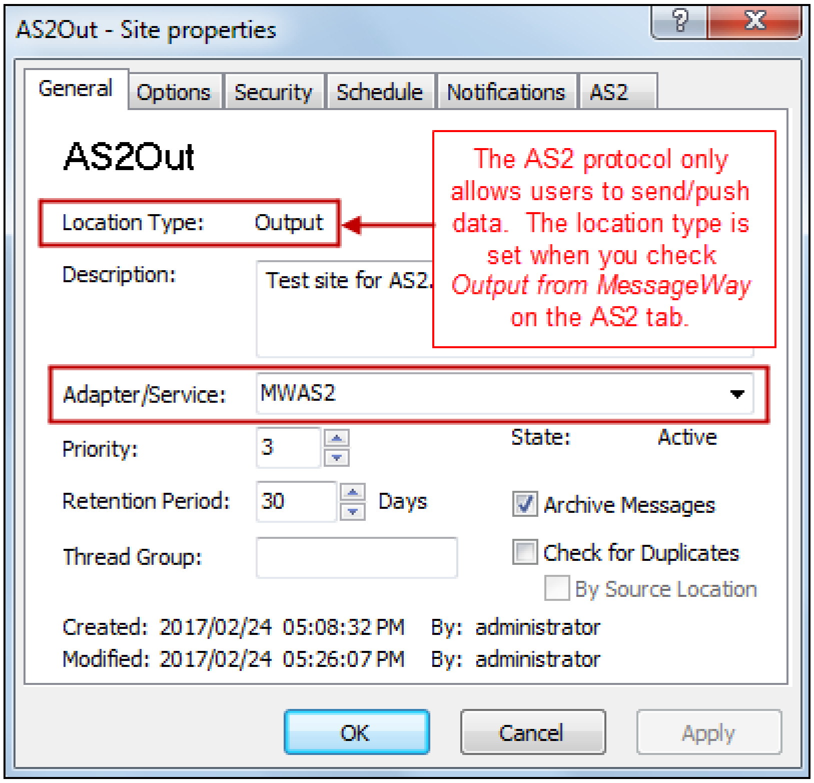
To allow MessageWay to send messages to an AS2 server through the AS2 Interface, you create an AS2 site in MessageWay.

To create an output site to send AS2 messages to your trading partner, proceed as follows:

1 Create a location with the following properties:

- Site name of **AS2Out**
- Adapter/Service should be **MWAS2**

The **General** page of the **AS2Out** site should look similar to the following:



AS2Out

Location Type: Output

Description: Test site for AS2.

Adapter/Service: MWAS2

Priority: 3

State: Active

Retention Period: 30 Days

Thread Group:

☑ Archive Messages

□ Check for Duplicates

□ By Source Location

Created: 2017/02/24 05:08:32 PM By: administrator

Modified: 2017/02/24 05:26:07 PM By: administrator

The AS2 protocol only allows users to send/push data. The location type is set when you check *Output from MessageWay* on the AS2 tab.

2 On the AS2 tab, configure the following:

Output from MessageWay Check this box.

Remote URL This address is required to connect to the remote AS2 server. Type the remote URL.

To Type the name for the recipient, upon which both parties agree, such as a DUNS number or company name. This value will appear as the AS2-To address on the AS2 message.

From MessageWay Sender Do not select this unless you want MessageWay to specify the sender of the message.

From

This field identifies the sender. Select this radio button, and type a value that identifies the sender to the remote AS2 server. This value will be the AS2-From address on the AS2 message.

For messages that will be signed, this value must uniquely match part of the sender's private key subject within the Java keystore (.jks). A private key subject includes the common name (CN), organizational unit (OU), organization (O), location (L), state (ST), and country (C), for example:

CN=MWayAS2, OU=AS2 Testing, O=MessageWay Solutions, L=Livonia, ST=MI, C=US

Request Timeout

Select the amount of time in seconds or minutes to allow the AS2 outbound processing cycle to complete. Initially, this default value comes from the value defined on the AS2 adapter, which users can override here.

Compress Data

Check this box to compress the data.

Encrypt Data

Check this box to encrypt the data.

Sign Message

Check this box to sign the message.

Request MDN

Check this box to request a return synchronous MDN.

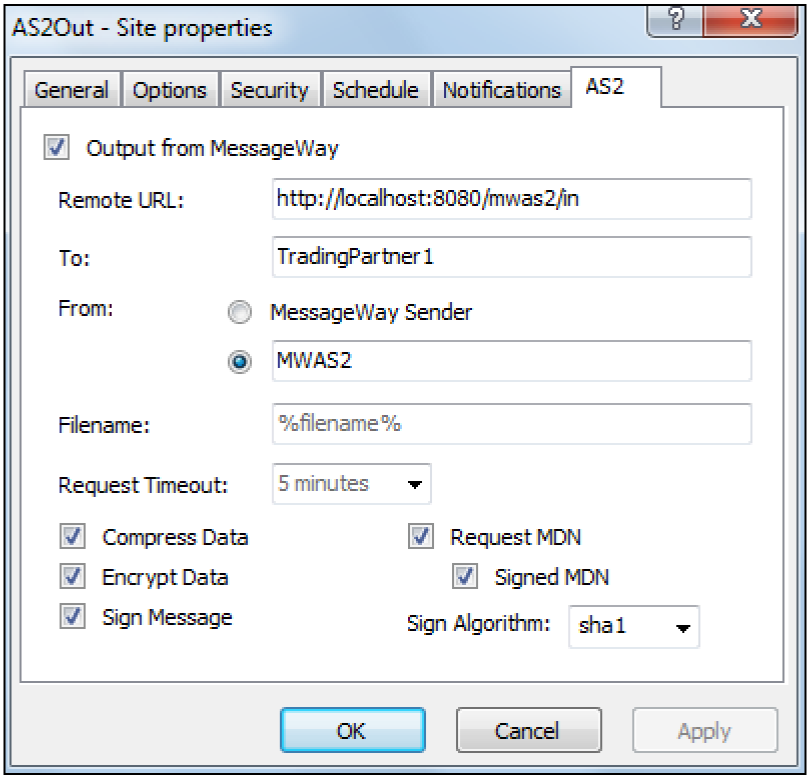
Sign MDN

Do not check this box, unless you want your partner to sign the returned MDN.

Sign Algorithm

If requesting a Signed MDN, select the MDN signing algorithm that your trading partner will use. Select one of the options, **sha1**, **md5**, **sha-256**, **sha-384**, **sha-512**, or **sha-224**.

The **AS2** page of the **AS2Out** site should look similar to the following:



AS2Out - Site properties

☑ Output from MessageWay

Remote URL: http://localhost:8080/mwas2/in

To: TradingPartner1

From: ○ MessageWay Sender

● MWAS2

Filename: %filename%

Request Timeout: 5 minutes

☑ Compress Data

☑ Encrypt Data

☑ Sign Message

☑ Request MDN

☑ Signed MDN

Sign Algorithm: sha1

3 Click **Apply** or **OK** to save your changes.

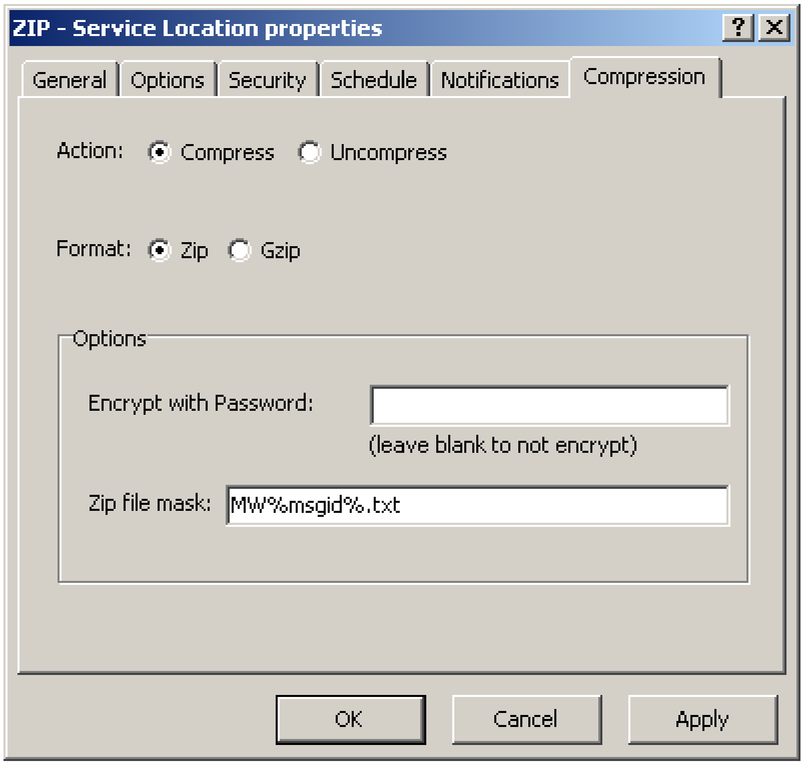
Configuring a Compression Service Location

Locations using the Compression service allow users to specify whether messages sent to this service location will be compressed or uncompressed using the zip or gzip format. For the zip format, users may specify whether the messages will be password protected and encrypted or decrypted using Zip 2.0 encryption format.

The MessageWay Compression Service compresses (zips) and uncompresses (unzips) files. It supports the PKWARE zip file format using the DEFLATE compression algorithm (RFC 1951) and the GZIP file format (RFC1952).

IMPORTANT: This type of location does not allow you to specify routing, so the routing instructions must come from an earlier process.

The options available depend on the combination of Compress/Uncompress and zip/gzip.



Action: ● Compress ○ Uncompress

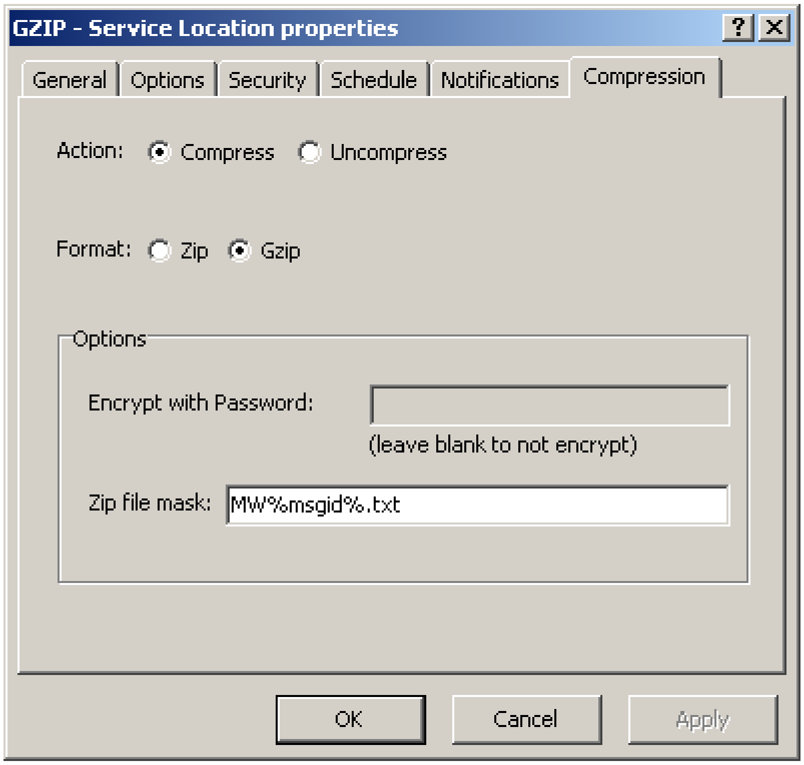
Format: ● Zip ○ Gzip

Options

Encrypt with Password:

(leave blank to not encrypt)

Zip file mask: MW%msgid%.txt



Action: ● Compress ○ Uncompress

Format: ○ Zip ● Gzip

Options

Encrypt with Password:

(leave blank to not encrypt)

Zip file mask: MW%msgid%.txt

Any messages sent to this ZIP or GZIP site will be compressed. The output will be sent to another destination specified by a compound address on the input location configuration. When no output location is specified, the output will be placed in the system mailbox, {Unknown}.

For more information about routing and compound addresses, refer to ***Specifying Routing Addresses*** (on page 653).

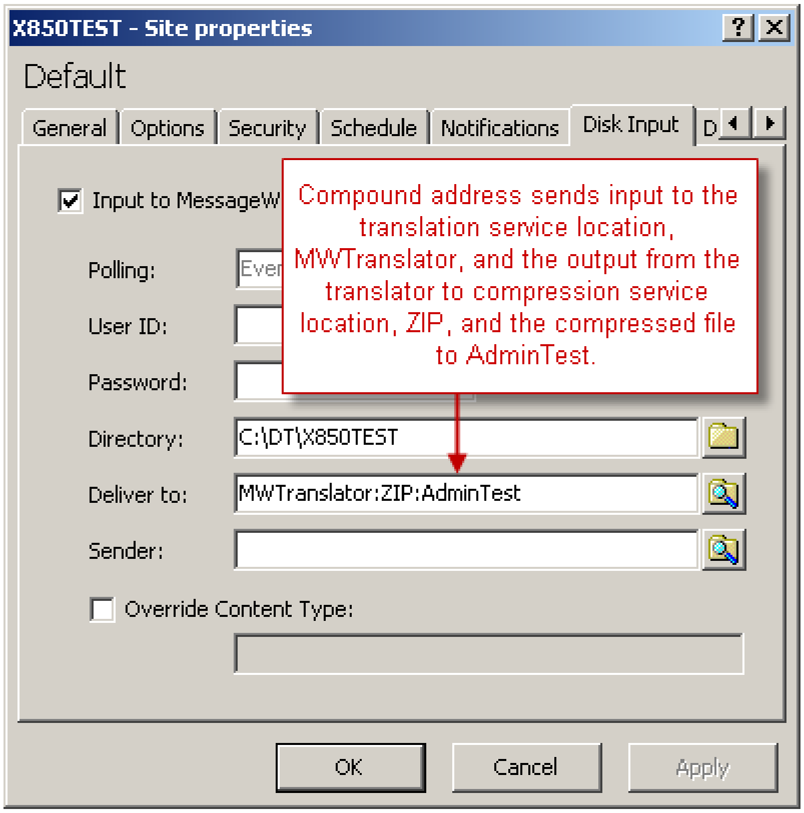
Routing Messages for Compression

Compression service locations do not have delivery parameters, so the routing information must come from an earlier location configuration. This is typically an input location that uses a compound address to pipe the message through various processes before its final destination.

For example, the following X850TEST input site uses a compound address to send messages to various locations before final delivery, as follows:

1. *MWTranslator*: message is sent from X850TEST to the MWTranslator service location.
2. *ZIP*: the output from MWTranslator is sent to the compression service location, ZIP. This part of the compound address overrides the routing that the translator would use for the output. This does not affect notifications or backward acknowledgments, whose destination locations are provided by the translator.
3. *AdminTest*: the compressed file is delivered to the output site, AdminTest.

NOTE: The name of the output file is determined by the mask on the destination location, which would be AdminTest in this example.



☑ Input to MessageW

Polling: Ever

User ID:

Password:

Directory: C:\DT\X850TEST

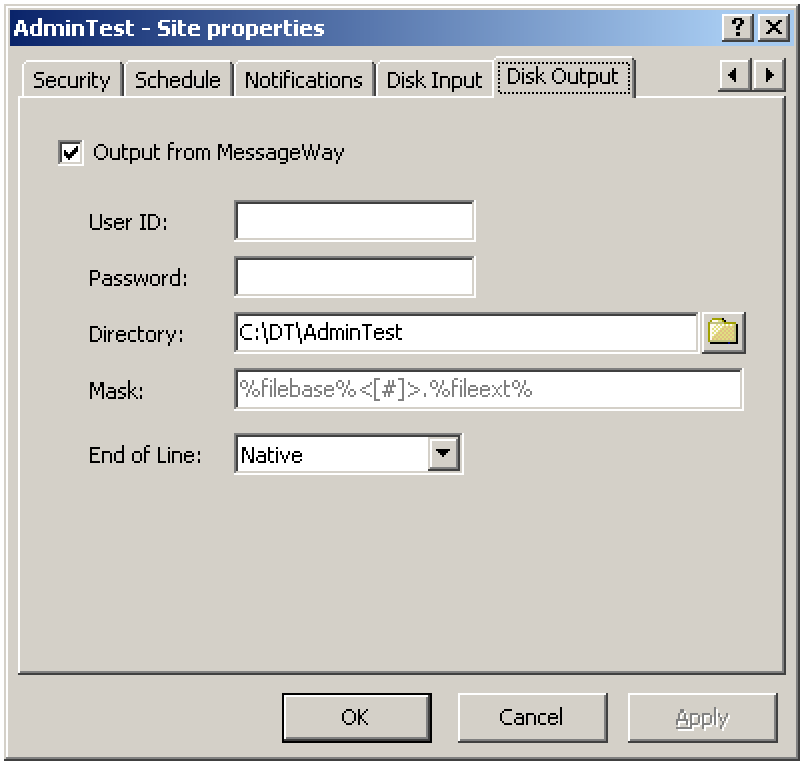
Deliver to: MWTranslator:ZIP:AdminTest

Sender:

□ Override Content Type:

Compound address sends input to the translation service location, MWTranslator, and the output from the translator to compression service location, ZIP, and the compressed file to AdminTest.

This compound address overrides the location where the translator specifies to send the output, which would have been to TESTREC-MAILBOX. Since the ZIP location has no delivery address option, the compressed file uses the compound address from the input site, X850TEST.



☑ Output from MessageWay

User ID:

Password:

Directory: C:\DT\AdminTest

Mask: %filebase%<[#]>.%fileext%

End of Line: Native

Best Practice

When necessary, MessageWay determines file extensions based on the content type. For output files, when users include the token %fileext% at the end of the file mask, MessageWay will add the appropriate extension to the end of the file name.

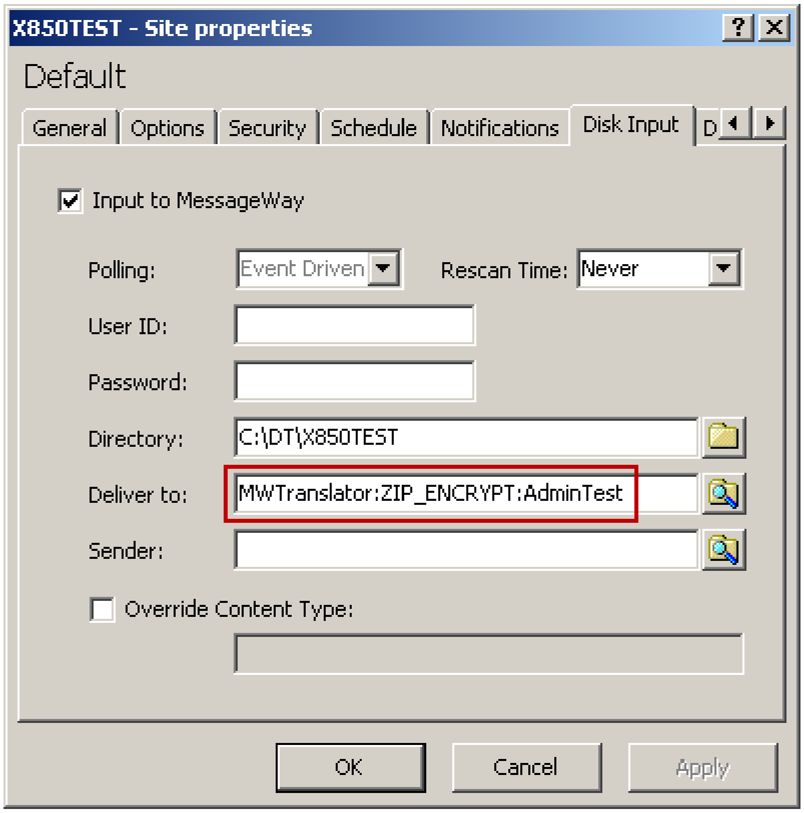
Since the destination location determines the name of the output file, you can have MessageWay supply a *.zip* or *.gz* extension to the file name. Simply put the following at the end of the mask: **.%fileext%**. This way, you can use this destination location mask for other types of files as well.

Example of Encryption with Compression

When you use the zip format to compress or decompress files, you also have the option to encrypt or decrypt the files using a password. Currently, this feature is not available for the gzip format.

In the following example, we will send a file to the translator, and the output will be zipped and encrypted before it is sent to its final destination location, AdminTest. The configurations are as follows

1 On the input location, specify the compound address, which is required because the compression service does not provide routing capabilities.



X850TEST - Site properties

Default

☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

Password:

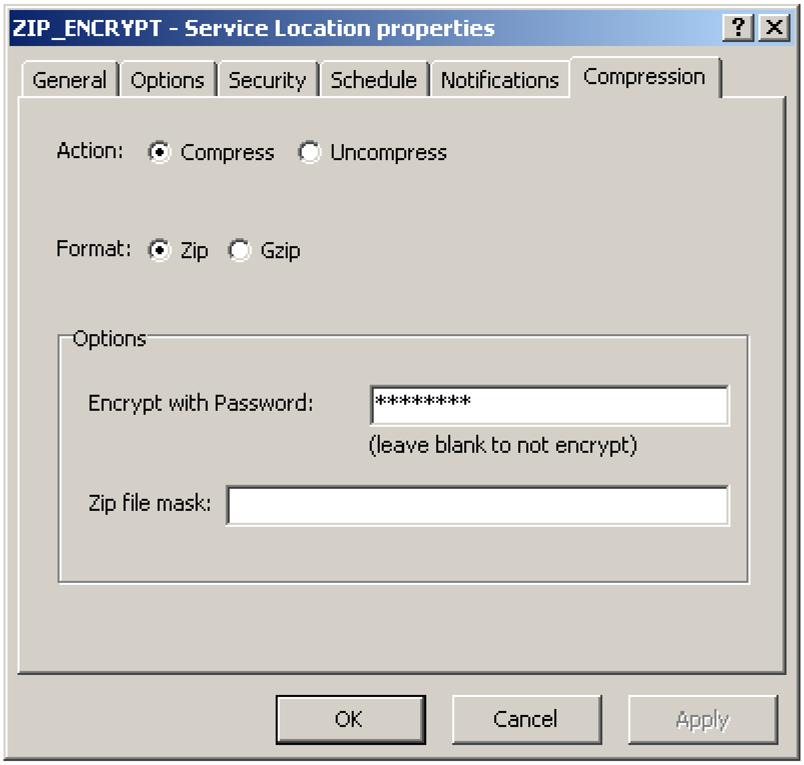
Directory: C:\DT\X850TEST

Deliver to: MWTranslator:ZIP_ENCRYPT:AdminTest

Sender:

□ Override Content Type:

2 On the **Compression** page of the compression location, type the password required to encrypt the message.



ZIP_ENCRYPT - Service Location properties

Action: ● Compress ○ Uncompress

Format: ● Zip ○ Gzip

Options

Encrypt with Password: *********

(leave blank to not encrypt)

Zip file mask:

3 The file mask configured for the final delivery location, AdminTest, determines the name of the output file.

The compression process is as follows:

1 Send an input file to MessageWay using an input location, such as X850TEST. In this case, we place the file on disk for MessageWay to pick up.

2 The file is sent to the translator service. The translator service produces three types of messages: the output of the translation, an acknowledgment and a translation report. The translation process determines where to send these last two, which are not affected by the compound address routing used for the output.

3 The translated output then goes to the compression service to be compressed and encrypted with a password.

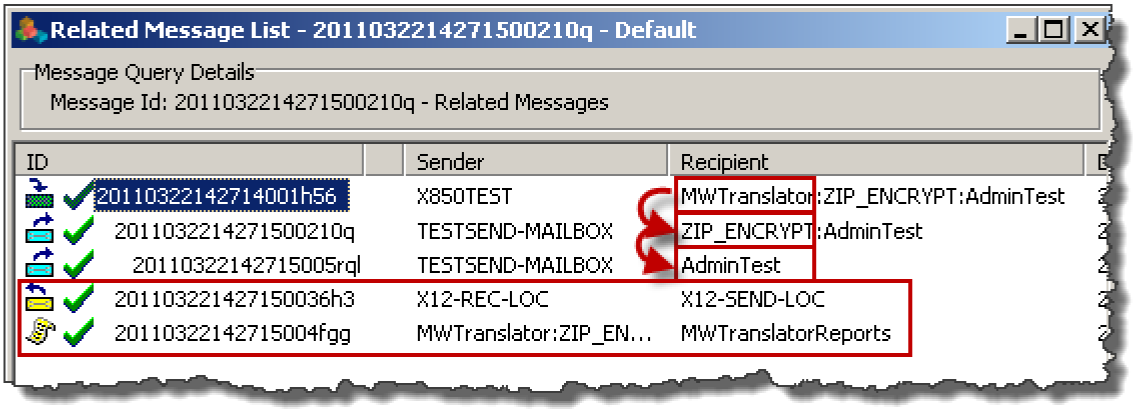
4 The output is sent to a delivery location, AdminTest, which delivers it to disk.

To view the output of the process from the MessageWay Manager:

1 ***Locate one of the messages associated with this process*** (on page 735).

2 From the message list, select the message, right-click and select **Get Related Messages**.

The Related Message List window appears. It shows the progression of the output message through the various processes and to final delivery. The last two messages are not affected by the compound address routing.



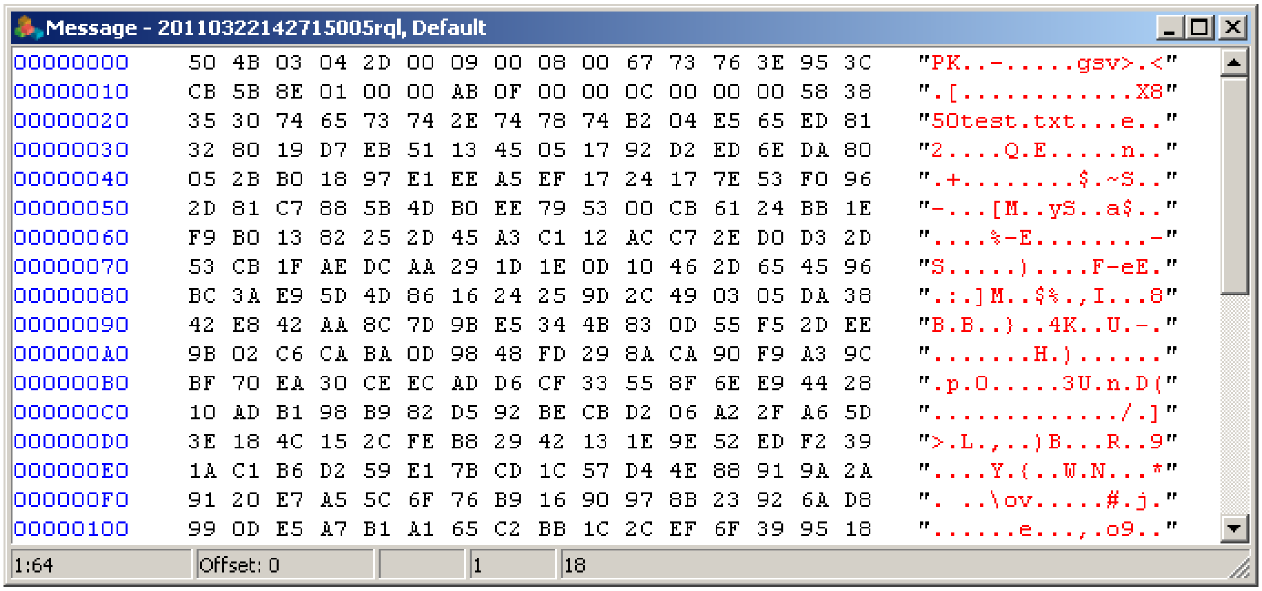
Related Message List - 2011032214271500210q - Default

Message Query Details

Message Id: 2011032214271500210q - Related Messages

ID	Sender	Recipient
20110322142714001h56	X850TEST	MWTranslator:ZIP_ENCRYPT:AdminTest
2011032214271500210q	TESTSEND-MAILBOX	ZIP_ENCRYPT:AdminTest
20110322142715005rql	TESTSEND-MAILBOX	AdminTest
201103221427150036h3	X12-REC-LOC	X12-SEND-LOC
20110322142715004fgg	MWTranslator:ZIP_EN...	MWTranslatorReports

3 To view the content of the output message sent to AdminTest, double-click the message. The following is a hex view of the content.

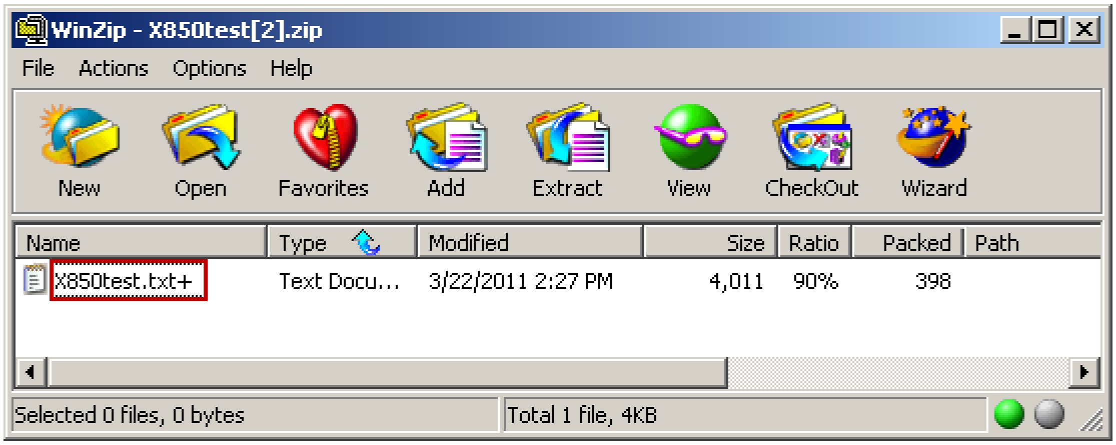


Message - 20110322142715005rql, Default

```
00000000     50 4B 03 04 2D 00 09 00 08 00 67 73 76 3E 95 3C     "PK..-.....gsv>.<"
00000010     CB 5B 8E 01 00 00 AB 0F 00 00 0C 00 00 00 58 38     ".[............X8"
00000020     35 30 74 65 73 74 2E 74 78 74 B2 04 E5 65 ED 81     "50test.txt...e.."
00000030     32 80 19 D7 EB 51 13 45 05 17 92 D2 ED 6E DA 80     "2....Q.E.....n.."
00000040     05 2B B0 18 97 E1 EE A5 EF 17 24 17 7E 53 F0 96     ".+........$.~S.."
00000050     2D 81 C7 88 5B 4D B0 EE 79 53 00 CB 61 24 BB 1E     "-...[M..yS..a$.."
00000060     F9 B0 13 82 25 2D 45 A3 C1 12 AC C7 2E D0 D3 2D     "....%-E.........-"
00000070     53 CB 1F AE DC AA 29 1D 1E 0D 10 46 2D 65 45 96     "S.....)....F-eE."
00000080     BC 3A E9 5D 4D 86 16 24 25 9D 2C 49 03 05 DA 38     ".:.]M..$%.,I...8"
00000090     42 E8 42 AA 8C 7D 9B E5 34 4B 83 0D 55 F5 2D EE     "B.B..}..4K..U.-."
000000A0     9B 02 C6 CA BA 0D 98 48 FD 29 8A CA 90 F9 A3 9C     ".......H.)......"
000000B0     BF 70 EA 30 CE EC AD D6 CF 33 55 8F 6E E9 44 28     ".p.0.....3U.n.D("
000000C0     10 AD B1 98 B9 82 D5 92 BE CB D2 06 A2 2F A6 5D     "............./.]"
000000D0     3E 18 4C 15 2C FE B8 29 42 13 1E 9E 52 ED F2 39     ">.L.,..)B...R..9"
000000E0     1A C1 B6 D2 59 E1 7B CD 1C 57 D4 4E 88 91 9A 2A     "....Y.{..W.N...*"
000000F0     91 20 E7 A5 5C 6F 76 B9 16 90 97 8B 23 92 6A D8     ".  ..\ov.....#.j."
00000100     99 0D E5 A7 B1 A1 65 C2 BB 1C 2C EF 6F 39 95 18     "......e...,.o9.."
```

1:64 | Offset: 0 | | 1 | 18

4 From your operating system, view the zip file on disk. From WinZip, we see that the plus sign indicates that a password is required to view the contents of the file.



Name	Type	Modified	Size	Ratio	Packed	Path
X850test.txt+	Text Docu...	3/22/2011 2:27 PM	4,011	90%	398	

Selected 0 files, 0 bytes

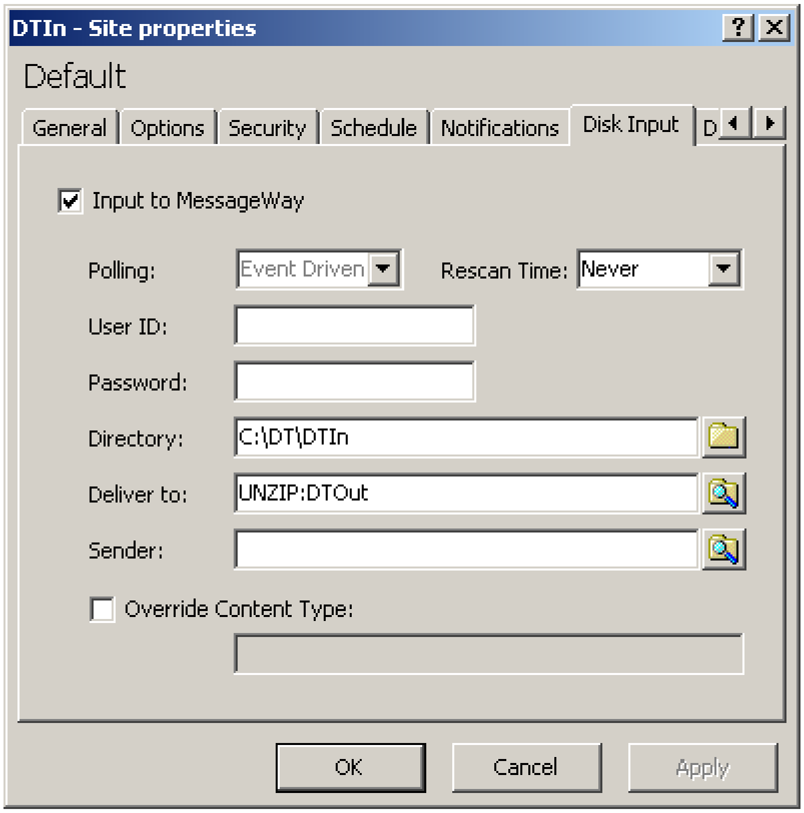
Total 1 file, 4KB

Example of Decryption with Decompression

In the following example, we will send a compressed and password-protected file to the compression service to be uncompressed and unencrypted before it is sent to its final destination location, DTOut.

The configurations are as follows:

1 On the input location, specify the compound address in the **Deliver To** field, which is required because the compression service does not provide routing capabilities.



☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

Password:

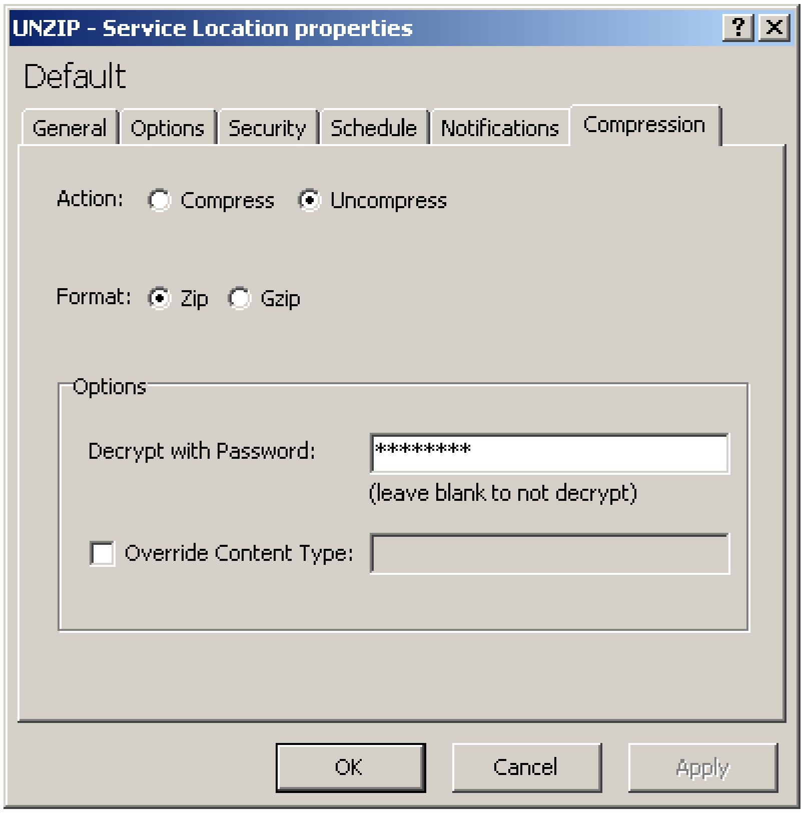
Directory: C:\DT\DTIn

Deliver to: UNZIP:DTOut

Sender:

□ Override Content Type:

2 On the **Compression** page of the compression location, type the password required to decrypt the message.



UNZIP - Service Location properties

Default

Action: ○ Compress ● Uncompress

Format: ● Zip ○ Gzip

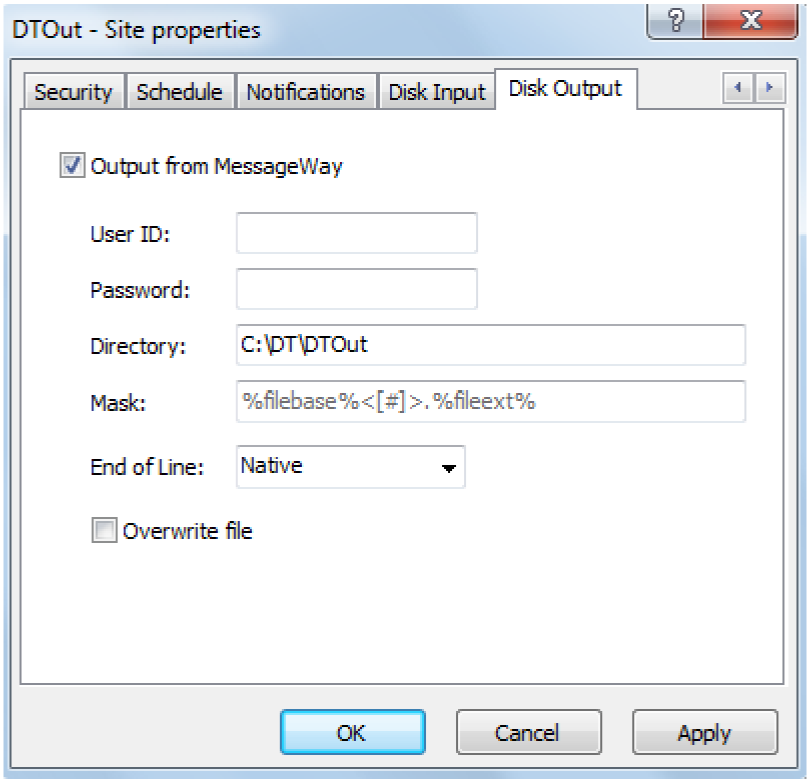
Options

Decrypt with Password: *********

(leave blank to not decrypt)

□ Override Content Type:

3 The file mask configured for the final delivery location, DTOut, determines the name of the output file.



☑ Output from MessageWay

User ID:

Password:

Directory: C:\DT\DTOut

Mask: %filebase%<[#]>.%fileext%

End of Line: Native

☐ Overwrite file

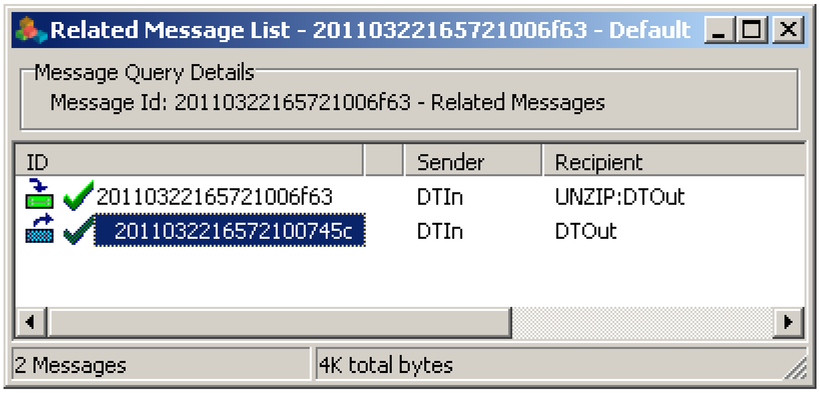
The compression process is as follows:

1 Send a compressed file to MessageWay. In this case, we place the file on disk for MessageWay to pick up from the DTIn directory.
2 The input then goes to the compression service to be uncompressed and decrypted with a password.
3 The output is sent to an output location, DTOut, which delivers it to disk.

To view the output of the process from the MessageWay Manager:

1 ***Locate one of the messages associated with this process*** (on page 735).
2 From the message list, select the message, right-click and select **Get Related Messages**.

The Related Message List window appears, showing the progression of the output message.

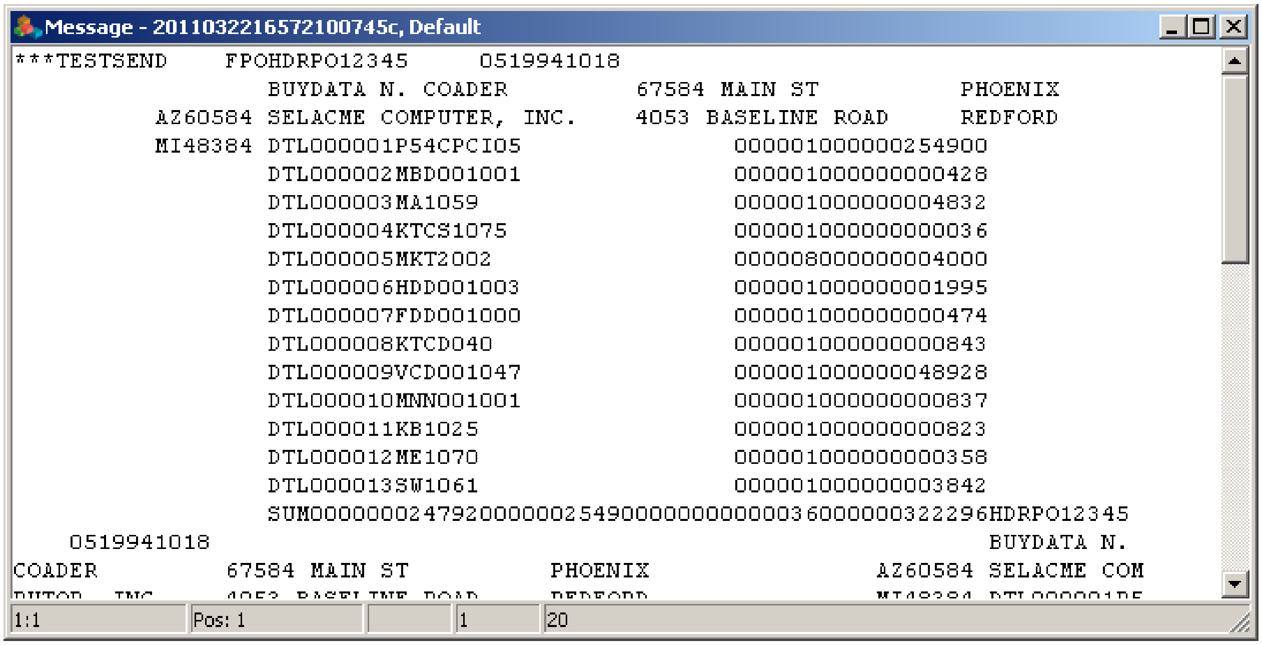


Message Query Details
Message Id: 20110322165721006f63 - Related Messages

ID	Sender	Recipient
✓ 20110322165721006f63	DTIn	UNZIP:DTOut
✓ 2011032216572100745c	DTIn	DTOut

2 Messages | 4K total bytes

3 To view the content of the message sent to DTOut, double-click the message.

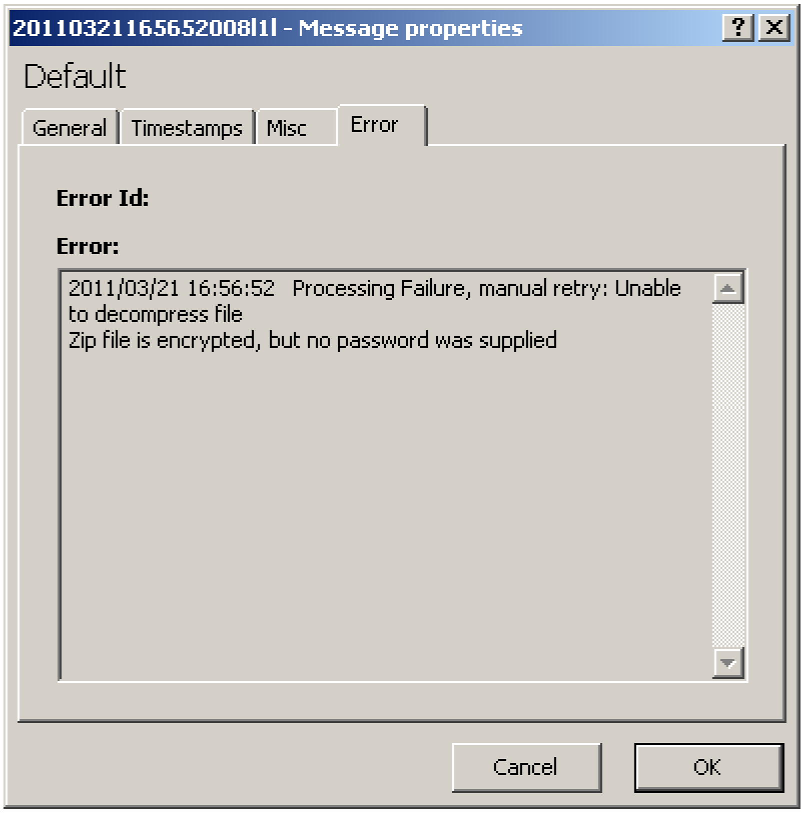


Message - 2011032216572100745c, Default

```
***TESTSEND    FPOHDRPO12345     0519941018
                  BUYDATA N. COADER          67584 MAIN ST          PHOENIX
          AZ60584 SELACME COMPUTER, INC.     4053 BASELINE ROAD     REDFORD
          MI48384 DTL000001P54CPCI05                000001000000254900
                  DTL000002MBD001001                000001000000000428
                  DTL000003MA1059                   000001000000004832
                  DTL000004KTCS1075                 000001000000000036
                  DTL000005MKT2002                  000008000000004000
                  DTL000006HDD001003                000001000000001995
                  DTL000007FDD001000                000001000000000474
                  DTL000008KTCD040                  000001000000000843
                  DTL000009VCD001047                000001000000048928
                  DTL000010MNN001001                000001000000000837
                  DTL000011KB1025                   000001000000000823
                  DTL000012ME1070                   000001000000000358
                  DTL000013SW1061                   000001000000003842
                  SUM00000002479200000025490000000000003600000322296HDRPO12345
    0519941018                                                        BUYDATA N.
COADER         67584 MAIN ST          PHOENIX               AZ60584 SELACME COM
PUTOR, INC.    4053 BASELINE ROAD     REDFORD               MI48384 DTL000001P5
```

NOTE: When you specify a password for files that are to be uncompressed, and files are sent to this location without a password, the password specified for this location is ignored, and the files will be uncompressed. Therefore, this UNZIP location will uncompress messages that have a correct password or that have no password.

4 When there is an error in decryption, information appears on the **Error** tab of the Message Properties window. In the following example, the file was encrypted with a password, but there was no password specified on the Compress service location to decrypt the file.



Error Id:

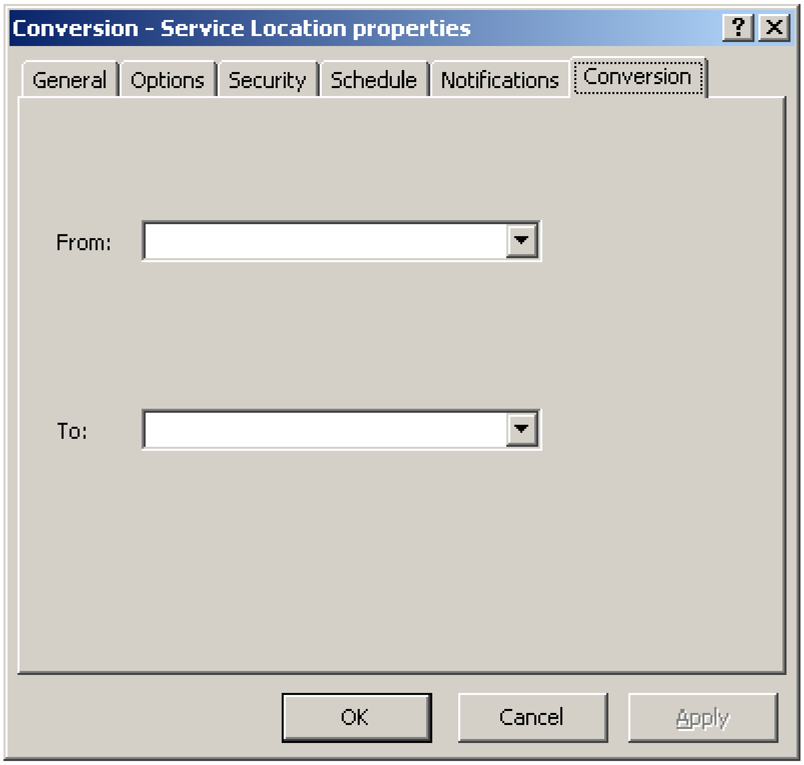
Error:

```
2011/03/21 16:56:52   Processing Failure, manual retry: Unable
to decompress file
Zip file is encrypted, but no password was supplied
```

Configuring a Conversion Service Location

Locations using the Conversion service allow users to specify how the character encoding of the message will be changed. The encoding schemes, algorithms and tables used to perform the conversions are from the ***International Components for Unicode (ICU)*** (***http://site.icu-project.org/***).

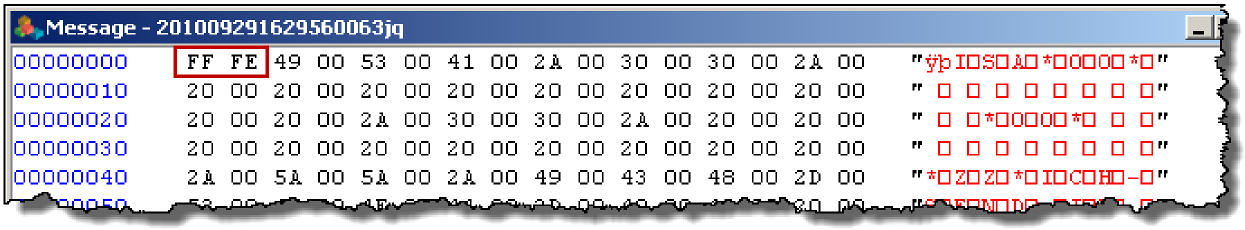
IMPORTANT: This location does not allow you to specify routing, so the routing instructions must come from an earlier process or be determined by rules processing.



Conventions for Converting Unicode

The ICU follows certain conventions for encoding. Although you can encode from any of the supported schemes to any other scheme, the focus is primarily on the newer schemes, such as Unicode.

Many Unicode schemes, not just UTF, use an optional signature at the beginning of the data called a byte order mark (BOM). This can facilitate recognition of the encoding scheme. The following message content viewed in MessageWay as hexadecimal and ASCII code shows the BOM for a UTF-16 with little-endian (LE) encoding:



```
00000000    FF FE 49 00 53 00 41 00 2A 00 30 00 30 00 2A 00    "ÿþI□S□A□*□0□0□*□"
00000010    20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00    " □ □ □ □ □ □ □ □"
00000020    20 00 20 00 2A 00 30 00 30 00 2A 00 20 00 20 00    " □ □*□0□0□*□ □ □"
00000030    20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00    " □ □ □ □ □ □ □ □"
00000040    2A 00 5A 00 5A 00 2A 00 49 00 43 00 48 00 2D 00    "*□Z□Z□*□I□C□H□-□"
```

There are some conventions for using the BOM:

- When text data is declared as UTF-16BE, UTF-16LE, UTF-32BE or UTF-32LE, a BOM must not be used
- For unmarked UTF-16 or UTF-32 text (unknown endian), you may use a BOM as a signature. If there is no BOM, the text should be interpreted as big-endian (BE)

- BOM may be required for some systems, for example Microsoft conventions for .txt files require use of the BOM on certain Unicode data streams
- BOM is optional for some systems, for example in the case of untagged text
- Some byte-oriented systems expect ASCII characters at the beginning of a file (X12, EDIFACT for EDI or UNIX/Linux scripts). If a BOM is used, remove the BOM or its converted form after conversion
- **Best Practice**: for UTF-8 backward compatibility with ASCII, do not use a BOM

Expected Behavior of Conversions

The ICU provides algorithms and tables for the conversions. As a result, you should understand what to expect from these conversions.

- Converting from non-Unicode encodings to UTF-8, UTF-16BE, UTF-16LE, UTF-32BE, or UTF-32LE does not insert BOM
- Converting to UTF-16 or UTF-32 does insert BOM
- 0x1A is a substitute character that is used to replace values that are not valid in the output encoding, including the BOM
- Additional processing may be required to remove BOM or converted values that may cause problems, such as 0x1A

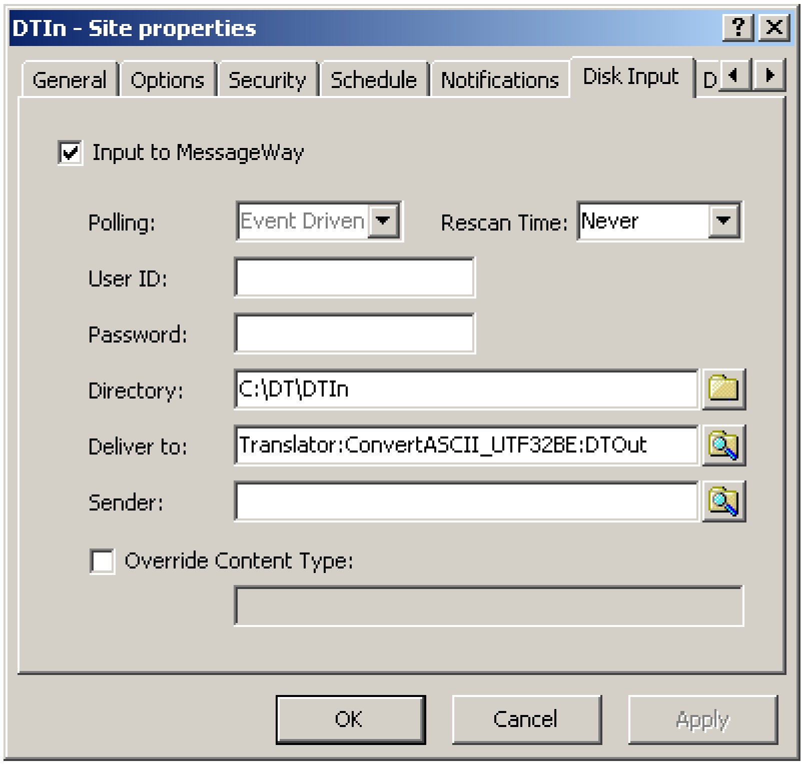
IMPORTANT: 0x1A (decimal 26, octal 032) values in a text file may be construed by some applications or systems as an end-of-file marker, which truncates the file or causes an EOF error

Conversion Example ASCII to Unicode

In the following example, MessageWay converts the character set of any messages sent to this site from ASCII (original 128 character set) to UTF 32BE. The output will be sent to another destination specified by a compound address on the input location configuration. When no output location is specified on the input location or a subsequent service location, the output will be placed in the system mailbox, {Unknown}.

The following DTIn site uses a compound address in the **Deliver To** field:

Translator:ConvertASCII_UTF32BE:DTOut



☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

Password:

Directory: C:\DT\DTIn

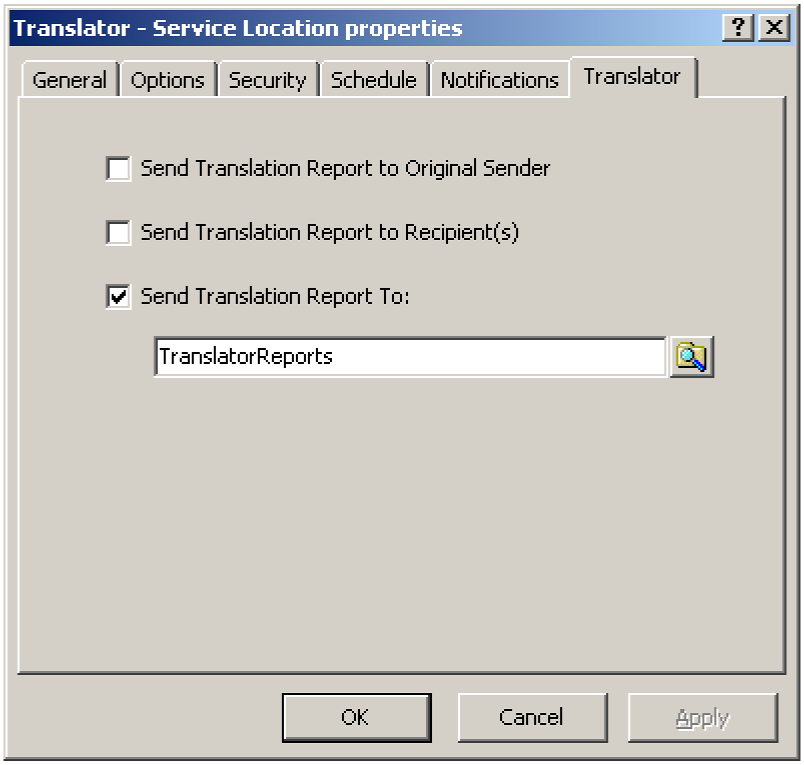
Deliver to: Translator:ConvertASCII_UTF32BE:DTOut

Sender:

□ Override Content Type:

This address sends messages to the following locations, including a final output address:

1 *Translator*: message is sent from DTIn to the Translator service location.



Translator - Service Location properties

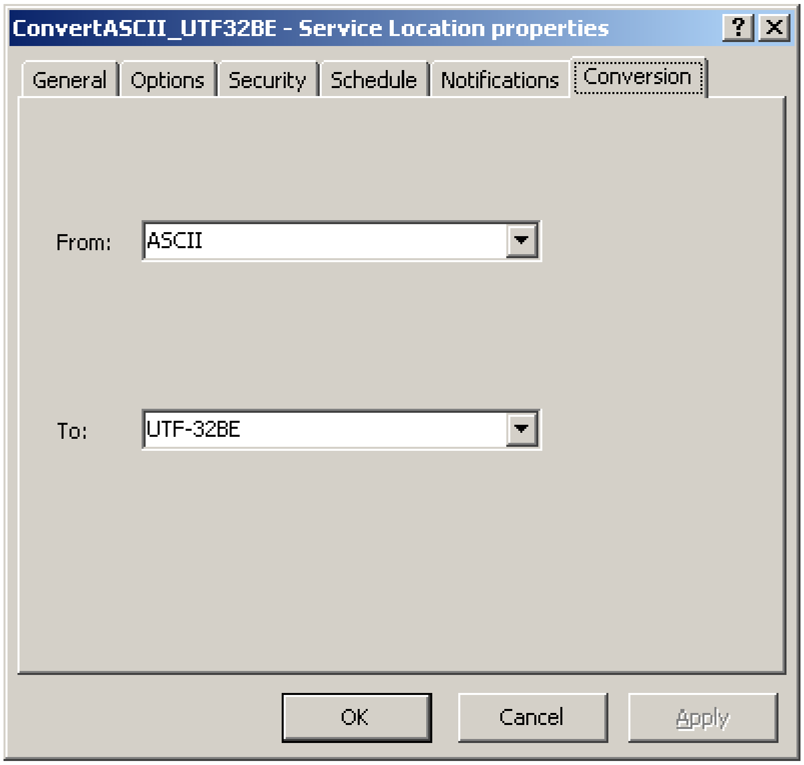
□ Send Translation Report to Original Sender

□ Send Translation Report to Recipient(s)

☑ Send Translation Report To:

TranslatorReports

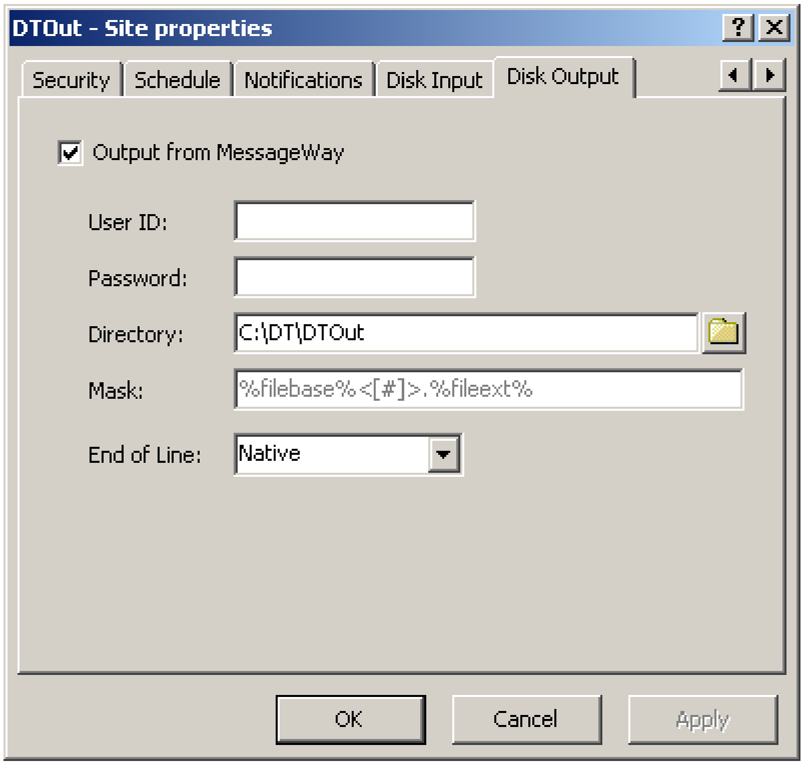
2 *ConvertASCII_UTF32BE*: the output from Translator is sent to this conversion service location. This part of the compound address overrides the routing that the translator would use for the output. This does not affect notifications or backward acknowledgments, which are routed by the translator.


ConvertASCII_UTF32BE - Service Location properties

From: ASCII

To: UTF-32BE

3 DTOut: the converted file is delivered to the output site, DTOut.



DTOut - Site properties

Security | Schedule | Notifications | Disk Input | Disk Output

☑ Output from MessageWay

User ID:

Password:

Directory: C:\DT\DTOut

Mask: %filebase%<[#]>.%fileext%

End of Line: Native

For more information about routing and compound addresses, refer to ***Specifying Routing Addresses*** (on page 653).

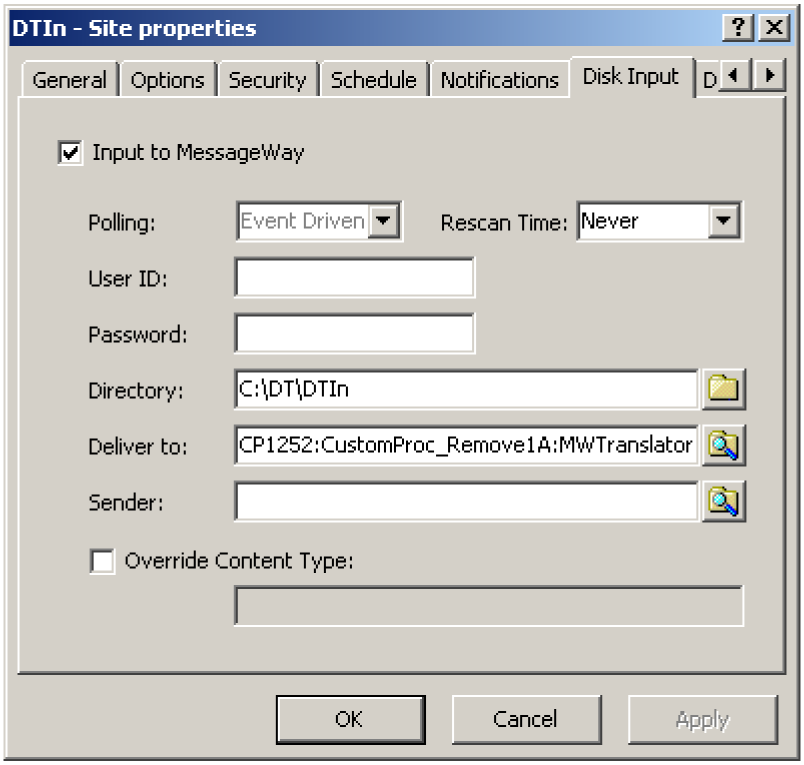
Conversion Example Unicode to CP1252

For this example, assume that the input file is destined for EDI translation, but it is encoded as UTF-8 with a byte order mark (BOM). First, we must convert it to CP1252, which the translator can read, and then remove the first character, a non-displayable character, 0x1A, before it is sent to the translator. The translation service will determine where to send the output.

NOTE: When no output location is specified on the input location or a subsequent service location, the output will be placed in the system mailbox, {Unknown}.

The following DTIn site uses a compound address shown in the **Deliver To** field:

ConvertUTF8_CP1252:CustomProc_Remove1A:MWTranslator



☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

Password:

Directory: C:\DT\DTIn

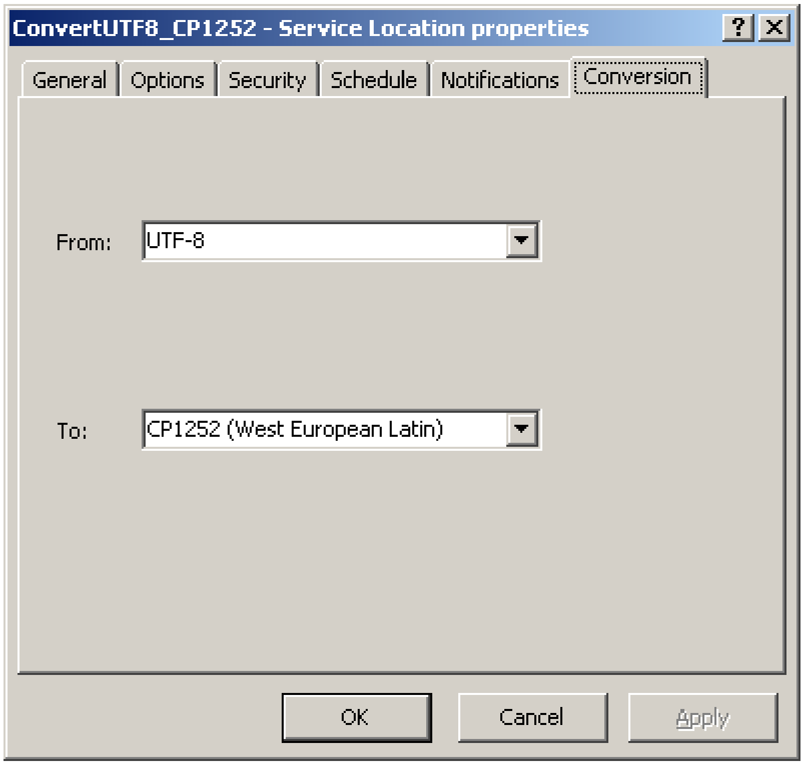
Deliver to: CP1252:CustomProc_Remove1A:MWTranslator

Sender:

□ Override Content Type:

This address sends messages to the following locations, and the translator determines where to send the output for delivery:

1 *ConvertUTF8_CP1252*: message is sent from DTIn to the ConvertUTF8_CP1252 service location. This process replaces any characters that are not in the CP1252 encoding scheme with 0x1A. So it will replace the initial byte order mark with 0x1A.

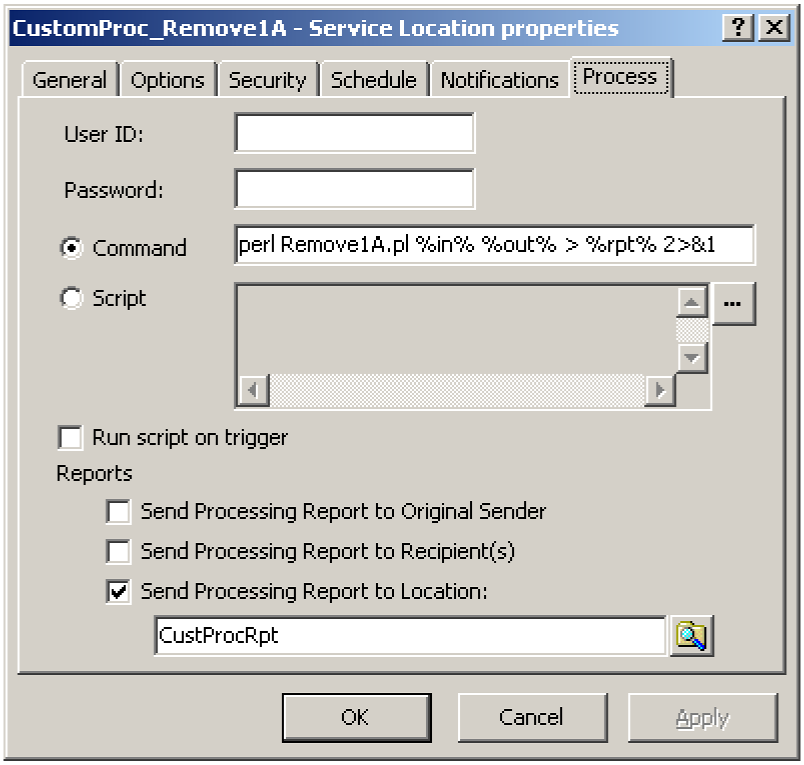


ConvertUTF8_CP1252 - Service Location properties

From: UTF-8

To: CP1252 (West European Latin)

2 *CustomProc_Remove1A*: the output from conversion is sent to this custom processing location that runs a script to remove the 0x1A.



User ID:

Password:

● Command: perl Remove1A.pl %in% %out% > %rpt% 2>&1

○ Script

□ Run script on trigger

Reports

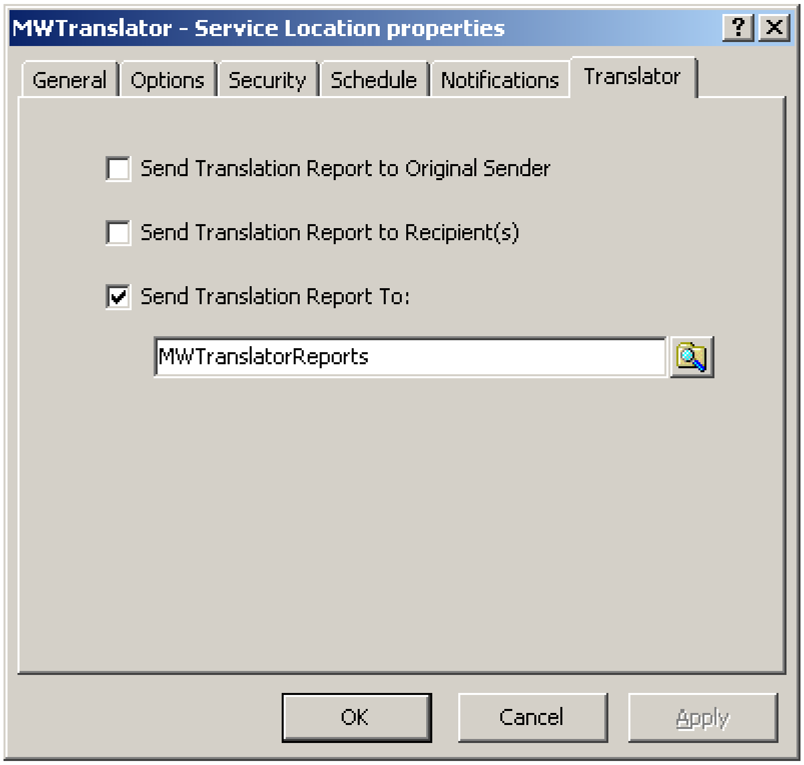
□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

☑ Send Processing Report to Location:

CustProcRpt

3 *MWTranslate*: the file returned from custom processing is sent to a translation service location. The translation process determines where to send the output after translation, so there is no final destination specified on the DTIn site, as we did in the previous example.



□ Send Translation Report to Original Sender

□ Send Translation Report to Recipient(s)

☑ Send Translation Report To:

MWTranslatorReports

For more information about routing and compound addresses, refer to ***Specifying Routing Addresses*** (on page 653).

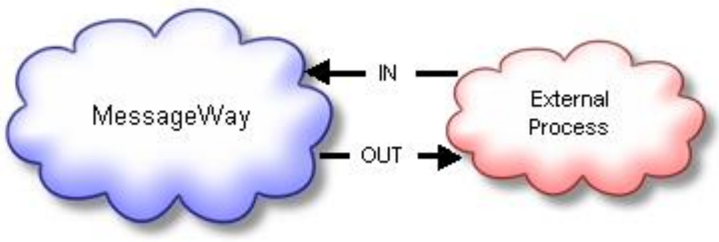
Configuring a Custom IO Site

The MessageWay Custom I/O Adapter is a generic adapter that executes user-defined programs or scripts to do one of the following:

- Transfer messages to MessageWay
- Transfer messages from MessageWay
- Send a trigger message to start an external process

Users may send messages to and from MessageWay or simply start an external process by running a shell script or an executable program. Valid scripting languages include those that are installed on and supported by the operating system.

The concepts of in and out as seen in the default subdirectories and the replaceable parameters, are relative to MessageWay. The terms *in* and *input* refer to messages transferred to MessageWay from the external process, and *out* and *output* refer to messages transferred from MessageWay to the external process.



This service includes the following configurable entities:

- Custom I/O Adapter
- Custom I/O locations, created by users

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Understanding Custom IO

The Custom IO Adapter provides two services: input and output.

For input, the adapter runs commands or scripts it finds when polling the custom I/O sites. Note that this differs from the way polling works for other sites, which poll locations for messages to transfer into MessageWay, rather than for scripts to run.

For output, when a message arrives at the site, the adapter runs the command or script defined for the site.

Understanding Custom IO Input

The adapter follows these basic steps for input to MessageWay:

1. Responds to an event for a custom I/O input site
2. Prepares information to exchange with the external process, which includes resolving replaceable parameters
3. Initiates the external process
4. Determines the completion status of the external process
5. Uploads files created by the external process based on completion status
6. Removes the temporary files from disk after successful completion of all uploads

Respond to an Event to Upload Files

Input scripts are activated by one of two types of events:

- Polling configured for the adapter
- Triggers sent by the MessageWay Server, initiated by one of the following:
    - Service Interface
    - **Input Now** command

When the adapter passes a file name to the process, the process can then read the file for further processing. For example, when a message arrives at the site, the adapter might initiate an SFTP script that issues a PUT command to send the message to a trading partner's SFTP server.

Prepare Information to Exchange

The Custom IO Adapter may receive information from an external process. The adapter uses replaceable parameters or tokens to pass most of this information, although it can also pass literals.

Information that the adapter might send with tokens includes:

- Information about the input message:
  - Name of the input file created by the external process
  - Default directory for input files
- Logon information for an external application
  - User ID
  - Password
- Name of a temporary status file it expects to receive

Information that the adapter would receive from the external process includes:

- Input file, or files when using a status file
- Completion code
- Optional status file
- Optional report file

Determine the Completion Status

After the adapter or service has started the process, it expects a completion code from the process, from which it determines the state of the original message that initiated the process and then what error information, if any, to display on the **Error** tab of the Message Properties window.

- When the process does not return a completion code, the adapter or service assumes the process aborted and marks the message with a state of *Error*

  - or -
- If a status file is used:
  - When the process sends a completion code of zero, the adapter or service parses the status file and
    - Uses the status in the file to determine which files to upload, if any

      - and -
    - When the status is *X*, Abort, it displays an Error ID of 888nn on the **Error** tab and writes the description of the error to the Error box

    - or -

  - When the process sends a completion code other than zero, the adapter or service assumes the process aborted and marks the message with a state of Error. Any information sent by the script or program to STDOUT or STDERR is written to the Error box.

  - or -

- If a status file is *not* used:
  - When the process sends a completion code of zero, the adapter or service marks the message with a state of *Complete*

    - or -

  - When the process sends a completion code other than zero, the adapter or service assumes the process aborted and marks the message with a state of Error. Any information sent by the script or program to STDOUT or STDERR is written to the Error box.

    - or -

  - When the process does not send a completion code, the adapter or service assumes the process aborted and marks the message with a state of Error. Any information sent by the script or program to STDOUT or STDERR is written to the Error box.

Initiate the External Process

The adapter determines the process to initiate based on which one of the two options is selected on the **Input** page of the site configuration window: *Command* or *Script*:

- If **Command** is selected, the script or process resides outside MessageWay, and the adapter resolves replaceable parameters in memory, calls the external command or script, and passes the resolved values and any literals as arguments

  - or -

- If **Script** is selected, the script resides in MessageWay, and the adapter resolves any replaceable parameters, writes the script to the /tmp directory, and then initiates the script

Upload Returned Files

The adapter uploads files based on what it determines is the completion code.

- When the adapter receives a successful completion code, zero (0), the adapter uploads messages created by the external process:
  - If a status file is used, it uploads the files listed in the status file based on the status code in the status file

    - or -

  - If a status file is *not* used, it uploads the input file when the %in% token is used and the report file when the %rpt% token is used. If the adapter cannot upload expected files, it assumes the process aborted

- When the adapter does not receive a successful completion code, anything other than zero (0) or 100, it assumes the process aborted and all temporary files remain on disk. The %rpt% file will be uploaded if a report destination is configured on the custom IO site.

When the adapter uploads files, it must also determine where to send the files. How the adapter determines where to send the messages depends on whether the process returns a status file. The basic behavior to deliver input and report files are described here.

For input files:

- When a status file is *not* used, the input file whose name was resolved from the %in% token is either
    - Sent to the *Deliver Input To* location specified on the **Input** tab of the custom IO input site

      - or -
    - When no destination is specified, sent to a default mailbox called UNKNOWN (If a mailbox called UNKNOWN does not exist, it will be forwarded to the system mailbox {Unknown})
- When a status file is used, multiple input files may be uploaded. The name of the status file is resolved from the %status% token.
    - When the process returns a completion code of zero (0) or 100, the adapter parses the file, and each input file is either:
        - Sent to the destination locations specified for each of the input files, overriding any value in the *Deliver Input To* field

          - or -
        - When no destination is specified, sent to a default mailbox called UNKNOWN (If the mailbox called UNKNOWN does not exist, it will be forwarded to the system mailbox {Unknown})
    - When the process does not return a completion code of zero (0) or 100, the adapter does not parse the status file, assuming the process aborted, and leaves the input files on disk.

For reports:

- When a status file is *not* used, the report file whose name was resolved from the %rpt% token is:
    - Sent to the *Deliver Report To* location specified on the **Input** tab of the custom IO input site

      - or -
    - When no destination is specified, the report remains on disk
- When a status file is used, multiple report files may be uploaded. The name of the status file is resolved from the %status% token.
    - When the process returns a completion code of zero (0) or 100, the adapter parses the file, and each report file is:
        - Sent to the destination locations specified for each of the report files

          - and -

          Sent to the destination locations specified in the *Deliver Report To* field

          - or -
        - When no destination is specified, report files remains on disk

- When the process does not return a completion code of zero (0) or 100, the adapter assumes the process aborted, does not parse the status file and leaves the leaves the reports files on disk. The %rpt% file will be uploaded if a report destination is configured on the custom IO site.

When using a status file, each report uploaded will be related to the preceding IN file defined in the status file. When you issue a **Get Related** command from the Manager, the reports will appear on the message list with the appropriate input file.

For example, when the status file contains the following lines, the reports (RPT) are related to the first input file (IN):

```
A,Success
IN:src,dest,file
RPT:src,dest,file
RPT:src,dest,file
IN:src,dest,file
```

In the next example, each report (RPT) follows a different input file (IN), so each report is related to the input file that precedes it:

```
A,Success
IN:src,dest,file
RPT:src,dest,file
IN:src,dest,file
RPT:src,dest,file
```

Remove the Temporary Files

After MessageWay has completed its delivery process, it returns to the locations of any files it used, such as a status file and a temporary script file, and deletes them.

If MessageWay instead determines there was an abort in the external process, it does not delete the temporary files, leaving them for future debugging. In this case, users should remove the files.

Understanding Custom IO Output

The adapter follows these basic steps for output from MessageWay:

1. Responds to a message arriving in a custom I/O output site
2. Prepares information to exchange with the external process, which includes resolving replaceable parameters
3. Initiates the external process
4. Determines the completion status of the external process
5. Removes the temporary files from disk after successful completion of the process

Respond to a Message Sent to Custom IO Site

The adapter initiates the process specified in the **Command** box or in the **Script** box on the **Output** page of a custom IO site when a message is sent to that site, and the schedule is open. If the schedule is closed when the message arrives, the adapter initiates the process when the schedule opens. The adapter might send a file name to the process for further manipulation. The adapter might also simply start the process without sending a file name.

When the adapter passes a file name to the process, the process can then read the file for further processing. For example, when a message arrives at the site, the adapter might initiate an SFTP script that issues a GET command to retrieve a message from a trading partner's SFTP server.

Prepare the Information to Exchange

The Custom IO Adapter may send information to an external process. The adapter uses replaceable parameters or tokens to pass most of this information, although it can also pass literals.

Information that the adapter might send with tokens includes:

- Name of the output file in the MessageWay Message Store
- Information about the outbound message:
  - Message ID
  - Input message ID
  - Name of the input file meaningful to external process
  - Sender of the message
  - Recipient of the message
- Logon information for an external application
  - User ID
  - Password
- Name of a temporary status file it expects to receive

Information that the adapter would receive from the external process includes:

- Completion code
- Optional status file with status code and optional description, which overrides completion code
- Optional report file

Initiate the External Process

The adapter determines the process to initiate based on which one of the two options is selected on the **Output** page of the site configuration window: **Command** or **Script**:

- If **Command** is selected, the script or process resides outside MessageWay, and the adapter resolves replaceable parameters in memory, calls the external command or script, and passes the resolved values and any literals as arguments

  - or -

- If **Script** is selected, the script resides in MessageWay, and the adapter resolves any replaceable parameters, writes the script to the /tmp directory, and then initiates the script

Determine the Completion Status

After the adapter or service has started the process, it expects a completion code from the process, from which it determines the state of the original message that initiated the process and then what error information, if any, to display on the **Error** tab of the Message Properties window.

- When the process does not return a completion code, the adapter or service assumes the process aborted and marks the message with a state of *Error*

  - or -

- If a status file is used:
  - When the process sends a completion code of zero, the adapter or service parses the status file and
    - Uses the status in the file to determine which files to upload, if any

      - and -

    - When the status is *X*, Abort, it displays an Error ID of 888nn on the **Error** tab and writes the description of the error to the Error box

    - or -

  - When the process sends a completion code other than zero, the adapter or service assumes the process aborted and marks the message with a state of Error. Any information sent by the script or program to STDOUT or STDERR is written to the Error box.

  - or -

- If a status file is *not* used:
  - When the process sends a completion code of zero, the adapter or service marks the message with a state of *Complete*

    - or -

  - When the process sends a completion code other than zero, the adapter or service assumes the process aborted and marks the message with a state of Error. Any information sent by the script or program to STDOUT or STDERR is written to the Error box.

    - or -

  - When the process does not send a completion code, the adapter or service assumes the process aborted and marks the message with a state of Error. Any information sent by the script or program to STDOUT or STDERR is written to the Error box.

Remove the Temporary Files

After MessageWay has completed its delivery process, it returns to the locations of any files it used, such as a status file and a temporary script file, and deletes them.

If MessageWay instead determines there was an abort in the external process, it does not delete the temporary files, leaving them for future debugging. In this case, users should remove the files.

Specifying Custom I/O Properties

The site configuration specifies what function to perform, input or output or both, which determines the type of site, Input, Output or I/O, respectively. As a best practice, however, you should not use the same site for both input and output.

Commands or scripts may do one of the following:

- Transfer messages to MessageWay from an external process
- Transfer messages from MessageWay to an external process
- Start an external process

Using the Command and Script Fields (Custom I/O Site)

There are two ways to configure the site to send and receive messages:

- Enter the name of the file to be executed in the **Command** box

  - or -

- Enter the script in the **Script** box

Scripts may be written in any language supported by the native operating system. Also, natively compiled programs may be invoked from the command line or from a script.

The **Command** and **Script** boxes should be used as follows:

- The **Command** box should contain a single command line, which will be executed by the default shell. It may include replaceable parameters, and it may invoke a user script or program. Use the **Command** option for:
  - Long scripts with no embedded replaceable parameters and maintained outside MessageWay
  - Security, when you do not want a temporary copy of the script written to disk with a clear text user ID and password created from the replaceable parameters %user% and %password%
- The **Script** box should contain a complete multi-line script. The first line defines the program that will process the script. Subsequent lines contain the script, including any required replaceable parameters. Use the script option for:
  - Short scripts with embedded replaceable parameters and maintained inside MessageWay
  - Testing, where you can review scripts left in the temporary subdirectory, /tmp, when the process returns an abort completion code (>0 and not=100)
  - A cluster environment, to avoid storing multiple copies of the script

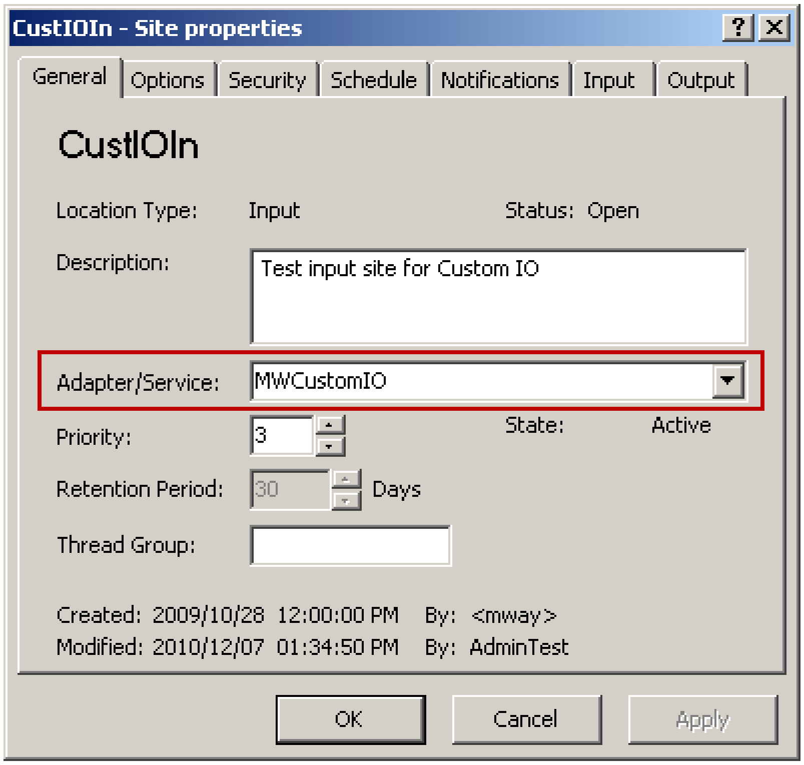
IMPORTANT: Replaceable parameters may only be used in the **Command** and **Script** boxes. They may not be included in scripts called from the **Command** box, because MessageWay resolves the parameters before it writes the script to memory and before execution.

Adding a Custom I/O Site

In case you have not already done so, you should create a custom IO site, as follows:

1 Add a location.

2 In the **Adapter/Service** box, select **MWCustomIO**.



CustIOIn

Location Type: Input

Status: Open

Description: Test input site for Custom IO

Adapter/Service: MWCustomIO

Priority: 3

State: Active

Retention Period: 30 Days

Thread Group:

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2010/12/07 01:34:50 PM By: AdminTest

3 ***Configure other general properties for the location*** (on page 467).

- For input transfers, ***complete the information on the* Input *tab*** (on page 540)

  - or -

- For output transfers, ***complete the information on the* Output *tab*** (on page 545)

4 Select **Apply** or **OK** to save the configuration.

Input Transfers

An input transfer command or script loads files into MessageWay. Once triggered, the adapter will call the script repeatedly until the status indicates there are no more inbound files to process. A script may be triggered by two events:

- Adapter polling

  - or -

- Manual triggers sent by the MessageWay Server, initiated by one of the following:
  - Service Interface
  - **Input Now** command

Adapters poll each active inbound site once every polling cycle and run the specified command or script. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15. An adapter will not poll a site when:

- The site is on hold

  - or -

- The site schedule is closed

  - or -

- The site command or script is still processing from a previous poll

Manual triggers are sent to the adapter from the Service Interface via the Messaging Server. External processes must send appropriate commands to the Service Interface. Manual triggers may be sent by clients to MessageWay servers that support the ***Service Interface*** (on page 95), such as the ***FTP Server*** (on page 185), or the ***SFTP Server*** (on page 298). Manual triggers sent from the Service Interface will be ignored when the site is on hold, whereas the **Input Now** command overrides closed schedules and sites that are on hold.

You specify how to transfer messages into MessageWay using the **Command** box or the **Script** box on the **Input** tab of the Site Properties window.

Specifying a User ID and Password

You may enter a user ID and password when required to connect to an external process. Then in the Command field or the Script box for the input transfer, use the ***replaceable parameters*** (on page 544), %user% and %password% to pass this information to the external process.

CAUTION: When used in the **Script** box, these values are resolved and written to the /tmp directory. In case MessageWay determines that the external process has aborted, it will *not* delete the file, as it does when all processes complete successfully. When this token is used in the **Command** box, it is resolved in memory and never written to a temporary file.

Specifying Commands or Scripts

You specify the process to be invoked using the **Command** box or the **Script** box. The **Command** box calls external commands or scripts. The **Script** box allows users to create and store scripts in MessageWay.

When you specify the process using the **Command** box, the syntax requirements are as follows:

- Name of the process or script is first, using
  - Only the file name, if the external script is located in the ***default script subdirectory*** (on page 947), or if the command can be found by the operating system

    - or -

  - Full path name and file name

- Arguments (replaceable parameters and literals) follow the name of the process and must be in the order required by the process, but the process or script itself must not contain any replaceable parameters

NOTE: MessageWay will resolve the parameters in memory and then pass them as arguments to the script or command for execution.

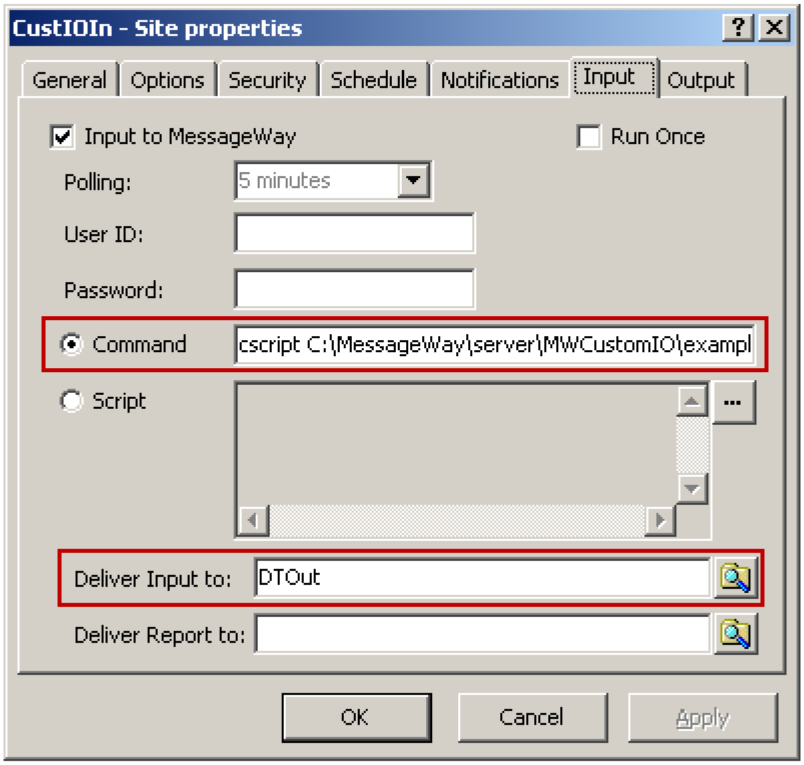
The following example does not use a status file. A status file is required to load more than one output or report file into MessageWay at a time. A status file is always required to load the other file types, acknowledgments and custom notifications. For examples that use a status file, refer to the topic, ***Examples Using Scripts and Status Files*** (on page 556).

In this example, the script, InputAndReexecute, loads the oldest file in the defined directory (dirPath) into MessageWay. The full text of the command line is as follows:

```
cscript C:\MessageWay\server\MWCustomIO\examples\InputAndReexecute.vbs "%in%"
```

Before being uploaded, the file is moved and renamed to the fully qualified file name provided by the %in% replaceable parameter, which avoids loading partial files. If a file was loaded, the MWCustomIO adapter immediately re-executes the script to load the next oldest file. This script re-executes until all files in the directory have been loaded. Any file the script returns will be sent to the location, DTOut.

NOTE: The schedule for the site must not be closed and the site must not be on hold.



☑ Input to MessageWay

□ Run Once

Polling: 5 minutes

User ID:

Password:

● Command cscript C:\MessageWay\server\MWCustomIO\exampl

○ Script

Deliver Input to: DTOut

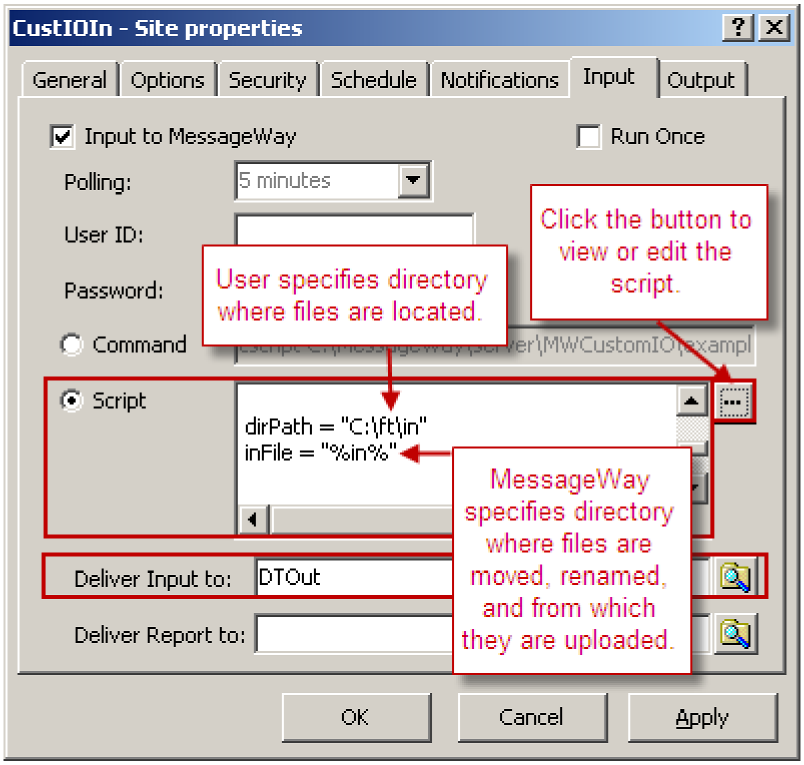
Deliver Report to:

When you specify the process in the **Script** box, the syntax requirements are as follows:

- The first line contains values to invoke the appropriate script process or, depending on the operating system as follows:
  - For Windows, this is the file extension required by the external process that is supported by the operating system, such as, .bat for a batch command, .vbs for Visual Basic or .js for Java Script.
  - For UNIX/linux, this is the standard #! line, such as, #!/bin/sh.
- Subsequent lines contain the instructions and include replaceable parameters and parameters required by the process.

NOTE: MessageWay will resolve the parameters and then write the script to a temporary file in the /tmp subdirectory. After successful execution, MessageWay will delete the temporary file.

In the following example, the script used in the command box was modified to run from the script box. It performs the same functions as the previous example, but after MessageWay resolves the parameters, it writes the script to a temporary directory. Again, all output will be sent to the DTOut location.



☑ Input to MessageWay

□ Run Once

Polling: 5 minutes

User ID:

Password:

○ Command cscript C:\MessageWay\server\MWCustomIO\exampl

● Script

```
dirPath = "C:\ft\in"
inFile = "%in%"
```

Deliver Input to: DTOut

Deliver Report to:

User specifies directory where files are located.

Click the button to view or edit the script.

MessageWay specifies directory where files are moved, renamed, and from which they are uploaded.

Both of these example scripts are located in the \server\MWCustomIO\examples directory.

NOTE: These examples happen to be for Windows, but comparable examples are installed with UNIX/Linux platforms.

Replaceable Parameters for Input Transfers (Custom I/O Site)

The **Command** and the **Script** boxes for the **Input** tab may include replaceable parameters. These parameters allow MessageWay to pass information to an external process. The replaceable parameters are resolved by MessageWay before the instructions are passed to the process as arguments.

IMPORTANT: All replaceable parameters must be lower case. The information for the parameter is always supplied by MessageWay, not the external process. Replaceable parameters may be in any order, but they must satisfy the syntax of the script or program.

If any data in the Command box or the Script box contains a percent sign (%), you must use a release character, another percent sign, immediately preceding each instance, giving two percent signs (%%). Then when MessageWay resolves the tokens, it will strip one of the signs, leaving one as part of the data.

All replaceable parameters are optional. The following table describes the valid parameters for input transfers.

Replaceable Parameters (Input Tab)	Description
%in%	The full path and file name of a single input message.
%status%	The full path and file name of a file to be created by the script to provide the return status and message information.
%indir%	Default subdirectory path, which is /in, for files transferred from the external process.
%tmpdir%	Directory path, which is /tmp, for temporary files or logs that are created by the script. The archive and delete program, mwarchive, may delete files in this directory based on the value in the Temp File Retention field on the **MWArchive** tab of the MWArchive Server Properties window.
%user%	The user specified on the **Input** tab of the Site Properties window.
%password%	The password specified on the **Input** tab of the Site Properties window.

NOTE: Additional tokens that are normally available to processes that use file masks are available to this process. For a complete list, refer to the topic, ***Mask*** (on page 1103).

The following table explains how to use the replaceable parameters.

Replaceable Parameters	Use
%in%	Required when you do *not* use a status file to specify the file names. MessageWay creates a fully qualified file name using the prefix **INP** and an extension of **.msg** pointing to the /in subdirectory. This value is ignored when a status file exists, because status files contain the file names.
%status%	Required if you want the external process to return a status file. A status file returns a status and description, but also allows you to specify the source and destination locations and name(s) of the input files.
%indir%	Required when you want the external process to create input files in the default /in subdirectory. This is useful when you use the %status% replaceable parameter with multiple input files, because the file name does not need to contain the full path. When you do not use this parameter, the file name in the status file must contain the full path name.
%tmpdir%	Useful when the script or process creates temporary processing files or logs. Before exiting, the script should clean up any temporary files it has created in the /tmp subdirectory, unless this cleanup is done by the archive program.
%user%	May be used when an external process requires it, such as for encryption. **CAUTION:** When used in the **Script** box, this value is resolved and written to the /tmp directory. In case MessageWay determines that the external process has aborted, it will not delete the file, as it does when all processes complete successfully. When this token is used in the **Command** box, it is resolved in memory and never written to a temporary file.
%password%	May be used when an external process requires it, such as for encryption. **CAUTION:** When used in the **Script** box, this value is resolved and written to the /tmp directory. In case MessageWay determines that the external process has aborted, it will not delete the file, as it does when all processes complete successfully. When this token is used in the **Command** box, it is resolved in memory and never written to a temporary file.

Output Transfers

An output transfer command or script will:

- Transfer one message from MessageWay

  - or -

- Initiate a process, without transferring a message

The adapter will call the script once for each output message to be delivered.

You specify how to transfer messages from MessageWay using the **Command** box or the **Script** box on the **Output** tab of the Site Properties window.

Specifying a User ID and Password

You may enter a user ID and password when required to connect to an external process. Then in the **Command** box or the **Script** box for the output transfer, use the ***replaceable parameters*** (on page 548), %user% and %password% to pass this information to the external process.

CAUTION: When used in the **Script** box, these values are resolved and written to the /tmp directory. In case MessageWay determines that the external process has aborted, it will not delete the file, as it does when all processes complete successfully. When this token is used in the **Command** box, it is resolved in memory and never written to a temporary file.

Specifying Commands or Scripts

You specify the process to be invoked using the **Command** box or the **Script** box. The **Command** box calls external commands or scripts. The **Script** box allows users to create and store scripts in MessageWay.

When you specify the process using the **Command** box, the syntax requirements are as follows:

- Name of the process or script is first, using
  - Only the file name, if the external script is located in the ***default script subdirectory*** (on page 947), or if the command can be found by the operating system

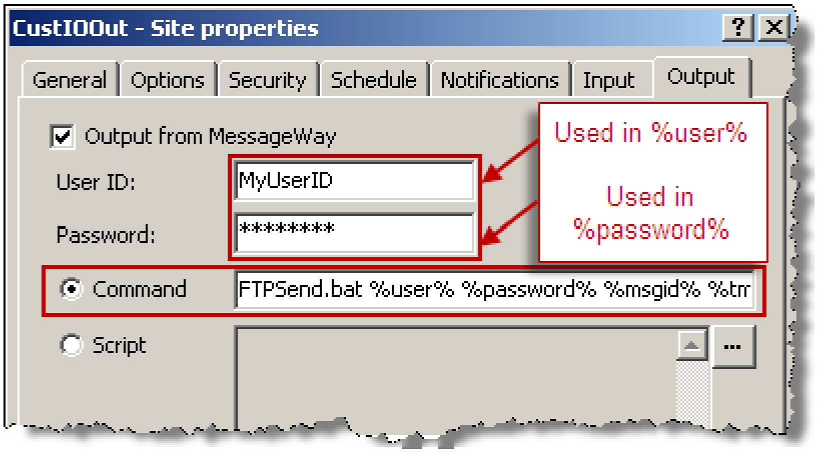
    - or -
  - Full path name and file name
- Arguments (replaceable parameters and literals) follow the name of the process and must be in the order required by the process, but the process or script itself must not contain any replaceable parameters

NOTE: MessageWay will resolve the parameters in memory and then pass them as arguments to the script or command for execution.

The following example does not use a status file. A status file is required to load more than one output or report file into MessageWay at a time. A status file is always required to load the other file types, acknowledgments and custom notifications.

This example invokes a batch (.bat) script, FTPSend.bat, which the adapter will find in the default script directory, \MessageWay\server\MWCustomIO\script. The adapter assigns values to the parameters. It then writes the expanded command to memory, from which it is run.

This script invokes an FTP session to send a file to an FTP site using a PUT command. The process includes error checking to interrogate the FTP responses for errors, such as invalid user ID or password, and whether the **PUT** command was successful. It creates four temporary files for troubleshooting, which are deleted upon successful completion of the command.



☑ Output from MessageWay

User ID: MyUserID

Password: ********

● Command FTPSend.bat %user% %password% %msgid% %tm

○ Script

Used in %user%

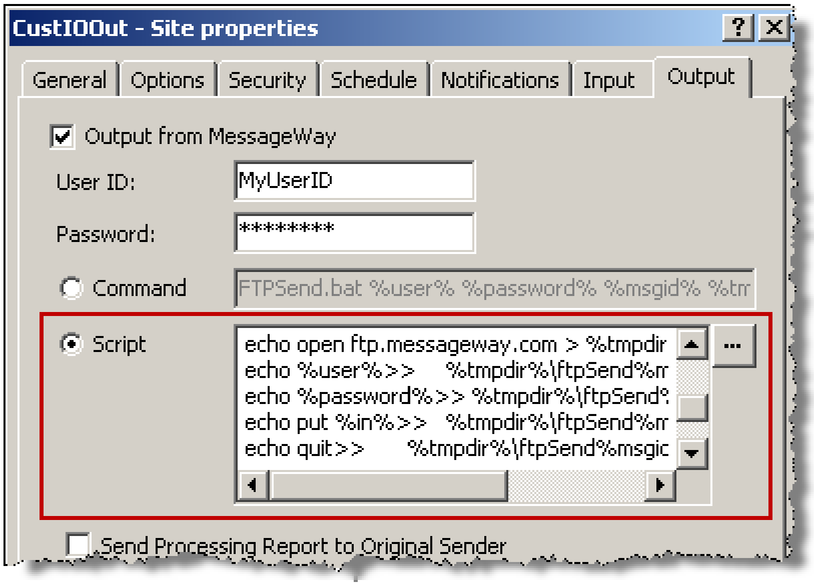
Used in %password%

When you specify the process in the **Script** box, the syntax requirements are as follows:

- The first line contains values to invoke the appropriate script process or, depending on the operating system as follows:
    - For Windows, this is the file extension required by the external process that is supported by the operating system, such as, .bat for a batch command, .vbs for Visual Basic or .js for Java Script.
    - For UNIX/linux, this is the standard #! line, such as, #!/bin/sh.
- Subsequent lines contain the instructions and include replaceable parameters and parameters required by the process.

NOTE: MessageWay will resolve the parameters and then write the script to a temporary file in the /tmp subdirectory. After successful execution, MessageWay will delete the temporary file.

The following example performs the same operations as the previous example, except that it is created in the **Script** box. Typically, you use the **Script** box when you need multiple lines of complex code that require you to embed replaceable parameters in the code. You should use the **Command** box for longer scripts.



CustIOOut - Site properties

☑ Output from MessageWay

User ID: MyUserID

Password: ********

○ Command FTPSend.bat %user% %password% %msgid% %tm

● Script

```
echo open ftp.messageway.com > %tmpdir
echo %user%>>    %tmpdir%\ftpSend%m
echo %password%>> %tmpdir%\ftpSend%
echo put %in%>>   %tmpdir%\ftpSend%m
echo quit>>      %tmpdir%\ftpSend%msgic
```

□ Send Processing Report to Original Sender

You would have to modify this script to call it from the **Command** box, because scripts that exist outside of MessageWay may not use replaceable parameters.

For additional examples using the command line to transfer files via FTP, go to the \server\MWCustomIO\examples directory. In these examples, the contents of the FTP session log are captured and sent to MessageWay and appear on the Error tab of the message.

NOTE: These examples happen to be for Windows, but comparable examples are installed with UNIX/Linux platforms.

Replaceable Parameters for Output Transfers (Custom I/O Site)

The **Command** box and the **Script** box for the **Output** tab may include replaceable parameters. The replaceable parameters are resolved by MessageWay before the instructions are passed to the operating system.

IMPORTANT: All replaceable parameters must be lower case. Replaceable parameters may be in any order, but they must satisfy the syntax of the script or program.

If any data in the **Command** box or the **Script** box contains a percent sign (%), you must use a release character, another percent sign, immediately preceding the first, giving two percent signs (%%). Then when MessageWay resolves the tokens, it will strip one of the signs, leaving you with one as part of the data.

The following table describes the valid replaceable parameters for the **Output** tab.

Replaceable Parameters (Output Tab)	Description
%out%	The full pathname of the message in the Message Store for the output message.
%outdir%	Default directory path, which is /out, to be used to create a temporary copy of the output file.
%tmpdir%	Directory path, which is /tmp, for temporary files created by the script. The archive and delete program, mwarchive, may delete files in this directory based on the value in the Temp File Retention field on the **MWArchive** tab of the MWArchive Server Properties window.
%status%	The name of a temporary file to be created by the script to provide the return status information about the delivery of the message.
%msgid%	The value shown for Message ID for the outbound message, viewable on the **General** tab of the Message Properties window.
%inputmsgid%	The value shown for Input Message ID, viewable on the **General** tab of the Message Properties window.
%inputname%	The value shown for Input Name, viewable on the **General** tab of the Message Properties window.
%filename%	The value shown for Filename, viewable on the **General** tab of the Message Properties window.
%user%	The user specified on the **Output** tab of the Site Properties window.
%password%	The password specified on the **Output** tab of the Site Properties window.
%sender%	The name of the sender of the outbound message, viewable on the Message Properties window.
%recipient%	The name of the recipient of the outbound message, viewable on the Message Properties window.

NOTE: Additional tokens that are normally available to processes that use file masks are available to this process. For a complete list, refer to the topic, ***Mask*** (on page 1103).

The following table explains how to use the replaceable parameters.

Replaceable Parameters	Description
%out%	Required to transfer a file from the Message Store. If you do not use this parameter, MessageWay will not send a message, but will just execute the script when a message arrives at the site. This allows you to execute an external process, without actually sending a message. The message that triggers the script without using this parameter will be marked Complete.

Replaceable Parameters	Description
%outdir%	Required when the external process needs to delete the message after it receives it, as in an FTP transfer that uses a delete command. Otherwise, the external process might attempt to delete the message from the Message Store.
%tmpdir%	Useful when the script or process creates temporary processing files or logs. Before exiting, the script should clean up any temporary files it has created in the /tmp subdirectory, unless this cleanup is done by the archive program.
%status%	Required if you want the external process to return a status file. A status file returns a status and an optional description. If the status is **A**, successful, the description should be blank or contain the input file name. If the status is **X**, failed, the description should contain the reason for failure.
%msgid%	Use this to relate the message ID to the file name used by an external process.
%inputmsgid%	Use this to relate the input message ID to the file name used by an external process.
%inputname%	Use this to relate the name of the input file to the file name used by an external process.
%filename%	Use this when you want a name for a message that will be constant throughout MessageWay processing.
%user%	May be used when external process requires it, such as for encryption. **CAUTION:** When used in the **Script** box, this value is resolved and written to the /tmp directory. In case MessageWay determines that the external process has aborted, it will not delete the file, as it does when all processes complete successfully. When this token is used in the **Command** box, it is resolved in memory and never written to a temporary file.
%password%	May be used when external process requires it, such as for encryption. **CAUTION:** When used in the **Script** box, this value is resolved and written to the /tmp directory. In case MessageWay determines that the external process has aborted, it will not delete the file, as it does when all processes complete successfully. When this token is used in the **Command** box, it is resolved in memory and never written to a temporary file.
%sender%	The name of the sender of the outbound message, viewable on the Message Properties window.
%recipient%	The recipient of the outbound message, viewable on the Message Properties window. When a ***compound address*** (on page 657) appears on the input location, the recipient comes from the

Replaceable Parameters	Description
	remaining portion of the compound address.

Understanding Statuses (Custom I/O Site)

When files are transferred to or from MessageWay, a completion code must be returned, which accomplishes two things:

- For input, indicates the status of operations
- For output, provides a completion status that MessageWay can use to mark messages as Complete or Error

The adapter determines the status in various ways:

- From the completion code of the script when a status file is not used
- From the status in the returned status file, which overrides a completion code
- Assumes abort when the process does not return a completion code or a status file with a valid status code

The adapter determines which files to upload to MessageWay depending on the status.

For Custom IO Input, the next table shows the type of returned messages the adapter will upload based on the status in a status file.

Value	Description	Input	Report
A	Accepted	Y	Y
X	Aborted	Y **NOTE**: 0 byte file with status of *Receive Error*	Y **NOTE**: Only one, and only if %rpt% token is used

NOTE: For a status of X, the uploaded files, input and optional report, will not be related, so you cannot use the command **Get Related**.

For Custom IO Output, the next table shows the type of returned messages the adapter will upload based on the status in a status file.

Value	Description	Report	Notification	Acknowledgment
A	Accepted	Y	Y	Y
X	Aborted	Y	Y	N

Statuses for Input Transfers (Custom I/O Site)

Status values themselves must always be returned to MessageWay from the external process, either implicitly using a completion code or explicitly using a status file.

When the status file is not used to explicitly return a status, the returned status is the result of the code returned from the script, as follows:

- **0** (zero) indicates successful transfer, and the adapter will call the script again for more messages

IMPORTANT: When the **Run Once** box is checked on the **Input** tab of the Site Properties window, the script will not be called again. This avoids endless loops, where a simple command in the **Command** box exits with a default code of **0**. Although users may use a code of **100** in a script to accomplish the same thing, this is often not normal practice, so this check box provides a safety net.

- **100** indicates there are no more messages, and the adapter terminates calls to the script
- **>0**, other than **100**, a message will be sent to MessageWay. The completion code will be the Error ID and any information written to STDOUT and STDERR will be displayed in the Error box. Also, the recipient on the message in error will be the configured *Deliver Input to* location. If *Deliver Input to* is *not* configured, the recipient will be blank. Also, a %rpt% file will be uploaded if a report destination is configured on the site.

  The message appears in the event log for the system:

Windows	Application Event Viewer
UNIX	/var/adm/messages
Linux	/var/log/messages

Best Practice To indicate failure without a status file, the script should exit with a value greater than zero (0), except 100. To indicate failure with a status file, the script should create a status file containing an X status and appropriate error description and then always exit with zero (0).

The status file allows you to provide additional and optional information to MessageWay as follows:

- Status value indicating the result of the transfer
- Multiple input and report files

The syntax for the file is as follows:

Line	Syntax
1	<status>,<description>
2-n	**IN:**[<source location>],<destination location>,<input file to upload>, [<assigned inputname>],[<assigned filename>],[assigned content type>]

Line	Syntax
	RPT:[<source location>],<destination location>,<report file to upload>, [<assigned inputname>],[<assigned filename>],[assigned content type>]

- The first line must contain a status, followed by a description if the status is **X**
- Subsequent lines describe the input files and reports and are optional
- Multiple fields on a line are always separated by commas
- When the source is not specified, the sender will be the name of the input location

The valid status values for input operations are shown in the following status table, and they must be in upper case:

Status Value	Description	Affect on Processing
A	Messages received. There are no more messages	No more processing until next poll
M	Messages received. There are more messages	Repeat processing after successful creation of message
N	No messages available	No more processing until next poll
X	I/O Error	No more processing until next poll

The following table explains how to use the components of the syntax.

Syntax Item	Notes
Status	See status table.
Description	Although the description of the status is optional, and not needed for successful processing, it is very useful when there is an I/O error to better explain the type of error.
IN: **RPT:**	These values identify the kind of message (Input and Report), viewable on the **General** tab of the Message Properties window. They must be uppercase characters followed by a colon. The lines may be in any order.
Source location	Should be a valid location defined in MessageWay, but not mandatory.
Destination location	Must be a valid compound address, dynamic distribution list or individual location defined in MessageWay, otherwise the message will be marked in error and sent to the system mailbox {Unknown}. Any address used here overrides the address in the **Deliver To** box on the **Input** tab.
Input file to upload	Fully qualified name of the input file, which may be in the default directory when you use the %indir% parameter or wherever the user specifies.
Report file to upload	Fully qualified name of the report file returned by the external process.

Syntax Item	Notes
Assigned inputname	Optional input file name used for the Input Name field of the message, which appears on the **General** page of the Message Properties window. Use this parameter to relate external file names to messages once they are in MessageWay.
Assigned filename	Optional file name used for the Filename field of the message, which appears on the **General** page of the Message Properties window. Use this parameter to provide a consistent name associated with the message.
Assigned content type	Optional content type used for the Content Type field of the message, which appears on the **General** page of the Message Properties window. Use this parameter to specify the content type, rather than have MessageWay determine the type.

Statuses for Output Transfers (Custom I/O Site)

Status values themselves must always be returned to MessageWay from the external process, either implicitly using a completion code or explicitly using a status file.

When the status file is not used to explicitly return a status, the returned status is the result of the code returned from the script, as follows:

- **0** (zero) indicates successful transfer
- **>=1**, the adapter sets the status to **X** (transfer failed) and provides error information, including any information written to STDOUT and STDERR, will be displayed in the Error box that appears on the **Error** tab of the Message Properties window as follows:
  - Error ID contains the completion code that the script returns to MessageWay
  - Error box contains a description of the completion code, as well as the error description from the operating system. The error box might also contain other information from a log file, if used.

  Also, the %rpt% file will be uploaded if a report destination is configured on the site.

IMPORTANT: When you do not use a status file, you should set the reply code for the script to a meaningful number, which will then appear as the Error ID. If you do not, you may not know exactly what caused the error, since the error descriptions returned by the operating system are not always helpful.

The status file allows you to provide additional and optional information to MessageWay as follows:

Line	Syntax
1	<status>,<description>
2-n	**RPT:**[<source location>],<destination location>,<report file to upload>, [<assigned inputname>],[<assigned filename>],[,assigned content type>]

Line	Syntax
	ACK:[<source location>],<destination location>,<acknowledgment file to upload>, [<assigned inputname>],[<assigned filename>],[,assigned content type>]
	NTF:[<source location>],<destination location>,<notification file to upload>, [<assigned inputname>],[<assigned filename>],[,assigned content type>]
	OUT:<assigned outputname>

NOTE: When the source is not specified, the sender will be used

The valid status values for output operations are shown in the following status table, and they must be in upper case:

Syntax Item	Notes
Status	▪ **A** (successful) ▪ **X** (failed)
Description	If the status is **A**, leave the description field blank If the status is **X**, describe the reason for failure.
RPT: **ACK:** **NTF:** **OUT:**	These values identify the kind of message (Report, Acknowledgment, Notification or Output), viewable on the **General** tab of the Message Properties window. They must be uppercase characters followed by a colon. The lines may be in any order. Note that there is a cumulative destination effect of %rpt%. %rpt% will be uploaded to each destination defined in an RPT line where %rpt% is the file to upload, as well as to any report destinations defined on the **Output** tab of the site.
Source location	Should be a valid location defined in MessageWay, but not mandatory.
Destination location	Must be a valid compound address, dynamic distribution list or individual location defined in MessageWay, otherwise the message will be marked in error and sent to the system mailbox {Unknown}.
Report file to upload	Fully qualified name of the report file that is returned from the external process.
Acknowledgment file to upload	Fully qualified name of the acknowledgment file returned from the external process.
Notification file to upload	Fully qualified name of the notification file returned from the external process.
Assigned inputname	Optional input file name used for the Input Name field of the message, which appears on the **General** page of the Message Properties window. Use this parameter to relate external file names to messages once they are in MessageWay.
Assigned filename	Optional file name used for the Filename field of the message, which appears on the **General** page of the Message Properties window. Use this parameter to provide a consistent name associated with the message.

Syntax Item	Notes
Assigned content type	Optional content type used for the Content Type field of the message, which appears on the **General** page of the Message Properties window. Use this parameter to specify the content type, rather than have MessageWay determine the type.
Assigned outputname	Optional file output name assigned by the application and used for the Output Name field of the message, which appears on the **General** page of the Message Properties window. By default, MessageWay generates the output file name but does not complete the Output Name field. The application must return a status file with an output name value to populate the Output Name field.

IMPORTANT: When you use a status file, you must set the reply code for the script to **0** (zero) or MessageWay will not parse the status file. When the return code is zero, and there is a status of **X**, the value **888nn** (status file parsed, 888, with additional code, nn) will then appear as the **Error ID**. The description is placed in the **Error** box, so make sure the description is meaningful.

Examples Using Scripts and Status Files

The following input examples show how to execute a script from a command box or script box using a status file. Status files allow users to upload multiple files, specify properties of the files and provide more information about the return status.

NOTE: These examples happen to be for Windows, but comparable examples are installed with UNIX/Linux platforms.

Though not used in this example, additional message header properties, such as class ID, input name, filename, and content type, can be set in the status file for each file uploaded. When an error occurs, such as when the directory to monitor does not exist, all information after *X*, in the first line of the status file will be displayed on the **Error** tab of the message in error in MessageWay. The information will also be displayed in an application event log event.

The following example script, InputAllUsingStatus, loads all files in the defined directory (dirPath) into MessageWay. This script will run once per polling interval.

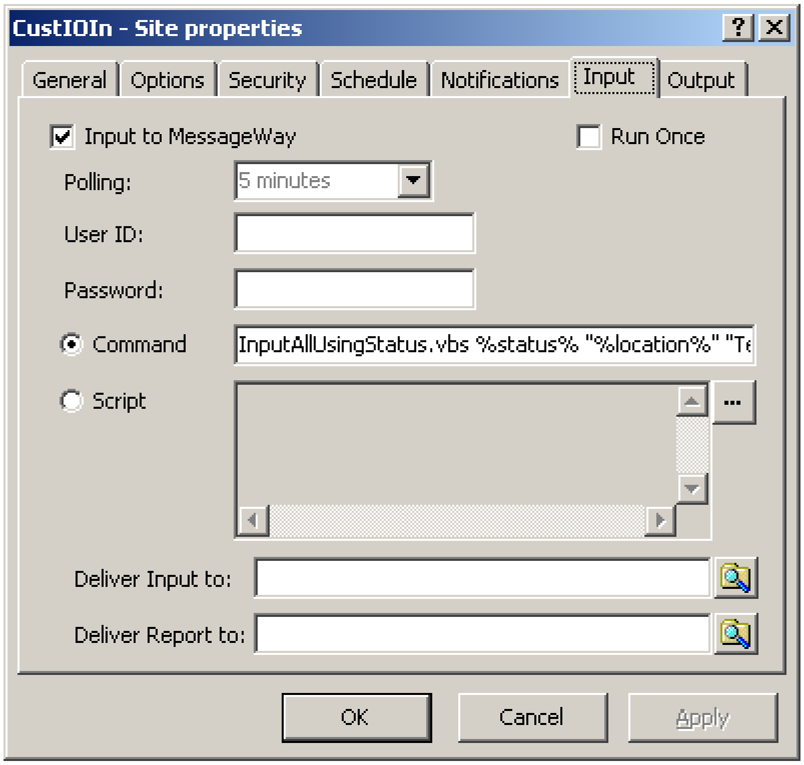
The full text of the command is as follows:

```
InputAllUsingStatus.vbs %status% "%location%" "TestPickup"
```

MessageWay assigns a fully qualified file name to %status% and a location where the script resides to %location%. The token %location% resolves to the name of the location where the script resides. The reason to use %location% rather than %sender% is that %sender% resolves to the sender on the message that triggered the script to run. For Custom IO input, the sender would be different depending on ***what initiated the script*** (on page 532): a polling event or an **Input Now** command.

The script will send all input files to the destination, TestPickup. It then writes the expanded command to memory and runs it. The script uses these resolved token values and the literal destination location as arguments to build the status file. Note that there is no value in the *Deliver input to* box, because the status file overrides whatever would be there.

This script creates a temporary status file, which MessageWay uses to determine the status of the transfer and, if successful, moves the named files from the subdirectory to the Message Store. In the script, each IN line represents a message, with a source and destination location


CustIOIn - Site properties

General | Options | Security | Schedule | Notifications | Input | Output

☑ Input to MessageWay

□ Run Once

Polling: 5 minutes

User ID:

Password:

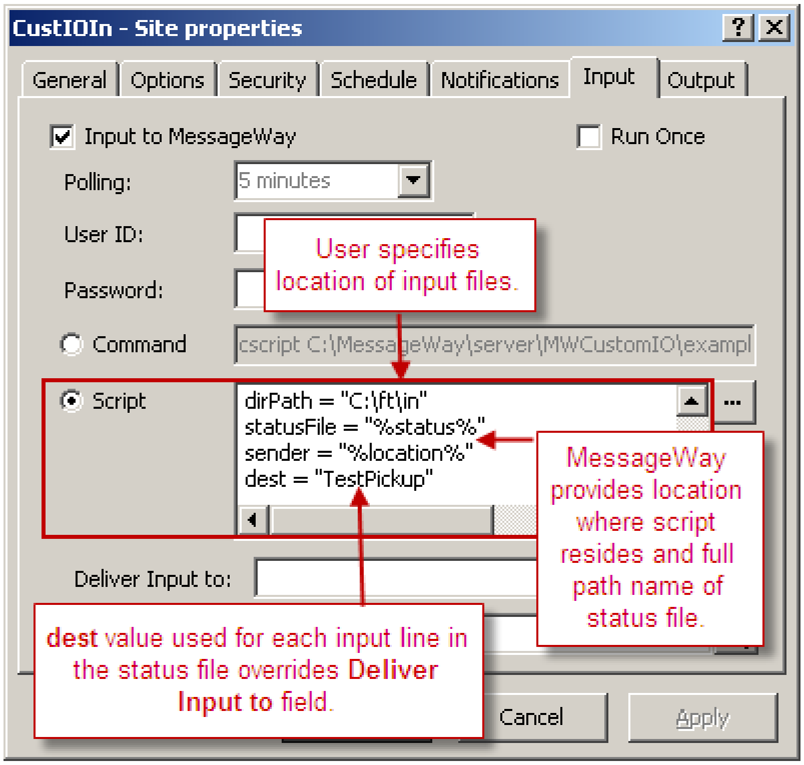
● Command: InputAllUsingStatus.vbs %status% "%location%" "Te

○ Script

Deliver Input to:

Deliver Report to:

The next example has the same effect as the first, but it was written to be executed from the script box.



☑ Input to MessageWay □ Run Once

Polling: 5 minutes

User ID:

Password:

○ Command cscript C:\MessageWay\server\MWCustomIO\exampl

● Script

```
dirPath = "C:\ft\in"
statusFile = "%status%"
sender = "%location%"
dest = "TestPickup"
```

Deliver Input to:

User specifies location of input files.

MessageWay provides location where script resides and full path name of status file.

dest value used for each input line in the status file overrides **Deliver Input to** field.

These example scripts are in the \server\MWCustomIO\examples directory for you to review and test.

Testing and Operations

To test your configurations, you must also have written a script or called a command or some other external process. Several sample scripts are loaded to the /examples subdirectory. You can use these to test to see how Custom IO works.

Once you determine what external process you want to call and have completed your adapter and site configurations, you are ready to test. Make sure the Custom IO and the Disk Transfer adapters are running.

1 To test the input process, use the sample script that creates an input message:

a) Copy the sample script **InputAllUsingStatus.vbs** for Windows or **InputAllUsingStatus.sh** for UNIX/Linux from the /examples directory to the /script directory.

b) Edit the script, and replace <*dest*> with the destination pickup mailbox in MessageWay where you will upload the information.

c) On the **Input** page of a custom IO site, in the **Command** box type the name of the script followed by the parameters specified in the description of the script itself, which will include **%status% "%location%" "**<*dest*>**"**.

d) Click **OK** to save the configuration. The script will execute at the next polling cycle

- or -

If you don't want to wait for the next polling cycle, or polling is set to **Never**, or the schedule is closed, ***issue the Input Now command*** (on page 559).

CAUTION: The script will continue to execute at the polling interval specified for the location, so don't forget to stop the Custom IO adapter when you have finished testing.

2 To test the output process, use a copy command to create an output message:

a) On the **Output** page of a custom IO site, in the **Command** box type **Copy %out% c:\MessageWay\server\MWCustomIO\out**. Make sure you adjust the output directory to a valid location.

b) Send a message from a disk transfer input site to the custom IO output site.

IMPORTANT: Make sure the locations are not on hold and the schedules are open.

Issuing the Input Now Command

The **Input Now** command provides a quick way to test an input script. The Custom IO Adapter must be running.

IMPORTANT: When the script is already running, the **Input Now** command is ignored. This command overrides the schedule, so it will be processed even when the schedule is closed or the site is on hold.

To generate a trigger message using this method:

1 In the left pane, select **Locations**.

2 In the right pane, right-click the appropriate custom IO site.

A menu appears.

3 From the menu, select **Input Now**.

The site queues an action to the adapter to run the script

Troubleshooting Custom IO

When the exit code from the external process is *not* zero (0), the custom IO adapter does not upload files. It leaves the temporary files created during the process for debugging.

In the Manager, when you view the adapter monitor, the counters work as follows:

- On input, the input counter for the MWCustomIO adapter increments temporarily, until the file is delivered to the output site, at which time the input count disappears, which is normal behavior
- On output, the output counter for the MWCustomIO adapter increments

CAUTION: On input, when you execute a script that does *not* use a status file, and the script returns a completion code of zero (0), the adapter assumes there is more work to be done and will immediately re-execute the script. This causes an infinite loop. To terminate the loop, you must stop the adapter , and then you can cancel the messages. You should also put the custom IO input site on hold until you have fixed the problem and before you restart the adapter. To fix the problem, on the **Input** tab check the box, **Run Once**, or change the completion code in the script to 100 for success.

If execution fails for an input script, there will be no error message in MessageWay. Users can find error messages in the event log of their system as follows:

Windows	Application Event Viewer
UNIX	/var/adm/messages
Linux	/var/log/messages

However, there will be no message in the event log if the script exits with zero (0), even when input fails or no message is uploaded. A script that uses a status file would normally attempt to exit with zero so that MessageWay would parse the status file. However, in case of failure, it is better to code the script to exit with some value other than zero or 100. Then a message appears in the event log and the status file remains in the /status subdirectory for users to view.

IMPORTANT: MessageWay captures STDOUT and STDERR information, so that when a non-zero exit code occurs, the information can be displayed on the *Error* tab of the message in error. To also capture standard output and error data in external logs, you can use nearly any application; the only known exception is the Windows command-line FTP client. For this program, the FTP Server responses are not included. Other FTP clients work properly. If you want to invoke an FTP client from your script and capture STDOUT and STDERR information in a log, use an FTP client other than the one the comes with Windows.

Cleanup After Failures

When either the input or the output process fails, temporary messages may be left in the MWCustomIO subdirectories. This allows users to better troubleshoot problems. The MessageWay Archive program will delete temporary files from the /tmp directory, if so configured.

However, users are then responsible for deleting other temporary files once they no longer need them. Users should remove any temporary files from the subdirectories as follows:

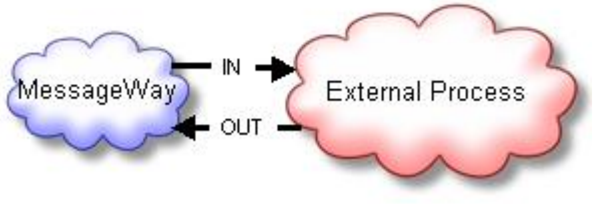
- Status files from /status
- Templates or scripts from /tmp
- Output files from /out
- Input files from /in

Configuring a Custom Processing Service Location

The MessageWay Custom Processing Service allows users to send messages from MessageWay to an external process, start the process and receive files back from the process. The external process typically manipulates the information and returns one or more related messages. However, the input message might simply be a trigger to run the process, which may not return any files.

The service runs a shell script, such as a batch file, or an executable program that is configured for a custom processing location. Valid scripting languages include those that are installed on and supported by the operating system. The scripts may reside in MessageWay or outside of MessageWay. Certain events will initiate the script or command.

The concepts of in and out as seen in the default subdirectories and the replaceable parameters, are relative to the external process. The terms *in* and *input* refer to messages transferred from MessageWay to the external process, and *out* and *output* refer to messages transferred from the external process to MessageWay.



This service includes the following configurable entities:

- Custom Processing Service
- Custom Processing service locations, created by users

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Understanding Custom Processing

The following steps show how MessageWay uses the Custom Processing Service and custom processing service location configurations. The service follows these basic steps:

1. Responds to an event to initiate an external process for a custom processing service location
2. Prepares information to exchange with the external process, which includes resolving replaceable parameters
3. Initiates the external process
4. Determines the completion status of the external process
5. Optionally, uploads files created by the external process based on completion code
6. Deletes the working files from disk after successful completion of all uploads

Respond to an Event to Initiate an External Process

One of the following types of events for a custom processing service location will cause the service to initiate a command or script:

- A message is sent to a custom processing service location, which is the default

  - or -

- A closed schedule opens for a custom processing service location that has the **Run script on trigger** box selected, and the schedule has a schedule item with the **Trigger** box checked

  - or -

- An operator issues a command, **Execute Now**, for a custom processing service location that has the **Run script on trigger** box selected

Prepare the Information to Exchange

The Custom Processing Service optionally sends information to and receives information from an external process. The service uses replaceable parameters or tokens to pass most of this information, although it can also pass literals.

Information that the service might send with tokens includes:

- Name of the input file in the MessageWay Message Store
- Information about the message:
  - Input message ID
  - Name of the input file
  - Message ID
- Logon information for an external system
  - User ID
  - Password
- Names of output files it expects to receive
  - Output file and report file, when not using a status file
  - List of output, report, link, acknowledgment and notification files when using a status file
- Name of temporary status file it expects to receive

Information that the service would receive from the external process includes:

- Completion code
- Optional status file with status and list of files to upload, which overrides the completion code
- Optionally, files to upload

Initiate the External Process

The service determines the process to initiate based on which one of the two options is selected on the **Process** page of the service location configuration window: **Command** or **Script**:

- If **Command** is selected, the script or process resides outside MessageWay, and the service resolves replaceable parameters in memory, calls the external command or script, and passes the resolved values and any literals as arguments

  - or -

- If **Script** is selected, the script resides in MessageWay, and the service resolves any replaceable parameters, writes the script to the /tmp directory, and then runs the script

Determine the Completion Status

After the adapter or service has started the process, it expects a completion code from the process, from which it determines the state of the original message that initiated the process and then what error information, if any, to display on the **Error** tab of the Message Properties window.

- When the process does not return a completion code, the adapter or service assumes the process aborted and marks the message with a state of *Error*

  - or -

- If a status file is used:
  - When the process sends a completion code of zero, the adapter or service parses the status file and
    - Uses the status in the file to determine which files to upload, if any

      - and -

    - When the status is *X*, Abort, it displays an Error ID of 888nn on the **Error** tab and writes the description of the error to the Error box

    - or -

  - When the process sends a completion code other than zero, the adapter or service assumes the process aborted and marks the message with a state of Error. Any information sent by the script or program to STDOUT or STDERR is written to the Error box.

  - or -

- If a status file is *not* used:
  - When the process sends a completion code of zero, the adapter or service marks the message with a state of *Complete*

    - or -

  - When the process sends a completion code other than zero, the adapter or service assumes the process aborted and marks the message with a state of Error. Any information sent by the script or program to STDOUT or STDERR is written to the Error box.

    - or -

  - When the process does not send a completion code, the adapter or service assumes the process aborted and marks the message with a state of Error. Any information sent by the script or program to STDOUT or STDERR is written to the Error box.

Upload the Returned Files

The service uploads files or not based on what it determines is the completion code.

- When the service receives a successful completion code, zero (0), the service uploads messages created by the external process:
    - If a status file is used, it uploads the files listed in the status file based on the status code in the status file. Based on the status code, it will also upload the output file when the %out% token is used and the report file when the %rpt% token is used even if they are not defined in the status file

      - or -
    - If a status file is *not* used, it uploads the output file when the %out% token is used and the report file when the %rpt% token is used. If the service cannot upload expected files, it assumes the process aborted
- When the service does not receive a successful completion code, anything other than zero (0), it assumes the process aborted and all temporary files remain where the process put them. The report file will be uploaded when the %rpt% token is used.

When the service uploads files, it must also determine where to send the files. How the service determines where to send the messages depends on whether the process returns a status file. The basic behavior is as follows:

- When a status file is *not* used, only two files can be uploaded:
    - One output file whose name was resolved from the %out% token is either:
        - Sent to the remaining portion of a compound address on the original input location

          - or -
        - Sent to a default location called UNKNOWN (If the location called UNKNOWN does not exist, it will be forwarded to the system mailbox {Unknown})
    - One report file whose name was resolved from the %rpt% token is either:
        - Sent to the report location(s) as specified on the **Process** page of the custom processing Service Location Properties window

          - or -
        - Ignored and not uploaded when the report location is *not* specified on the **Process** page of the custom processing Service Location Properties window
- When a status file is created, multiple files may be uploaded. The name of the status file is resolved from the %status% token. When the process returns a completion code of zero (0), the service parses the file, where it finds the source and destination locations for five types of files: output, report, linked, acknowledgment and notification. When the %rpt% token is used, report destination(s) can also come from the processing service location configuration. For specific information about how the service determines the destinations with a status file, refer to the topics, ***Specifying the Destination Locations for Returned Files*** (on page 583) and ***Specifying the Destination for Processing Reports*** (on page 574).

Remove the Temporary Files

After MessageWay has completed its delivery process, it returns to the locations of any files it used, such as a status file, a temporary script file, and any files it attempted to upload, and deletes them.

If MessageWay instead determines there was an abort in the external process, it does not delete the temporary files, leaving them for future debugging. In this case, users should remove the files.

Specifying Custom Processing Service Location Parameters

The configurations on the **Process** ***page*** (on page 1092) of the service location controls:

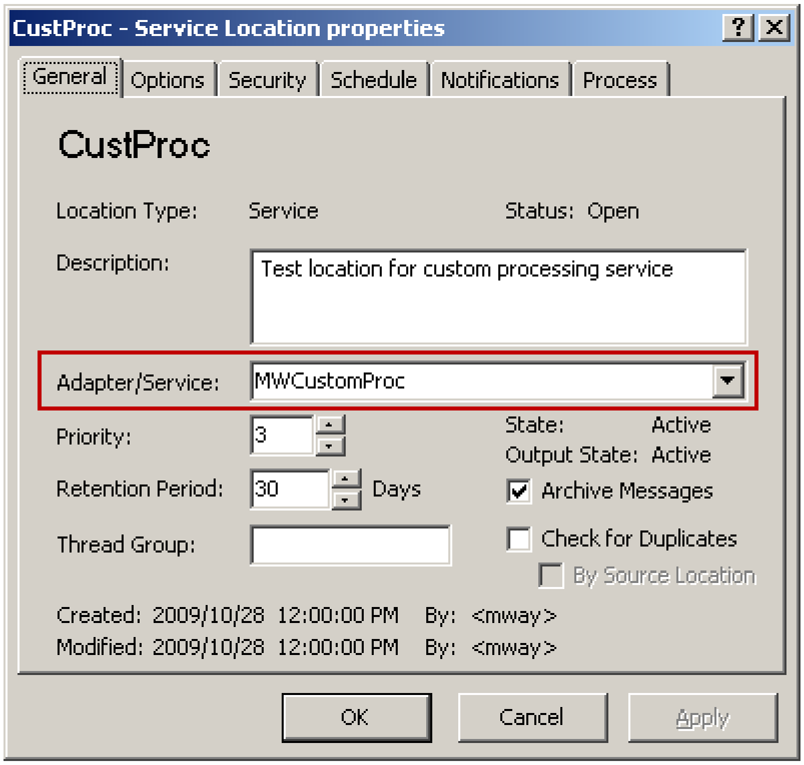
- How to initiate an external process
- What information to exchange with the process
- Where to send any report files generated by the external process, which can also be configured in the status file

Adding a Custom Processing Service Location

In case you have not already done so, you should create a custom processing service location, as follows:

1 Add a location.

2 In the **Adapter/Service** box, select **MWCustomProc**.



CustProc - Service Location properties

CustProc

Location Type: Service

Status: Open

Description: Test location for custom processing service

Adapter/Service: MWCustomProc

Priority: 3

State: Active

Output State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

☐ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/10/28 12:00:00 PM By: <mway>

3 ***Configure other properties for the location*** (on page 467).

IMPORTANT: For MWCustomProc (Custom Processing Service) locations configured for trigger messages, the priority must be less than 5 and the number of threads specified on the **General** page of the Custom Processing Service must be greater than 1. This is because trigger messages are assigned a default priority of 5. Other messages should not compete with this priority and there must be a reserved thread available for these messages so they will always appear in the queue. Otherwise, the trigger messages may not be added to the queue and, therefore, not be processed.

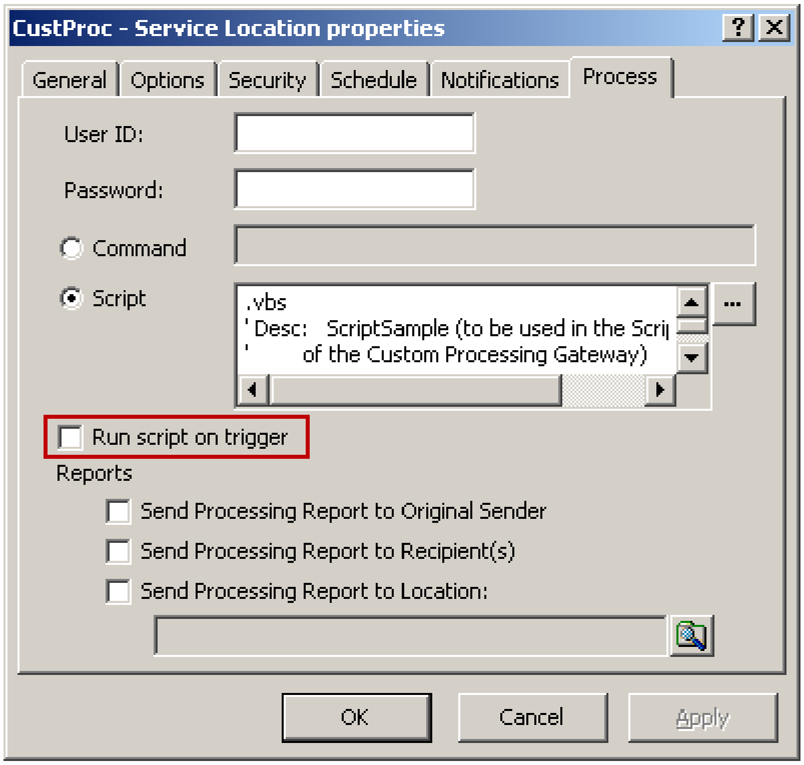
4 Select **Apply** or **OK** to save the configuration.

Defining Data or Trigger Service Locations

To avoid complications in processing, you should create separate service locations for data messages and trigger messages. In general, think of the difference as follows:

- Data messages are messages whose content is typically passed to the external process for manipulation
- Trigger messages are messages whose content is not typically passed to the external process, since their primary purpose is to simply start the process

To create a location for data messages, do *not* check the **Run script on trigger** box.



User ID:

Password:

○ Command

● Script

```
.vbs
' Desc:   ScriptSample (to be used in the Scri
'       of the Custom Processing Gateway)
```

□ Run script on trigger

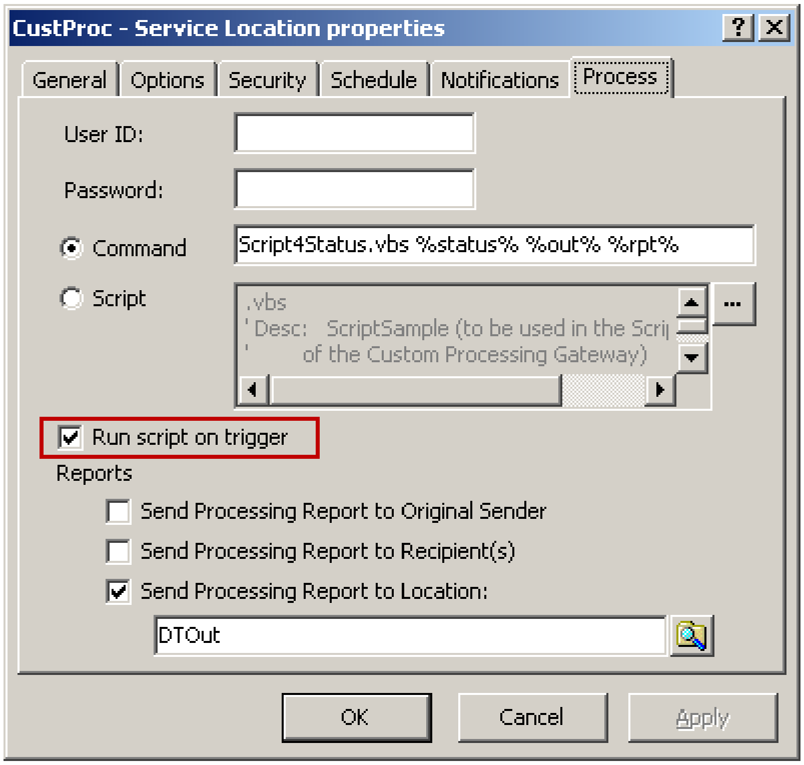
Reports

□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

□ Send Processing Report to Location:

To create a location for trigger messages, check the **Run script on trigger** box.


CustProc - Service Location properties

User ID:

Password:

● Command Script4Status.vbs %status% %out% %rpt%

○ Script
.vbs
' Desc: ScriptSample (to be used in the Scri
' of the Custom Processing Gateway)

☑ Run script on trigger

Reports

□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

☑ Send Processing Report to Location:

DTOut

IMPORTANT: For MWCustomProc (Custom Processing Service) locations configured for trigger messages, the priority must be less than 5 and the number of threads specified on the **General** page of the Custom Processing Service must be greater than 1. This is because trigger messages are assigned a default priority of 5. Other messages should not compete with this priority and there must be a reserved thread available for these messages so they will always appear in the queue. Otherwise, the trigger messages may not be added to the queue and, therefore, not be processed.

The Command and Script options on the location initiate different types of events based on whether the **Run script on trigger** box is checked. The service executes the instructions when:

- A message is sent to the location, which is the typical behavior

  - or -

- A closed schedule opens for a location that does have the **Run script on trigger** box checked, and a schedule item has the **Trigger** box checked, which automatically generates a trigger message that queues to the custom processing service location

  - or -

- For the location that does have the **Run script on trigger** box checked, an operator right-clicks the location and then clicks **Execute Now**, which manually generates a trigger message that queues to the custom processing service location

CAUTION: Do not send messages with data content to a service location where the **Run script on trigger** box is checked. The reason is that trigger messages can open closed schedules and override locations on hold. If you were to send a trigger message to a service location that had data messages on hold, it would queue any data messages in the location for delivery along with the trigger message and cause the service to initiate the external process once for the trigger message and once for each data message.

Specifying the Process

You specify the process to be invoked using the **Command** box or the **Script** box. The **Command** box calls external commands or scripts. The **Script** box allows users to create and store scripts in MessageWay.

When you specify the process using the **Command** box, the syntax requirements are as follows:

- Name of the process or script is first, using
  - Only the file name, if the external script is located in the ***default script subdirectory*** (on page 947), or if the command can be found by the operating system

    - or -
  - Full path name and file name
- Arguments (replaceable parameters and literals) follow the name of the process and must be in the order required by the process, but the process or script itself must not contain any replaceable parameters

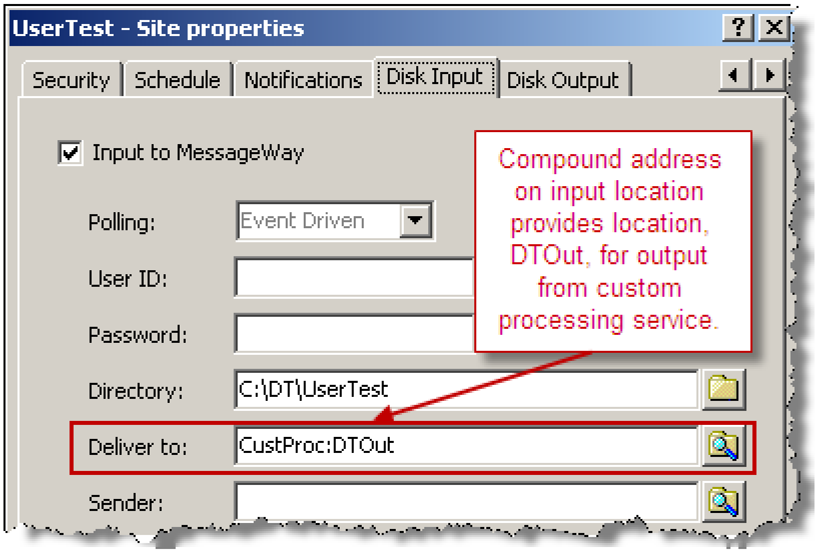
NOTE: MessageWay will resolve the parameters in memory and then pass them as arguments to the script or command for execution.

The following examples do not use a status file. A status file is required to load more than one output or report file into MessageWay at a time. A status file is always required to load the other file types, acknowledgments and custom notifications. For examples that use a status file, refer to the topic, ***Examples Using Scripts and Status Files*** (on page 586).

In these examples, the script does not provide a destination location for the file returned to MessageWay. Therefore, you must use a compound address on the input location that sends a message to the custom processing location to provide the destination for the returned output file.

IMPORTANT: When a status file is not used, the %out% parameter should always be used with a compound address on the original input location that sent the data or trigger message to the custom processing service location. Otherwise the returned file will be delivered by default to the location UNKNOWN, which, when it doesn't exist, will be delivered to the system mailbox, {Unknown}. For more information about compound addresses, refer to the topic ***Examples of Compound Routing Addresses*** (on page 657).

The following figure shows the compound address used on the input location, UserTest:



☑ Input to MessageWay

Polling: Event Driven

User ID:

Password:

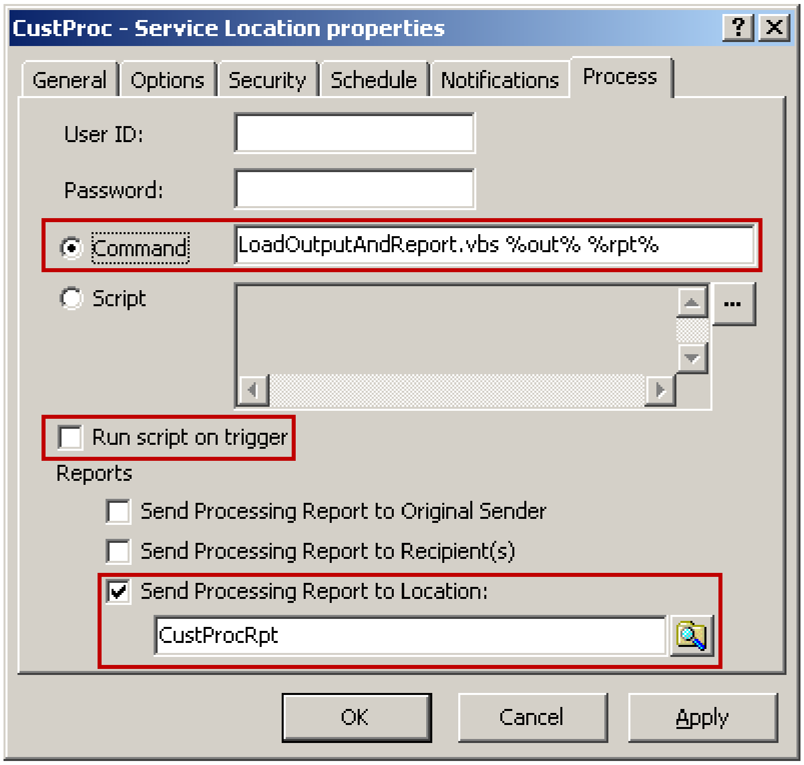
Directory: C:\DT\UserTest

Deliver to: CustProc:DTOut

Sender:

Compound address on input location provides location, DTOut, for output from custom processing service.

The following Windows example invokes the script, LoadOutputAndReports.vbs, from a command line. The service resolves the %in% and %out% replaceable parameters within memory and executes the script. This command copies the input file from the MessageWay Message Store and creates the output file in the \out subdirectory. Typically, when you pass a file from MessageWay with a script, you do not want to also use triggers to send data, so this box is clear. The destination of the report is also supplied on the **Process** page.



User ID:

Password:

● Command LoadOutputAndReport.vbs %out% %rpt%

○ Script

□ Run script on trigger

Reports

□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

☑ Send Processing Report to Location:

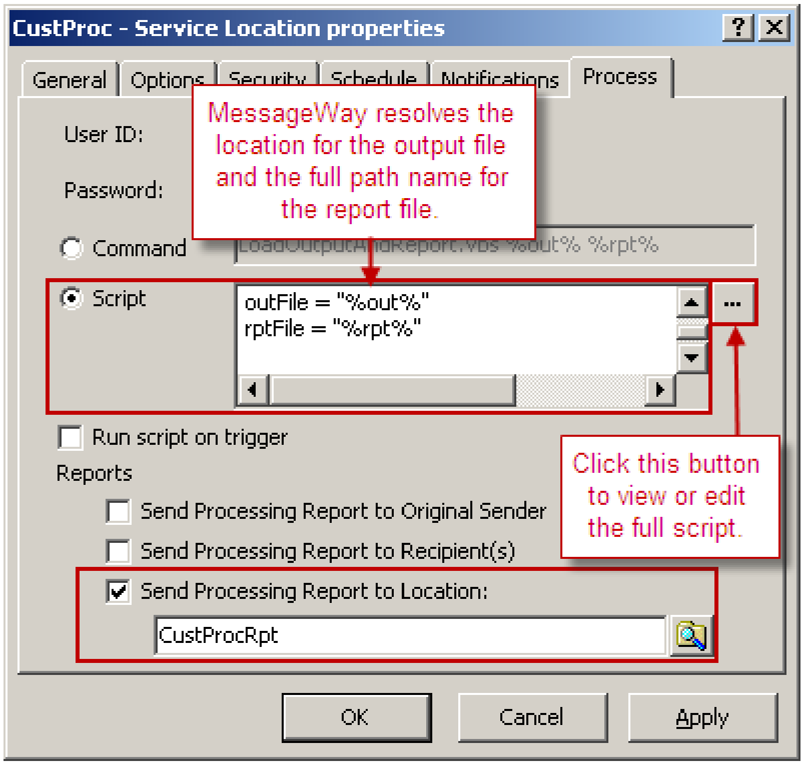
CustProcRpt

When you specify the process in the **Script** box, the syntax requirements are as follows:

- The first line contains values to invoke the appropriate script process or, depending on the operating system as follows:
  - For Windows, this is the file extension required by the external process that is supported by the operating system, such as, .bat for a batch command, .vbs for Visual Basic or .js for Java Script.
  - For UNIX/linux, this is the standard #! line, such as, #!/bin/sh.
- Subsequent lines contain the instructions and include replaceable parameters and parameters required by the process.

NOTE: MessageWay will resolve the parameters and then write the script to a temporary file in the /tmp subdirectory. After successful execution, MessageWay will delete the temporary file.

The following example is the same as the previous example, except it is called from the **Script** box.



User ID:

Password:

○ Command LoadOutputAndReport.vbs %out% %rpt%

● Script

```
outFile = "%out%"
rptFile = "%rpt%"
```

□ Run script on trigger

Reports

□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

☑ Send Processing Report to Location:

CustProcRpt

MessageWay resolves the location for the output file and the full path name for the report file.

Click this button to view or edit the full script.

CAUTION: When expected files are not returned to MessageWay, the service assumes that the process aborted. Under such circumstances, MessageWay does not delete any files from the subdirectories. When using the **Script** box, this may leave scripts in the /tmp directory with visible user IDs and passwords. If this is a potential problem, users should instead call an external script from the **Command** box, where tokens are resolved in memory and not written to the /tmp directory.

To view and test these example scripts, go to the \server\MWCustomProc\Examples directory.

Using Replaceable Parameters (Custom Processing Service Location)

The **Command** box and the **Script** box may include replaceable parameters. MessageWay resolves replaceable parameters before it initiates the external process.

IMPORTANT: All replaceable parameters must be lower case. Replaceable parameters may be in any order, but they must satisfy the syntax of the script or program.

The following table describes the valid replaceable parameters.

Replaceable Parameters	Description
%in%	The full pathname in quotes of the message in the Message Store. This allows the external process to access the content of the message. The process must have security to access the location of the Message Store when the content is stored on disk rather than in the MessageWay database.
%inputmsgid%	The message ID of the input file that was delivered to the external process, shown as the Input Message Id on the **General** tab of the Message Properties window. When the message is delivered to the external process, a separate message with its own message ID is linked to this input message.
%inputname%	The value shown for Input Name, viewable on the **General** tab of the Message Properties window. This includes the full pathname.
%filename%	The value shown for Filename, viewable on the **General** tab of the Message Properties window. This is the file name only, no path.
%out%	The full path name in quotes of the output file. MessageWay creates a temporary file name using a prefix of **OUT** followed by a unique name.
%status%	The name of a file that contains status information and potentially the names of multiple files for upload. MessageWay generates the name of the status file.
%rpt%	The full path name in quotes of the processing report file. MessageWay generates the name of the file.
%msgid%	The message ID of the inbound message when it is passed from MessageWay to the external process, shown as the Message Id on the **General** tab of the Message Properties window.
%outdir%	Directory path for returned output, report, acknowledgment and notification files, which are listed in the status file.
%tmpdir%	Directory path for temporary files. The archive and delete program, mwarchive, may delete files in this directory based on the value in the Temp File Retention field on the **MWArchive** tab of the MWArchive Server Properties window.
%sender%	Original sender of message sent to the custom processing service location. This token replaces %src%.
%recipient%	Original custom processing service location unless this is overridden by a compound address.

Replaceable Parameters	Description
%user%	The user specified on the **Process** tab of the Service Location Properties window. May be used when external process requires it, such as for encryption.
%password%	The password specified on the **Process** tab of the Service Location Properties window. May be used when external process requires it, such as for encryption.

NOTE: Additional tokens that are normally available to processes that use file masks are available to this process. For a complete list, refer to the topic, ***Mask*** (on page 1103).

All replaceable parameters are optional. The following table explains how to use them.

Replaceable Parameters	Use
%in%	Required when you want to send a file name to the external process. Not required if you send a message to trigger an external process, where input is not passed to the process.
%inputmsgid%	Required when you want to send the **Input Message ID** to the external process. View this value on the **General** tab of the Message Properties window. Not required if you send a message to trigger an external process, where the input is not passed to the process.
%inputname%	Use this to relate the name of the input file to the file name used by an external process.
%filename%	Use this when you want a name for a message that will be constant throughout MessageWay processing.
%out%	Required when you want the external process to return only one content file to MessageWay and you want MessageWay to create the file name. By default, MessageWay uses the /out subdirectory. **IMPORTANT:** By default, this token will resolve to a location called UNKNOWN. If you have not configured a location by this name, the message will be put in the system mailbox, {Unknown}. When you do not use a status file to specify the destination location, you should use a ***compound address*** (on page 657) on the original input message with this token. The compound address will also override an OUT destination location in a status file.
%status%	Required if you want the external process to return a status file to MessageWay. With a status file, you can specify multiple files to upload, the name(s) of notification files, report files, acknowledgment files, and output files and the source and destination locations for the acknowledgment, notification and output files.

Replaceable Parameters	Use
%rpt%	Required when you want the external process to return a processing report and you want MessageWay to create the file name. By default, MessageWay uses the /rpt subdirectory. This parameter is ignored when a status file is returned. **CAUTION:** When you use the %rpt% token, the report will be uploaded to each report destination defined on the **Process** tab of the custom processing Service Location Properties window, as well as to each destination defined in the status file RPT lines where %rpt% is the report to upload. If no report destinations are defined, the service ignores the generated report file and leaves it on disk.
%msgid%	Required when you want to pass the Message ID from the Message Store.
%outdir%	Required when you want the external process to create all files in the /out subdirectory. This is useful when you use a status file and want to put all files to be loaded into MessageWay in one subdirectory.
%tmpdir%	Useful when the script or process creates temporary processing files or logs. Before exiting, the script should clean up any temporary files it has created in the /tmp subdirectory. The archive and delete program, mwarchive, may delete files in this directory based on the value in the Temp File Retention field on the **MWArchive** tab of the MWArchive Server Properties window.
%sender%	Identifies the sender of the output message. This token replaces %src%.
%recipient%	Identifies the recipient of the output message. When a ***compound address*** (on page 657) is used for the input message, the destination comes from the remaining elements of the compound address. **CAUTION:** You must use a compound address on the input message with this token. By default, this token will resolve to the destination address of the original output message. Since this is the original custom processing service location, it will initiate another session of the external process and create a loop.
%user%	This passes the user specified on the **Process** tab of the Service Location Properties window. It may be used when an external process requires it, such as for encryption. **CAUTION:** When used in the **Script** box, this value is resolved and written to the /tmp directory. In case MessageWay determines that the external process has aborted, it will not delete the file, as it does when all processes complete successfully. When this token is used in the **Command** box, it is resolved in memory and never written to a temporary file.

Replaceable Parameters	Use
%password%	This passes the password specified on the **Process** tab of the Service Location Properties window. It may be used when an external process requires it, such as for encryption. **CAUTION:** When used in the **Script** box, this value is resolved and written to the /tmp directory. In case MessageWay determines that the external process has aborted, it will not delete the file, as it does when all processes complete successfully. When this token is used in the **Command** box, it is resolved in memory and never written to a temporary file.

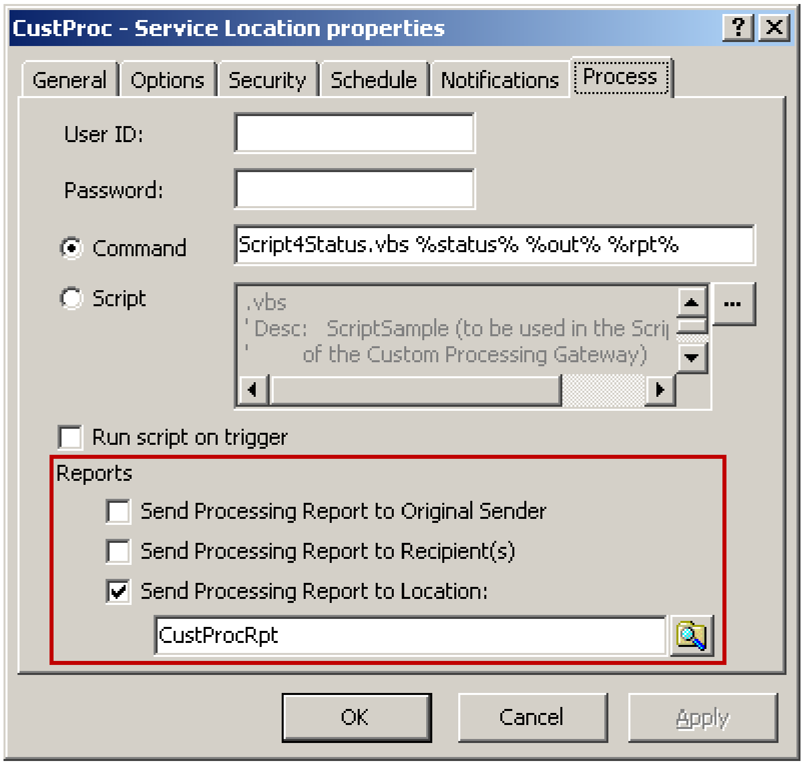
Specifying the Destination for Processing Reports

A custom processing service location defines the destination for any reports it expects from the external process on the **Process** tab, whether or not you use a status file. You must select from one of three options under the Reports group as follows:

Report Destination	Description
Original Sender	The report goes to the location associated with the sender of the original message.
Recipient(s)	The report is sent to the same location(s) as the output file(s).
Location	The report is sent to the specified location. When the location does not exist, the report goes to the system mailbox {Unknown}.

CAUTION: When you use the %rpt% token, the report will be uploaded to each report destination defined on the **Process** tab of the custom processing Service Location Properties window, as well as to each destination defined in the status file RPT lines where %rpt% is the report to upload. If no report destinations are defined, the service ignores the generated report file and leaves it on disk.

In the following example, the reports will be sent to the location, CustProcRpt.



User ID:

Password:

● Command Script4Status.vbs %status% %out% %rpt%

○ Script
.vbs
' Desc: ScriptSample (to be used in the Scri
' of the Custom Processing Gateway)

□ Run script on trigger

Reports

□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

☑ Send Processing Report to Location:

CustProcRpt

Understanding Statuses (Custom Processing Service Location)

The Custom Processing Service uses completion codes and, optionally, status values in status files returned from the external process to determine the status of the message it sent to the process. This input message is marked Complete or Error depending on the status. The service determines the status in various ways:

- From the exit code of the script when a status file is not used
- From the status in the returned status file, when the %status% parameter is used
- Assumes abort when the process does not return a return code or an expected status file

The following table shows the possible statuses and how they resolve to the state of the returned input messages. All of these statuses are possible when you use a status file, but only **A**, accepted, and **X**, aborted, are possible without a status file.

Value	Description	State on Input Message
A	Accepted	Complete
E	Accepted with errors	Complete
P	Partially accepted	Complete
R	Rejected	Complete

Value	Description	State on Input Message
X	Aborted	Error

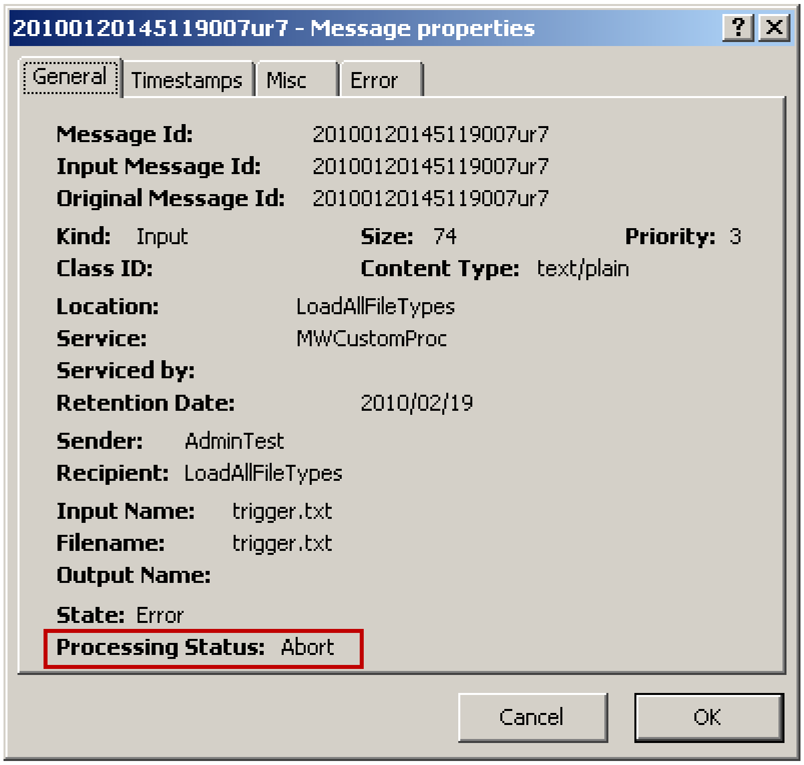
The service determines which files to upload to MessageWay depending on the status. The next table shows the type of returned messages the service will upload based on the status in a status file.

Value	Description	Output	Ack.	Report	Notification
A	Accepted	Y	Y	Y	Y
E	Accepted with errors	Y	Y	Y	Y
P	Partially accepted	Y	Y	Y	Y
R	Rejected	N	Y	Y	Y
X	Aborted	N	N	Y	Y

Statuses Returned without a Status File

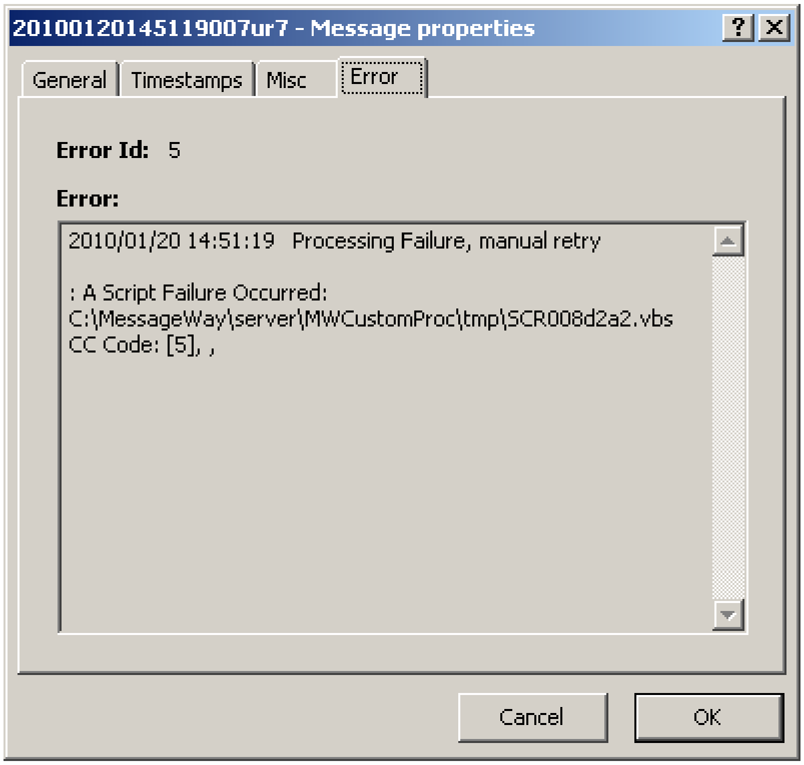
When the status file is not used to explicitly return a status, the returned status is the result code returned from the script, as follows:

- When the exit code is **0** (zero), the status of a returned file is set to **A** (accepted)
- When the exit code is *not* **0** (zero), the status is set to **X** (aborted)



Message Id: 20100120145119007ur7
Input Message Id: 20100120145119007ur7
Original Message Id: 20100120145119007ur7
Kind: Input **Size:** 74 **Priority:** 3
Class ID: **Content Type:** text/plain
Location: LoadAllFileTypes
Service: MWCustomProc
Serviced by:
Retention Date: 2010/02/19
Sender: AdminTest
Recipient: LoadAllFileTypes
Input Name: trigger.txt
Filename: trigger.txt
Output Name:
State: Error
Processing Status: Abort

The following error was caused because the exit code in the script was set to 5. Any error information returned from STDOUT or STDERR to MessageWay appears on the **Error** tab.



Error Id: 5

Error:

```
2010/01/20 14:51:19  Processing Failure, manual retry

: A Script Failure Occurred:
C:\MessageWay\server\MWCustomProc\tmp\SCR008d2a2.vbs
CC Code: [5], ,
```

IMPORTANT: When expected files are not returned to MessageWay, the service assumes that the process aborted.

Statuses Returned with a Status File

A status file must be returned when you use the %status% replaceable parameter. The service determines the status as follows:

- From the status code in the status file, when the external process returns a completion code of **0** (zero)

IMPORTANT: The external process must exit with a completion code of **0** (zero) for the service to parse the status file. If it exits with some other code, the service will not parse the status file.

- Assumes abort when
  - A status file is not returned

    - or -
  - The external process exits with something other than a **0** (zero) completion code

When an abort status (**X**) is returned, the Error Id on the **Error** tab of the Message Properties window for the message that was sent to the custom processing service location is 888 with an extension of nn, and any description appears in the Error box.

Creating a Status File

The external process must create the status file, using the name and location specified by MessageWay with the %status% token.

A status file must be returned when you use the %status% replaceable parameter or the service assumes that the process aborted. The status file allows you to provide additional information to MessageWay as follows:

- Status value indicating the result of the external processing for the input file
- Error description for an abort status (X)
- Multiple output files
- Multiple linked output files (input content is same as output)
- Multiple report files
- Multiple acknowledgment files
- Multiple notification files

The syntax for the status file is as follows:

Line	Syntax
1	<status>,<description>

Line	Syntax
2-n	**OUT:**[<source location>],<destination location>,<output file to upload>, [<assigned inputname>],[<assigned filename>],[<assigned content type>]
	LNK: [<source location>],<destination location>,[<assigned filename>], [<assigned content type>]
	RPT:[<source location>],<destination location>,<report file to upload>, [<assigned inputname>],[<assigned filename>],[<assigned content type>]
	ACK:[<source location>],<destination location>,<acknowledgment file to upload>, [<assigned inputname>],[<assigned filename>],[<assigned content type>]
	NTF:[<source location>],<destination location>,<notification file to upload>, [<assigned inputname>],[<assigned filename>],[<assigned content type>]

- The first line must contain a status and an optional description.
  - For an abort status (X), the description is placed on the Error tab of the message in error.
  - For all other statuses, the description is ignored.
- Subsequent lines are optional and may be in any order:
  - One line for each output file (OUT) with the following parameters:
    - Optional source location
    - Destination location, which may be a compound address or dynamic distribution list

      IMPORTANT: The destination location in the OUT parameter that is specified in the status file will be overridden when a compound address is used on the original input location. For more information, refer to the topic, ***Specifying the Destination Locations for Returned Files*** (on page 583).
    - Fully qualified output file name
    - Optional assigned input file name that will be used as the Input Name value on the General tab of the uploaded output
    - Optional assigned file name that will be used as the Filename value on the Message Properties window
    - Optional assigned content type that will be used as the Content Type value on the Message Properties window

    NOTE: When only one output exists, the %out% replaceable parameter is normally used within a script to provide a unique output file name.
  - One line for each linked output file (LNK) with the following parameters:

    NOTE: Use the LNK option instead of the OUT option when you do not modify the input message to create output, but rather simply create copies of the input file. Examples would be when you use custom distribution lists or customized routing rules that cannot be specified in the rules processing profiles in MessageWay. Then you can use the ***Get Linked command*** (on page 748) to view all output messages that share the same content as the input message. When you create custom distributions lists, you can use LNK instead of OUT to avoid having to explicitly copy the input message to each destination on the list.

  - Optional source location
  - Destination location, which may be a compound address or a dynamic distribution list

    IMPORTANT: The destination location in the LNK parameter that is specified in the status file will be overridden when a compound address is used on the original input location. For more information, refer to the topic, ***Specifying the Destination Locations for Returned Files*** (on page 583).
  - Optional assigned file name that will be used as the Filename value on the Message Properties window.
  - Optional content type that will appear as the Content Type value on the Message Properties window.

  NOTE: When only one output exists, for outputs files that are the same as the input file, the %lnk% replaceable parameter is normally used within a script to provide a unique output file name.

- One line for each report file (RPT) with the following parameters:

  NOTE: There are two syntax options for RPT to specify reports. Use the short form when all report destinations are defined on the **Process** page of the custom processing Service Location Properties window. For more robust naming and deliver options, use the long form.

  - Optional source location
  - Fully qualified report file name

    NOTE: The report name may be created by the program rather than by MessageWay, which also allows the external process to place the file in a temporary location other than the default RPT subdirectory.
  - Optional assigned input file name that will be used as the Input Name value on the Message Properties window.
  - Optional assigned file name that will be used as the Filename value on the Message Properties window.
  - Optional content type that will appear as the Content Type value on the Message Properties window.

  NOTE: When only one report exists, the %rpt% replaceable parameter is normally used within a script to provide a unique report file name.

CAUTION: When you use the %rpt% token, the report will be uploaded to each report destination defined on the **Process** tab of the custom processing Service Location Properties window, as well as to each destination defined in the status file RPT lines where %rpt% is the report to upload. If no report destinations are defined, the service ignores the generated report file and leaves it on disk.

- One line for each acknowledgment file (ACK), with the following parameters:
  - Optional source location
  - Destination location, which may be a compound address or dynamic distribution list
  - Fully qualified acknowledgment file name
  - Optional assigned input file name that will be used as the Input Name value on the Message Properties window.

    - Optional assigned file name that will be used as the Filename value on the Message Properties window.
    - Optional content type that will appear as the Content Type value on the Message Properties window.
  - One line for each notification file (NTF), with the following parameters:
    - Optional source location
    - Destination location, which may be a compound address or dynamic distribution list
    - Notification file name
    - Optional assigned input file name that will be used as the Input Name value on the Message Properties window.
    - Optional assigned file name that will be used as the Filename value on the Message Properties window.
    - Optional content type that will appear as the Content Type value on the Message Properties window.
- Multiple fields on a line are always separated by commas
- When the source location is not specified, the sender will be used, or if the process is initiated by an *Execute Now* command, the source will be the location that performs the processing

The valid status values are shown in the following status table, and they must be in upper case:

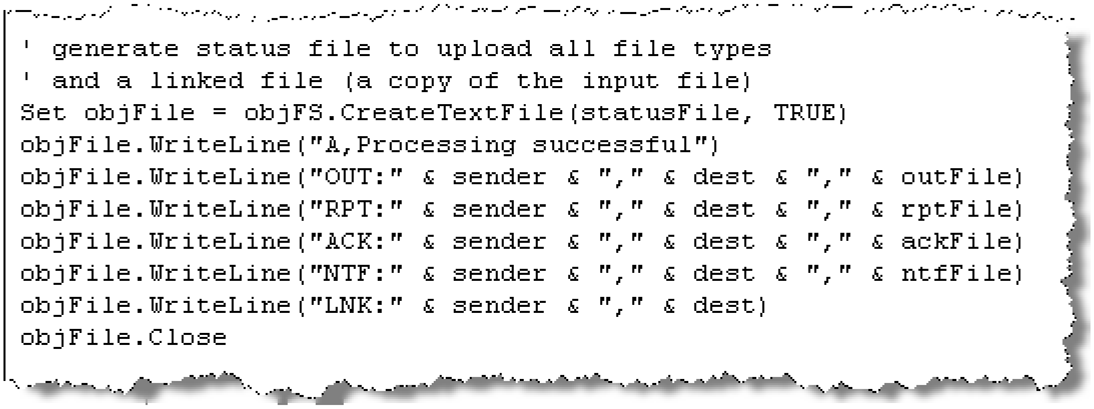
Status Value	Description
A	Accepted. There were no problems processing the input file.
E	Accepted with errors. This file was accepted and processed, but there were problems with the input file.
P	Partially accepted. Part of the input file was accepted and processed. Some parts were not processed.
R	Rejected. The input file was rejected and not processed.
X	Aborted. The process aborted. The external process should return a reason for the abort in the description parameter.

There following table explains how to use the components of the syntax.

Syntax Item	Notes
status	See status table.
file names	When you use the replaceable parameter to pass file names to and from the external process, by default, MessageWay processes the files using the file names it creates. When the process returns a Status file with full file names, MessageWay processes the files named in the Status file.

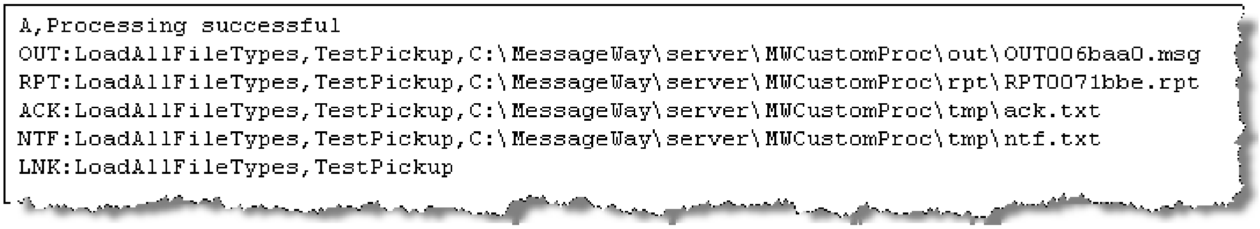
Syntax Item	Notes
OUT: **LNK:** **RPT:** **ACK:** **NTF:**	These values identify the kind of message (Output, Linked output, Report, Acknowledgment or Notification), viewable on the **General** tab of the Message Properties window. They must be uppercase characters followed by a colon. The lines may be in any order.
source location	Should be a valid location defined in MessageWay
destination location	Must be a valid location or series of locations when used with a compound address or dynamic distribution list, otherwise the message goes to the system mailbox, {Unknown}. **IMPORTANT:** For output files only, this value will be overridden by a compound address configured on the original inbound location that delivers the message to the custom processing service location. For output, acknowledgment and notifications files, the %recipient% parameter will also use the compound address.
content type	Assign a specific content type that appears on the **General** tab of the Message Properties window, rather than allow MessageWay to determine the content type.
filename	Assign a specific filename that appears on the **General** tab of the Message Properties window, rather than allow MessageWay to determine the filename.
input name	Assign a specific input name that appears on the **General** tab of the Message Properties window, rather than allow MessageWay to determine the input name.

This is an example of code in the example Visual Basic script LoadAllFileTypes that creates a status file.



```
' generate status file to upload all file types
' and a linked file (a copy of the input file)
Set objFile = objFS.CreateTextFile(statusFile, TRUE)
objFile.WriteLine("A,Processing successful")
objFile.WriteLine("OUT:" & sender & "," & dest & "," & outFile)
objFile.WriteLine("RPT:" & sender & "," & dest & "," & rptFile)
objFile.WriteLine("ACK:" & sender & "," & dest & "," & ackFile)
objFile.WriteLine("NTF:" & sender & "," & dest & "," & ntfFile)
objFile.WriteLine("LNK:" & sender & "," & dest)
objFile.Close
```

This is an example of the status file this code creates. The status file is deleted from the /status directory when the process completes successfully.



```
A,Processing successful
OUT:LoadAllFileTypes,TestPickup,C:\MessageWay\server\MWCustomProc\out\OUT006baa0.msg
RPT:LoadAllFileTypes,TestPickup,C:\MessageWay\server\MWCustomProc\rpt\RPT0071bbe.rpt
ACK:LoadAllFileTypes,TestPickup,C:\MessageWay\server\MWCustomProc\tmp\ack.txt
NTF:LoadAllFileTypes,TestPickup,C:\MessageWay\server\MWCustomProc\tmp\ntf.txt
LNK:LoadAllFileTypes,TestPickup
```

TIP: During testing, you may want to view the output files created by your script. To keep MessageWay from uploading and then deleting files from disk, you must change the exit code to something other than zero. Make sure you change it back to zero, after testing, or MessageWay will never upload the files.

Specifying the Destination Locations for Returned Files

The Custom Processing Service must determine where to send files it uploads. It determines the destinations differently depending on whether a status file is returned from the process.

When you do *not* use a status file, there are two types of files that may be returned to MessageWay, one of each type:

- Report
- Output

When you use a status file, there are five types of files that may be returned to MessageWay, multiples of each type:

- Report
- Output
- Linked Output
- Acknowledgment
- Custom Notification

Without Using a Status File

Typically, the %rpt% and %out% tokens are used when the external process does not return a status file. These tokens are limited in how they can return files, and there may be only one file per token. The following table shows the possible destinations when you use the %out% and %rpt% tokens. To avoid the default destination location, UNKNOWN, use the recommended configuration options.

Token	Default Destination	Recommended Configuration Options
%rpt%	UNKNOWN	Report options on **Process** page of custom processing service location.
%out%	UNKNOWN	Remaining portion of a compound address on the original input location that sent the message to the custom processing service location.

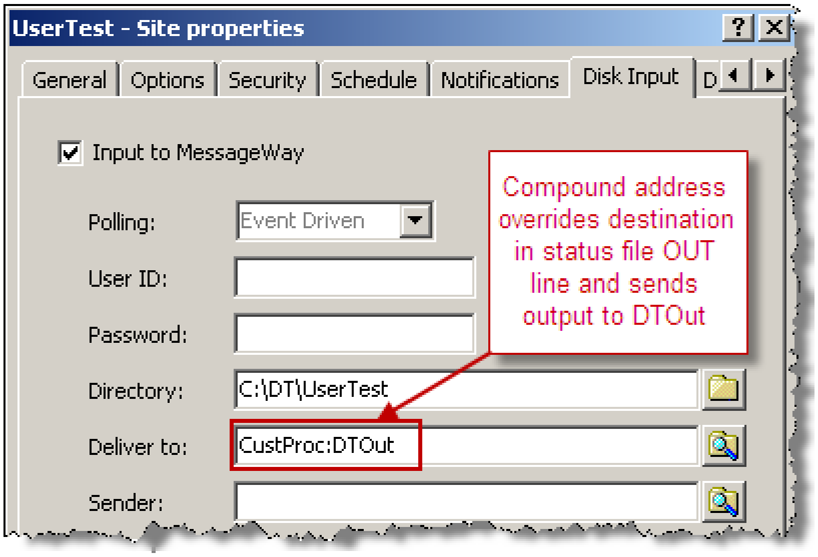
Using a Status File

A custom processing service location does not specify the destination location for output, acknowledgment, or notification files received from an external process. A status file returned from the external process allows users to specify the destination locations for these types of files.

There are two ways to define where to send output files:

- Define the destination location in a returned status file
- Use a compound address on the input location that delivers the files to the custom processing service location, which also overrides any OUT destination location defined in the status file

For more information about compound addresses, refer to the topic ***Examples of Compound Routing Addresses*** (on page 657). The following figure shows the compound address used in the input location, UserTest.



☑ Input to MessageWay

Polling: Event Driven

User ID:

Password:

Directory: C:\DT\UserTest

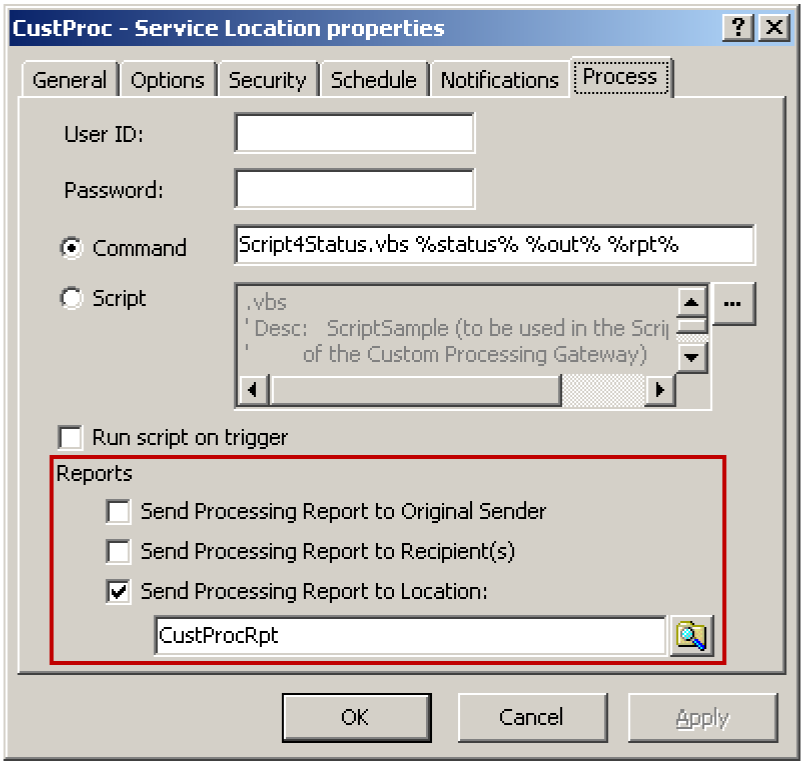
Deliver to: CustProc:DTOut

Sender:

Compound address overrides destination in status file OUT line and sends output to DTOut

There are two ways to define where to send report files, which will result in reports sent using both, when both are defined:

- Define the destination on the **Process** page of custom processing service location
- Define the destination in a report (RPT) line in a status file



User ID:

Password:

● Command Script4Status.vbs %status% %out% %rpt%

○ Script

```
.vbs
' Desc:   ScriptSample (to be used in the Scri
'        of the Custom Processing Gateway)
```

□ Run script on trigger

Reports

□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

☑ Send Processing Report to Location:

CustProcRpt

There is only one way to define to which locations the acknowledgment, linked output and notification files will be sent:

- Define the destination location in a returned status file

For more information about status files, refer to the topic ***Understanding Statuses*** (on page 575).

The following table shows how the Custom Processing Service resolves the destination location for the output (OUT), acknowledgment (ACK) and notification (NTF) message types (Msg. Type), when the destination slot contains one of the following:

- Nothing (Null value), which resolves to a location called UNKNOWN

  - or -

- Status file location name (SF Location) with or without a compound address on the original input location that sent the message to the custom processing service location (Input CA)

  - or -

- Token %recipient%, with or without a compound address on the original input location that sent the message to the custom processing service location (Input CA)

Msg. Type	Null Value	SF Location and Input CA	SF Location and no Input CA	%recipient% and Input CA	%recipient% and no Input CA
OUT	UNKNOWN	Input CA	SF Location	Input CA	Custom processing service location
ACK	UNKNOWN	SF Location	SF Location	Input CA	Custom processing service location
NTF	UNKNOWN	SF Location	SF Location	Input CA	Custom processing service location

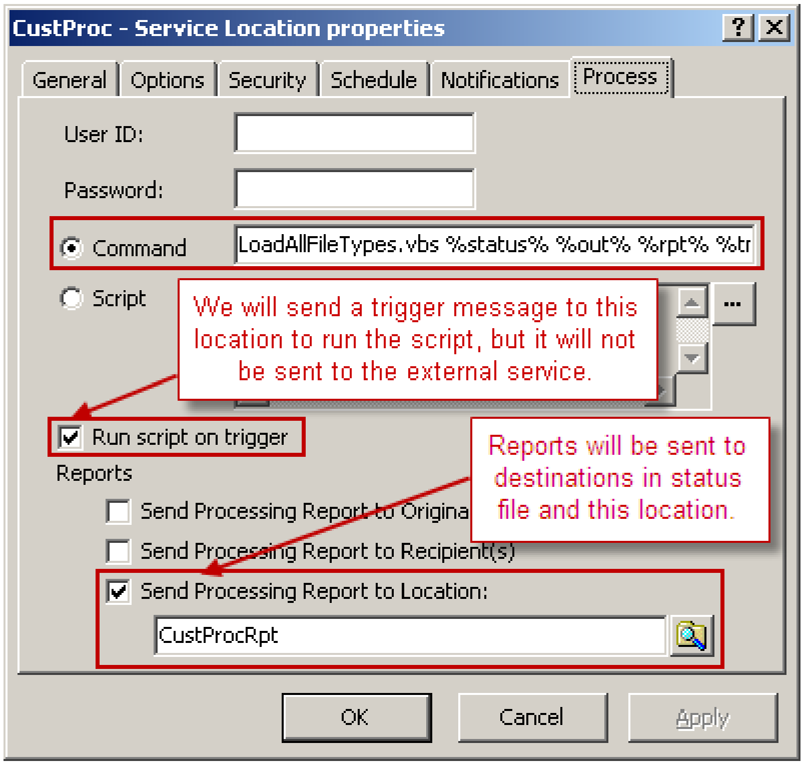
CAUTION: Notice that if you use the token %recipient% in the destination slots in a status file when the original input location does not have a compound address, the files will be sent back to the custom processing service location, which will create a loop. Always use a compound address with %recipient%.

Examples Using Scripts and Status Files

The following input examples show how to execute a script from a command box or script box using a status file. Status files allow users to upload multiple files, specify properties of the files and provide more information about the return status.

NOTE: These examples happen to be for Windows, but comparable examples are installed with UNIX/Linux platforms.

The following example executes a script from the Command box that creates one file of each file type (OUT, RPT, ACK, and NTF). It then creates a status file for the MWCustomProc service to parse in order to upload the files. A copy of the input file is also routed to another location with the use of the LNK line in the status file. The following screen shows the configuration for the custom processing service location, LoadAllFileTypes. Note that the **Run Script on Trigger** box is checked, because, for testing, we will right-click the location and click **Execute Now** to send a trigger.



CustProc - Service Location properties

User ID:

Password:

● Command LoadAllFileTypes.vbs %status% %out% %rpt% %tr

○ Script

We will send a trigger message to this location to run the script, but it will not be sent to the external service.

☑ Run script on trigger

Reports

□ Send Processing Report to Origina

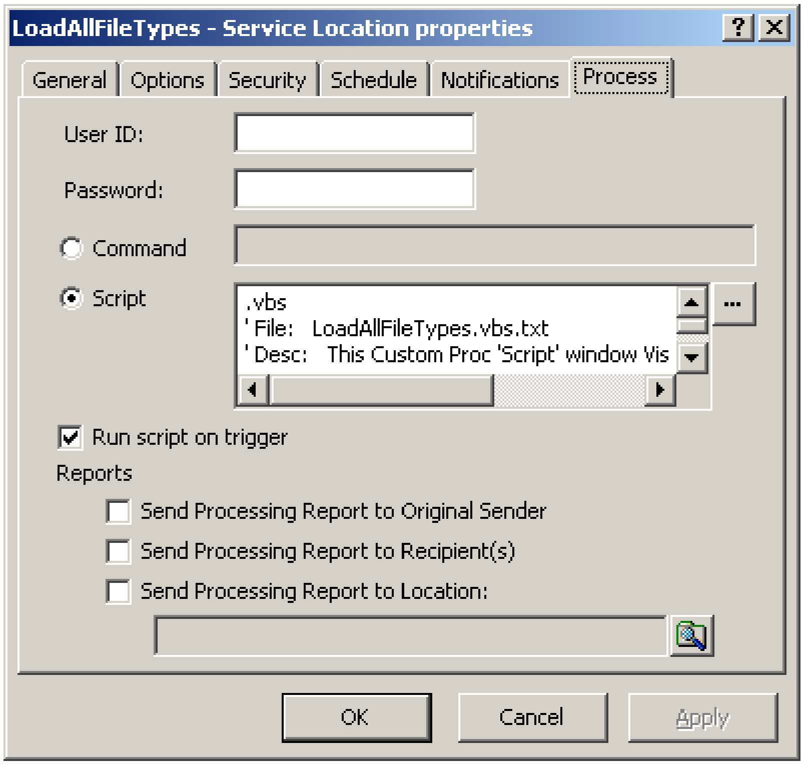
□ Send Processing Report to Recipient(s)

☑ Send Processing Report to Location:

CustProcRpt

Reports will be sent to destinations in status file and this location.

This next example performs the same functions as the first example, but it is called from the Script box.



LoadAllFileTypes - Service Location properties

User ID:

Password:

○ Command

● Script

```
.vbs
' File:   LoadAllFileTypes.vbs.txt
' Desc:   This Custom Proc 'Script' window Vis
```

☑ Run script on trigger

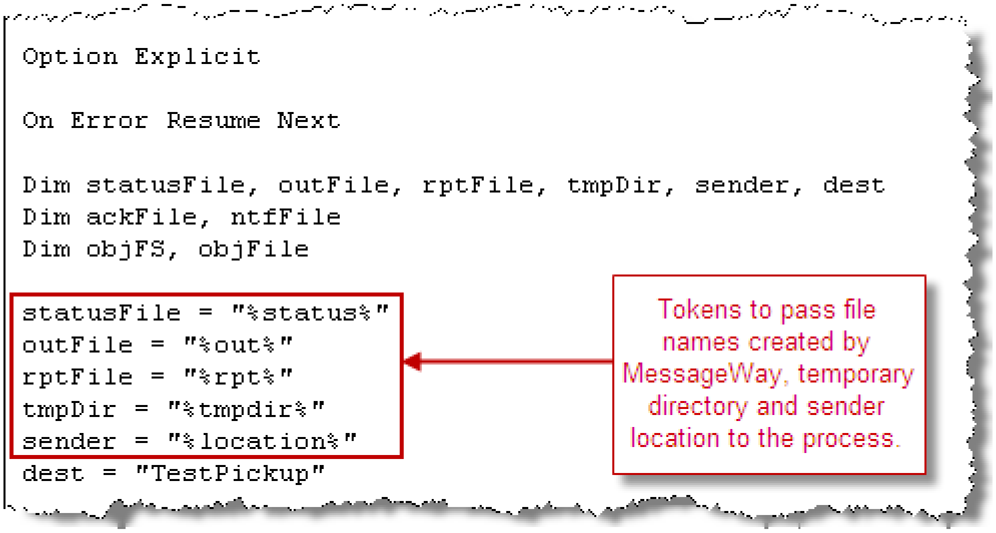
Reports

□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

□ Send Processing Report to Location:

To view the complete script, select the **Edit Script** button, ..., or view LoadAllFileTypes.vbs.txt from the /MWCustomProc/examples directory. To execute this script from the **Command** box, you would have to execute the example LoadAllFileTypes.vbs, because scripts that exist outside of MessageWay cannot use replaceable parameters.



```
Option Explicit

On Error Resume Next

Dim statusFile, outFile, rptFile, tmpDir, sender, dest
Dim ackFile, ntfFile
Dim objFS, objFile

statusFile = "%status%"
outFile = "%out%"
rptFile = "%rpt%"
tmpDir = "%tmpdir%"
sender = "%location%"
dest = "TestPickup"
```

Tokens to pass file names created by MessageWay, temporary directory and sender location to the process.

CAUTION: When expected files are not returned to MessageWay, the service assumes that the process aborted. Under such circumstances, MessageWay does not delete any files from the subdirectories. When using the **Script** box, this may leave scripts in the /tmp directory with visible user IDs and passwords. If this is a potential problem, users should instead call an external script from the **Command** box, where tokens are resolved in memory and not written to the /tmp directory.

To view and test these examples yourself, go to the \server\MWCustomProc\Examples directory.

Testing and Operations (Custom Processing Service Location)

To test your configurations, you must also have written a script or called a command or some other external process. Several sample scripts are loaded to the /examples subdirectory. You can use these to test to see how the Custom Processing Service works.

Once you determine what external process you want to call and have completed your service and service location configurations, you are ready to test.

- To test a data message, send the message to your custom processing service location configured for data messages. This location must *not* have the **Run script on trigger** box checked.

  - or -
- To test a trigger message, make sure the **Run script on trigger** box is checked:
  - ***Send the Execute Now command*** (on page 589)

    - or -
  - Wait for a closed schedule to open that sends a trigger message, as shown in the ***archive example*** (on page 802) in the "Maintaining Message Information" section

As an operations task, you should review the status of the message that was sent to the external process, to determine whether the process finished. You should also review any returned messages. For more information, refer to the topic, ***Finding Related Messages*** (on page 590).

CAUTION: If you find that counts are incrementing rapidly and unexpectedly, put the custom processing service location ***on hold*** (on page 709) rather than stopping the service. Then you will be able to modify the locations configurations or fix the script before you ***release it from hold*** (on page 710).

Sending the Execute Now Command

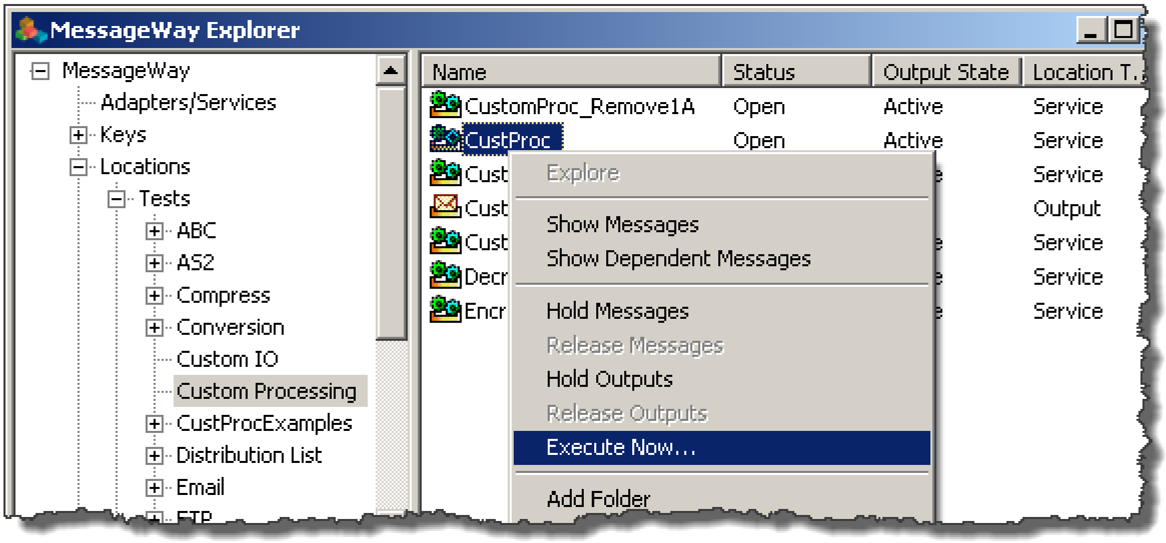
Operators may send the **Execute Now** command from the MessageWay Manager to initiate scripts. The **Execute Now** command creates a trigger message and sends it to the custom processing service location. When the trigger appears in the location, the Custom Processing Service will initiate the script. This is a quick way to test scripts that do not process message data. This command has no effect unless the **Run script on trigger** box is checked.

The Custom Processing Service must be running and the **Run script on trigger** must be checked.

IMPORTANT: This command will override a closed schedule or a location that is on hold.

To manually create a trigger message, proceed as follows:

1. From the left pane of MessageWay Explorer, select **Locations**.
2. From the right pane, right-click a custom processing service location, and select **Execute Now** from the menu.



Name	Status	Output State	Location T.
CustomProc_Remove1A	Open	Active	Service
CustProc	Open	Active	Service
Cust		e	Service
Cust			Output
Cust		e	Service
Decr		e	Service
Encr		e	Service

A confirmation dialog box appears to make sure you want to execute the action.

3. Click **OK**.

When the **Execute Now** command is processed, a trigger message will be queued to the custom processing service with the name of the user as its source location and the custom processing service location as its destination location.

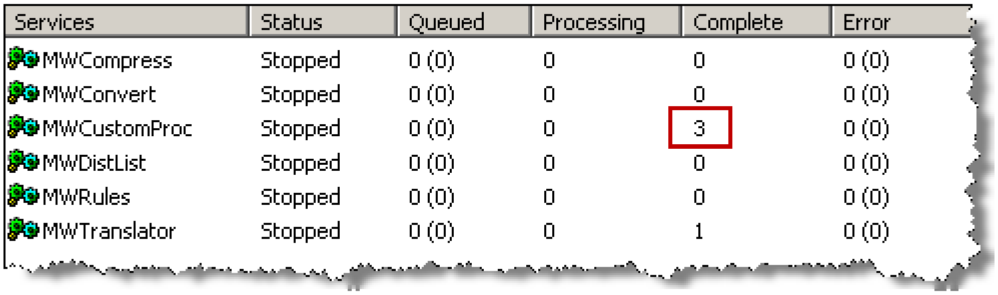
IMPORTANT: When the Custom Processing Service is not running or the box **Run script on trigger** is not checked, no trigger message will be created.

Finding Related Messages

When the external process returns files for MessageWay to deliver, you can find these files and the original input message by using the **Get Related Messages** command. For more information about this command, refer to the topic ***Finding Related and Linked Messages*** (on page 748).

To find related messages, proceed as follows:

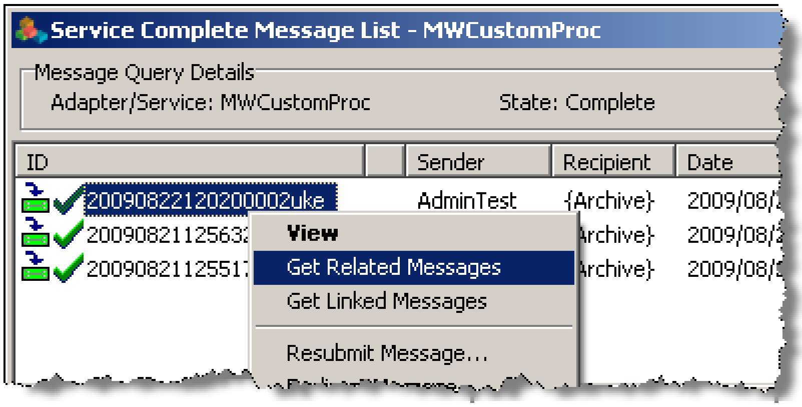
1. Double-click the MWCustomProc service statistics under the Complete column.



Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0	3	0 (0)
MWDistList	Stopped	0 (0)	0	0	0 (0)
MWRules	Stopped	0 (0)	0	0	0 (0)
MWTranslator	Stopped	0 (0)	0	1	0 (0)

A Message List window appears with all the completed messages sent to this service.

2. Right-click one of your messages, and select **Get Related Messages** from the menu.

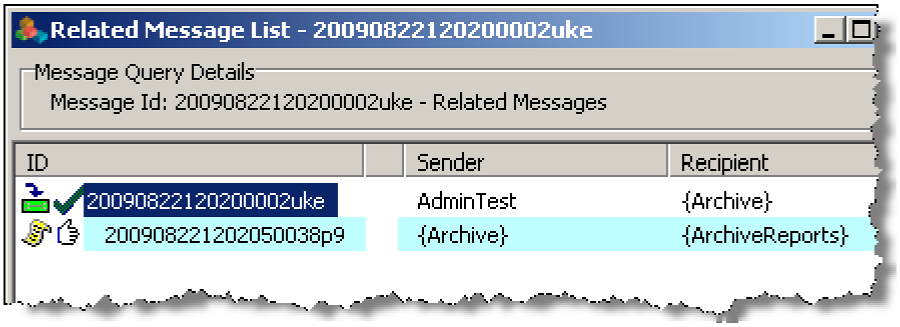


Service Complete Message List - MWCustomProc

Message Query Details
Adapter/Service: MWCustomProc State: Complete

ID		Sender	Recipient	Date
20090822120200002uke		AdminTest	{Archive}	2009/08/
2009082112563			rchive}	2009/08/
2009082112551			rchive}	2009/08/

Another Message List window appears with the original input message and all files returned by the external process.



Related Message List - 20090822120200002uke

Message Query Details
Message Id: 20090822120200002uke - Related Messages

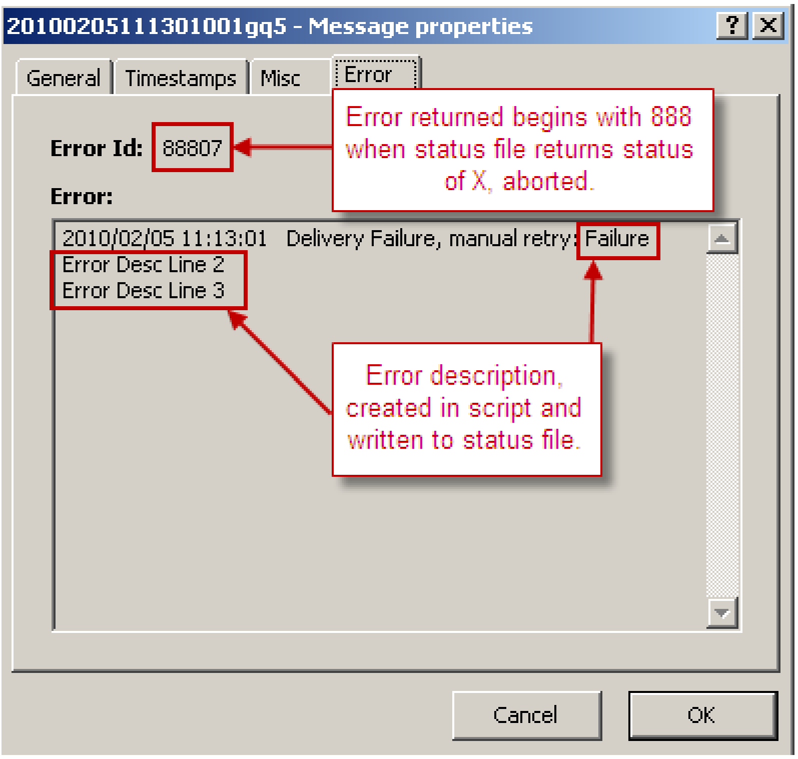
ID		Sender	Recipient
20090822120200002uke		AdminTest	{Archive}
200908221202050038p9		{Archive}	{ArchiveReports}

Understanding Error Messages

Typically, error messages are written to the *Error* tab of the Message Properties window for the input message that was delivered to the custom processing service location. Similar information may be found in an event log. The location of the event log depends on the system where the service is running, as follows:

Windows	Application Event Viewer
UNIX	/var/adm/messages
Linux	/var/log/messages

When the service assumes or knows the process has aborted, it writes an error ID and description to the **Error** tab and logs similar information to the event log. In the following example, the script returned an error code and some text. The rest of the information in the error box is from MessageWay.



Error Id: 88807

Error:

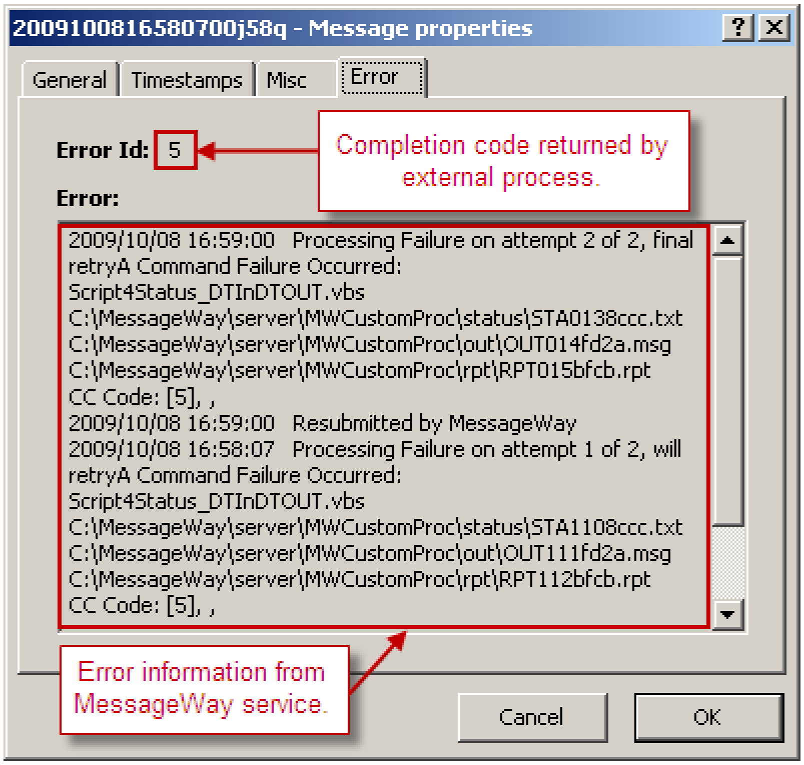
```
2010/02/05 11:13:01   Delivery Failure, manual retry: Failure
Error Desc Line 2
Error Desc Line 3
```

Error returned begins with 888 when status file returns status of X, aborted.

Error description, created in script and written to status file.

When an abort status (**X**) is returned in the status file, the Error Id on the **Error** tab of the message properties window is 888nn, and any description appears in the **Error** box.

When the external process returns a completion code other than **0** (zero), that code appears as the Error Id on the **Error** tab, and the service writes additional information to the **Error** box. In the following example, the process returned a completion code of 5, so the service did not parse the status file:



Error Id: 5

Completion code returned by external process.

Error:

```
2009/10/08 16:59:00   Processing Failure on attempt 2 of 2, final
retryA Command Failure Occurred:
Script4Status_DTInDTOUT.vbs
C:\MessageWay\server\MWCustomProc\status\STA0138ccc.txt
C:\MessageWay\server\MWCustomProc\out\OUT014fd2a.msg
C:\MessageWay\server\MWCustomProc\rpt\RPT015bfcb.rpt
CC Code: [5], ,
2009/10/08 16:59:00   Resubmitted by MessageWay
2009/10/08 16:58:07   Processing Failure on attempt 1 of 2, will
retryA Command Failure Occurred:
Script4Status_DTInDTOUT.vbs
C:\MessageWay\server\MWCustomProc\status\STA1108ccc.txt
C:\MessageWay\server\MWCustomProc\out\OUT111fd2a.msg
C:\MessageWay\server\MWCustomProc\rpt\RPT112bfcb.rpt
CC Code: [5], ,
```

Error information from MessageWay service.

IMPORTANT: MessageWay captures STDOUT and STDERR information, so that when a non-zero exit code occurs, the information can be displayed on the *Error* tab of the message in error. To also capture standard output and error data in external logs, you can use nearly any application; the only known exception is the Windows command-line FTP client. For this program, the FTP Server responses are not included. Other FTP clients work properly. If you want to invoke an FTP client from your script and capture STDOUT and STDERR information in a log, use an FTP client other than the one the comes with Windows.

Using Encryption with a Custom Processing Service Location

Users may access an encryption or decryption process using a custom processing service location. The process is external to MessageWay.

For purposes of an example, we will use a product that implements a public version, OpenPGP, of the proprietary standard Pretty Good Privacy (PGP) to encrypt e-mail using public key cryptography. OpenPGP is defined by the OpenPGP Working Group of the Internet Engineering Task Force (IETF) Proposed Standard RFC 2240. For more information about how to use OpenPGP and its Public Key Infrastructure (PKI), refer to the IETF Web site at ***IETF OpenPGP, RFC 2240*** (***http://www.ietf.org/rfc/rfc2240.txt***).

NOTE: Users must supply and install the GPG software to encrypt and decrypt the data. The examples shown here use the open source software called GnuPG. For more information about the Gnu Privacy

Guard software, refer to the Web site at ***www.gnupg.org http://www.gnupg.org***. MessageWay Solutions does not provide the GnuPG software.

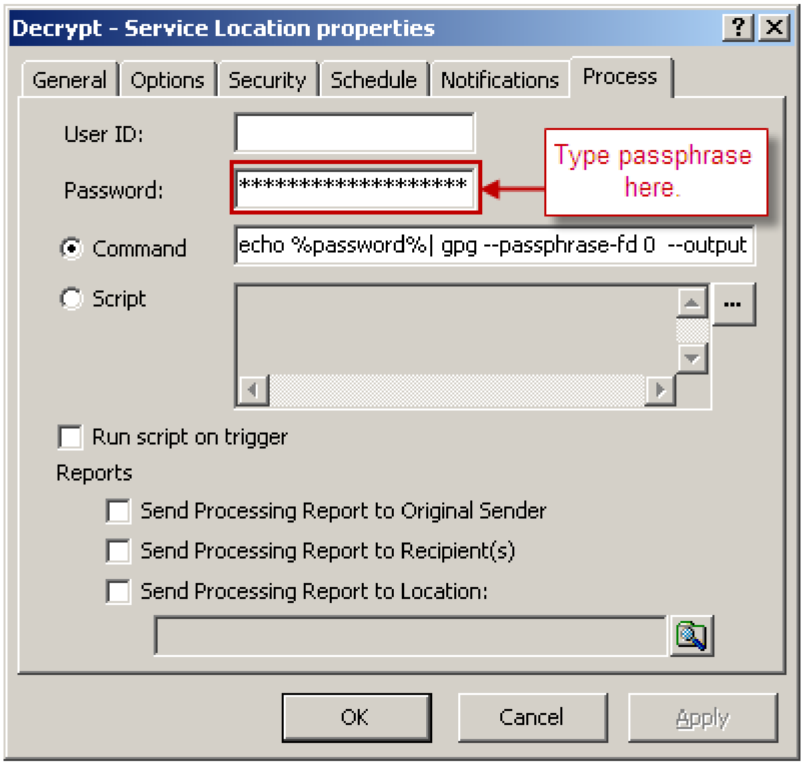
GnuPG is a tool for secure communication. It uses public-key cryptography to communicate securely. In a public-key system, each user has a pair of keys consisting of a private key and a public key. A user's private key is kept secret; it need never be revealed. The public key may be given to anyone with whom the user wants to communicate. The keys should be generated according to the documentation. To communicate with others, you must exchange public keys. So, the public keys must be imported and validated.

To decrypt a message, users must configure a service location, as shown in the next example.

1 Type the passphrase in the **Password** box.

2 Type the following command in the **Command** box:

echo %password%| gpg --passphrase-fd 0   --output "%out%" --decrypt "%in%"



Decrypt - Service Location properties

User ID:

Password: *******************

● Command echo %password%| gpg --passphrase-fd 0 --output

○ Script

□ Run script on trigger

Reports

□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

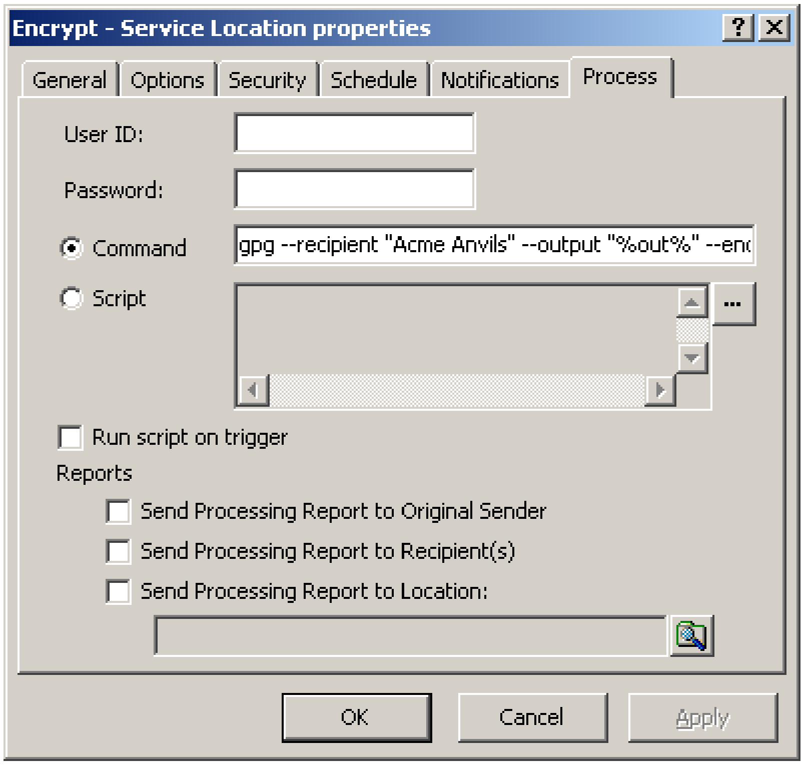
□ Send Processing Report to Location:

Type passphrase here.

To encrypt a message, users must configure a processing service location, as shown in the next example.

Type the following command in the **Command** box:

gpg --recipient "Acme Anvils" --output "%out%" --encrypt "%in%"



User ID:

Password:

● Command gpg --recipient "Acme Anvils" --output "%out%" --enc

○ Script

□ Run script on trigger

Reports

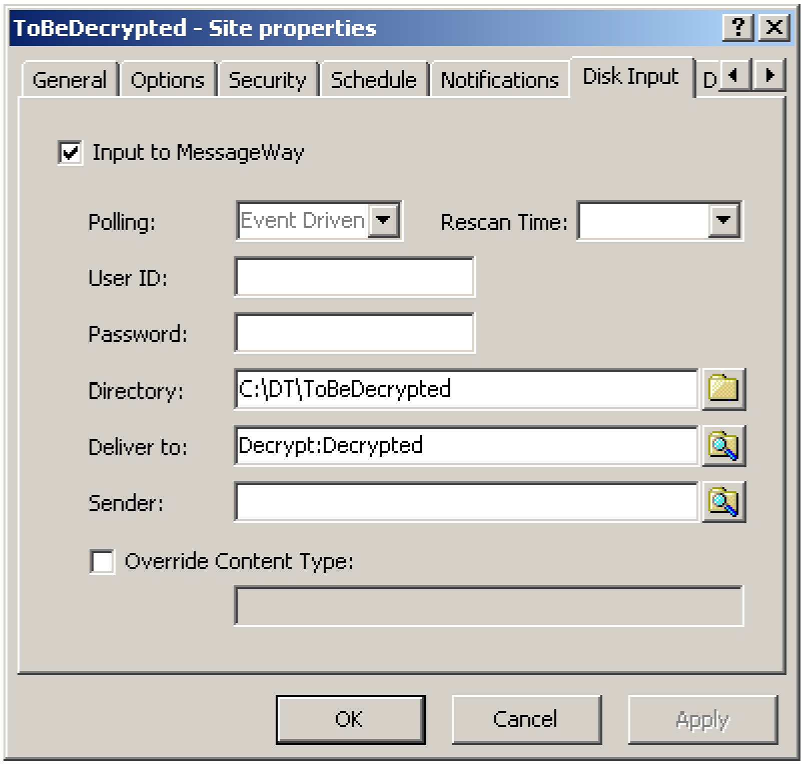
□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

□ Send Processing Report to Location:

To send the data to the Decrypt processing service location, for testing purposes, configure a Disk Transfer site that uses a compound address. The next example shows this option.

The compound address sends messages first to the Decrypt processing service location, which sends it to GPG for decryption. GPG then returns the decrypted file to MessageWay, which sends it to the second part of the compound address, the location called Decrypted.



☑ Input to MessageWay

Polling: Event Driven

Rescan Time:

User ID:

Password:

Directory: C:\DT\ToBeDecrypted

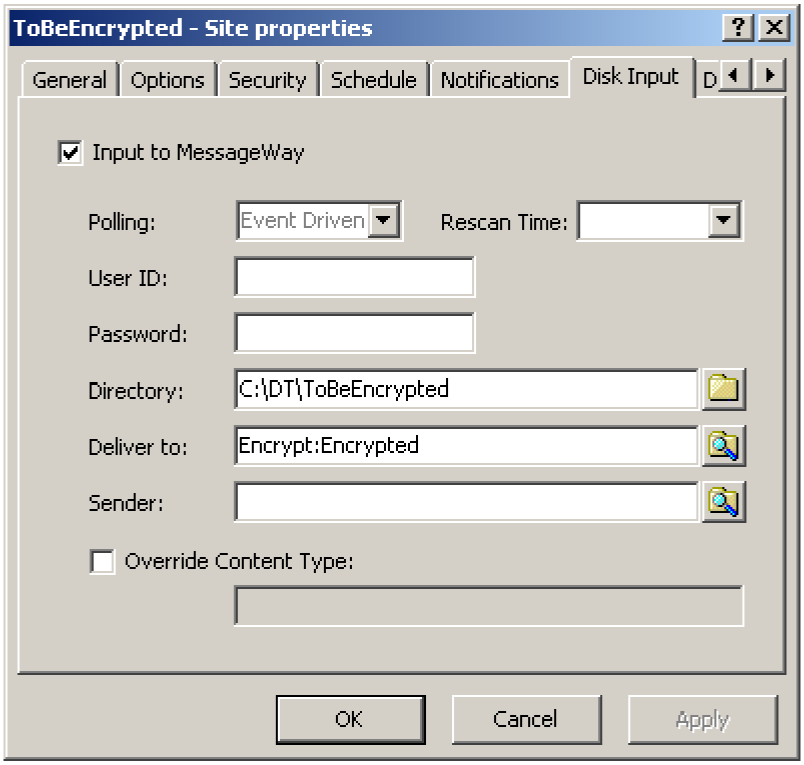
Deliver to: Decrypt:Decrypted

Sender:

□ Override Content Type:

To send the data to the Encrypt processing service location, for testing purposes, configure a Disk Transfer site that uses a compound address. The next example shows this option.

The compound address sends messages first to the Encrypt processing service location, which sends it to GPG for encryption. GPG then returns the encrypted file to MessageWay, which sends it to the second part of the compound address, the location called Encrypted.



☑ Input to MessageWay

Polling: Event Driven

Rescan Time:

User ID:

Password:

Directory: C:\DT\ToBeEncrypted

Deliver to: Encrypt:Encrypted

Sender:

☐ Override Content Type:

Configuring a Distribution List Service Location

The **Distribution List** page of the Service Location Properties window allows users to specify a list of locations to which a message will be sent. This page appears only for a distribution list service location.

IMPORTANT: When you send messages to a distribution list for delivery to multiple locations, the storage option on the Distribution List Service Location is what determines how a message is stored, not the option on the final destination location. This is because the message is stored once, and the final destination locations point back to the original message sent to the distribution list.

Options for a Distribution List Service Location

Users may create a distribution list to broadcast messages to many locations at once. When users create a distribution list, they may add existing locations or other distribution lists to the list.

To configure a distribution list service location:

1 Open an existing Distribution List service location.

2 To add locations, on the **Distribution List** page, select the **Add** button.

The **Select Location** dialog box appears.

3 Select one from a list of existing locations, identified by the icon, ✉, or other distribution lists, identified by the icon, ✉ .
- or -
Type the name of a location.
A distribution list may not contain itself.

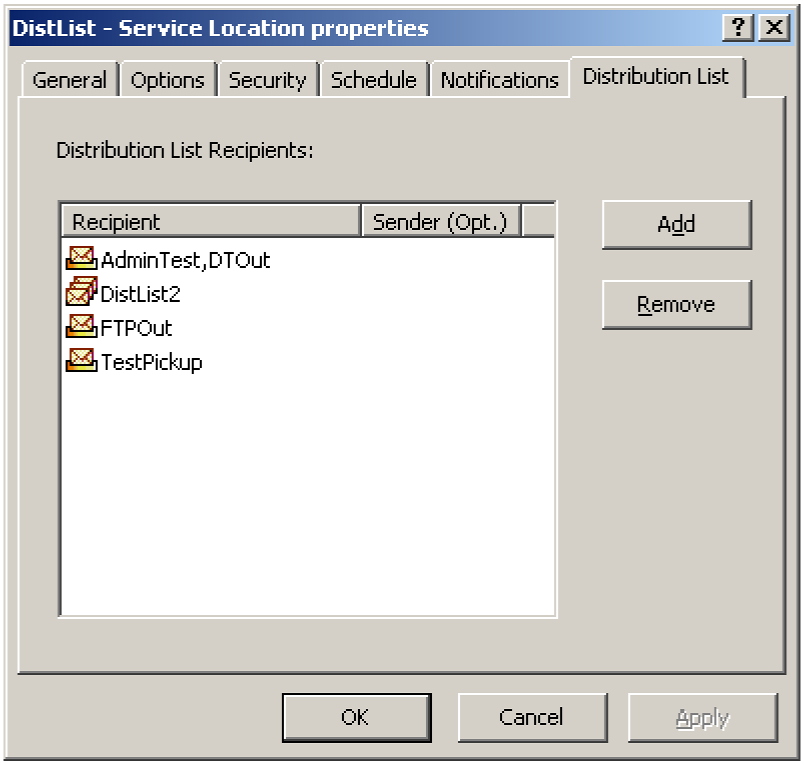
4 Optionally, type the name of a sender, and then click **Select**.

5 To delete locations, on the **Distribution List** page:
a) Select the locations you want to delete from the list.
b) Click the **Remove** button.

Example of Distribution List Service Location Parameters

The following window shows a distribution list that will send a message to various locations, including another distribution list. Note that you can enter multiple locations on one line, which you may want to do if you are changing the sender of the message for some of the destination locations, but not for others or you want a different sender for the others.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.



Distribution List Recipients:

Recipient	Sender (Opt.)
AdminTest,DTOut	
DistList2	
FTPOut	
TestPickup	

Example of Locations on Distribution List (Distribution List Page, Service Location Properties Window)

Configuring a Disk Transfer Site

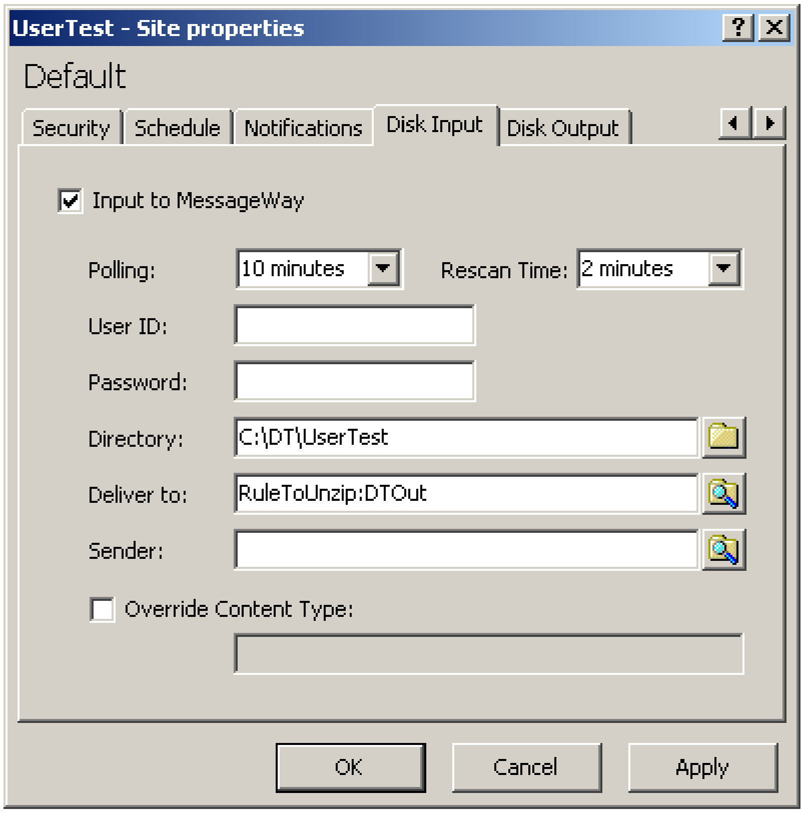
The **Disk Input** and **Disk Output** pages of the Site Properties window allow users to specify when the site is used to transfer messages from a disk location into MessageWay and from MessageWay to a disk location. Users may specify parameters for message transfers, as follows:

- (Windows only) To connect to another system:
    - User ID
    - Password
- To use the site for input to MessageWay:
    - Polling
    - Rescan time
    - Directory for input
    - Output location for delivery
    - Sender which may be different from original sender
    - Content type
- To use the site for output from MessageWay:
    - Directory where MessageWay delivers output
    - Mask to create name of the output file
    - End of line value
    - (UNIX/Linux only) Create mode
    - Overwrite file

You may configure a site for input, output or both input and output. Refer to the topic ***Recommendations for Sites*** (on page 463) for further information.

Disk Input Options

To retrieve files from a disk location and send them into MessageWay, specify options on the **Disk Input** page. For specific information about the fields, refer to the reference topic, ***Disk Input Page*** (on page 1095).



☑ Input to MessageWay

Polling: 10 minutes

Rescan Time: 2 minutes

User ID:

Password:

Directory: C:\DT\UserTest

Deliver to: RuleToUnzip:DTOut

Sender:

□ Override Content Type:

1 Check the box, **Input to MessageWay**.

2 (Windows only) In the **User ID** and **Password** boxes, type a user ID and password, if required to access the file.

3 Accept the default polling option from the adapter, or select another ***polling option*** (on page 1097).

4 To avoid receiving partial files when they are large, select or type a *Rescan Time*, which should be less than the polling time.

Messages retrieved from disk for this site are often large files. To avoid bringing partial files into MessageWay, it will use the rescan option. The rescan option tells the adapter to continue to check the file size every so often after the initial polling based on the *Rescan Time* until the size no longer changes. When the adapter determines the file is stable, it initiates the transfer into MessageWay. To accomplish this previously, you had to write to a temporary subdirectory and then rename the file to the polling directory.

NOTE: Since this feature will input files only after at least three readings of the file properties, it will slow down input for smaller files as well. Use it primarily for locations that typically receive large files.

To use rescan:

- The rescan time should be less than the polling interval and long enough to allow a remote server to update the file properties between rescans
- The polling interval may *not* be *Event Driven*, *Never* or *Schedule*
- The *Input Now* command is disabled when a Rescan Time is specified

5 In the **Directory** box, type a valid directory that the Disk Transfer adapter will scan for messages to transfer into MessageWay. You may also add a file name at the end of the directory path. The file name may be static or dynamic with the * wildcard. If you want to pull a static filename you still have to put an asterisk after it, for example *abc.txt**. Otherwise, MWDisk will interpret it as a directory name.

6 In the **Deliver to** box, type or select a location where the adapter will transfer the messages.

This may be an output site for delivery, a pickup mailbox or a service location capable of routing messages, such as distribution list. The format may be a ***simple or compound address*** (on page 653). This example shows a compound address where the message goes to a rules processing location to unzip the file and then to the final location. When the location does not exist, the message is sent to the {Unknown} system mailbox.

7 To specify a ***content type*** (on page 1130) type for the input message or override an existing type:

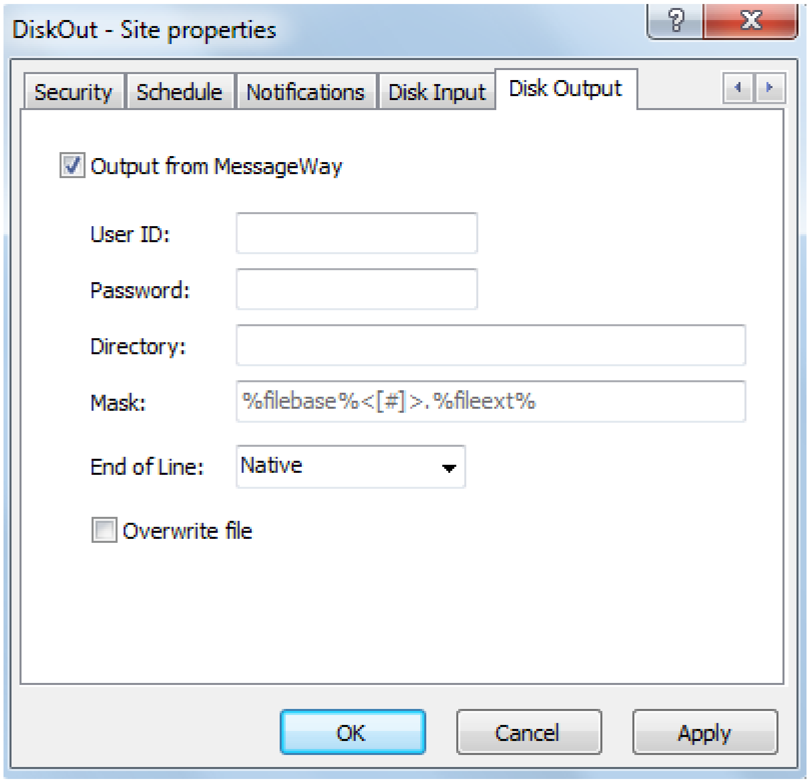
a) Check the **Override Content Type** box.

b) Type a value for the content type in the data entry box.

Disk Output Options

To send messages from MessageWay to a disk location, specify options on the **Disk Output** tab. For specific information about the fields, refer to the reference topic, ***Disk Output Page*** (on page 1101).

Note that the *User ID* and *Password* fields only appear for Windows systems, not for UNIX/Linux systems.



☑ Output from MessageWay

User ID:

Password:

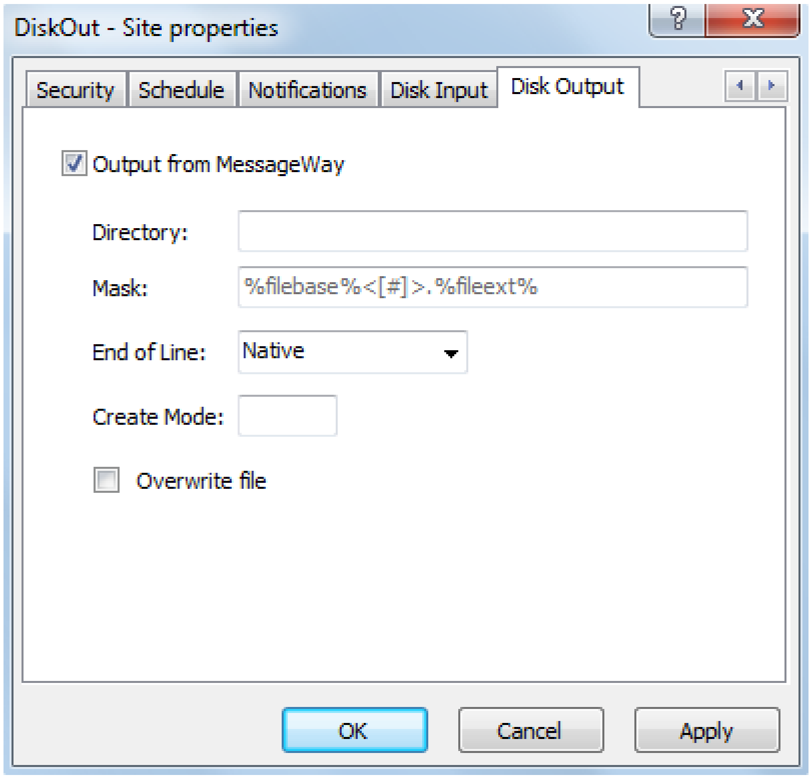
Directory:

Mask: %filebase%<[#]>.%fileext%

End of Line: Native

□ Overwrite file

Not that the additional field *Create Mode* appears for UNIX/Linux systems, but not Windows systems.



☑ Output from MessageWay

Directory:

Mask: %filebase%<[#]>.%fileext%

End of Line: Native

Create Mode:

□ Overwrite file

1. Check the **Output from MessageWay** box.
2. (Windows only) In the **User ID** and **Password** boxes, type a user ID and password, if authentication is required to access the remote location.
3. In the **Directory** box, type a valid directory where the Disk Transfer adapter will deposit the file.

   NOTE: When the destination directory does not exist for an outbound Disk Transfer site, the MessageWay Messaging Server will attempt to create one. If it does not exist, the \temp directory will be created beneath this directory. The Messaging Server writes the file to the \temp directory and then moves the file to this directory. This ensures that the file is complete before it appears in this directory.

4. To override the value provided from the Disk Transfer adapter configuration, type a ***mask*** (on page 1103) that will be used to create the file name of the file transferred from MessageWay to the specified directory. Use two percent (%) signs to enclose the tokens.Add constants outside of these signs as required.

   CAUTION: This must have a value, or MessageWay will deliver it to the system mailbox, {Unknown}.

5. For the ***End of Line*** (on page 1107), select an appropriate option: **Native**, **CRLF**, **NL** or **Unchanged**.
6. (UNIX/Linux only) For ***Create mode*** (on page 1107), type a numeric value to specify permissions.
7. Check the **Overwrite file** box if you want to overwrite the output file on disk if it already exists.

Configuring an E-mail Site

To configure parameters for an E-mail site, users must specify those for POP3 and SMTP on the **POP3** and **SMTP** pages, respectively, of the Site Properties window.

You may configure a site for input, output or both input and output. Refer to the topic ***Recommendations for Sites*** (on page 463) for further information.

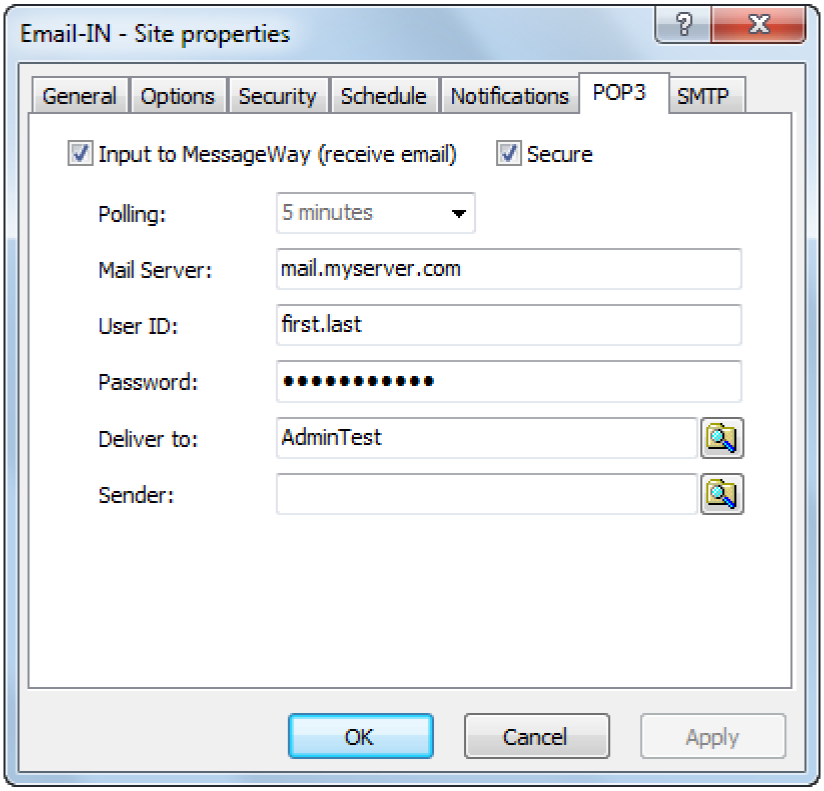
E-mail Input Options

The **POP3** page of the Site Properties window allows users to specify how to transfer e-mail messages using POP3 into MessageWay. The polling interval is inherited from the adapter configuration, but it can be overridden here.

The purpose of this client's input option is to extract the payload, either from the body or from an attachment. It does not preserve the e-mail headers. It delivers the payload as a message as follows:

- If there is an attachment, it delivers the attachment as a message and discards the body text of the e-mail
- If there is no attachment, it delivers the text in the body as a message

IMPORTANT: This e-mail client preserves the content/payload when it transfers text-only messages into MessageWay. Do not try to accept messages that have anything other than text in the body.



Email-IN - Site properties

☑ Input to MessageWay (receive email) ☑ Secure

Polling: 5 minutes

Mail Server: mail.myserver.com

User ID: first.last

Password: ●●●●●●●●●●●

Deliver to: AdminTest

Sender:

Complete the fields as follows:

1 Check the box, **Input to MessageWay**, to allow the site to receive e-mail messages.

2 Check the box, **Secure**, to enable a secure POP3 connection to the e-mail server you want to connect to.

3 To override the default polling interval configured for the E-mail adapter, select a value from the **Polling** drop-down box.

4 Type the name of the e-mail server to which you want to connect. Leave this blank to accept the default value of the e-mail adapter.

5 Type a valid user ID and password to connect to the mail server from which you want to transfer e-mail messages.

6 Type or select a location where the adapter will transfer the messages. This may be an output site, a pickup mailbox or a service location. The format of the address may be ***simple or compound*** (on page 653). When the location does not exist, the message is sent to the {Unknown} system mailbox.

7 To override the original sender, type or select another sender.

E-mail Output Options

The **SMTP** page of the Site Properties window allows users to specify how to transfer e-mail messages using SMTP from MessageWay.

In accordance with industry practice, e-mail output via SMTP does not accept Unicode e-mail addresses. Unicode characters can only be present in the e-mail's mask.

For example:

Can be Unicode	Cannot be Unicode
Bob Smith	<bob@company.com>
ボブ- スミス	<bob@company.com>

Here is a full example:

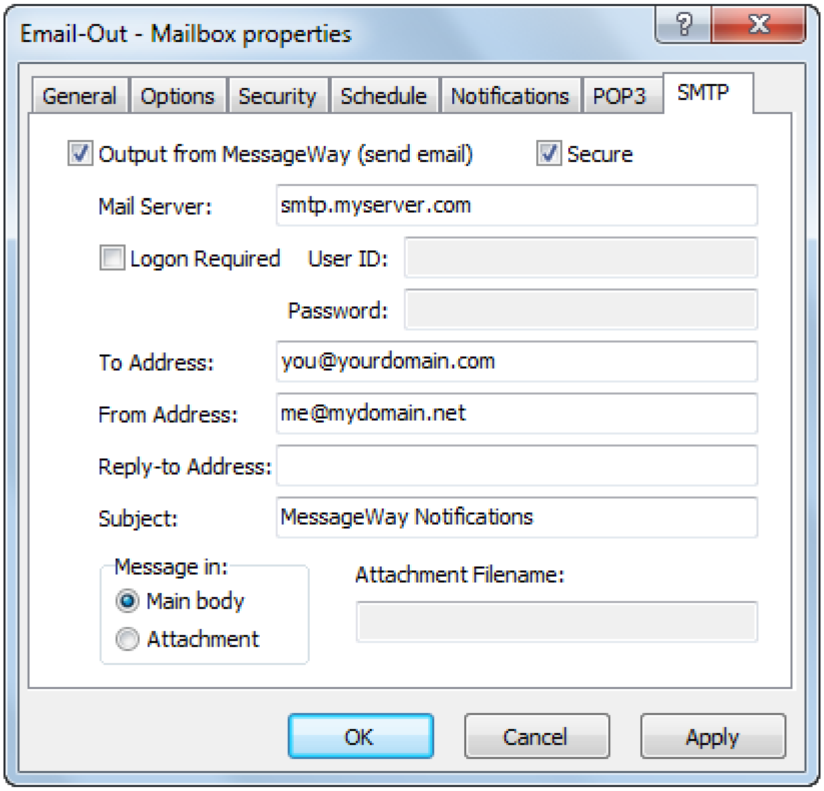
To Address: κόσμε <you@yourcompany.com>

From Address: ジェイソン <me@mycompany.com>

Reply To Address: 素晴らしい男 <anyone@anywhere.com>

Subject: This is a Unicode Subject Line: これは、Unicode の件名行です。

[Content can either be in main body or attached.]



Email-Out - Mailbox properties

☑ Output from MessageWay (send email) ☑ Secure

Mail Server: smtp.myserver.com

□ Logon Required User ID:

Password:

To Address: you@yourdomain.com

From Address: me@mydomain.net

Reply-to Address:

Subject: MessageWay Notifications

Message in:
● Main body
○ Attachment

Attachment Filename:

1 Check the box, **Output from MessageWay**, to send e-mail messages from this site.

2 Check the box, **Secure**, to enable a secure SMTP connection to the e-mail server you want to connect to.

3 Type the name of the e-mail server to which you want to connect. Leave this blank to accept the default value specified on the e-mail adapter.

4 Check whether the e-mail server requires a logon, and if so, type a valid user ID and password. Leave the User ID blank to accept the default value of the e-mail adapter. Even though the server may not require a logon, specifying a user ID may avoid messages being rejected because the value in the From Address is unknown to the mail server.

5 Type a valid e-mail address to which this e-mail message will be sent. To request a notification of successful delivery, include the optional parameter described in the ***To address*** (on page 1114) reference material.

6 Type a valid e-mail address from which this e-mail message will be sent. To request a notification of successful delivery, include the optional parameters described in the ***From address*** (on page 1114) reference material.

7 Type a valid e-mail address to which replies will be sent.

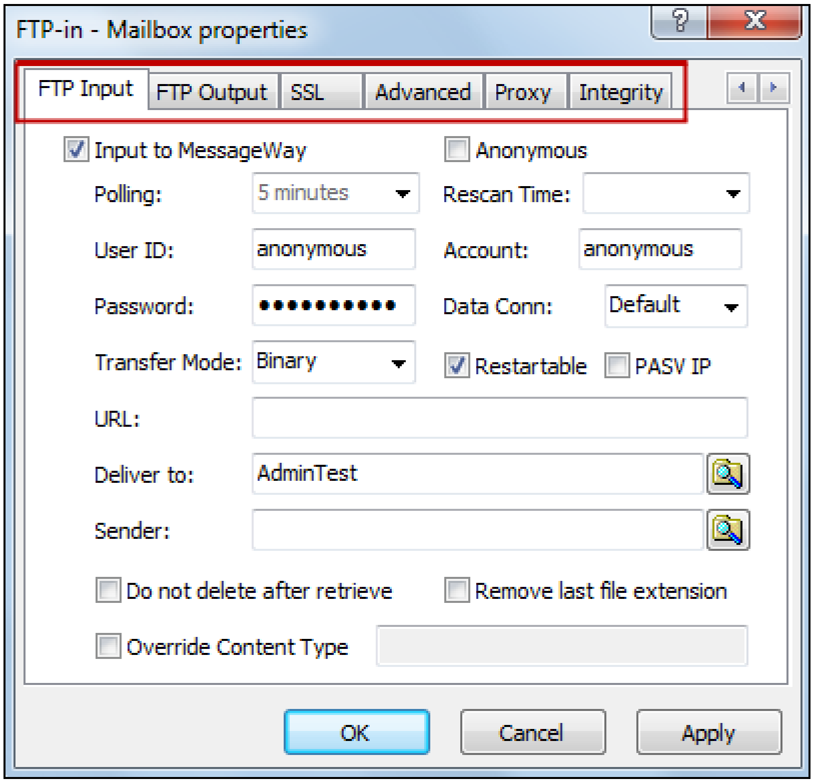
8 Type a subject for this message using any combination of literals and tokens.

9 Select how the message will be sent with the e-mail: as part of the main body or as an attachment. When selecting **Attachment**, users must also supply a name for the attached file using any combination of literals and tokens. There is a maximum of one attachment per e-mail message.

TIP: Messages sent in the body of the e-mail are encoded as quoted-printable, which is best for text. Messages sent as an attachment are encoded as base64, which is best for binary data.

Configuring an FTP Site

The FTP site configuration has six additional pages where users configure how this site is to be used. To access all the pages, use the arrow keys at the top of the Site Properties window.



☑ Input to MessageWay
☐ Anonymous
Polling: 5 minutes
Rescan Time:
User ID: anonymous
Account: anonymous
Password: ●●●●●●●●●●
Data Conn: Default
Transfer Mode: Binary
☑ Restartable
☐ PASV IP
URL:
Deliver to: AdminTest
Sender:
☐ Do not delete after retrieve
☐ Remove last file extension
☐ Override Content Type

Users may configure the pages as follows:

FTP Input
Use this tab to configure the site to download messages from an FTP site, based on polling intervals.

FTP Output
Use this tab to configure the site to send messages to an FTP site, based on schedules.

SSL
Use this tab to configure secure socket layer (SSL) encryption/decryption communication with an FTP server.

Advanced
Use this tab to send QUOT or SITE commands as pre-process and post-process commands.

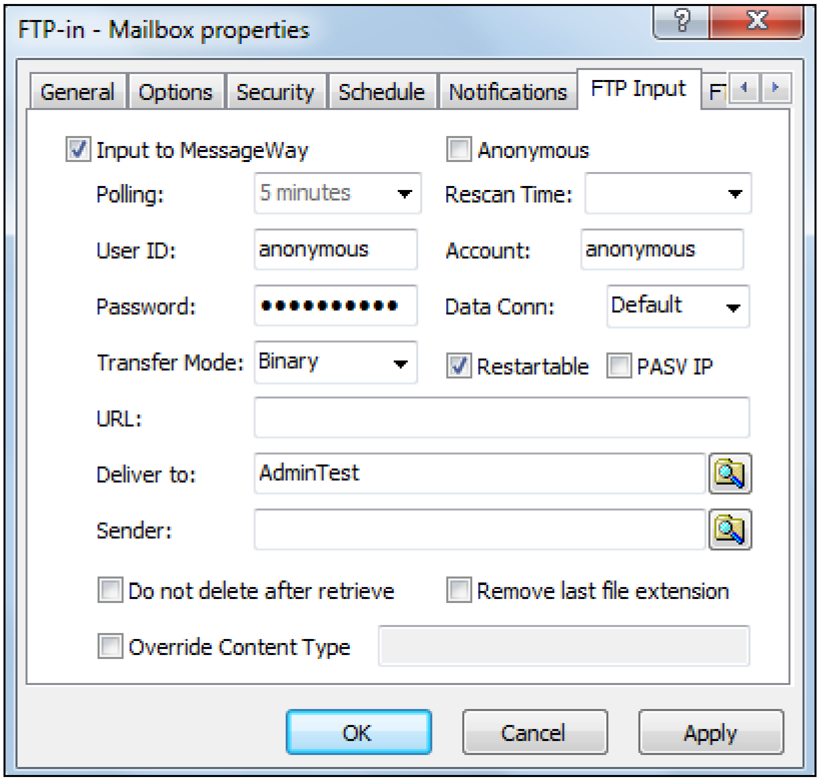
Proxy
Use this tab to send messages through the MessageWay FTP Perimeter Server rather than directly to an external FTP server.

Integrity
Use this tab to check the validity of a message sent or received by generating a hash value of a file and comparing that value with one created by the FTP server for the same content.

You may configure a site for input, output or both. Refer to the topic ***Recommendations for Sites*** (on page 463) for further information.

FTP Input Options

To retrieve messages from an FTP site and send them into MessageWay, specify options on the **FTP Input** tab. For specific information about the fields, refer to the reference topic, ***FTP Input Page*** (on page 1123).



☑ Input to MessageWay
☐ Anonymous
Polling: 5 minutes
Rescan Time:
User ID: anonymous
Account: anonymous
Password: ●●●●●●●●●●
Data Conn: Default
Transfer Mode: Binary
☑ Restartable
☐ PASV IP
URL:
Deliver to: AdminTest
Sender:
☐ Do not delete after retrieve
☐ Remove last file extension
☐ Override Content Type

1. Check the **Input to MessageWay** box.
2. Select a ***polling interval*** (on page 1124), if you want it to be different from what is set for the adapter.
3. If you have large files sent to this location, set the **Rescan Time** to less than the polling time. The adapter will wait until the properties of the file are stable before it initiates the transfer to MessageWay.

   NOTE: Since this feature will input files only after at least three readings of the file properties, it will slow down input for smaller files as well. Use it for locations that typically receive large files. Note that the *Input Now* command is disabled when a Rescan Time is specified.

4. Type the user information that is required to connect to the FTP server.

   Some FTP sites allow users to connect without a user ID or password. Check the *Anonymous* box if you want to connect to the FTP site as an anonymous user. If you do not want to connect as an anonymous user, enter a valid user ID and password to connect to the FTP server. The account is sent only when the FTP server requests it.

IMPORTANT: To connect to a MessageWay FTP Perimeter Server as an anonymous user, the User ID must be **Anonymous**, and it must exist as a valid user ID in the MessageWay environment where the perimeter server connects.

5 Select one of the ***transfer mode options*** (on page 1126), **Binary** or **Text** or **Strict** (UNIX/Linux only), in which format the message(s) will be transferred.

IMPORTANT: If you are performing integrity checks, the *Transfer Mode* must be **Binary**.

A file that appears to be text or other ASCII format should be transferred in text mode. A file that appears to be data, an executable, or compressed should be transferred in binary mode. Binary mode should also be used if there is no file extension or the file extension is not registered.

IMPORTANT: Transferring a binary file in text format may damage the file. Never transfer both binary and text data using the same location.

6 Select one of the ***data connection options*** (on page 1127): **Default**, **Passive**, **Active** or **Ext-Passive**.

The FTP client determines the type of data connection to be used with the server, so you specify the type of data connection here. The *Default* option will first attempt a passive connection, and if this fails, it will try an active connection. To avoid problems with client firewalls, the client often initiates a passive connection. To support network addressing other than IPv4, which only allows 32 characters, use the extended passive option, *Ext-Passive*, instead of *Passive*. For network addresses other than those using IPv4, such as IPv6, you must use *Ext-Passive*.

The difference between active and passive transfers can be confusing. FTP uses two ports: a command port and a data port. For active transfers, the server initiates a data connection to a client's data port, and the client sends ACKs back to the server's data port. For passive transfers, the client initiates a data connection to the server's data port, and the server sends ACKs and data back to the client's data port.

7 To enable check-point restart, check the **Restartable** box.

IMPORTANT: Transfers are restartable from a check-point only if the remote server supports restart. If it does not, MessageWay proceeds as if this box were not checked. When restart is not supported, MessageWay will use retry strategies listed on the **Options** page, which attempt to retransmit files from the beginning of the file, not from a check-point.

Note: Messages that fail an antivirus scan are put in {Quarantine} and are not eligible for restart.

8 To force the use of IP Address returned in PASV response for the data channel connection, check the **PASV IP** box.

9 Type a ***valid URL*** (on page 1128) for the FTP connection.

IMPORTANT: For generic FTP servers, the directories must exist at the server site.

For the MessageWay FTP Server, this URL may only contain the URL for the server, an optional port, and possibly a location that will override the default MessageWay mailbox for the user.

10 Type or select a location where the adapter will transfer the messages.

This may be an output site, a pickup mailbox or a service location capable of routing messages, such as MWTranslator. The format may be a ***simple or compound address*** (on page 653). When the location does not exist, the message is sent to the {Unknown} system mailbox.

11 To override the sender determined by the FTP adapter, in the **Sender** box, type a sender or select an existing location.

12 If you want to keep a copy of the file on the server or if the site does not allow you to delete files after a successful transfer, check the **Do not delete after retrieve** box.

The default behavior is to delete the file after the message successfully enters MessageWay. If MessageWay attempts to delete a file, but does not have authority to do so, it assumes the transfer failed and discards what it has received to that point.

IMPORTANT: When you connect to a MessageWay FTP Perimeter Server to send messages from MessageWay, you must check this box, because MessageWay does not allow messages to be deleted this way. Messages are conditionally archived and then deleted when the archive program runs.

13 To specify a ***content type*** (on page 1130) type for the input message or override an existing type:

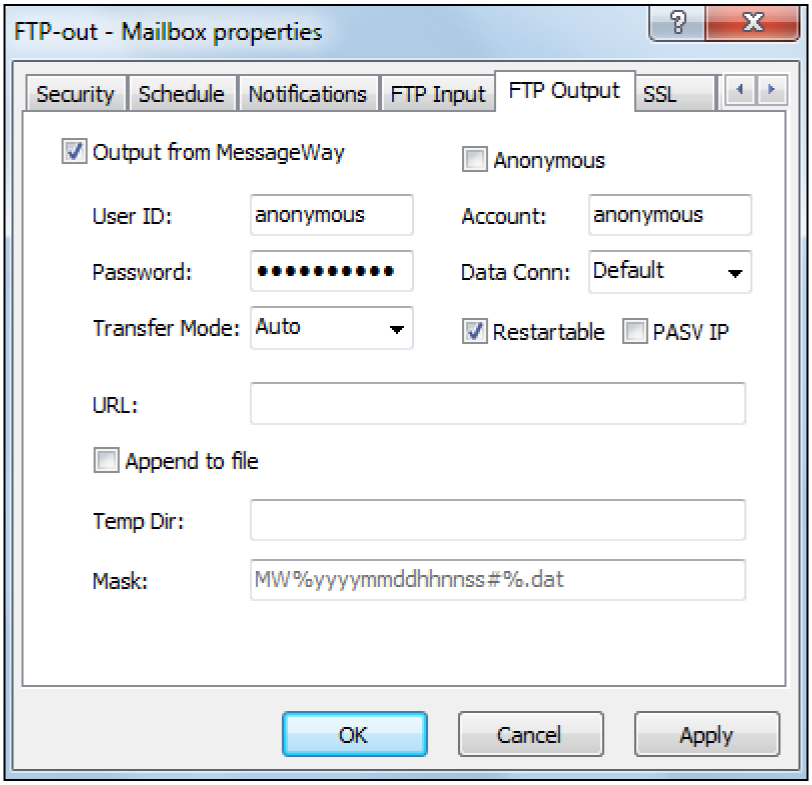
a) Check the **Override Content Type** box.

b) Type a value for the content type in the box.

14 Check **Remove last file extension** when you have determined through an FTP trace that the FTP server has appended an erroneous file extension to the end of the file name. This behavior of some FTP servers will cause the GET command to fail, because the file name on the system does not contain the final extension shown by the server.

FTP Output Options

To send messages from MessageWay to an FTP site, specify options on the **FTP Output** tab. For specific information about the fields, refer to the reference topic, ***FTP Output Page*** (on page 1131).



☑ Output from MessageWay

□ Anonymous

User ID: anonymous

Account: anonymous

Password: ●●●●●●●●●●●

Data Conn: Default

Transfer Mode: Auto

☑ Restartable

□ PASV IP

URL:

□ Append to file

Temp Dir:

Mask: MW%yyyymmddhhnnss#%.dat

1 Check the **Output from MessageWay** box.

2 Enter the user information that is required to connect to the FTP server.

Some FTP sites allow users to connect without a user ID or password. Check the *Anonymous* box if you want to connect to the FTP site as an anonymous user. If you do not want to connect as an anonymous user, enter a valid user ID and password to connect to the FTP server. The account is sent only when the FTP server requests it.

IMPORTANT: To connect to a MessageWay FTP Perimeter Server as an anonymous user, the User ID must be **Anonymous**, and it must exist as a valid user ID in the MessageWay environment where the perimeter server connects.

3 Select one of the ***transfer mode options*** (on page 1133), **Auto**, **Binary** or **Text** or **Strict** (UNIX/Linux only), to specify the format in which the message(s) will be transferred.

A file that appears to be text or other ASCII format should be transferred in text mode. A file that appears to be data, an executable, or compressed should be transferred in binary mode. Binary mode should also be used if there is no file extension or the file extension is not registered. Auto determines the transfer mode based on the ***content type*** (on page 1099).

IMPORTANT: Transferring a binary file in text format may damage the file. Never transfer both binary and text data using the same site.

4 Select one of the ***data connection options*** (on page 1134): **Default**, **Passive**, **Active** or **Ext-Passive**.

The FTP client determines the type of data connection to be used with the server, so you specify the type of data connection here. The *Default* option will first attempt a passive connection, and if this fails, it will try an active connection. To avoid problems with client firewalls, the client often initiates a passive connection. To support network addressing other than IPv4, which only allows 32 characters, use the extended passive option, *Ext-Passive*, instead of *Passive*. For network addresses other than those using IPv4, such as IPv6, you must use *Ext-Passive*.

The difference between active and passive transfers can be confusing. FTP uses two ports: a command port and a data port. For active transfers, the server initiates a data connection to a client's data port, and the client sends ACKs back to the server's data port. For passive transfers, the client initiates a data connection to the server's data port, and the server sends ACKs and data back to the client's data port.

5 To enable check-point restart, check the **Restartable** box.

IMPORTANT: Transfers are restartable from a check-point only if the remote server supports restart. If it does not, MessageWay proceeds as if this box were not checked. When restart is not supported, MessageWay will use retry strategies listed on the **Options** page, which attempt to retransmit files from the beginning of the file, not from a check-point.

Note: Messages that fail an antivirus scan are put in {Quarantine} and are not eligible for restart.

6 To force the use of IP Address returned in PASV response for the data channel connection, check the **PASV IP** box.

7 Type a valid URL for the FTP connection.

IMPORTANT: The directories must exist at the FTP server site.

8 To add this message to an existing file of the same name, check the **Append to file** box. Since MessageWay writes directly to a permanent file in this case, the program picking up the file must ensure the file is complete before it accesses the file.

NOTE: Append is not compatible with Integrity checks. If the **Append to** box is checked and integrity checking is mandatory, the transfer will fail, and an error will be logged to the error log and placed on the **Error** tab of the Message Properties window. If the **Append to** box is checked and integrity checking is optional, integrity will be ignored, the transfer will proceed, and a warning will appear on the **Misc** tab of the Message Properties window.

When this is unchecked, the default behavior is to replace existing files with newer versions.

CAUTION: When you check **Append to file**, you must only specify a permanent file mask, not both permanent and temporary file masks. If you specify both masks, the new file will be appended to the temporary file and then renamed to the permanent file. If you want to use the append option, only specify a permanent mask.

9 Type a valid temporary directory to ensure the file is transferred completely and avoid partial transfers.

- or -

Leave this blank, but specify both a permanent file name mask and a temporary file name mask in the next step, which also assures the file is transferred completely and available for access under the permanent file name.

NOTE: This option is dimmed when you check the **Append to file** box.

10 To override the default mask provided from the FTP adapter configuration, type the mask for the file name to be used for both a temporary file and a permanent file,

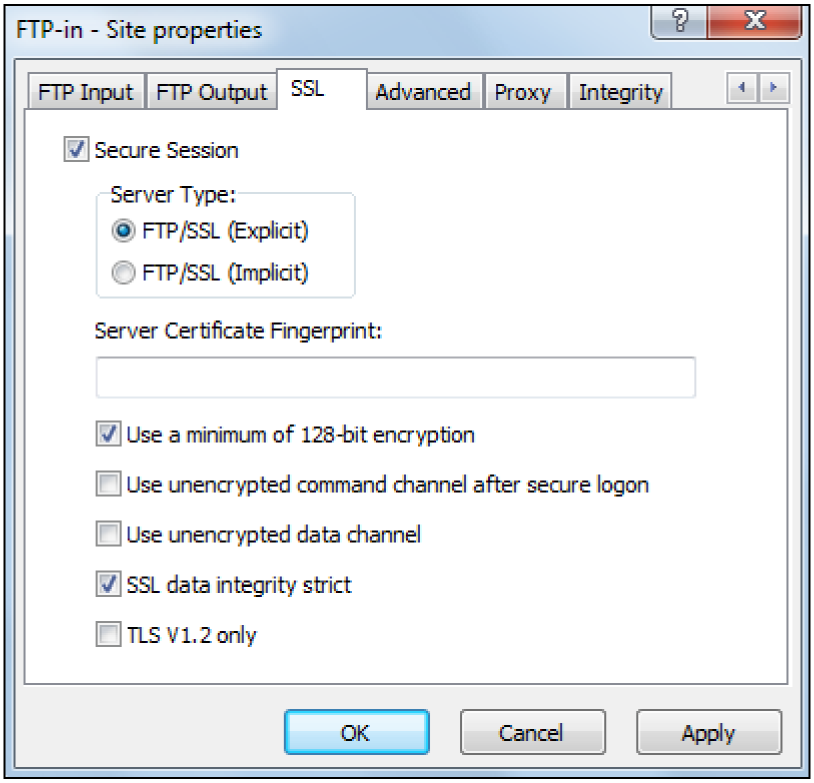
- or -

Type both a permanent mask and a temporary mask, separated by a forward slash, /, for example, **CO1%yyyymmddhhnnss#%.dat/CO1temp%yyyymmddhhnnss#%.dat**.

IMPORTANT: When this field is blank, MessageWay uses a default mask (**FTP** tab of FTP Adapter Properties window). When one mask is specified, it is used for both the temporary and the permanent file names. You should always use different permanent and temporary masks when there is no temporary directory.

FTP SSL Encryption Options

To enable TLS/SSL security for the FTP adapter, specify options on the **SSL** tab. For specific information about the fields, refer to the reference topic, ***FTP SSL Page*** (on page 1146).



FTP-in - Site properties

☑ Secure Session

Server Type:

● FTP/SSL (Explicit)

○ FTP/SSL (Implicit)

Server Certificate Fingerprint:

☑ Use a minimum of 128-bit encryption

□ Use unencrypted command channel after secure logon

□ Use unencrypted data channel

☑ SSL data integrity strict

□ TLS V1.2 only

1 To configure a secure FTP connection, check the box, **Secure Session**.

All fields are now available.

2 In the **Server Type** ***box*** (on page 1147), select **FTP/SSL (Explicit)** or **FTP/SSL (Implicit)**.

3 If you are using a ***public key fingerprint*** (on page 1148) to identify the server instead of the full public key, enter that fingerprint in the **Server Certificate Fingerprint** box. Leave this field blank if you will identify the server with the certificate in the repository identified on the FTP adapter.

4 To ***enforce a higher level of encryption*** (on page 1148), check the box, **Use a minimum of 128-bit encryption**.

5 To use a ***clear command channel (CCC)*** (on page 1148) after a successful secure connection, check the box, **Use unencrypted command channel after a secure logon**.

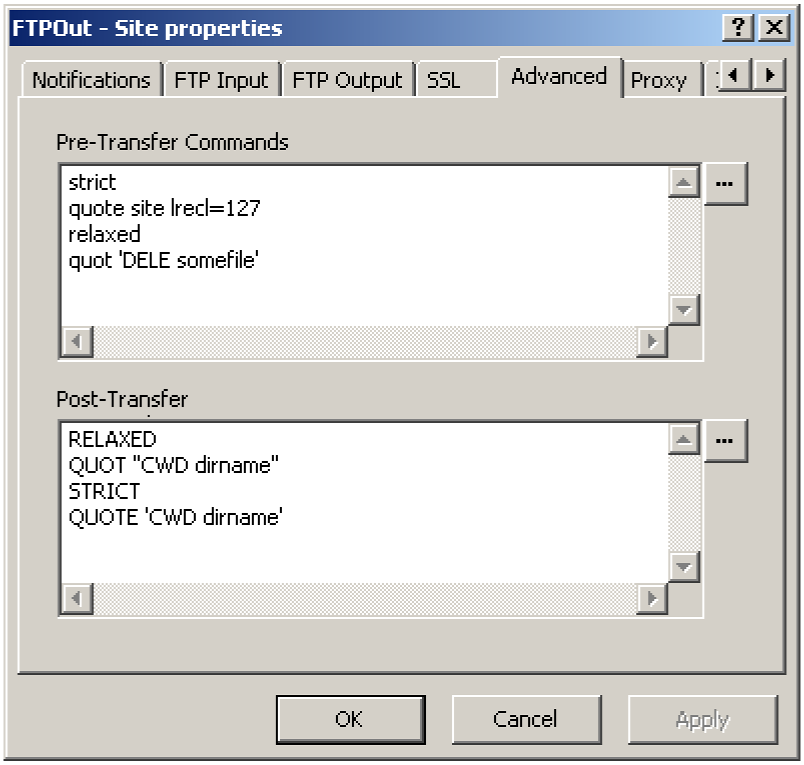
6 To use a ***clear data channel (CDC)*** (on page 1149), check the box, **Use unencrypted data channel**.

7 To enforce ***strict SSL data integrity*** (on page 1149), check the box, **SSL data integrity strict**.

8 To force the use of the TLS V1.2 protocol for the connection to the external FTP server, check the box, **TLS V1.2 only**.

FTP Advanced Options

To send commands to be processed before or after a transfer, enter them on the **Advanced** tab. For specific information about the fields, refer to the reference topic, ***FTP Advanced Page*** (on page 1118).



Pre-Transfer Commands

```
strict
quote site lrecl=127
relaxed
quot 'DELE somefile'
```

Post-Transfer

```
RELAXED
QUOT "CWD dirname"
STRICT
QUOTE 'CWD dirname'
```

1 For input sites, enter one command per line:

a) In the **Pre-Transfer Commands** box, type the commands that will be sent before the RETR (get) command.

b) In the **Post-Transfer Commands** box, type the commands that will be sent after a file is successfully received from the FTP server.

2 For output sites, enter one command per line:

a) In the **Pre-Transfer Commands** box, type the commands that will be sent before the STOR (put) command.

b) In the **Post-Transfer Commands** box, type the commands that will be sent after a file is successfully sent to the FTP server.

NOTE: For **PUTFILE** and **PUTLINE** commands, if you use the persistent counter token, #, in a filename, this counter remains the same throughout the 3 stages of the FTP session: pre-transfer, transfer and post-transfer. If the filenames are the same in all three stages, and you are not appending the latter files to the first, the files will be overlaid successively. For example, assume that you do the following: In the pre-transfer command box you type **PUTFILE somefile Test%#%.txt**, and for the transfer you specify a file mask on the FTP Output tab of the location of T**est%#%.txt**, and in the post-transfer command box you type, **PUTFILE someotherfile Test%#%**. The result is that the file from the pre-transfer stage is overlaid with the file from the transfer stage, which is then overlaid with the file from the post-transfer stage.

Changing Remote Files with Pre and Post Transfer Commands

MessageWay allows you to configure commands for FTP locations on the Advanced tab of the site properties window that are executed before or after the transfer.

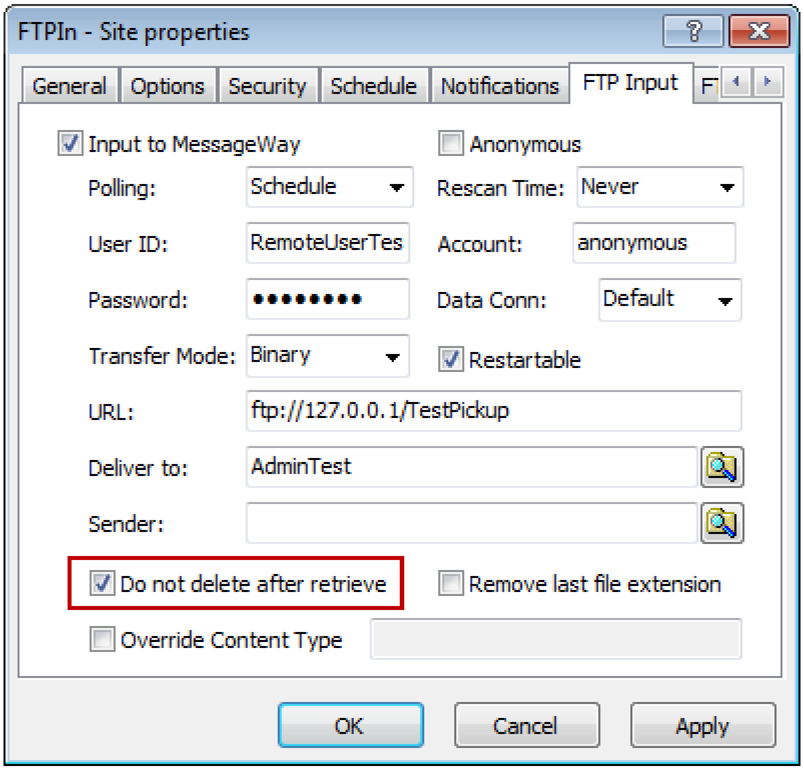
NOTE: A special token %remotefile% is available only for pre and post transfer commands. This token resolves to the name of a file on a remote system, not in MessageWay. The token %remotefile% is replaced with the filename that is picked up for inbound transfers or replaced with the filename that is sent for outbound transfers, and it can be used in either Pre-Transfer or Post-Transfer command boxes. The token %filename% cannot be used this way, because it refers to the filename of a message in MessageWay.

Here are some possible uses of the %remotefile% token:

- Rename a file on a remote system that was just retrieved by MessageWay
- Change the security on a remote file that was just sent by MessageWay

The following example renames the input file on the remote system after the adapter pulled it into MessageWay.

- By default, MessageWay deletes files from remote systems after they have been successfully retrieved, so before the transfer, make sure that you check the *Do not delete after retrieve* box on the FTP Input tab.



☑ Input to MessageWay

□ Anonymous

Polling: Schedule

Rescan Time: Never

User ID: RemoteUserTes

Account: anonymous

Password: ●●●●●●●●●

Data Conn: Default

Transfer Mode: Binary

☑ Restartable

URL: ftp://127.0.0.1/TestPickup

Deliver to: AdminTest

Sender:

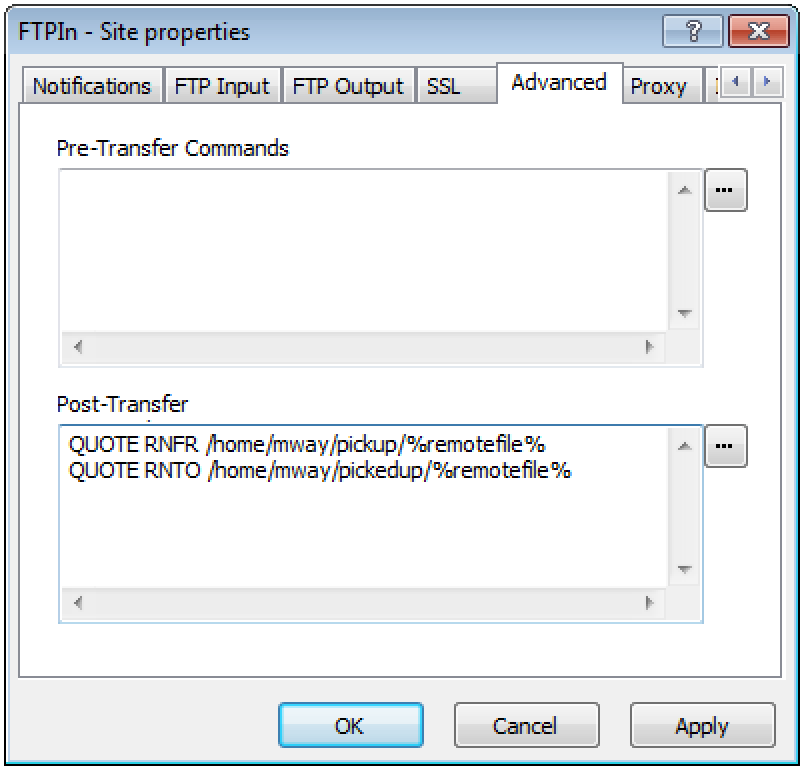
☑ Do not delete after retrieve

□ Remove last file extension

□ Override Content Type

- On the Advanced tab, you would type the commands in the Post-Transfer box.

NOTE: If the adapter retrieved the file from a non-root directory, you would need to change to the proper directory (cwd abcdir) before performing the rename or fully qualify the rename (rename abcdir/%remotefile% abcdir/%remotefile%.done).

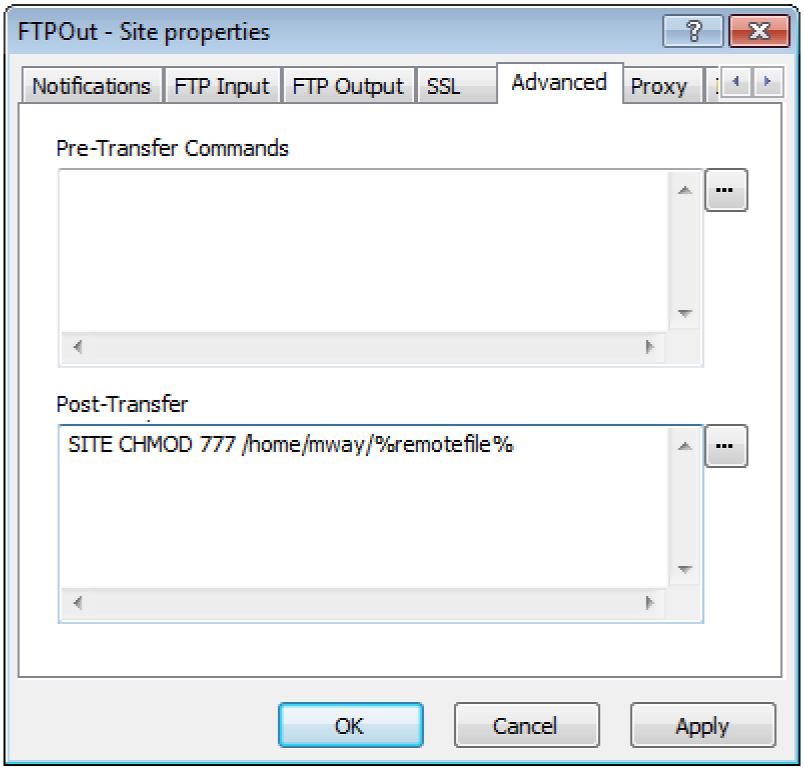


```
QUOTE RNFR /home/mway/pickup/%remotefile%
QUOTE RNTO /home/mway/pickedup/%remotefile%
```

The next example changes the security of the output file on the remote system after it was sent by MessageWay.

- On the Advanced tab, you would type the command in the Post-Transfer box.

NOTE: chmod is a UNIX/linux command; so FTP servers on Windows may not support this command.



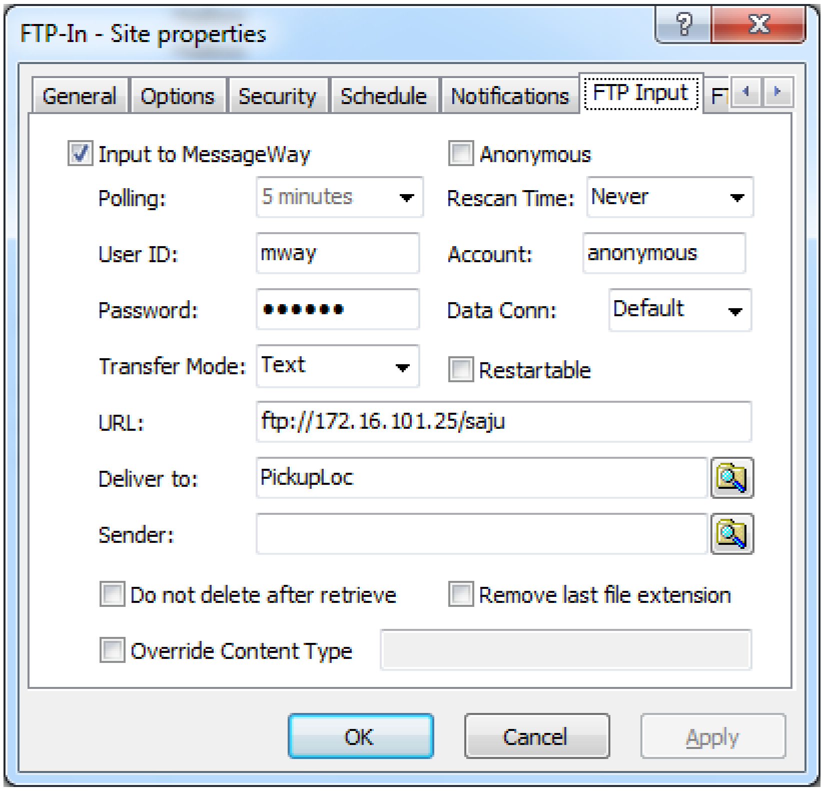
SITE CHMOD 777 /home/mway/%remotefile%

Creating a Transfer Log with Pre and Post Transfer Commands

You can create a transfer log that logs all transfers initiated by the MessageWay adapter. This example captures all inbound and outbound file transfers. The PUTLINE+ command appends a new line to the log file.

Here are the configurations and commands for inbound file transfers:

- The FTP Input tab indicates where to go to upload the file.



FTP-In - Site properties

☑ Input to MessageWay

☐ Anonymous

Polling: 5 minutes

Rescan Time: Never

User ID: mway

Account: anonymous

Password: ●●●●●●

Data Conn: Default

Transfer Mode: Text

☐ Restartable

URL: ftp://172.16.101.25/saju

Deliver to: PickupLoc

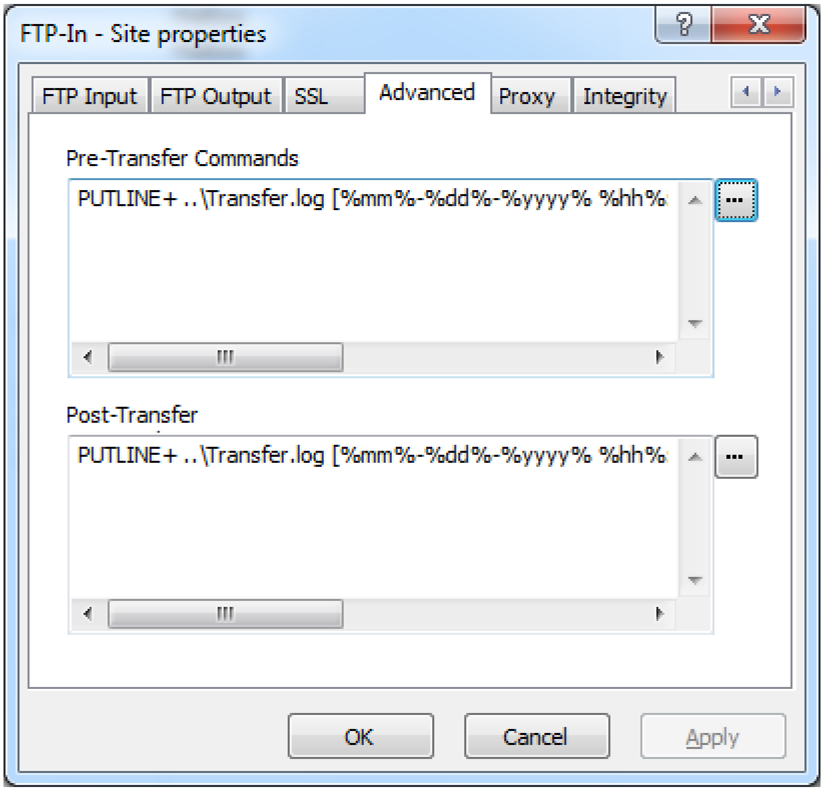
Sender:

☐ Do not delete after retrieve

☐ Remove last file extension

☐ Override Content Type

- The Advanced tab contains the commands to execute before and after the upload.



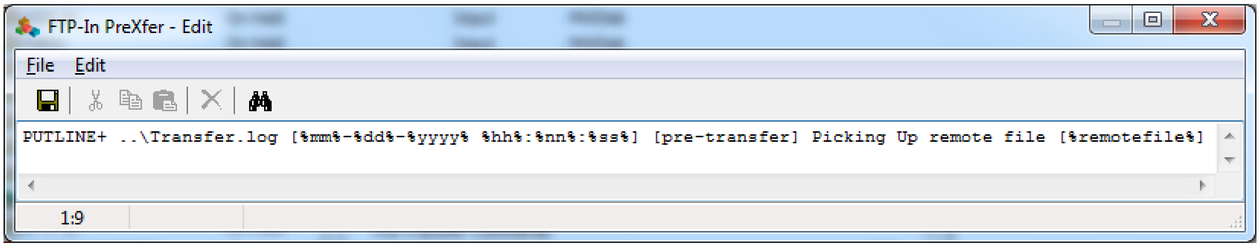
Pre-Transfer Commands

```
PUTLINE+ ..\Transfer.log [%mm%-%dd%-%yyyy% %hh%
```

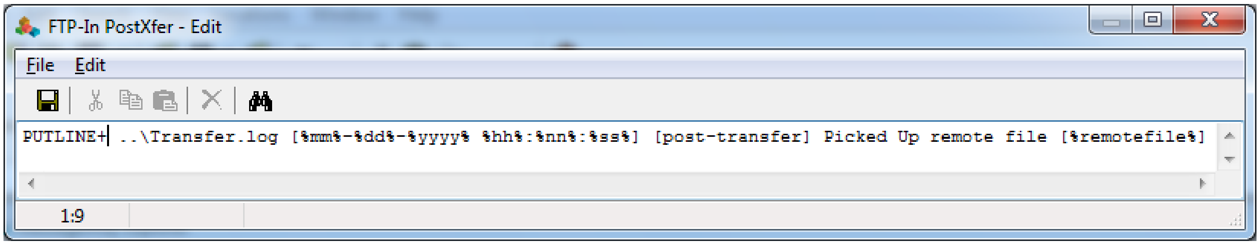
Post-Transfer

```
PUTLINE+ ..\Transfer.log [%mm%-%dd%-%yyyy% %hh%
```

Click the button to the right of the box to open an edit window.



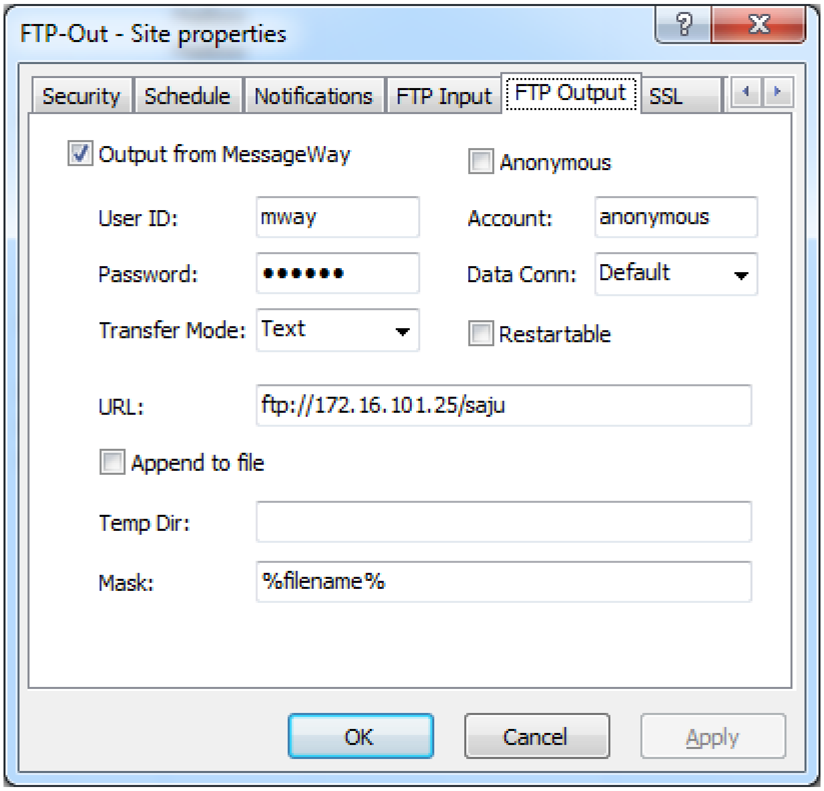
```
PUTLINE+ ..\Transfer.log [%mm%-%dd%-%yyyy% %hh%:%nn%:%ss%] [pre-transfer] Picking Up remote file [%remotefile%]
```



```
PUTLINE+ ..\Transfer.log [%mm%-%dd%-%yyyy% %hh%:%nn%:%ss%] [post-transfer] Picked Up remote file [%remotefile%]
```

Here are the configurations and commands for outbound file transfers:

- The FTP Output tab indicates where to send the file and uses the %filename% token to create the filename of the output file.



☑ Output from MessageWay

☐ Anonymous

User ID: mway

Account: anonymous

Password: ••••••

Data Conn: Default

Transfer Mode: Text

☐ Restartable

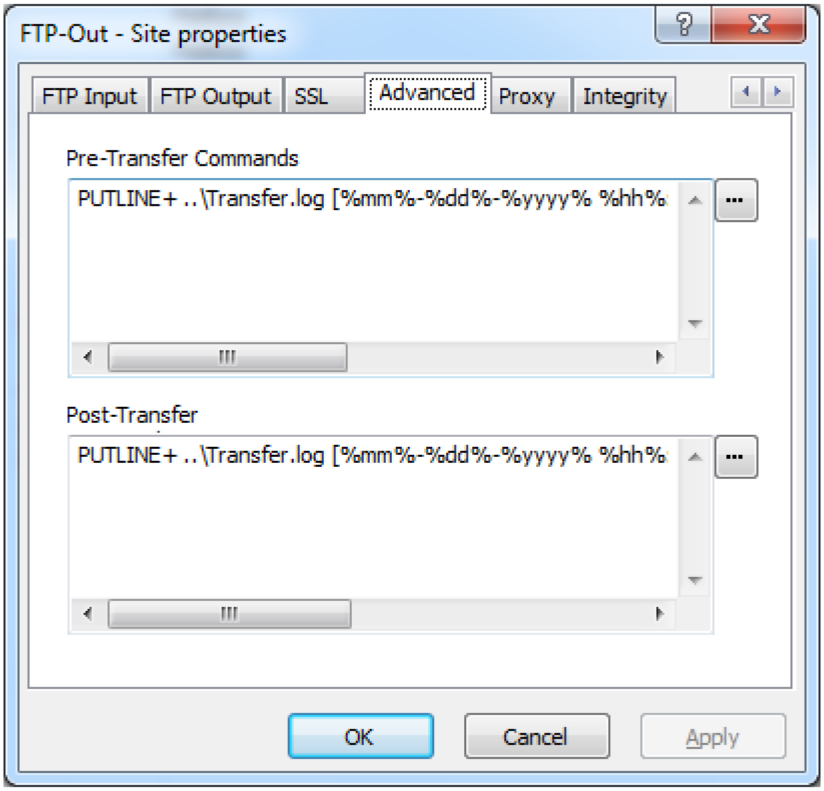
URL: ftp://172.16.101.25/saju

☐ Append to file

Temp Dir:

Mask: %filename%

- The Advanced tab contains the commands to execute before and after the download.



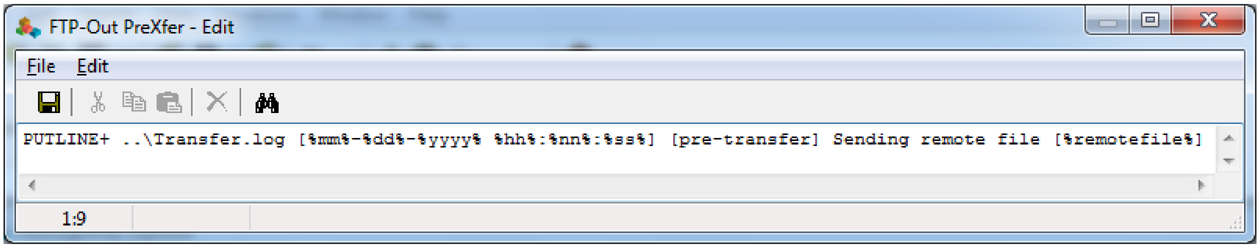
Pre-Transfer Commands

```
PUTLINE+ ..\Transfer.log [%mm%-%dd%-%yyyy% %hh%
```

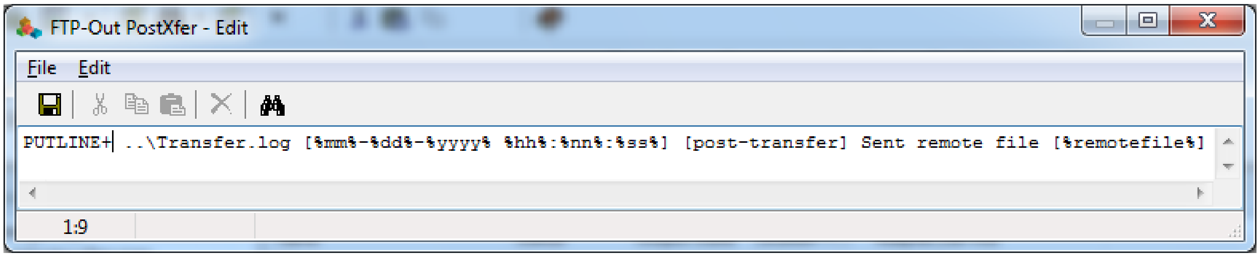
Post-Transfer

```
PUTLINE+ ..\Transfer.log [%mm%-%dd%-%yyyy% %hh%
```

Click the button to the right of the box to open an edit window.

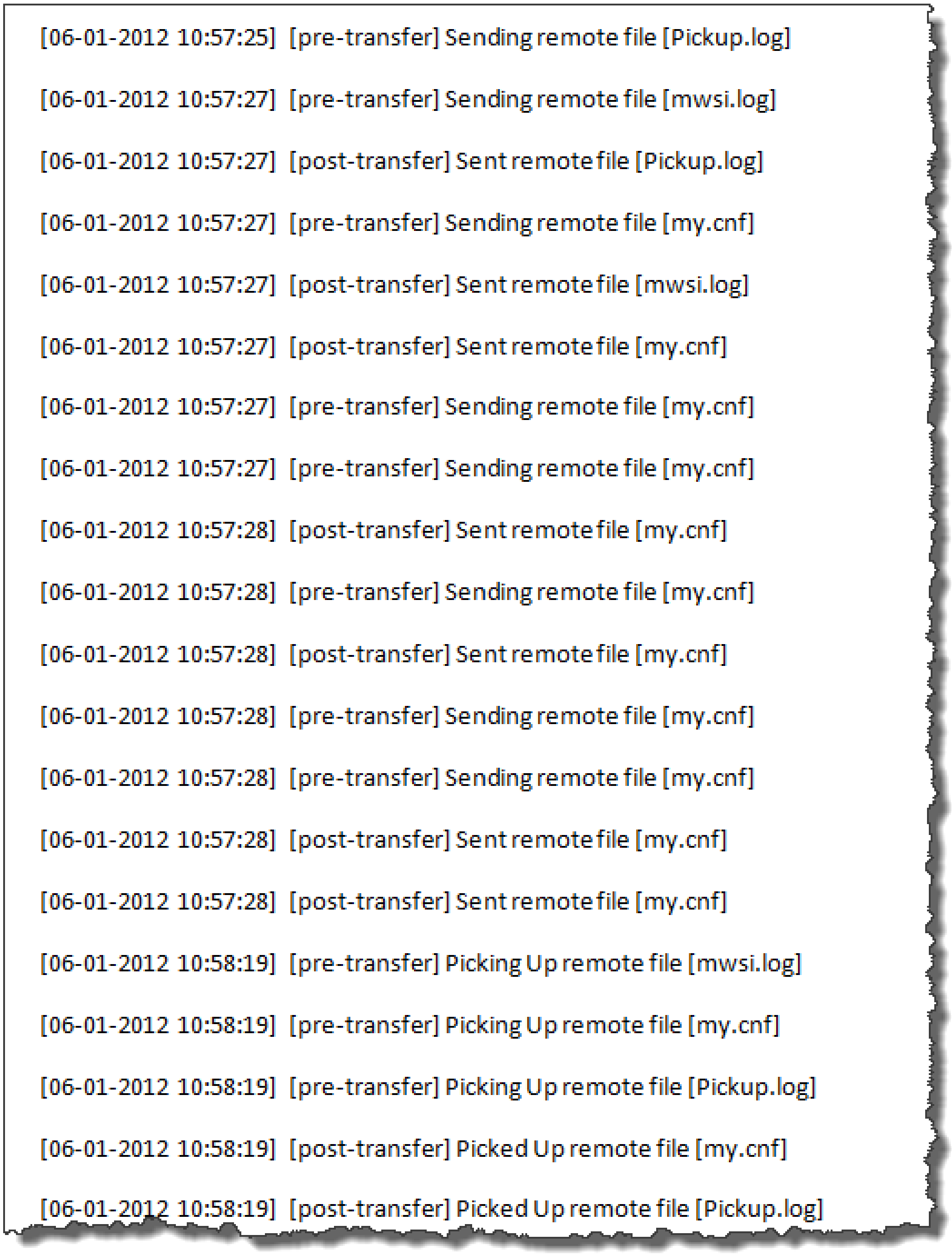


```
PUTLINE+ ..\Transfer.log [%mm%-%dd%-%yyyy% %hh%:%nn%:%ss%] [pre-transfer] Sending remote file [%remotefile%]
```



```
PUTLINE+ ..\Transfer.log [%mm%-%dd%-%yyyy% %hh%:%nn%:%ss%] [post-transfer] Sent remote file [%remotefile%]
```

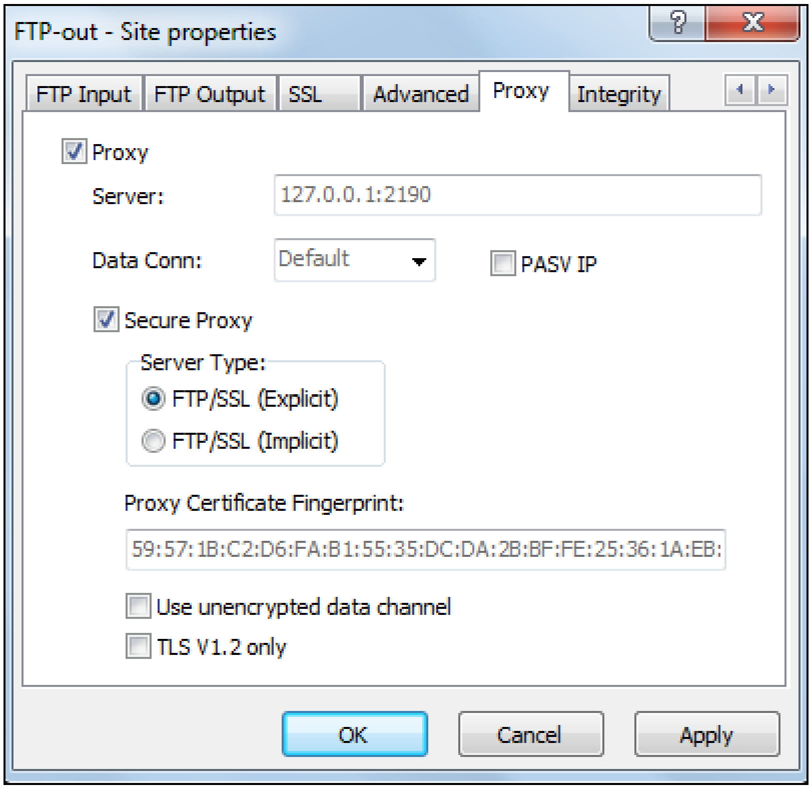
Here is a sample transfer log report file Transfer.log from the remote system.



```
[06-01-2012 10:57:25]  [pre-transfer] Sending remote file [Pickup.log]
[06-01-2012 10:57:27]  [pre-transfer] Sending remote file [mwsi.log]
[06-01-2012 10:57:27]  [post-transfer] Sent remote file [Pickup.log]
[06-01-2012 10:57:27]  [pre-transfer] Sending remote file [my.cnf]
[06-01-2012 10:57:27]  [post-transfer] Sent remote file [mwsi.log]
[06-01-2012 10:57:27]  [post-transfer] Sent remote file [my.cnf]
[06-01-2012 10:57:27]  [pre-transfer] Sending remote file [my.cnf]
[06-01-2012 10:57:27]  [pre-transfer] Sending remote file [my.cnf]
[06-01-2012 10:57:28]  [post-transfer] Sent remote file [my.cnf]
[06-01-2012 10:57:28]  [pre-transfer] Sending remote file [my.cnf]
[06-01-2012 10:57:28]  [post-transfer] Sent remote file [my.cnf]
[06-01-2012 10:57:28]  [pre-transfer] Sending remote file [my.cnf]
[06-01-2012 10:57:28]  [pre-transfer] Sending remote file [my.cnf]
[06-01-2012 10:57:28]  [post-transfer] Sent remote file [my.cnf]
[06-01-2012 10:57:28]  [post-transfer] Sent remote file [my.cnf]
[06-01-2012 10:58:19]  [pre-transfer] Picking Up remote file [mwsi.log]
[06-01-2012 10:58:19]  [pre-transfer] Picking Up remote file [my.cnf]
[06-01-2012 10:58:19]  [pre-transfer] Picking Up remote file [Pickup.log]
[06-01-2012 10:58:19]  [post-transfer] Picked Up remote file [my.cnf]
[06-01-2012 10:58:19]  [post-transfer] Picked Up remote file [Pickup.log]
```

FTP Proxy Options

If you connect to an FTP perimeter server rather than directly to an external FTP server, complete this page. For specific information about the fields, refer to the reference topic, ***FTP Proxy Options*** (on page 1143).



FTP-out - Site properties

☑ Proxy

Server: 127.0.0.1:2190

Data Conn: Default □ PASV IP

☑ Secure Proxy

Server Type:

● FTP/SSL (Explicit)

○ FTP/SSL (Implicit)

Proxy Certificate Fingerprint:

59:57:1B:C2:D6:FA:B1:55:35:DC:DA:2B:BF:FE:25:36:1A:EB:

□ Use unencrypted data channel

□ TLS V1.2 only

The dimmed values you see in the *Server* field, for example, are inherited from adapter settings. To override inherited values, select another value of type a new value in the field. The dimmed fields are not accessible until you check an appropriate box, such as the *Secure Proxy* box.

1 To configure a connection to an FTP perimeter server, check **Proxy**.

2 Type the location of the proxy server in the **Server** box, if blank or to override a default value from the FTP adapter properties.

3 Select one of the data connection options: **Default**, **Passive**, **Active** or **Ext-Passive**.

4 To force the use of IP Address returned in PASV response for the Proxy data channel connection, check the **PASV IP** box.

5 For a secure connection, check **Secure Proxy**.

a) Choose a server type: explicit or implicit.

b) To verify the server with a fingerprint rather than a certificate, type a value in the box, **Proxy Certificate Fingerprint**, if blank or to override a value inherited from the FTP adapter properties.

c) To use an unencrypted data channel, check the box.

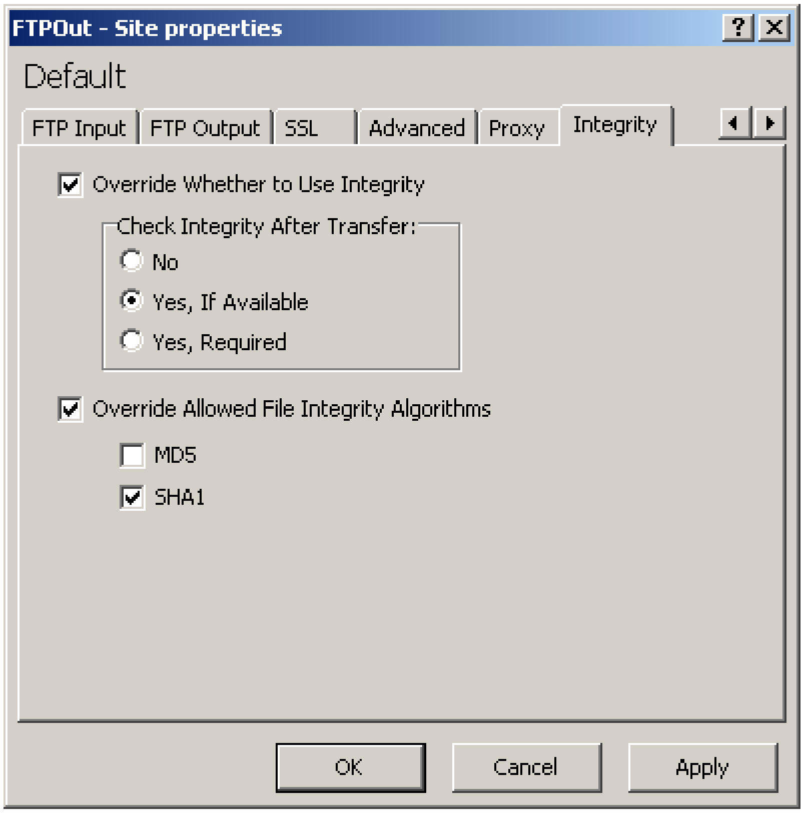
6 To use a fingerprint instead of a full certificate to authenticate the Proxy, fill in the **Proxy Certificate Fingerprint**. Leave blank if you want to authenticate the Proxy with a full certificate.

7 To use a clear data channel (CDC) to the Proxy, check the box, **Use unencrypted data channel**.

8 To force the use of the TLS V1.2 protocol for the connection to the Proxy, check the box, **TLS V1.2 only**.

FTP Integrity Options

To configure a MessageWay FTP site to check the integrity of files, either input or output, specify options on the **Integrity** tab. For specific information about the fields, refer to the reference topic, ***FTP, Integrity Page*** (on page 1141).



☑ Override Whether to Use Integrity

Check Integrity After Transfer:

○ No

● Yes, If Available

○ Yes, Required

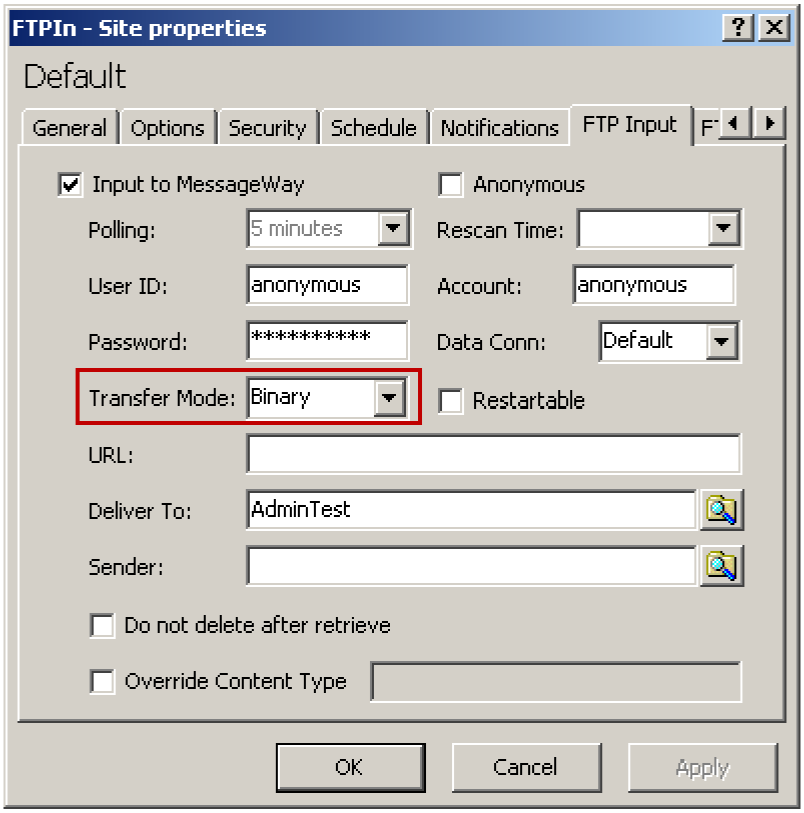
☑ Override Allowed File Integrity Algorithms

□ MD5

☑ SHA1

These configurations will override the properties inherited from the FTP adapter. For further discussion of the integrity check process, refer to the topic, ***Recommendations for Integrity Checking for an FTP Adapter*** (on page 431).

1 For input or output transfers, the *Transfer Mode* must be set to **Binary** to avoid potential errors with text transfers during the integrity check:



☑ Input to MessageWay ☐ Anonymous

Polling: 5 minutes Rescan Time:

User ID: anonymous Account: anonymous

Password: ********** Data Conn: Default

Transfer Mode: Binary ☐ Restartable

URL:

Deliver To: AdminTest

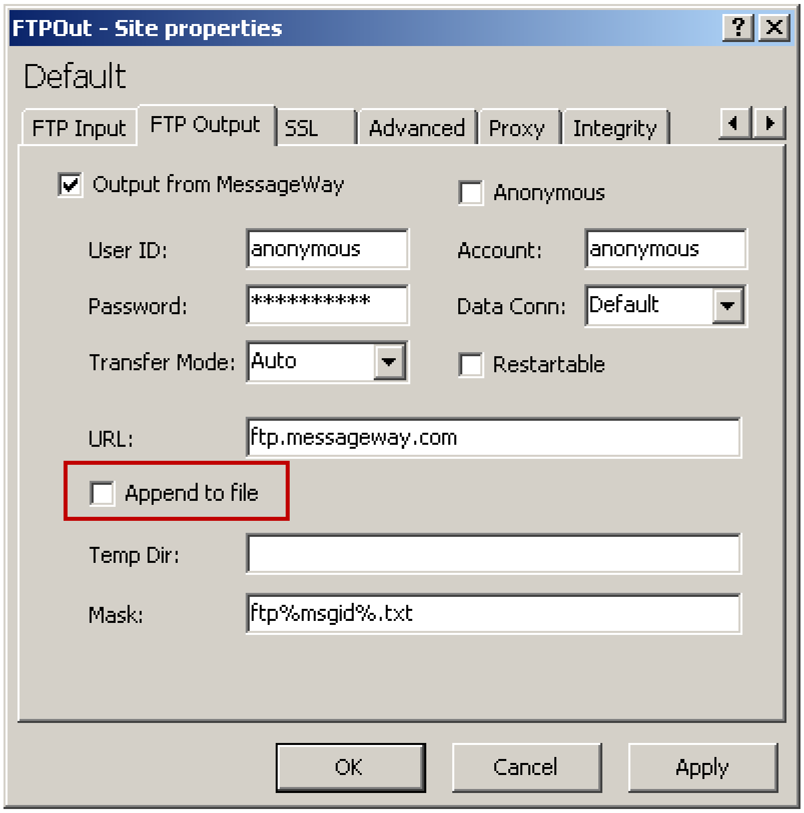
Sender:

☐ Do not delete after retrieve

☐ Override Content Type

- and -

For output transfers, you should *not* select the *Append* option, to also avoid problems with integrity check.



Default

☑ Output from MessageWay

□ Anonymous

User ID: anonymous

Account: anonymous

Password: **********

Data Conn: Default

Transfer Mode: Auto

□ Restartable

URL: ftp.messageway.com

□ Append to file

Temp Dir:

Mask: ftp%msgid%.txt

2 To override the adapter setting whether to use integrity checks, check the box *Override Whether to Use Integrity* (on page 1142).

3 In the *Check Integrity After Transfer* box, select the type of check you want to perform: **No** (on page 1142), **Yes, If Available** (on page 1142) or **Yes, Required** (on page 1143).

4 To override the adapter settings for the algorithms, check the box *Override Allowed File Integrity Algorithms* (on page 1143).

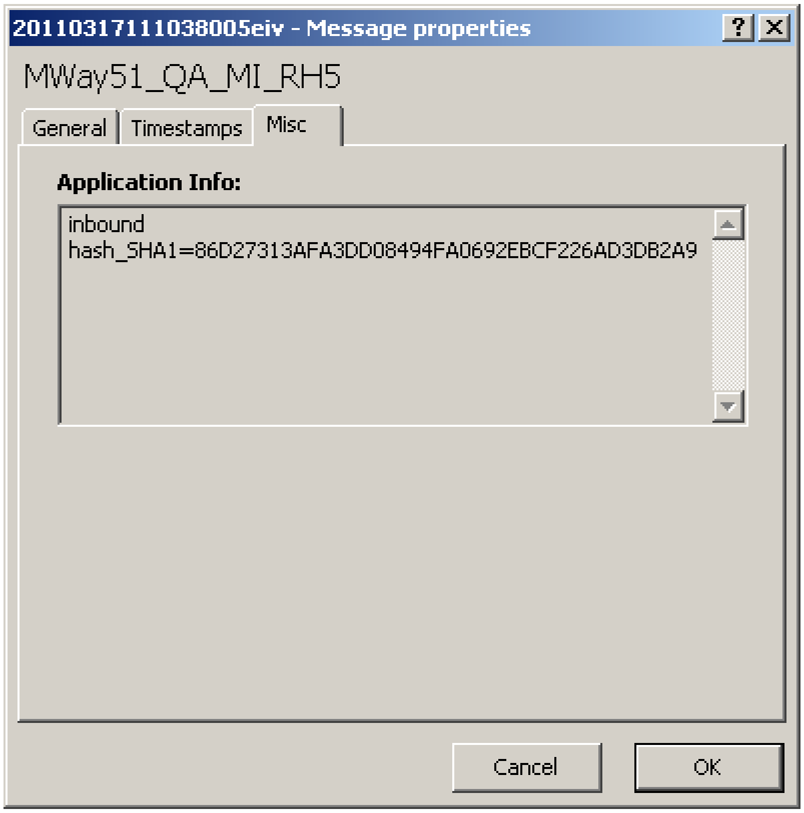
5 Select any algorithms that you want to use for this site.

MessageWay will issue FEAT commands to the FTP server to determine which algorithms it supports, in the order of strongest to weakest. MessageWay uses the first one that the server also supports to create the hash value.

IMPORTANT: The algorithm strength affects the time it takes to verify file integrity. The stronger the algorithm, the longer the transfer verification usually takes.

6 To view the results of the integrity check:

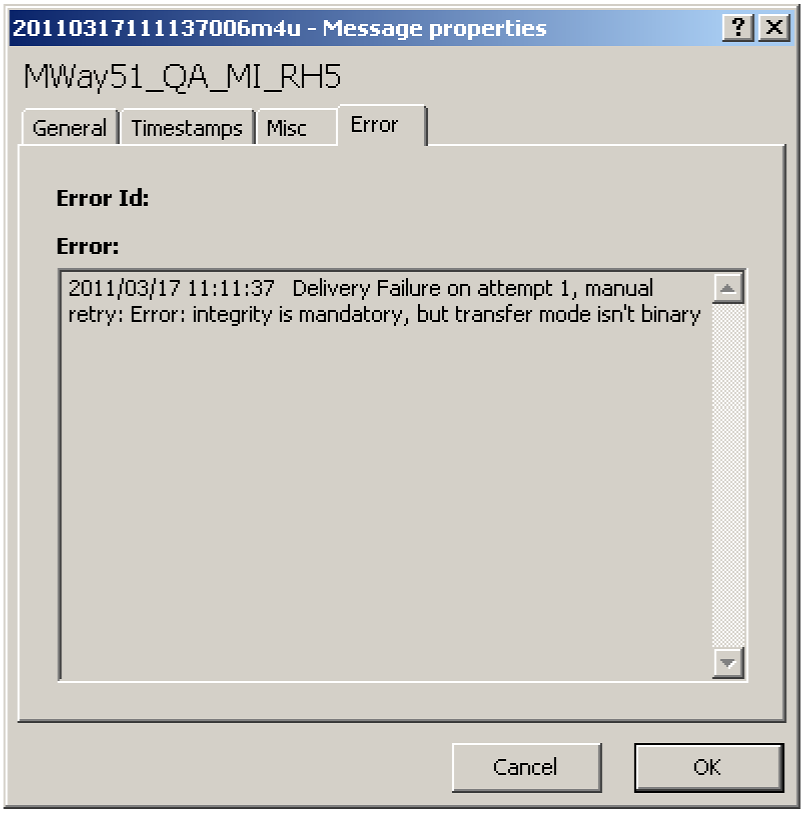
a) If the hash values matched, the check was successful, and the algorithm and hash value appear on the **Misc** page.



Application Info:

```
inbound
hash_SHA1=86D27313AFA3DD08494FA0692EBCF226AD3DB2A9
```

b) If there are errors during the integrity check, additional error information appears on the **Error** page.



Error Id:

Error:

2011/03/17 11:11:37 Delivery Failure on attempt 1, manual retry: Error: integrity is mandatory, but transfer mode isn't binary

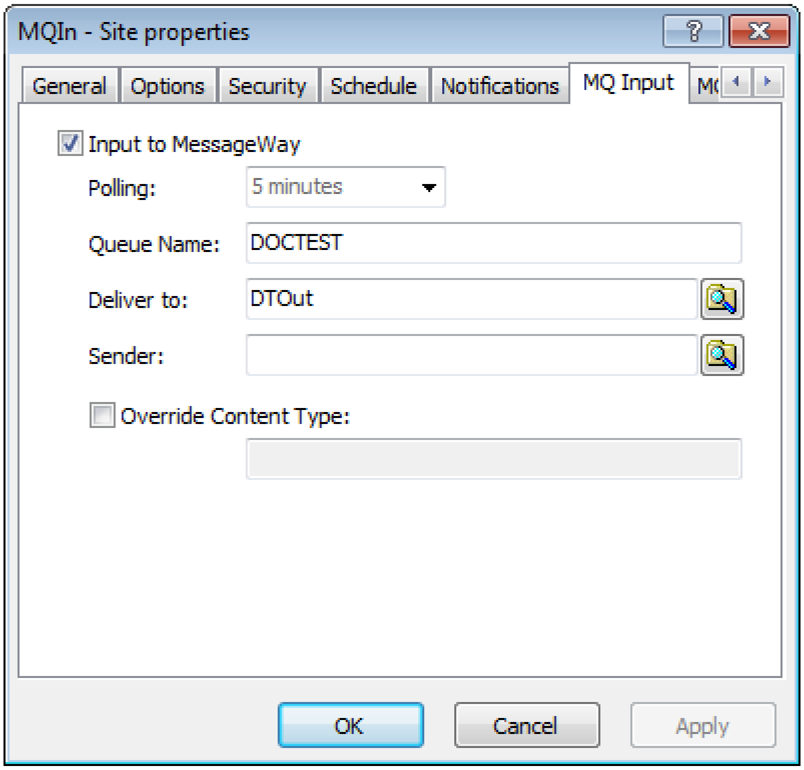
Configuring an MQ Site

NOTE: The MessageWay MQ Adapter requires a license from Progress. You must have a license in order to start the adapter. For more information, contact MessageWay Technical Support.

Locations that use the MessageWay MQ Adapter may be configured for input and/or output.

MQ Input Options

To retrieve files from an MQ queue and send them into MessageWay, specify options on the **MQ Input** page. For specific information about the fields, refer to the reference topic, ***MQ Input Page*** (on page 1149).



MQIn - Site properties

☑ Input to MessageWay

Polling: 5 minutes

Queue Name: DOCTEST

Deliver to: DTOut

Sender:

□ Override Content Type:

1 Check the box, **Input to MessageWay**.

2 Accept the default polling option from the adapter, or select another polling option.

3 In the **Queue Name** box, type the name of a queue that MessageWay will query for messages to transfer into MessageWay.

NOTE: The queue name must be associated with the queue manager that is defined for the adapter.

4 In the **Deliver to** box, type or select a location where the adapter will transfer the messages.

This may be an output site for delivery, a pickup mailbox or a service location capable of routing messages, such as distribution list. The format may also be a ***simple or compound address*** (on page 653). When the location does not exist, the message is sent to the {Unknown} system mailbox.

5 To override the sender that was determined by MessageWay, type or select a different sender location.

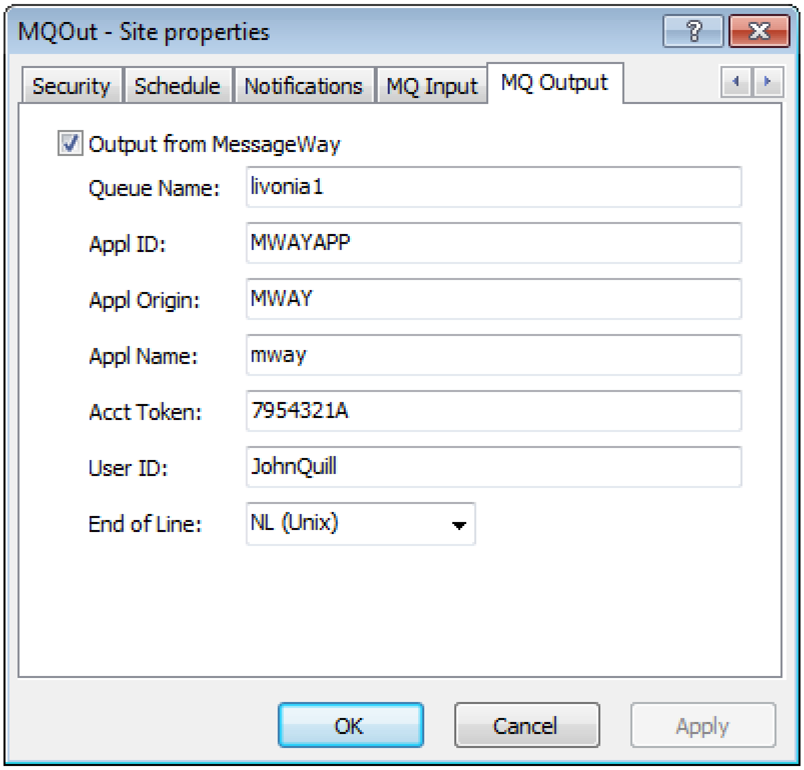
6 To specify a ***content type*** (on page 1130) type for the input message or override an existing type:

a) Check the **Override Content Type** box.

b) Type a value for the content type in the data entry box.

MQ Output Options

To send messages from MessageWay to an MQ server, specify options on the **MQ Output** tab. For specific information about the fields, refer to the reference topic, ***MQ Output Page*** (on page 1151).



☑ Output from MessageWay

Queue Name: livonia1

Appl ID: MWAYAPP

Appl Origin: MWAY

Appl Name: mway

Acct Token: 7954321A

User ID: JohnQuill

End of Line: NL (Unix)

1 Check the **Output from MessageWay** box.

2 In the **Queue Name** box, type the name of the queue where MessageWay will transfer the message.

NOTE: The queue name must be associated with the queue manager that is defined for the adapter.

Configuring a Rules Processing Service Location

A rules processing service location allows you to route messages based on message properties or content. The rules definitions in the rules profile defined for the location determine what happens next.

The options available are:

Action	Description
Route	Route message to another service location or to an output site or mailbox
Link	Route message to another rules processing profile
Reject	Reject the message without creating any output

You may use several strategies to determine where to route data using rules processing:

- Define multiple rules on a single profile, where the sequence determines the order of testing, and the first rule that succeeds will be the one executed
- Define multiple profiles that are linked to provide a branching decision tree.
- Some combination of the above two.

To use a rules service location, you perform the following tasks:

1. Create a rules processing profile.
2. Specify one or more rule definitions, each with an action and a destination location.
3. Create expressions to test data for each action.
4. Create a rules processing service location and specify the rules profile on the **Rules** tab.

To Create a Rules Processing Profile

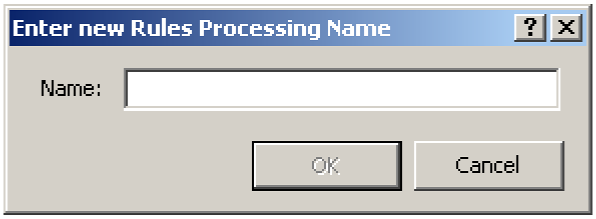
To create a rules processing profile, from MessageWay Explorer, proceed as follows:

1. Use one of three methods:
   - In the left pane, right-click the **Rule Processing** folder or existing subfolder, and select **Add Rules Processing Profile** from the **Rules Processing** menu.

     - or -
   - In the left pane, select **Rules Processing**, and then right-click in a open area of the right pane or on an existing folder and select **Add Rules Processing Profile** from the pop-up menu.

     - or -
   - In the right pane, right-click an existing rules profile and select **Copy**, then right-click again and select **Paste**.

   The **Enter New Rules Processing Name** dialog box appears.
2. Type a Rules Processing Profile name of up to 64 characters, and select **OK**.



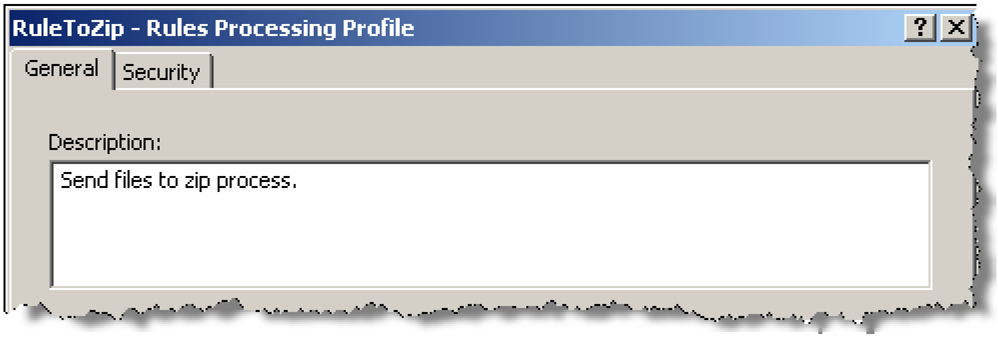
   The Rules Processing Profile window appears.

To Specify Rules for a Rules Processing Profile

For more information about the rules processing profiles, refer to the reference topics:

- ***Rules Processing Profile Window*** (on page 1262)
- ***Process Rule Window*** (on page 1239)

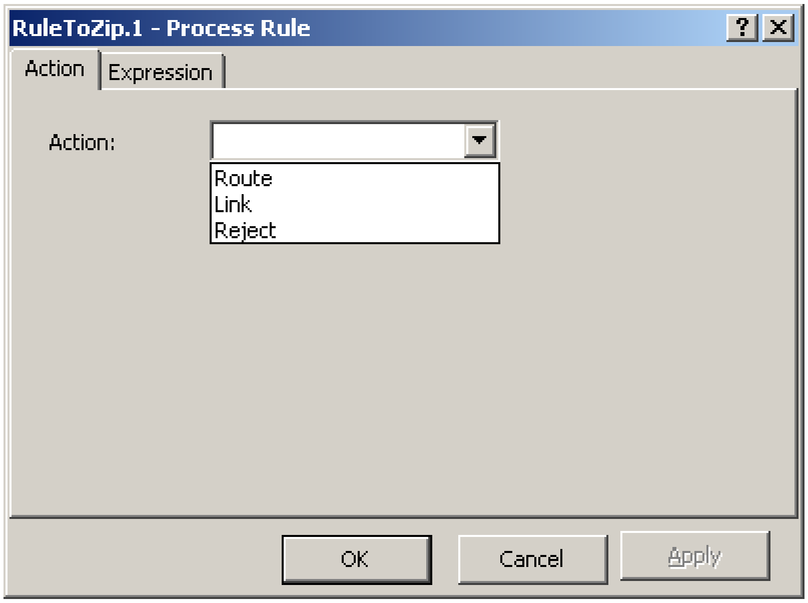
1 Open the Rules Processing Profile window, and type a description of the purpose of this rule.



Description: Send files to zip process.

2 Click **Add**.

The Process Rule window appears showing the **Action** tab.

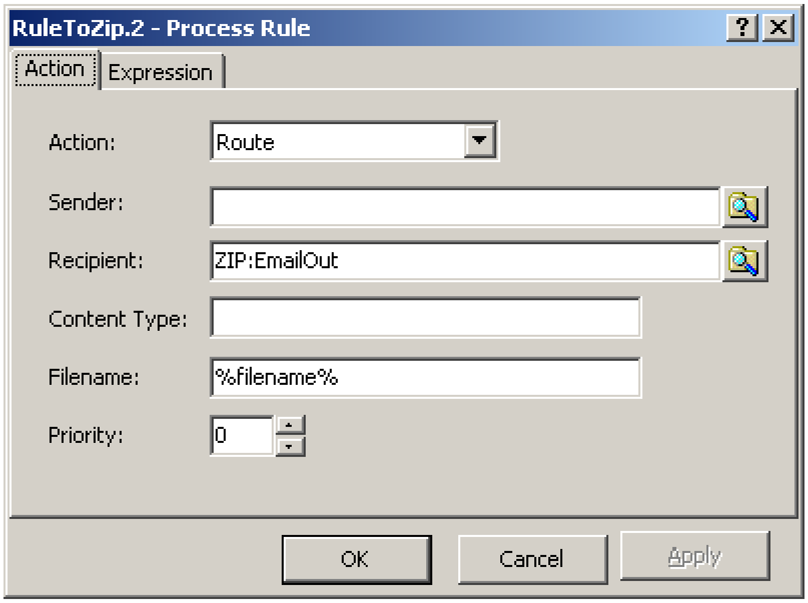


3 Choose one of the three actions, and select **OK**.

Route	Route this message to the specified location.
Link	Link to another process rule to apply additional rules.
Reject	Reject this message and notify the sender using the specified text. When a message is rejected, no output message is created, and the input message has a status of error.

4 The Process Rule window reappears with options based on the action you selected.

- For the *Route* action, at minimum, enter or select the name of the destination location. If the destination is a service location that does not provide routing itself, you must use a compound address in the **Recipient** field. For example, the Compression service (zip/unzip), does not route messages, so it must receive routing instructions from an input location or service that does provide routing, such as Rules Processing.



Action: Route

Sender:

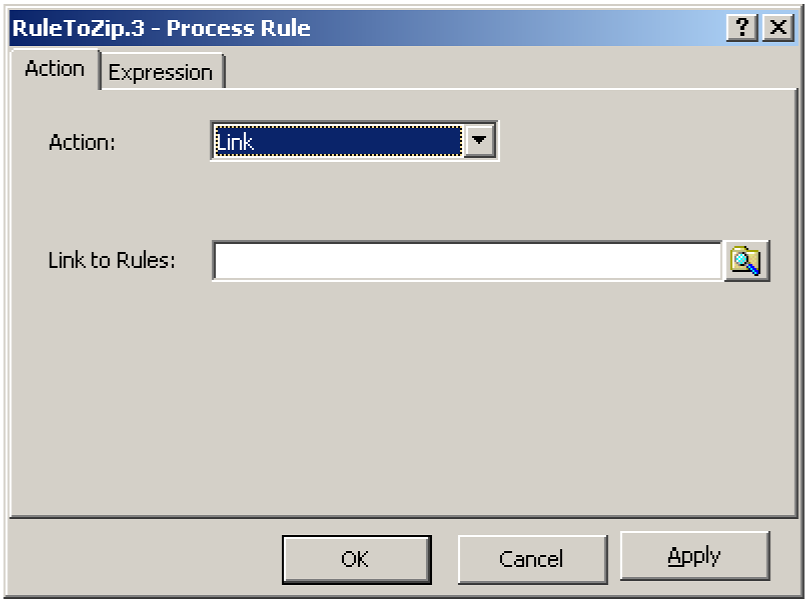
Recipient: ZIP:EmailOut

Content Type:

Filename: %filename%

Priority: 0

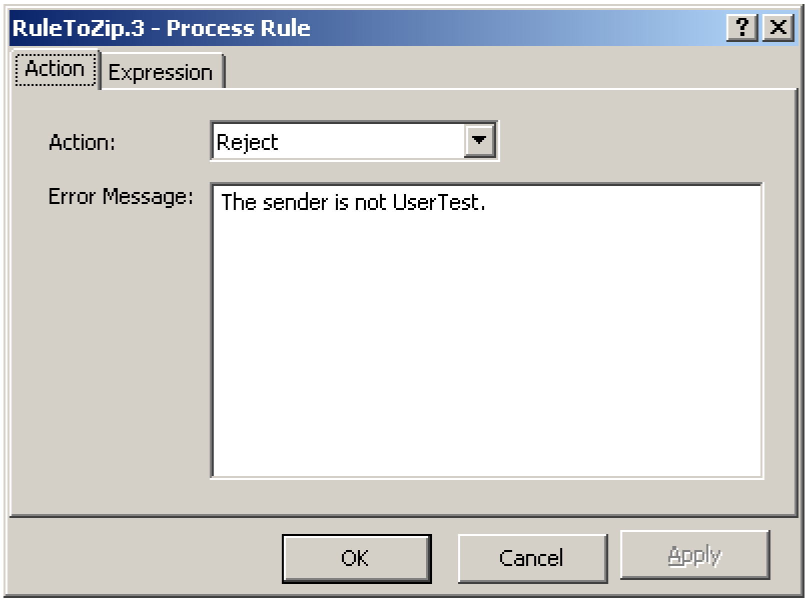
- For the *Link* action, enter the name of another rules profile.



Action: Link

Link to Rules:

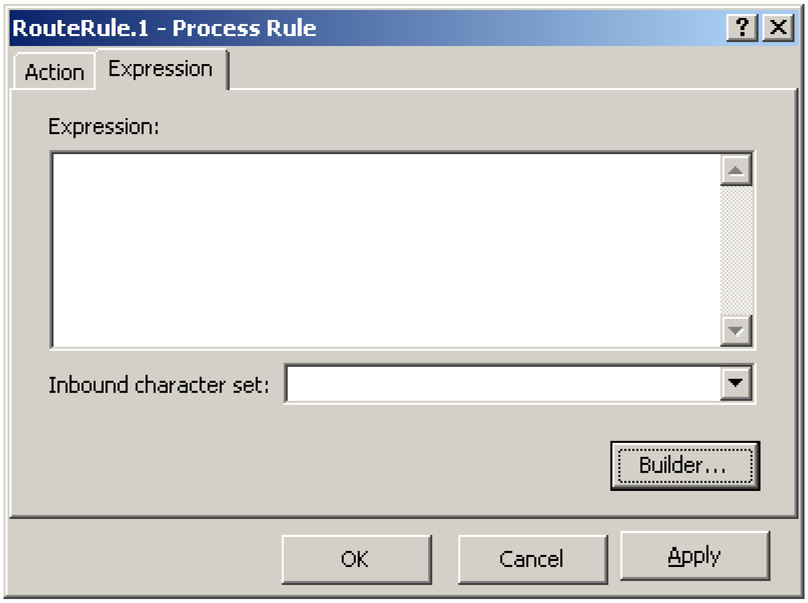
- For the *Reject* action, enter a brief message that will appear on an **Misc** tab of the Message Properties window.



Action: Reject

Error Message: The sender is not UserTest.

5 On the **Expression** tab, select the **Builder** button.



The Expression Builder window appears.

To Create Expressions for Rules Processing Profiles

When you use the Expression Builder, you may choose among options to create the expression. The expression is then generated using correct syntax and added to the Rules box on the Rules Processing Profile window.

For more information about these fields, refer to the reference topic, ***Expression Builder Window*** (on page 1249)

NOTE: A null expression is always true.

The syntax options to negate or to change the associativity of expressions are available when you select one or more rows of expressions.

- To select an expression to which you want to apply one of these options, press **SHIFT**, and click to the left of the expression.
- To select multiple expressions, press **SHIFT** and drag the cursor down the left side of the window.

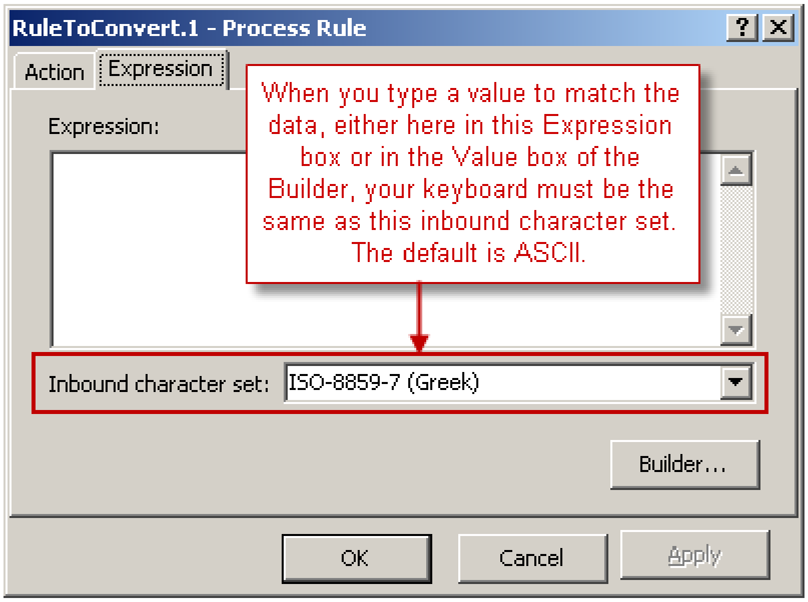
Add parentheses Button	[...]	This is a toggle button that places and removes parentheses around expressions to change the associativity of the And and Or operators. To control the order of evaluation of the expressions, move your cursor to the left of one or more rows until you the cursor changes to a hand. Click the mouse to highlight the selected expressions, dragging your cursor down the left side to select as many as required. Then select the parentheses button. Note that the expressions you selected are now surrounded by a pair of parentheses.
Add NOT Button	NOT	This is a toggle button that applies and removes the negative operator **Not** for expressions. To negate expressions, move your cursor to the left of one or more rows until the cursor changes to a hand. Click the mouse to highlight the selected expressions, dragging your cursor down the left side to select as many as required. Then select the **Not** button. Note that the expressions you selected are now surrounded by a pair of parentheses preceded by **Not**.

When MessageWay parses the data, the only assumptions it can make are those based on specific standards, such as X12 or EDIFACT, conventions, such as XML or ZIP, or character sets, such as UTF-8, UTF-16BE, UTF-16LE, UTF-32BE, and UTF-32LE. When you enter arguments for comparison, remember that MessageWay will use syntax rules if it knows the standard, convention or character set. Otherwise, it will count bytes.

Enter the arguments for the type of input you want to use for comparison. The square brackets [and] enclose optional items. The signs < and > enclose names that describe the type of value actually used. Special characters that are part of the syntax, such as brackets or commas, are highlighted.

Enter the operator you want to use for comparison.

When an inbound character set is specified on the **Expression** tab of the Process Rule window, your keyboard must use the same character set when you type the value either in the **Expression** box directly or in the **Value** box of the Expression Builder. The parameters of the rule must be in ASCII, so it may be easier to use the Expression Builder.



Inbound character set: ISO-8859-7 (Greek)

When you type a value to match the data, either here in this Expression box or in the Value box of the Builder, your keyboard must be the same as this inbound character set. The default is ASCII.

The following table specifies constraints on values based on the source selected:

Source	**Constraint**
Size	The literal must be a decimal value for the integer comparison.
Not Size	Literal values must be enclosed in double quotation marks for the byte-by-byte comparison. Escape sequences may be used before the opening quotation marks, as specified in the following table.
Filename or InputName	▪ If a "\" is used to fully qualify the filename or inputname, another "\" must be used to escape it. For example: C:\\folder\\subfolder\\filename
Data Type	Select one of the following: ▪ X12 ▪ EDIFACT ▪ XML ▪ ZIP ▪ Unknown ▪ UTF-8 ▪ UTF-16BE ▪ UTF-16LE ▪ UTF-32BE ▪ UTF-32LE

Source	Constraint
Content Type	▪ application/edifact ▪ application/edi-x12 ▪ application/gzip ▪ application/pdf ▪ application/vnd.hp-pcl ▪ application/vnd.lotus-1-2-3 ▪ application/vnd.ms-excel ▪ application/vnd.ms-powerpoint ▪ application/vnd.realmedia ▪ application/x-bzip ▪ application/xml ▪ application/x-shockwave-flash ▪ application/zip ▪ audio/basic ▪ audio/mpeg ▪ audio/vnd.rn-realaudio ▪ audio/x-aiff ▪ audio/x-wav ▪ image/bmp ▪ image/gif ▪ image/jpeg ▪ image/png ▪ image/tiff ▪ image/x-psd ▪ text/plain ▪ video/mpeg ▪ video/quicktime ▪ video/x-msvideo ▪ video/x-ms-wmv

This table shows special character options available for values:

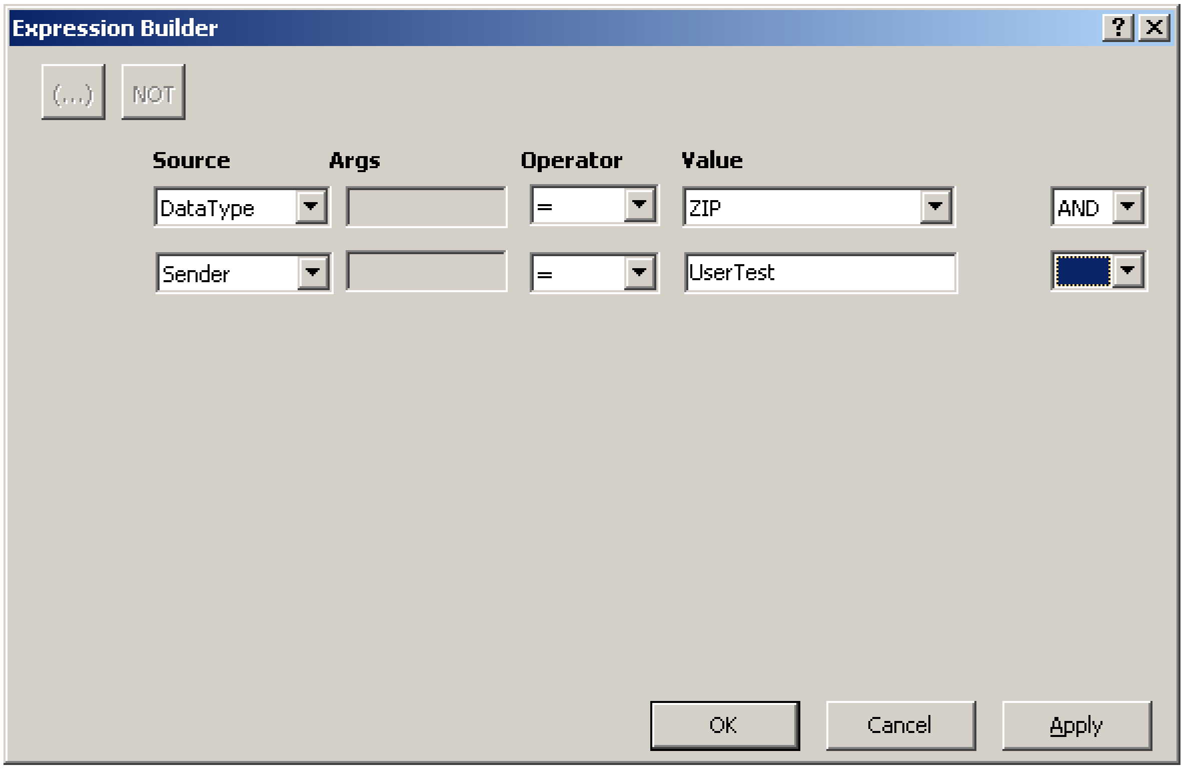
Option	Description
i	Use lower case **i** before the value, which will be in double quotation marks, to indicate that the comparison is not case sensitive. The default is case insensitive.
E	Use upper case **E** before the value, which will be in double quotation marks, to indicate that this is EBCDIC data.

Option	Description
K, M or G	Use upper case K immediately after the numeric value for kilobytes (10*2^10), e.g. *10K*. Use upper case M immediately after the numeric value for megabytes (10*2^20), e.g. *10M*. Use upper case G immediately after the numeric value for gigabytes (10*2^30), e.g. *10G*. **CAUTION:** Any other combination of letters, e.g. MB, or any lower case characters will display an error message, "Size value must be numeric."
\"	Escape sequence to include double quotation mark in the value, which is within quotation marks.
\\	Escape sequence to include back-slash in the value, which is within quotation marks.

To add another rule to this expression, select **AND OR** from the drop-down list. Another line of options appears. You may add up to eight rules for a single expression.

Add rules as required. Use the **Move Up** or **Move Down** buttons to adjust the order of the rules. Rules are evaluated in sequence from top to bottom, and the first one that evaluates to true is executed.

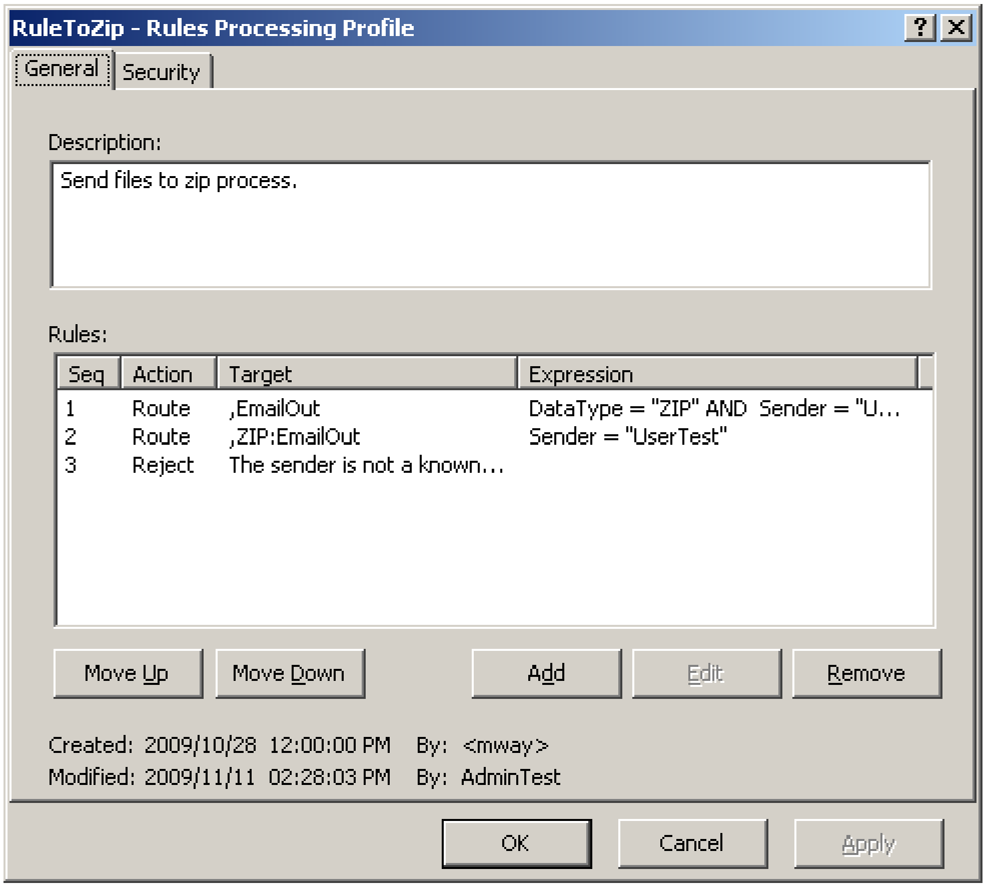
This example shows one of the expressions created with Expression Builder.



Expression Builder

Source	Args	Operator	Value	
DataType		=	ZIP	AND
Sender		=	UserTest	

This example shows the rules created for this profile.



Description:

Send files to zip process.

Rules:

Seq	Action	Target	Expression
1	Route	,EmailOut	DataType = "ZIP" AND Sender = "U...
2	Route	,ZIP:EmailOut	Sender = "UserTest"
3	Reject	The sender is not a known...	

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/11 02:28:03 PM By: AdminTest

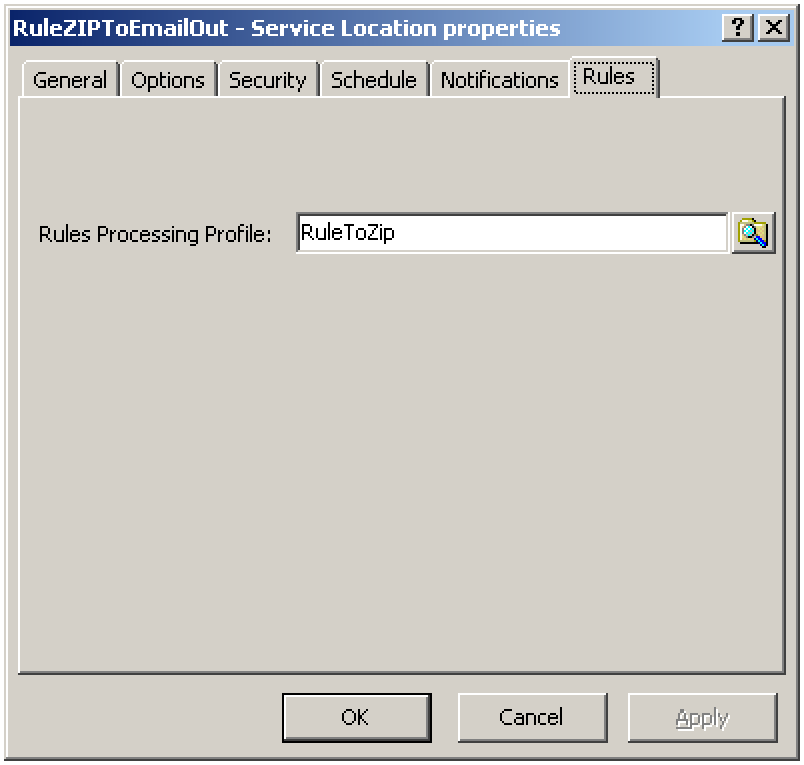
To Specify the Rules Processing Profile for the Rules Service Location

1 If necessary, create the rules service location:

a) Follow the instructions, ***How to Create a Location*** (on page 461).

b) For the Adapter/Service, select **MWRules**.

2 On the **Rules** tab, enter the name of the rules processing profile.


RuleZIPToEmailOut - Service Location properties

Rules Processing Profile: RuleToZip

Configuring an SFTP Site

Locations that use the MessageWay SFTP Adapter may be configured for input and/or output. You may also configure it to connect through the MessageWay Proxy Server rather than directly to an external SFTP server.

All SFTP communications require SSH key exchanges. MessageWay provides a way to manage your SSH keys from the Manager. For more information, refer to the topic, ***Managing SSH Client Keys*** (on page 642).

Creating an SFTP Location

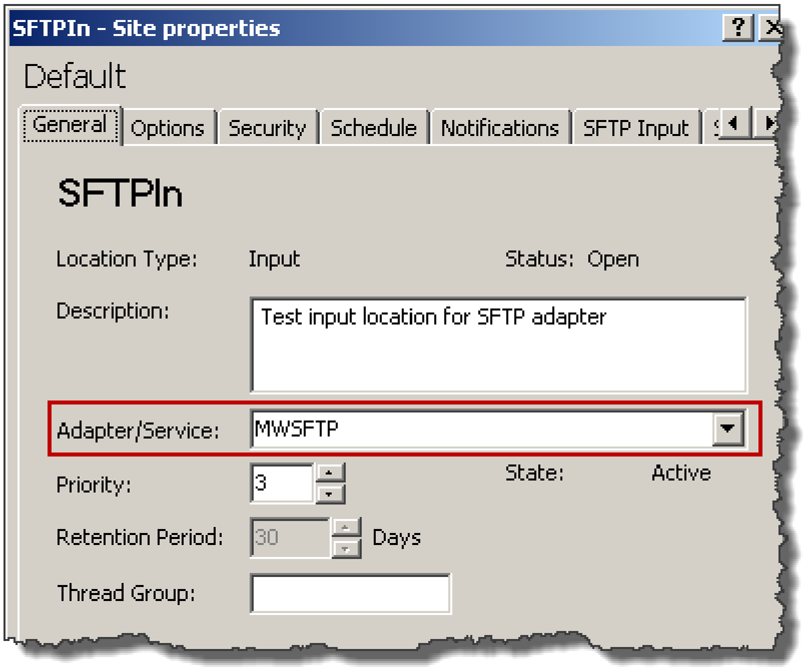
To create an SFTP location and configure some general options, such as those on the **General**, **Options** and **SFTP Auth** tabs:

1 ***Add a location*** (on page 461), such as SFTPIn or SFTPOut.

2 On the **General** tab, select the SFTP adapter.

For more information about specific fields and values, refer to the reference topic, ***General Page (Location Properties)*** (on page 1043).

NOTE: If the SFTP adapter does not appear on the list, you may need to install it.



SFTPIn

Location Type: Input

Status: Open

Description: Test input location for SFTP adapter

Adapter/Service: MWSFTP

Priority: 3

State: Active

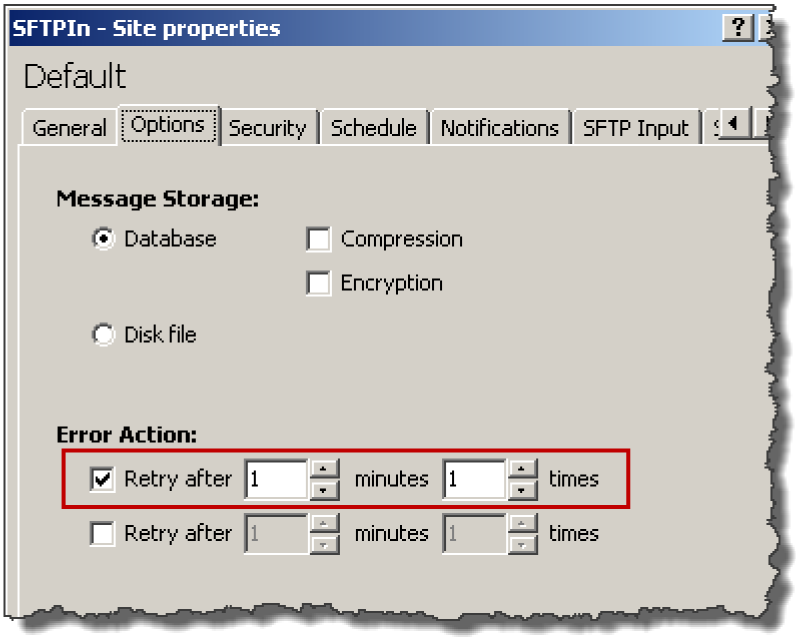
Retention Period: 30 Days

Thread Group:

3 On the **Options** tab, check **Retry** to provide at least one retry option.

For more information about specific fields and values, refer to the reference topic, ***Options (Location Properties)*** (on page 1051).

TIP: It is always a good idea to select a retry action to properly handle send or receive errors.



Message Storage:

● Database

□ Compression

□ Encryption

○ Disk file

Error Action:

☑ Retry after 1 minutes 1 times

□ Retry after 1 minutes 1 times

4 Authentication is required for both input and output, on the **SFTP Auth** tab:

a) You must supply a fingerprint so the adapter can validate the server. For testing purposes you can check **Accept Next Server Key**. For production, of course, you would typically enter the fingerprint for the server's SSH key.' You can check Always to accept a new server key for each new session, provided the server changes its server key per session.

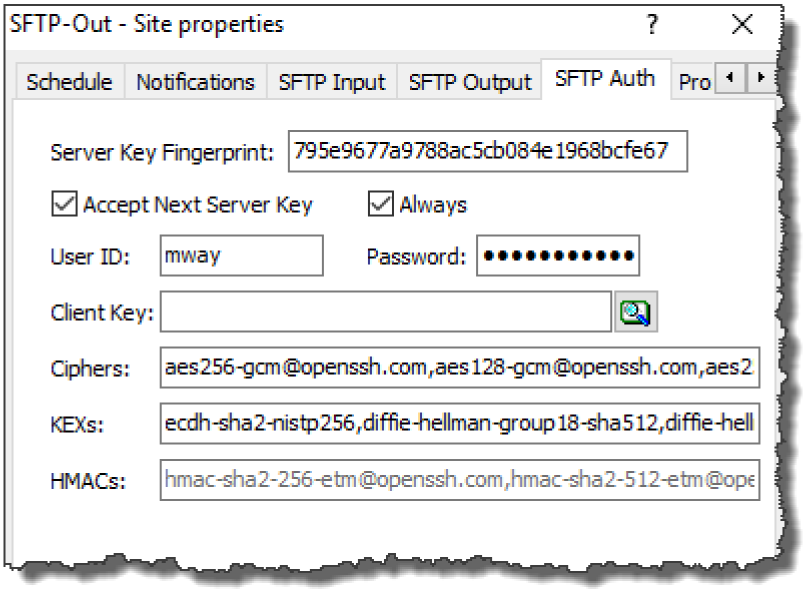
b) Type the name of a valid user on the SFTP server system.

c) Enter either or both the password for the user and/or a client key. The SFTP server determines which to use, but public key authentication is more secure.

d) Enter/update the ciphers, KEX algorithms and HMACs, or use the adapter defaults (displayed in gray).

For more information about specific fields and values, refer to the reference topic, ***SFTP Auth Page*** (on page 1154).

IMPORTANT: The public key must already be stored in the MessageWay database. To create or import keys, refer to the topic ***Managing SSH Public Keys*** (on page 642).



Server Key Fingerprint: 795e9677a9788ac5cb084e1968bcfe67

☑ Accept Next Server Key ☑ Always

User ID: mway Password: ●●●●●●●●●●●

Client Key:

Ciphers: aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes2

KEXs: ecdh-sha2-nistp256,diffie-hellman-group18-sha512,diffie-hell

HMACs: hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@ope

1 To create an input site, refer to the topic ***Configuring an SFTP Location to Receive Messages Into MessageWay*** (on page 648).

2 To create an output site, refer to the topic ***Configuring an SFTP Location to Send Messages from MessageWay*** (on page 649).

Managing SSH Client Keys

MessageWay provides a method to manage your SSH Client Keys, which it stores in the MessageWay database.

SSH keys contain 2 parts: a public key that is available to everyone, and a private key that is known only to you. When connecting to the SSH server, the client uses this private part to determine a session key with the server, which is known as the shared secret. The SSH server sends its own public key plus a part of the shared secret key to assure the client that the server is who it says it is. The SSH server uses the public part of the client key and other information to identify the client.

To add keys to the key store, from the MessageWay Manager, you can:

- Generate a key
- Import a key

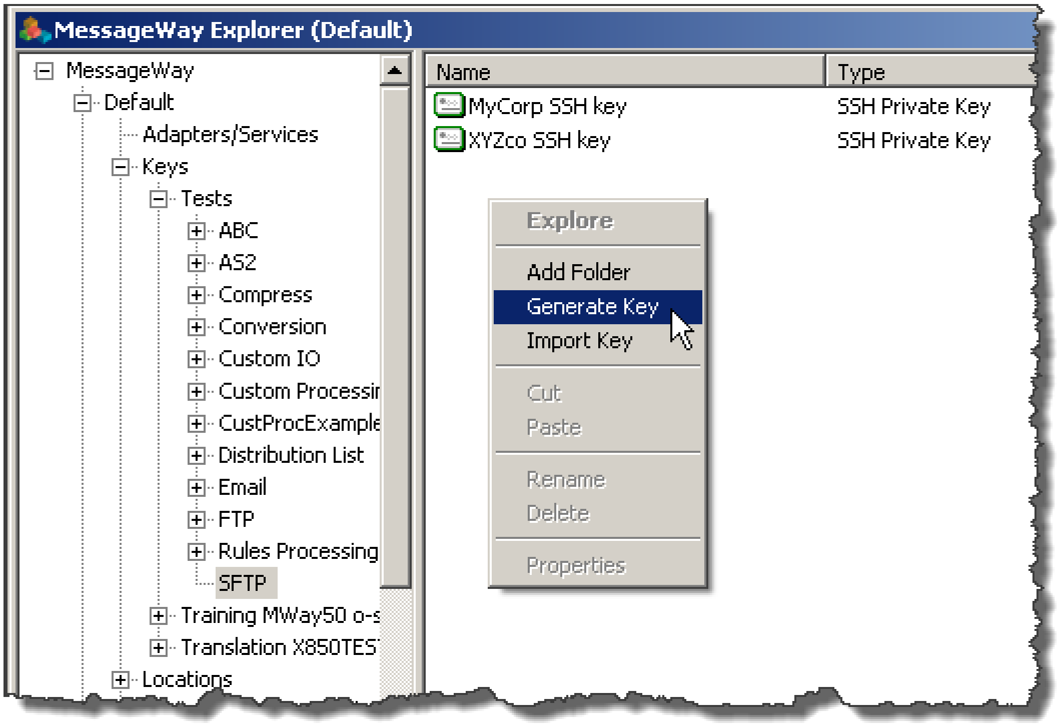
Generating Client Keys

To generate a client key from the MessageWay Manager, proceed as follows:

1 In the left pane of MessageWay Explorer, click the **Keys** folder.

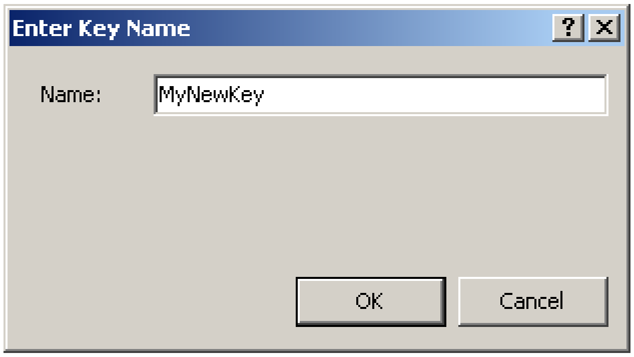
2 In the right pane, navigate to the folder where you want to store the key. Since one key can be used by many locations, you may decide to store the keys directly under the **Keys** folder, rather than under one of the existing location folders.

3 Right click and select **Generate Key**.



The **Enter Key Name** dialog box appears.

4 Type the name of the key and click **OK**.

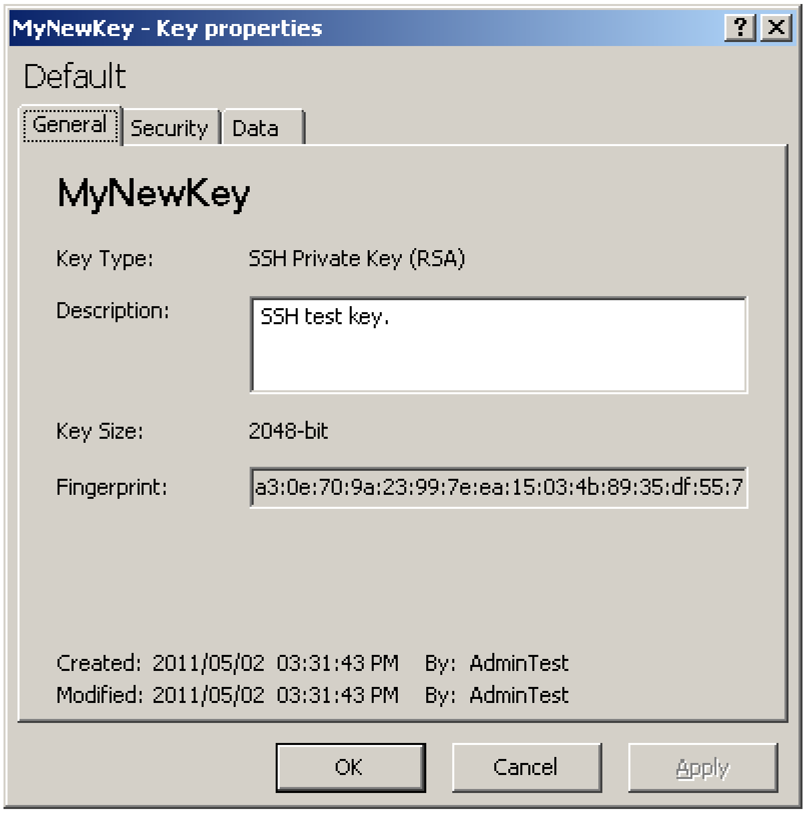


Enter Key Name

Name: MyNewKey

The Key Properties window appears.

5 On the **General** page, type a description. The other information available, key type, key length and the fingerprint of the public portion of the key are display-only.



MyNewKey - Key properties

Default

MyNewKey

Key Type: SSH Private Key (RSA)

Description: SSH test key.

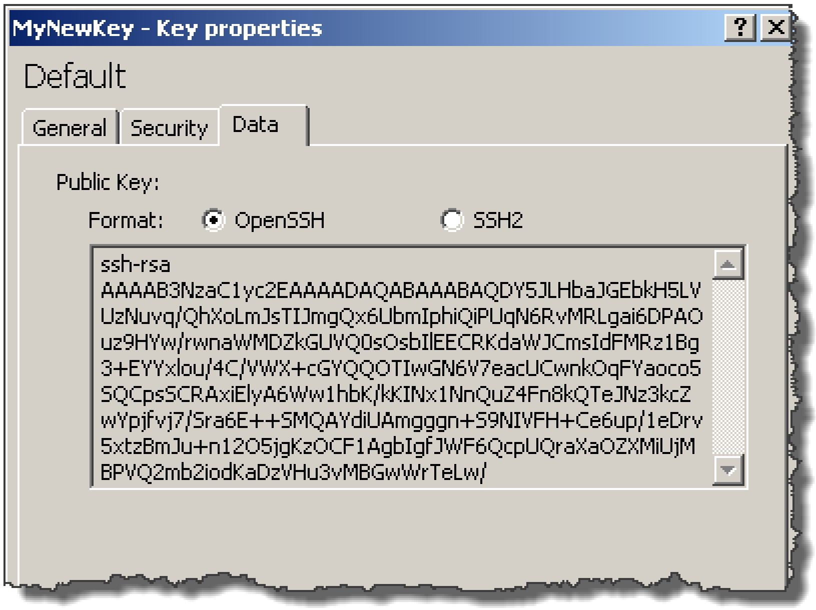
Key Size: 2048-bit

Fingerprint: a3:0e:70:9a:23:99:7e:ea:15:03:4b:89:35:df:55:7

Created: 2011/05/02 03:31:43 PM By: AdminTest
Modified: 2011/05/02 03:31:43 PM By: AdminTest

6 On the **Security** page, enter those MessageWay users or groups that should have access to this key, and the type of access they should have. For more detailed information, refer to the topic, ***Configuring Object Security*** (on page 391).

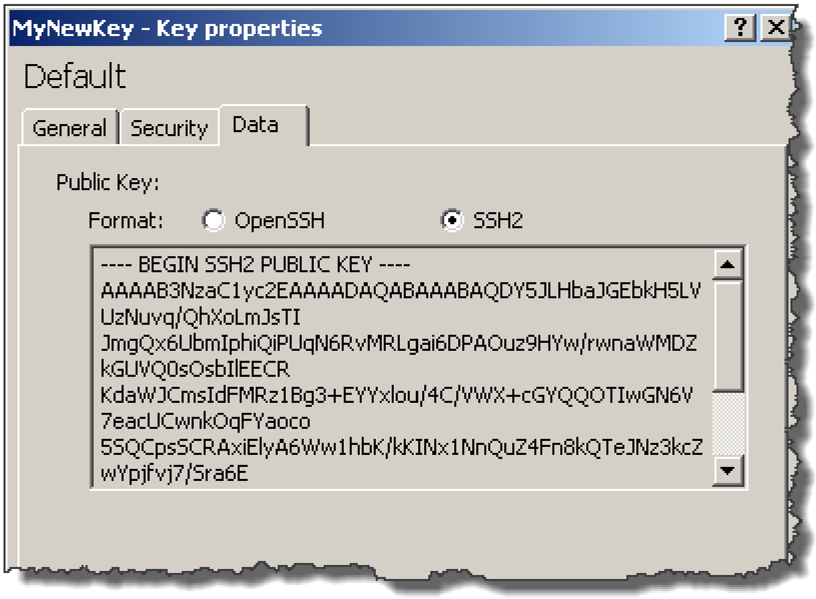
7 On the **Data** page, select the format you want to use to view the public part of the key, OpenSSH or SSH2.



Public Key:

Format: ● OpenSSH ○ SSH2

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDY5JLHbaJGEbkH5LV
UzNuvq/QhXoLmJsTIJmgQx6UbmIphiQiPUqN6RvMRLgai6DPAO
uz9HYw/rwnaWMDZkGUVQ0sOsbIlEECRKdaWJCmsIdFMRz1Bg
3+EYYxlou/4C/VWX+cGYQQOTIwGN6V7eacUCwnkOqFYaoco5
5QCpsSCRAxiElyA6Ww1hbK/kKINx1NnQuZ4Fn8kQTeJNz3kcZ
wYpjfvj7/Sra6E++SMQAYdiUAmgggn+S9NIVFH+Ce6up/1eDrv
5xtzBmJu+n12O5jgKzOCF1AgbIgfJWF6QcpUQraXaOZXMiUjM
BPVQ2mb2iodKaDzVHu3vMBGwWrTeLw/
```



Public Key:

Format: ○ OpenSSH ● SSH2

```
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAABAQDY5JLHbaJGEbkH5LV
UzNuvq/QhXoLmJsTI
JmgQx6UbmIphiQiPUqN6RvMRLgai6DPAOuz9HYw/rwnaWMDZ
kGUVQ0sOsbIlEECR
KdaWJCmsIdFMRz1Bg3+EYYxlou/4C/VWX+cGYQQOTIwGN6V
7eacUCwnkOqFYaoco
55QCpsSCRAxiElyA6Ww1hbK/kKINx1NnQuZ4Fn8kQTeJNz3kcZ
wYpjfvj7/Sra6E
```

8 Click **Apply** or **OK**.

Importing Client Keys

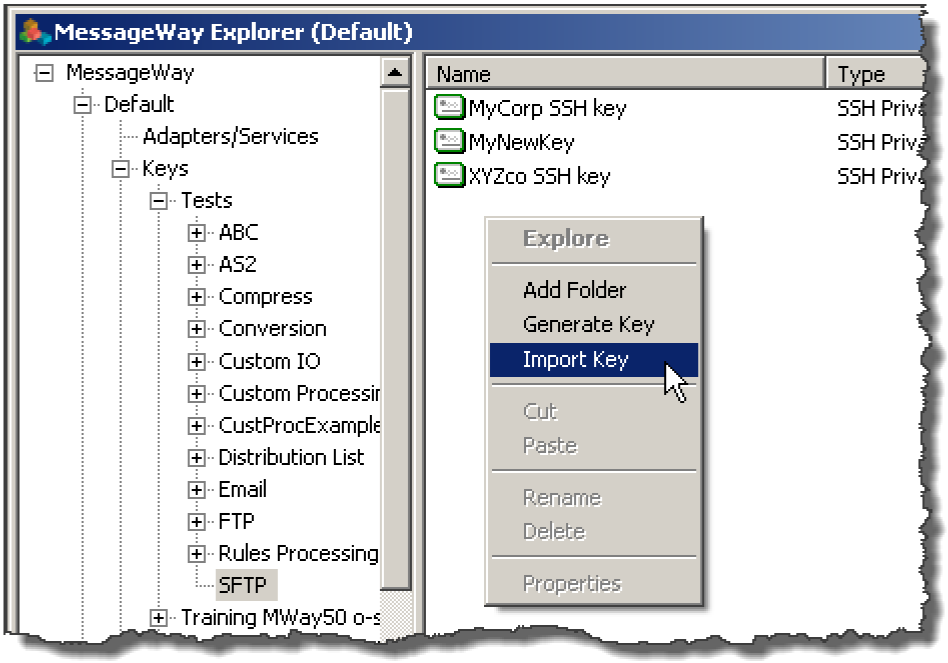
IMPORTANT: The import function only imports keys that are in OpenSSH format. To import keys in other formats, such as SSH2, you must first convert the key to an OpenSSH format.

To import a client key using the MessageWay Manager, proceed as follows:

1 In the left pane of MessageWay Explorer, click the **Keys** folder.

2 In the right pane, navigate to the folder where you want to store the key. Since one key can be used by many locations, you may decide to store the keys directly under the **Keys** folder, rather than under one of the existing location folders.

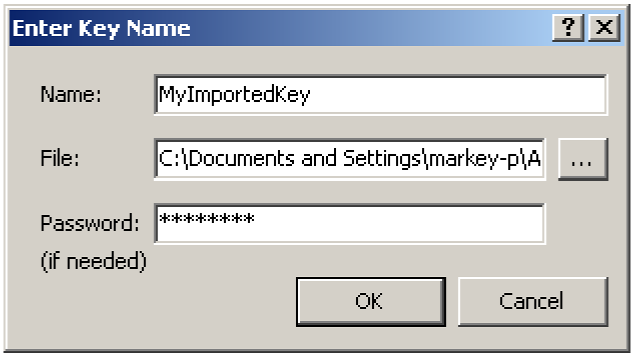
3 Right click and select **Import Key**.



Name	Type
MyCorp SSH key	SSH Priv
MyNewKey	SSH Priv
XYZco SSH key	SSH Priv

The **Enter Key Name** dialog box appears.

4 Type the name of the key, the location of the key file, a password if required and click **OK**.



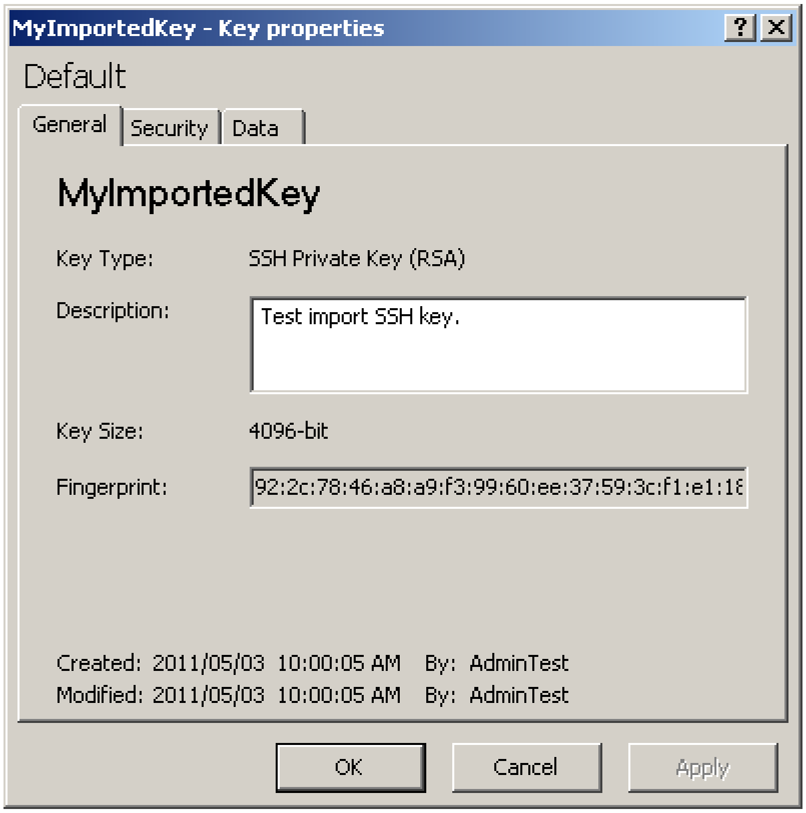
Name: MyImportedKey

File: C:\Documents and Settings\markey-p\A

Password: (if needed) *********

The Key Properties window appears.

5 On the **General** page, type a description. The other information available, key type, key length and the fingerprint of the public portion of the key are display-only.



MyImportedKey

Key Type: SSH Private Key (RSA)

Description: Test import SSH key.

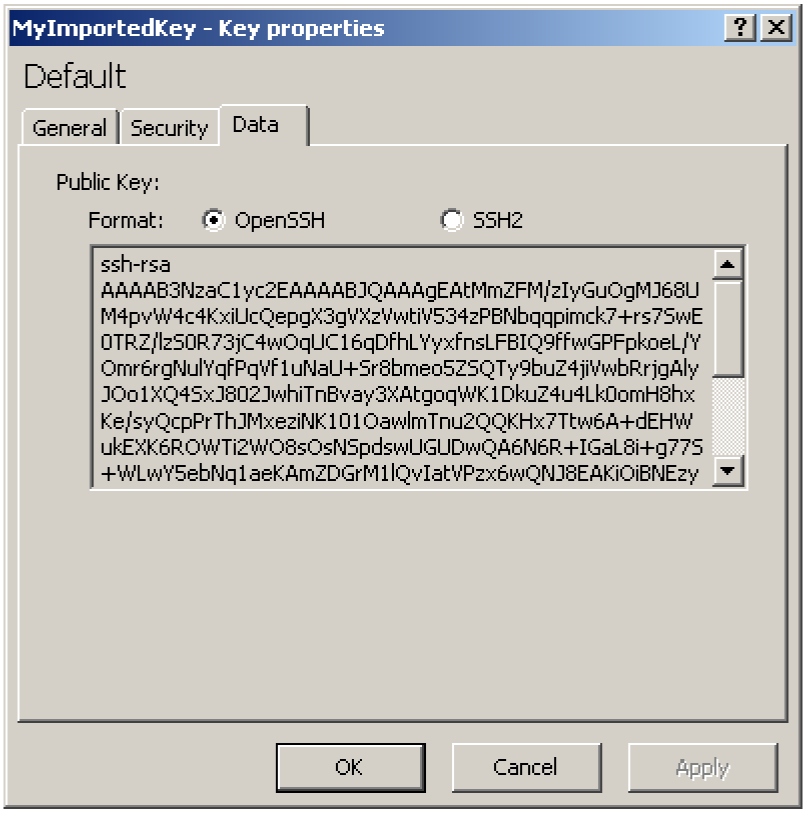
Key Size: 4096-bit

Fingerprint: 92:2c:78:46:a8:a9:f3:99:60:ee:37:59:3c:f1:e1:1ε

Created: 2011/05/03 10:00:05 AM By: AdminTest
Modified: 2011/05/03 10:00:05 AM By: AdminTest

6 On the **Security** page, enter those MessageWay users or groups that should have access to this key, and the type of access they should have. For more detailed information, refer to the topic, ***Configuring Object Security*** (on page 391).

7 On the **Data** page, select the format you want to use to view the public part of the key, OpenSSH or SSH2.



Public Key:

Format: ● OpenSSH ○ SSH2

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAgEAtMmZFM/zIyGuOgMJ68U
M4pvW4c4KxiUcQepgX3gVXzVwtiV534zPBNbqqpimck7+rs7SwE
0TRZ/lzS0R73jC4wOqUC16qDfhLYyxfnsLFBIQ9ffwGPFpkoeL/Y
Omr6rgNulYqfPqVf1uNaU+Sr8bmeo5ZSQTy9buZ4jiVwbRrjgAly
JOo1XQ4SxJ802JwhiTnBvay3XAtgoqWK1DkuZ4u4Lk0omH8hx
Ke/syQcpPrThJMxeziNK101OawlmTnu2QQKHx7Ttw6A+dEHW
ukEXK6ROWTi2WO8sOsNSpdswUGUDwQA6N6R+IGaL8i+g77S
+WLwY5ebNq1aeKAmZDGrM1lQvIatVPzx6wQNJ8EAKiOiBNEzy
```

8 Click **Apply** or **OK**.

Configuring an SFTP Location to Receive Messages Into MessageWay

To create an SFTP input site:

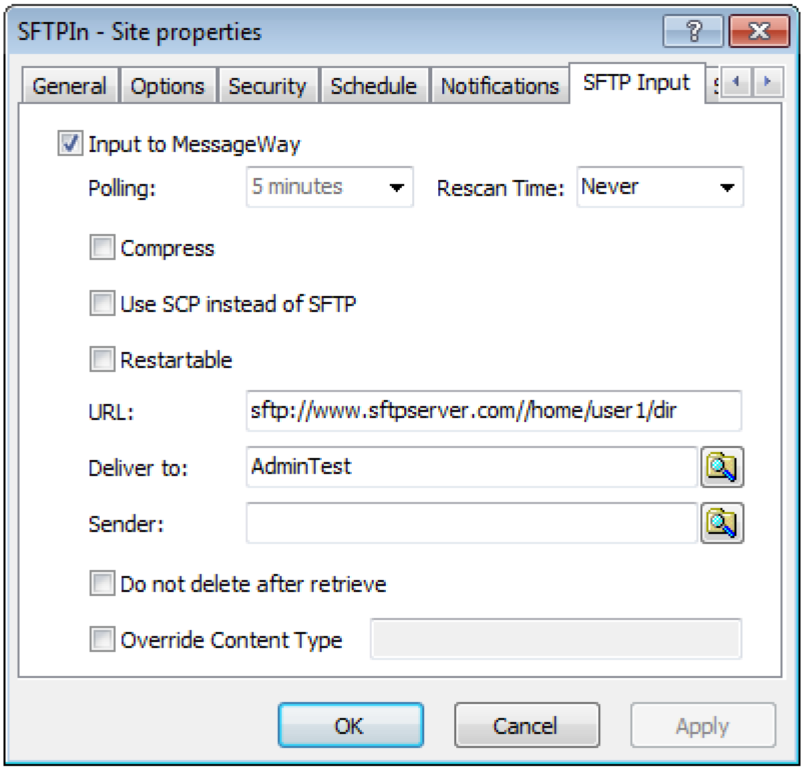
1 On the **SFTP Input** tab, check **Input to MessageWay**.

2 In the **URL** box, type a URL for the SFTP with a directory path server where you will retrieve messages. If you are to access a port other than 22, which is the default, type a colon after the URL, and then the port number.

3 In the **Deliver** box, enter a MessageWay location where you will deliver the messages.

4 To send traffic through an SFTP proxy server instead of directly to the SFTP server, refer to the topic, ***Configuring an SFTP Location to Use the SFTP Proxy Server*** (on page 650).

For more information about specific fields and values, refer to the reference topic, ***SFTP Input Page*** (on page 1157).



☑ Input to MessageWay

Polling: 5 minutes Rescan Time: Never

□ Compress

□ Use SCP instead of SFTP

□ Restartable

URL: sftp://www.sftpserver.com//home/user1/dir

Deliver to: AdminTest

Sender:

□ Do not delete after retrieve

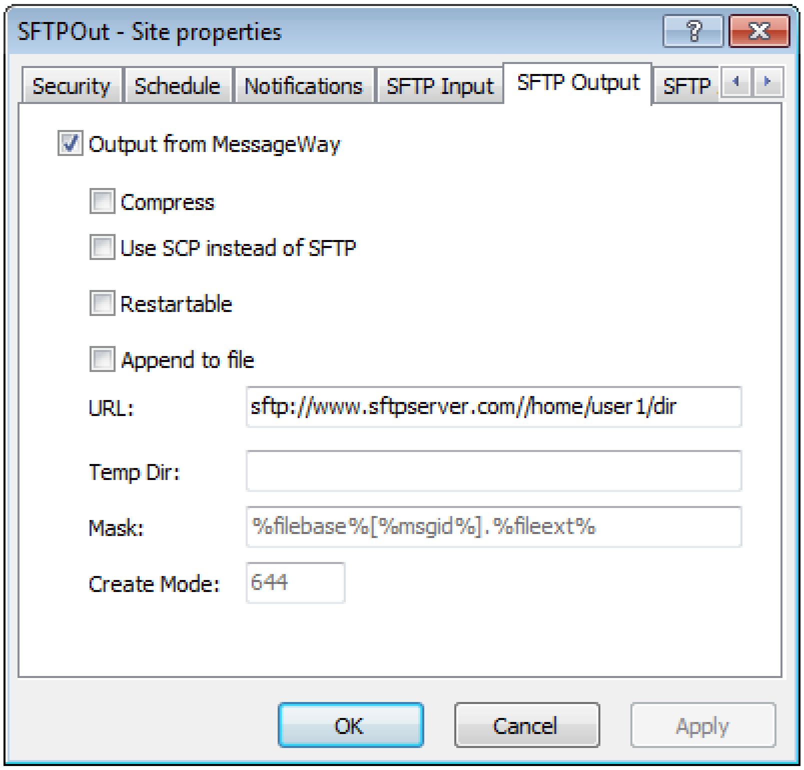
□ Override Content Type

Configuring an SFTP Location to Send Messages From MessageWay

To create an SFTP output site:

1. On the **SFTP Output** tab, check **Output from MessageWay**.
2. In the **URL** box, type a URL for the SFTP with a directory path server where you will send messages. If you are to access a port other than 22, which is the default, type a colon after the URL, and then the port number.
3. Make sure there is a value in the **Mask** box. If not, provide one to create a file name on the SFTP system. There should be one that is inherited from the SFTP adapter configuration.
4. Enter a numeric value in the **Create Mode** box to create the file with required rights.
5. To send traffic through an SFTP proxy server instead of directly to the SFTP server, refer to the topic, ***Configuring an SFTP Location to Use the SFTP Proxy Server*** (on page 650).

For more information about specific fields and values, refer to the reference topic, ***SFTP Output Page*** (on page 1163).



☑ Output from MessageWay

☐ Compress

☐ Use SCP instead of SFTP

☐ Restartable

☐ Append to file

URL: sftp://www.sftpserver.com//home/user1/dir

Temp Dir:

Mask: %filebase%[%msgid%].%fileext%

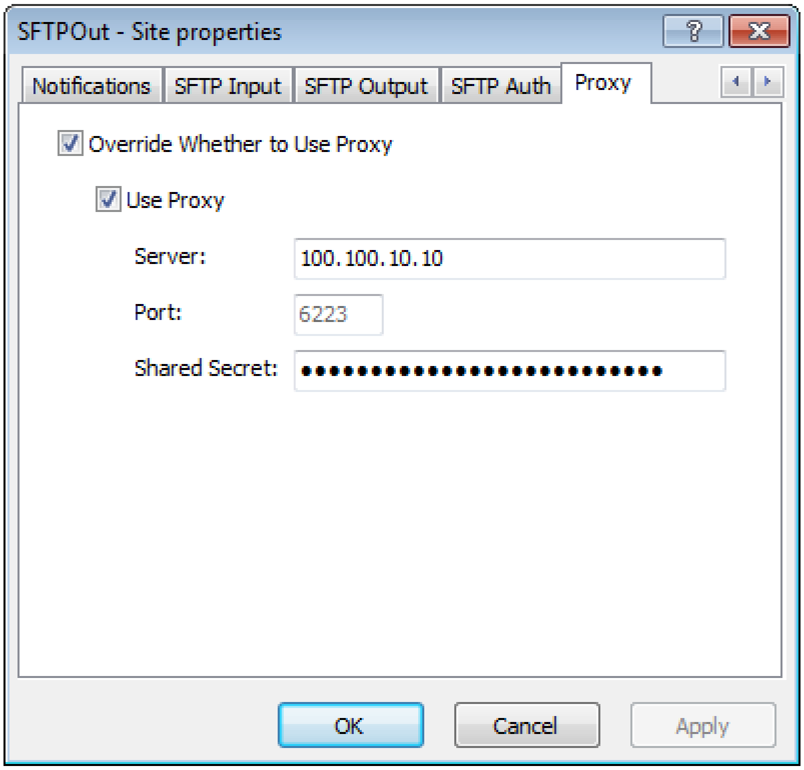
Create Mode: 644

Configuring an SFTP Location to Use the SFTP Proxy Server

The SFTP adapter can transfer information directly with an SFTP server or through the SFTP proxy server. To configure either an input or output SFTP location to use the SFTP proxy server, proceed as follows:

1. Assuming that the adapter does not configure the proxy server as a default, on the **Proxy** tab, check **Override Whether to Use Proxy**.
2. Check **Use Proxy**.
3. In the **Server** box, type the IP address of the proxy server.
4. In the **Port** box, type the port number of the proxy server.
5. In the **Shared Secret** box, type the ASCII string that the proxy server also uses, or copy the string from the ***proxy server configuration file*** (on page 366), mwproxy.conf.

For more information about specific fields and values, refer to the reference topic, ***SFTP, Proxy Page*** (on page 1170).



☑ Override Whether to Use Proxy

☑ Use Proxy

Server: 100.100.10.10

Port: 6223

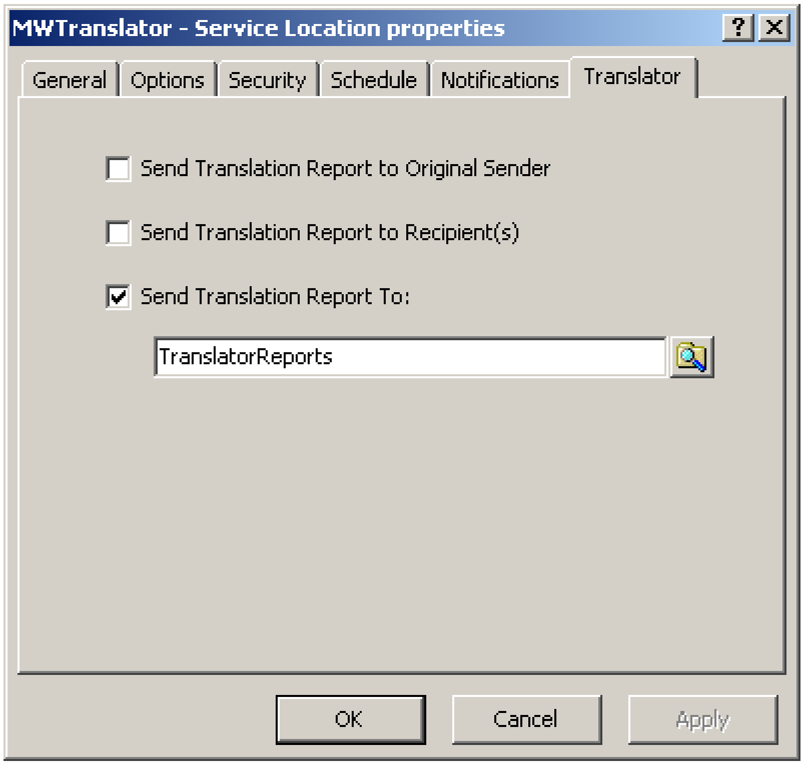
Shared Secret: ●●●●●●●●●●●●●●●●●●●●●●●●●●

Configuring a Translation Service Location

The MWTranslator service location parameters control where to send the translation reports generated during translation. Users must set these options when they want to send a translation report to a specific location. Configurations within the MW Translator Operator Program control when the translator will generate such reports and the type of information on the reports. For more information, refer to the *MW Translator Operator Guide and Reference*.

For more information about the translation process as it applies to MessageWay, refer to the topic in the "Options" section ***Translation Service*** (on page 902).

Typically, you would send the report to a pickup type mailbox, as in this example.



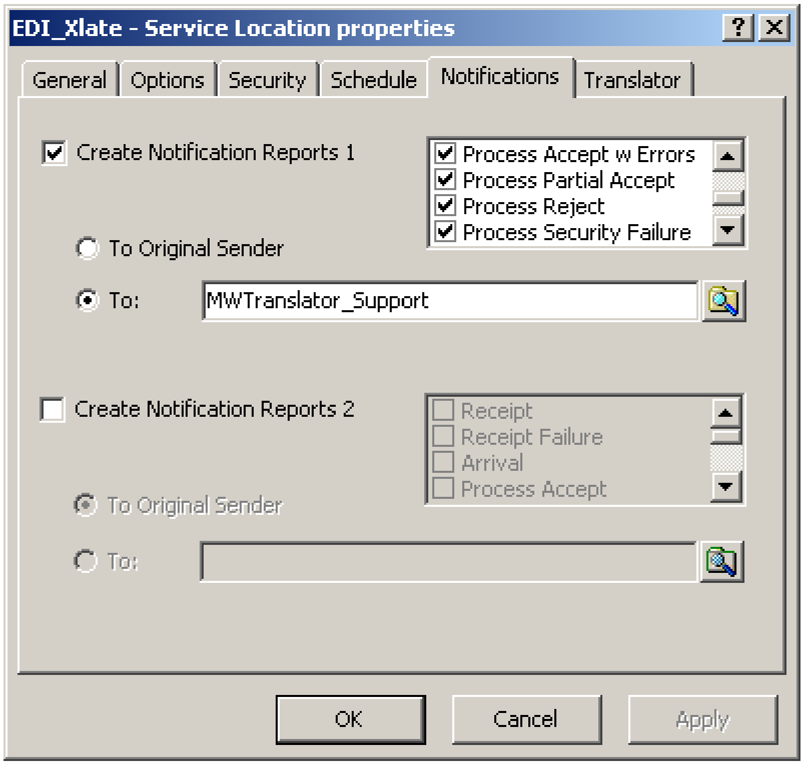
□ Send Translation Report to Original Sender

□ Send Translation Report to Recipient(s)

☑ Send Translation Report To:

TranslatorReports

Additionally, you may want to send a notification as an e-mail to alert the recipient of the translation error. This implies that a report is available in the pickup mailbox.



☑ Create Notification Reports 1

☑ Process Accept w Errors
☑ Process Partial Accept
☑ Process Reject
☑ Process Security Failure

○ To Original Sender

● To: MWTranslator_Support

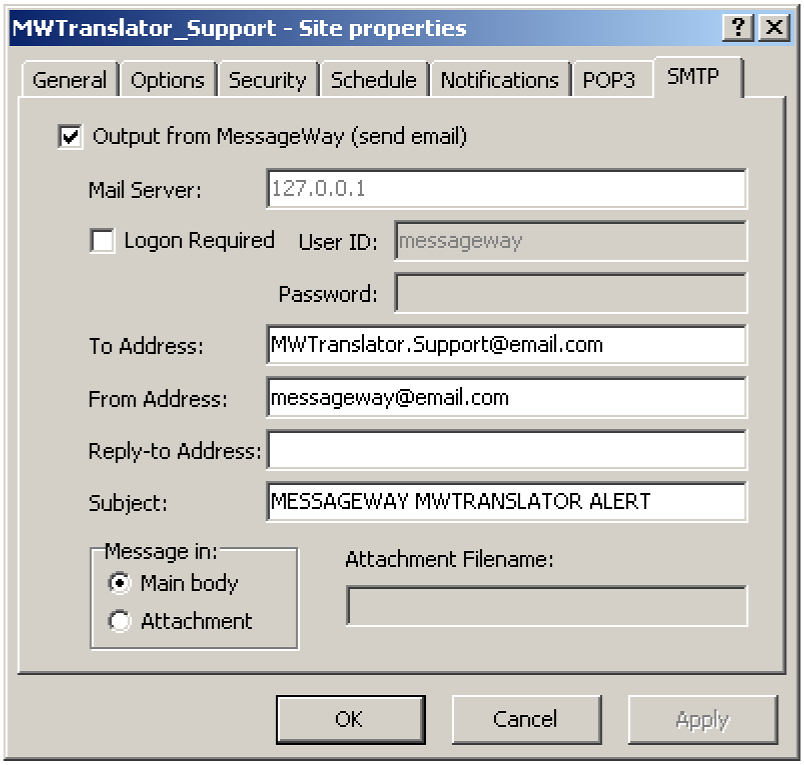
□ Create Notification Reports 2

□ Receipt
□ Receipt Failure
□ Arrival
□ Process Accept

● To Original Sender

○ To:

Here is an example of an e-mail recipient configuration.



MWTranslator_Support - Site properties
? ×
General | Options | Security | Schedule | Notifications | POP3 | SMTP
OK
Cancel
Apply

☑ Output from MessageWay (send email)

Mail Server: 127.0.0.1

□ Logon Required User ID: messageway

Password:

To Address: MWTranslator.Support@email.com

From Address: messageway@email.com

Reply-to Address:

Subject: MESSAGEWAY MWTRANSLATOR ALERT

Message in:
● Main body
○ Attachment

Attachment Filename:

NOTE: The MWTranslator service requires a license from Progress. You must have a license in order to start the service. Contact MessageWay Technical Support for more information.

Specifying Routing Addresses

MessageWay determines routing based on location configurations or addresses provided by a MessageWay process, such as MWTranslator. For more information about how MWTranslator determines addresses for messages it generates, refer to the *MW Translator User's Guide and Reference.*

Here, we discuss how MessageWay determines the routing for messages from its own configurations. Input messages will be routed to either a service location, an output site or a pickup mailbox. For delivery from MessageWay, messages must ultimately be sent to an output or pickup mailbox.

Syntax for Routing Addresses

Routing addresses may be simple, compound or a dynamic distribution list. A simple address is a name for a location of the type service, output site or pickup mailbox. A compound address comprises one or more service location names optionally followed by an output or pickup location, and possibly an external address. A dynamic distribution list allows users to send messages to multiple recipients instead of using the Distribution List service, where the recipients are static.

Routing addresses may be a maximum of 128 characters long. MessageWay uses the following syntax for routing addresses:

Component	Syntax
mw_address	*simple* **|** *compound* **|** *dynamic distribution list*
simple	*output site* **|** *service location* **|** *pickup mailbox*
compound	(*service location*:*mw_address*) | (*output_site*:*external_address*)
external_address	Depends on the adapter. Refer to the output information on the adapter page of location properties window, e.g. FTP, SMTP
dynamic distribution list	[**{Dist}**:]*simple*,*simple*,*simple*[,...]

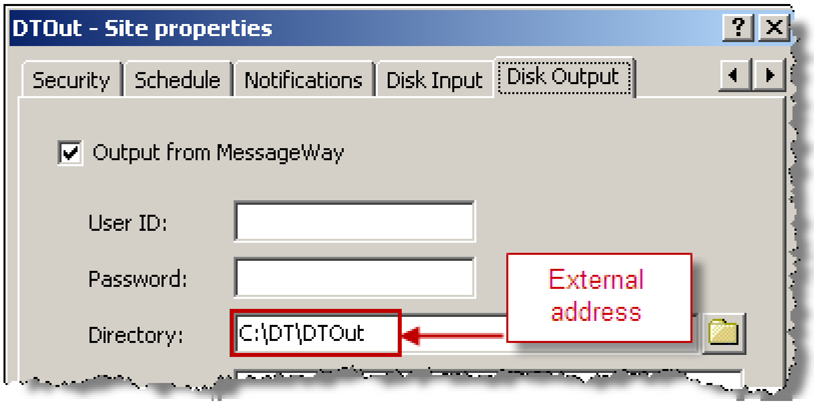
Examples of External Addresses

Output locations typically provide the external address information to complete delivery of the message. The type of external address depends on the adapter that delivers the message. As you will see, users may override the external address configured for the output site by modifying the delivery address on an input location. Therefore, it is important to understand the structure of external addresses.

The following table shows examples of external addresses for various types of adapters. It includes the field name for output information on the adapter page of a location properties window, where external addresses are typically entered.

Adapter Page	Field Name	Example
Disk Transfer	Deliver to	C:\DT\DTOut
FTP	URL	ftp.messageway.com
SMTP	To Address	you@yourdomain.com

The **Directory** box shows an external address used by the Disk Transfer adapter.



☑ Output from MessageWay

User ID:

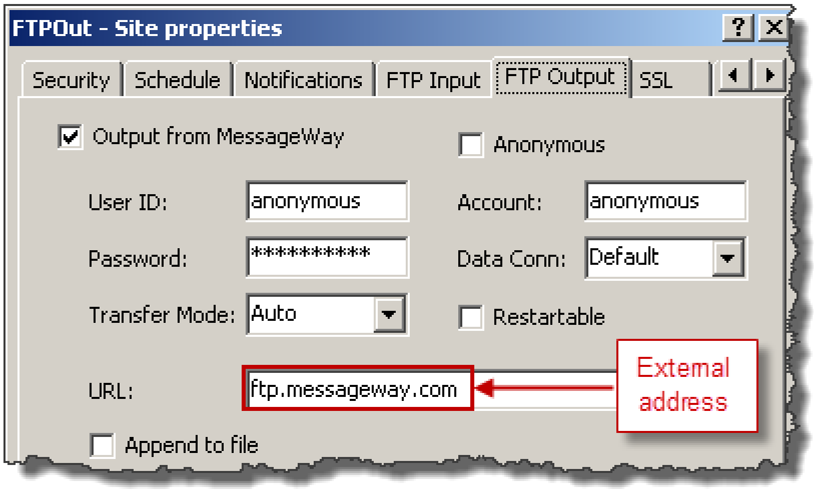
Password:

Directory: C:\DT\DTOut

External address

Example of an External Address for a Disk Transfer Site

The **URL** box shows an external address used by the FTP adapter.



☑ Output from MessageWay

□ Anonymous

User ID: anonymous

Account: anonymous

Password: **********

Data Conn: Default

Transfer Mode: Auto

□ Restartable

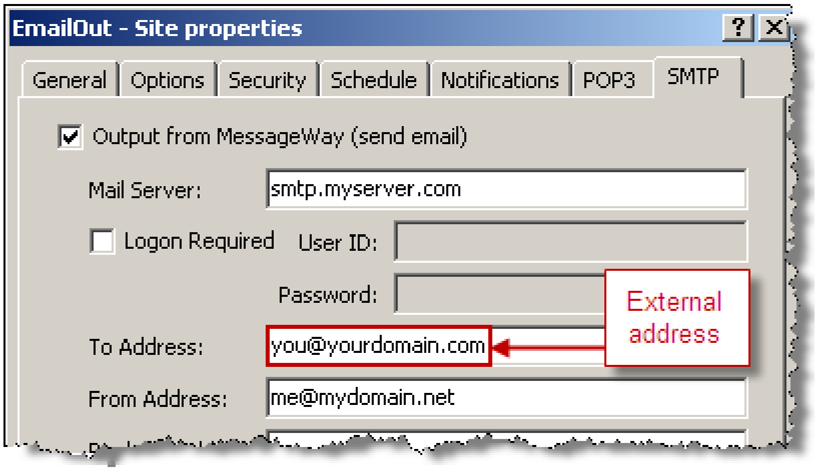
URL: ftp.messageway.com

□ Append to file

External address

Example of an External Address for an FTP Site

The **To Address** box shows an external address used by the E-mail adapter.



☑ Output from MessageWay (send email)

Mail Server: smtp.myserver.com

□ Logon Required User ID:

Password:

To Address: you@yourdomain.com

From Address: me@mydomain.net

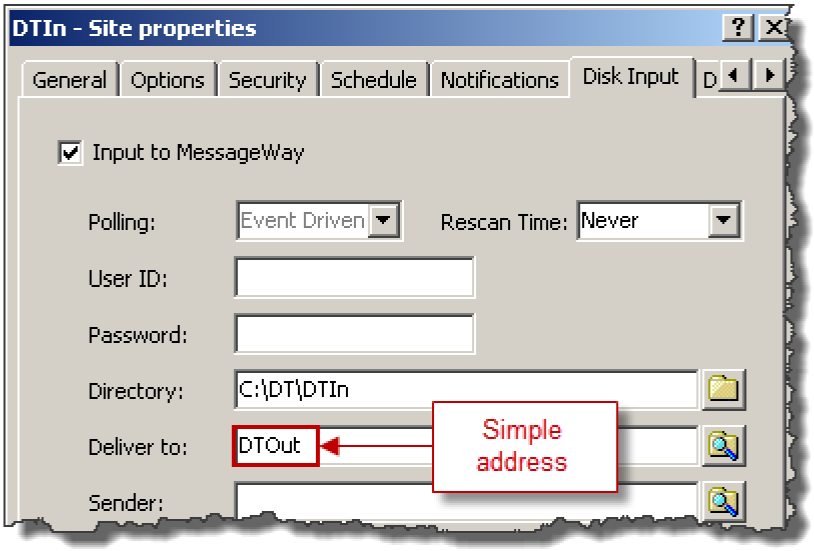
External address

Example of an External Address for an E-mail Site

Examples of Simple Routing Addresses

Simple routing addresses are specified in the configurations for an input location. The routing address may be either an output site or pickup location or a service location.

The following example shows an input site, DTIn, which routes messages to an output site, DTOut. The **Deliver To** box contains a simple routing address.



☑ Input to MessageWay

Polling: Event Driven Rescan Time: Never

User ID:

Password:

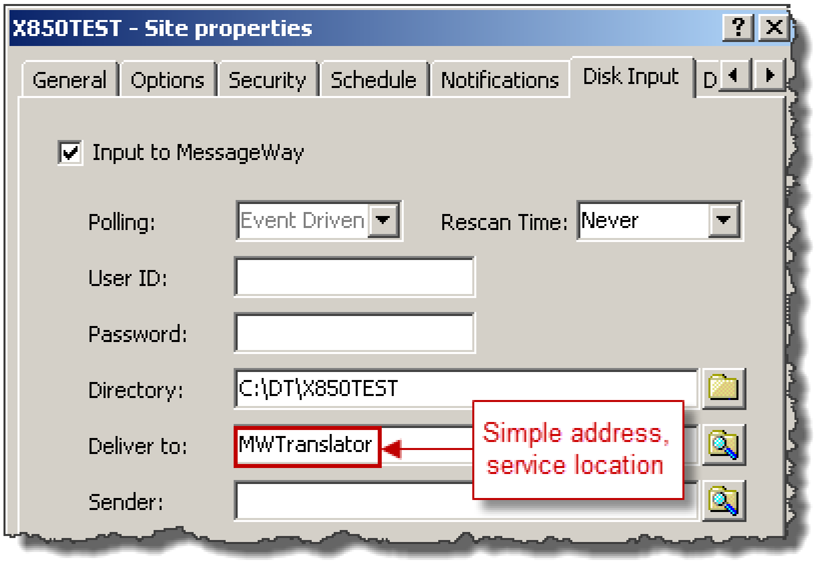
Directory: C:\DT\DTIn

Deliver to: DTOut

Sender:

Simple address

The following example shows an input site, X850TEST, which routes messages to a service location. The **Deliver To** box contains a simple routing address, MWTranslator. Remember that, typically, the output from MWTranslator service is determined by its own configurations.



☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

Password:

Directory: C:\DT\X850TEST

Deliver to: MWTranslator

Sender:

Simple address, service location

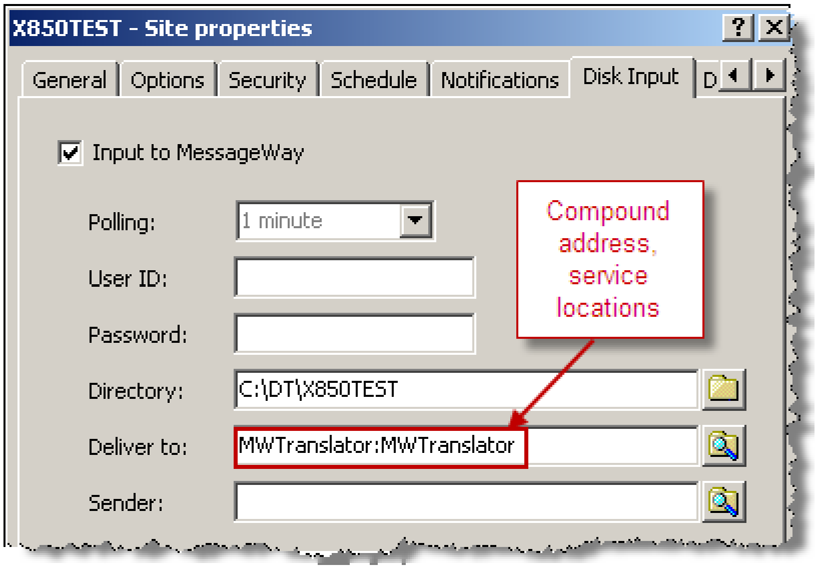
Examples of Compound Routing Addresses

Compound routing addresses allow users to perform the following:

- Concatenate processes to pass the output of one as the input to another (colons separate the processes)
- Override the output location(s) determined during processing
- Provide an external address from the input location in order to:
    - Override the external address configured for an output location, or
    - Provide an external address for a generic location

IMPORTANT: Overrides do not affect the routing of notifications, processing reports, or acknowledgments generated as a result of a service, such as MWTranslator. Overrides affect output messages only. When a status file is used for a custom I/O or custom processing location, the information in the status file will override a compound address routing.

The following example shows an input site, X850TEST, which sequentially routes messages to two service locations. Here, the **Deliver To** box contains a compound routing address, MWTranslator:MWTranslator. The service location, MWTranslator, is followed by another service location, MWTranslator. Using this compound address, the output from the first translation will be delivered back to MWTranslator. This allows users to easily configure multiple pass translations, for example.



☑ Input to MessageWay

Polling: 1 minute

User ID:

Password:

Directory: C:\DT\X850TEST

Deliver to: MWTranslator:MWTranslator

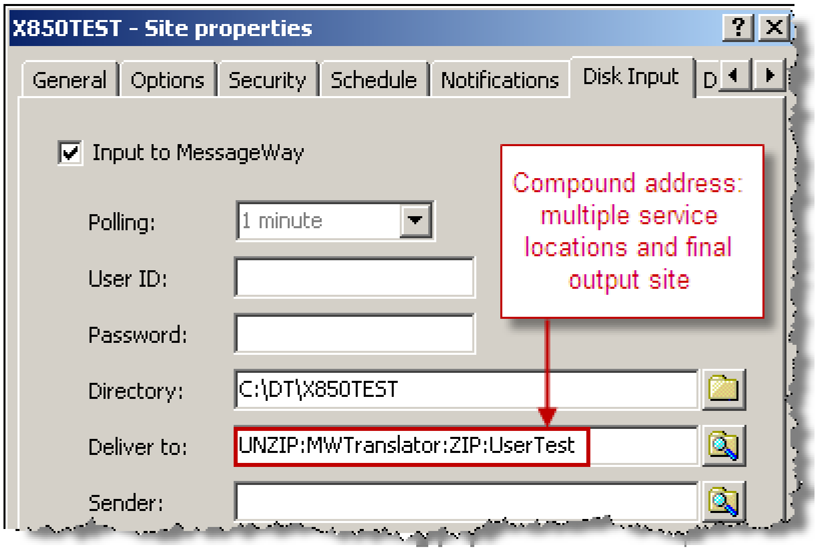
Sender:

Compound address, service locations

Example of Compound Address to Multiple Service Locations

The next example shows an input site, X850TEST, which routes messages to a series of service locations, and finally to an output site. The output is routed to an output site that is different from one supplied by the process. Here, the **Deliver To** box contains a compound routing address, UNZIP:MWTranslator:ZIP:UserTest, that will perform the following:

1. The message is sent to the UNZIP service location, where it is uncompressed.
2. The uncompressed message is sent to the MWTranslator service location for translation.
3. The output of translation is sent to the ZIP service location, where it is compressed.
4. The compressed message is sent to the output site, UserTest. Using this compound address, the output from MWTranslator will eventually be delivered to the output site, UserTest, instead of the location supplied by the MWTranslator process, TESTREC-MAILBOX. This functionality allows users to easily override routing of output normally determined by a service, such as MWTranslator.



☑ Input to MessageWay

Polling: 1 minute

User ID:

Password:

Directory: C:\DT\X850TEST

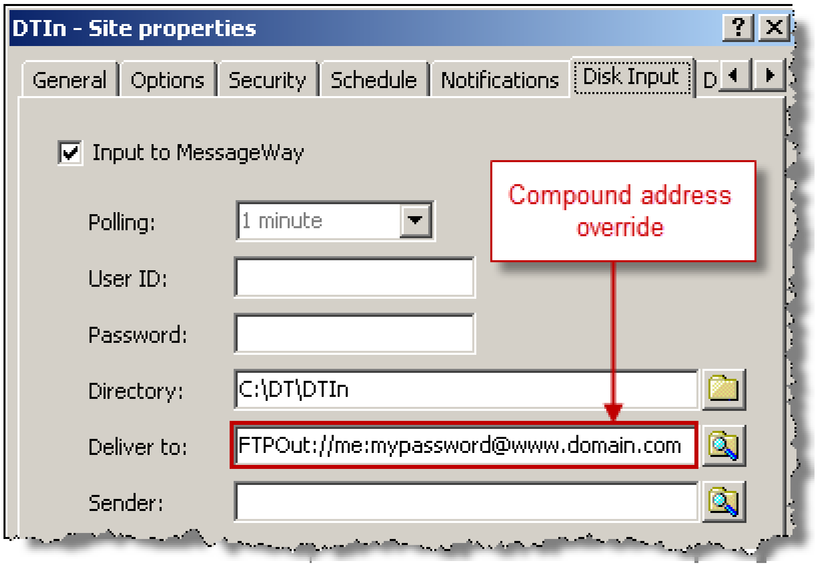
Deliver to: UNZIP:MWTranslator:ZIP:UserTest

Sender:

Compound address: multiple service locations and final output site

Example of Compound Address to Multiple Service Locations and Output Site

The next example shows an input site, DTIn, that routes messages to an output site using an external address to override the external address configured for the output site. Here, the **Deliver To** box contains a compound routing address, FTPOut://me:mypassword@www.domain.com. The output site, FTPOut, is followed by an FTP type URL. Using this compound address, the input messages picked up from disk by the Disk Transfer adapter will be delivered to the output site, FTPOut. The FTP adapter will use the logon and address supplied by the input site, instead of the logon and URL configured for the output site, FTPOut. This allows users to easily override routing normally configured for an output site.



☑ Input to MessageWay

Polling: 1 minute

User ID:

Password:

Directory: C:\DT\DTIn

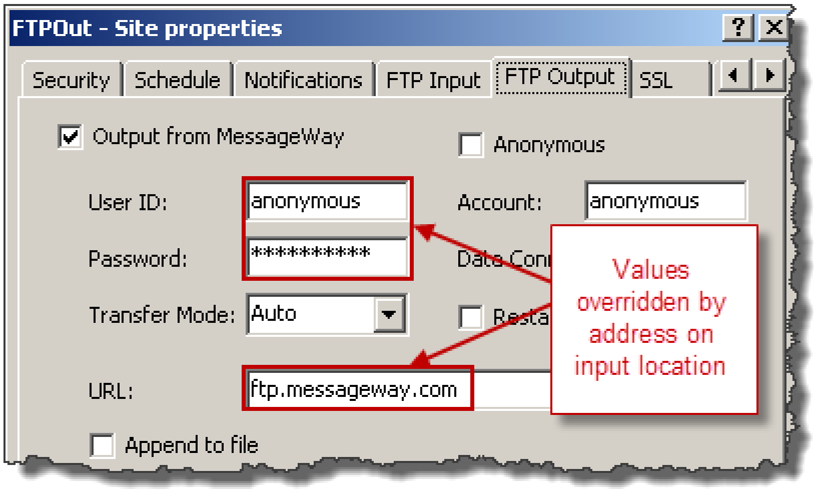
Deliver to: FTPOut://me:mypassword@www.domain.com

Sender:

Compound address override

Example of Compound Address Used to Override Output Site Address

The routing information on the output site, FTPOut, shown next, is overridden by the routing information on the input location, shown previously.



☑ Output from MessageWay

□ Anonymous

User ID: anonymous

Account: anonymous

Password: ***********

Data Con

Transfer Mode: Auto

□ Resta

URL: ftp.messageway.com

□ Append to file

Values overridden by address on input location

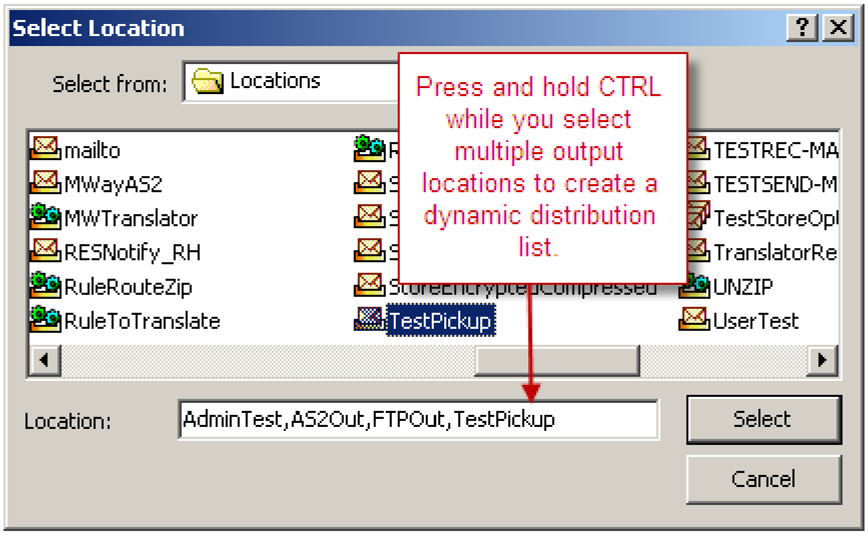
Example of Values on Output Site Overridden by Compound Address on Input Location

Examples of Dynamic Distribution List

Dynamic distribution lists may be used in any field that is capable of specifying a recipient. This is an alternative to a static distribution list users can configure for locations that use the ***Distribution List service*** (on page 596). In either case, the Distribution List service must be running.

NOTE: The {Dist}: part of the syntax is optional. If {Dist}: is not present, it is added to the address during processing.

To create a dynamic distribution list, we can type a list of recipients or select the browse button and select recipients. When you use the browse button, from the **Select Location** dialog box, click and hold **CTRL** while you select destination locations. You can also type a list of recipients, separated by commas in the dialog box.

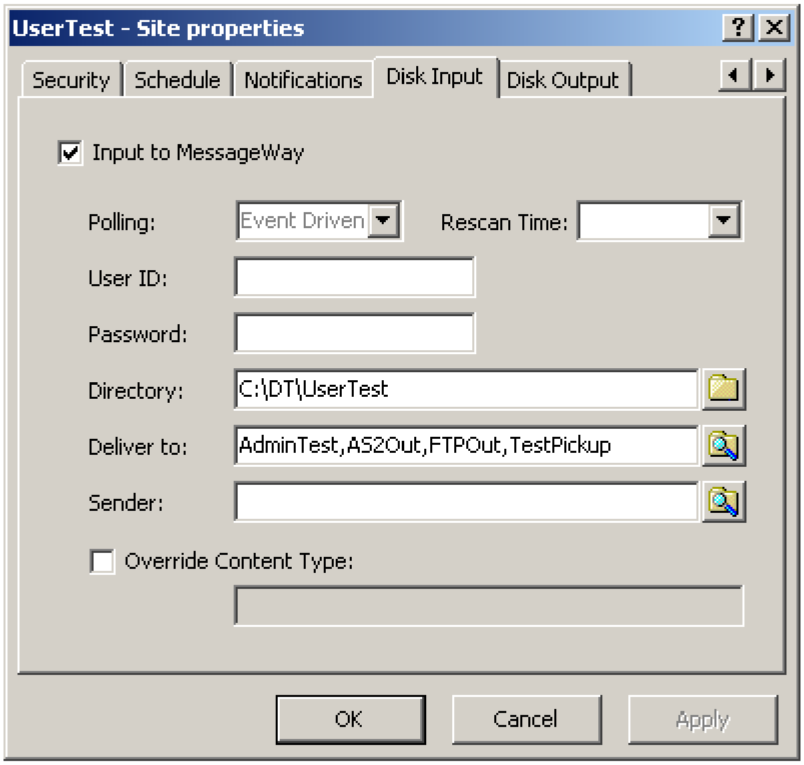


Press and hold CTRL while you select multiple output locations to create a dynamic distribution list.

Select from: Locations

Location: AdminTest,AS2Out,FTPOut,TestPickup

The list appears in the recipient box of the location's input page.



☑ Input to MessageWay

Polling: Event Driven

Rescan Time:

User ID:

Password:

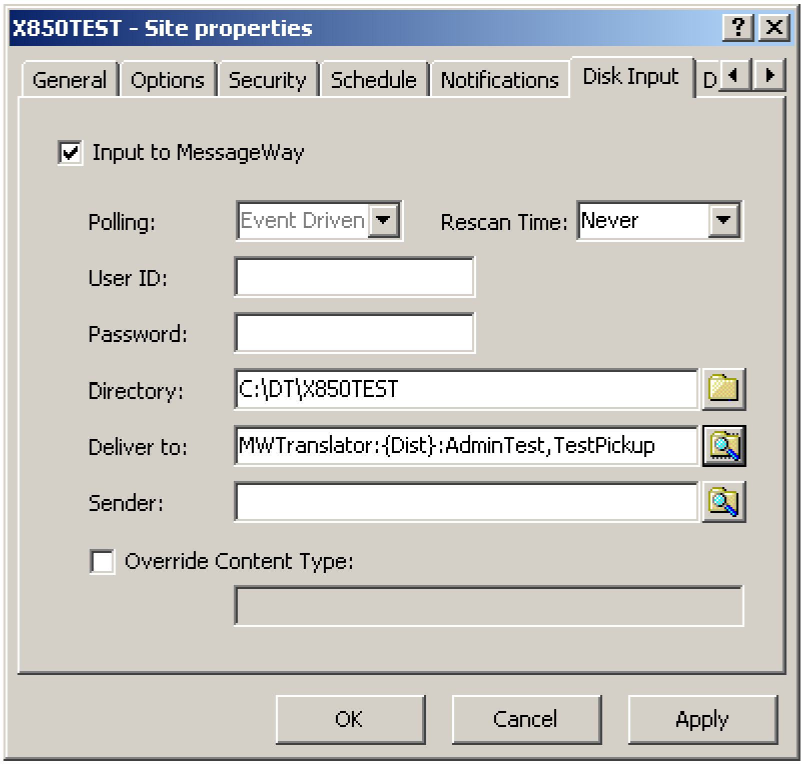
Directory: C:\DT\UserTest

Deliver to: AdminTest,AS2Out,FTPOut,TestPickup

Sender:

☐ Override Content Type:

You can also add a dynamic distribution list to the end of a compound address. In the following example, a file was sent to MWTranslator, and the delivery location of the output that would normally be determined by configurations in the translator, was overridden, and the output was sent to the distribution list instead.



X850TEST - Site properties

☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

Password:

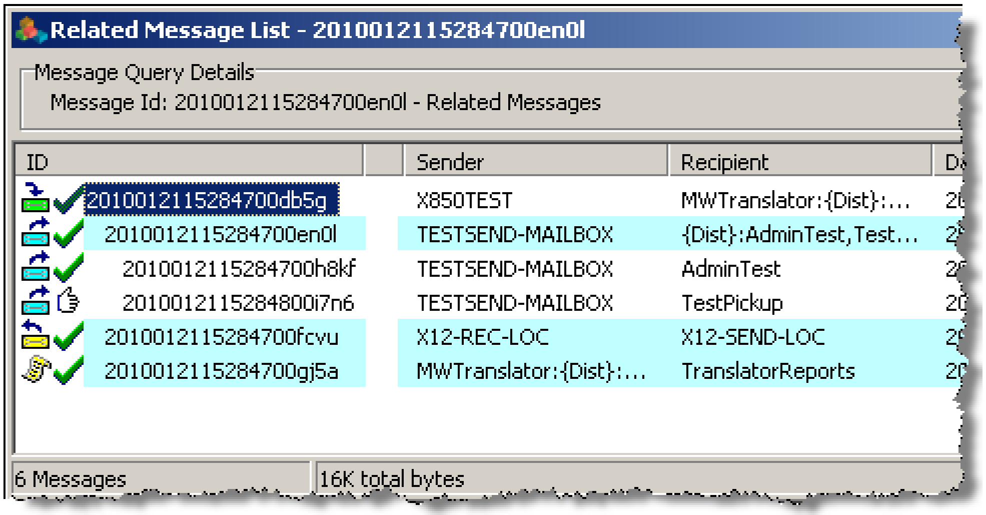
Directory: C:\DT\X850TEST

Deliver to: MWTranslator:{Dist}:AdminTest,TestPickup

Sender:

□ Override Content Type:

If you select the input message from a message list and click **Get Related**, you will see that the output has been sent to the distribution list, rather than TESTREC-MAILBOX, which is what the translator would have used.



Related Message List - 2010012115284700en0l

Message Query Details

Message Id: 2010012115284700en0l - Related Messages

ID	Sender	Recipient	D
✓ 2010012115284700db5g	X850TEST	MWTranslator:{Dist}:...	2
✓ 2010012115284700en0l	TESTSEND-MAILBOX	{Dist}:AdminTest,Test...	2
✓ 2010012115284700h8kf	TESTSEND-MAILBOX	AdminTest	2
2010012115284800i7n6	TESTSEND-MAILBOX	TestPickup	2
✓ 2010012115284700fcvu	X12-REC-LOC	X12-SEND-LOC	2
✓ 2010012115284700gj5a	MWTranslator:{Dist}:...	TranslatorReports	2

6 Messages | 16K total bytes

Using Generic Locations for Routing

Typically, users create locations to deliver messages to specific external addresses. There are instances where users may want to create locations that allow delivery of different external addresses at different times. In fact, users may create generic locations to accomplish such delivery.

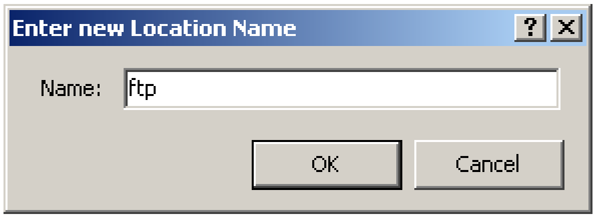
Configuring a Generic Location

Generic locations are output locations that have no specific external address. Users supply external addresses from input locations configurations or as the result of a service, such as MWTranslator. The **To Address** is used to collect problem e-mails that are not properly configured on the input location.

How to Create a Generic FTP Site

1 Create a location whose name is generic.

For instructions to create a location, refer to the topic, ***How to Create a Location*** (on page 461).

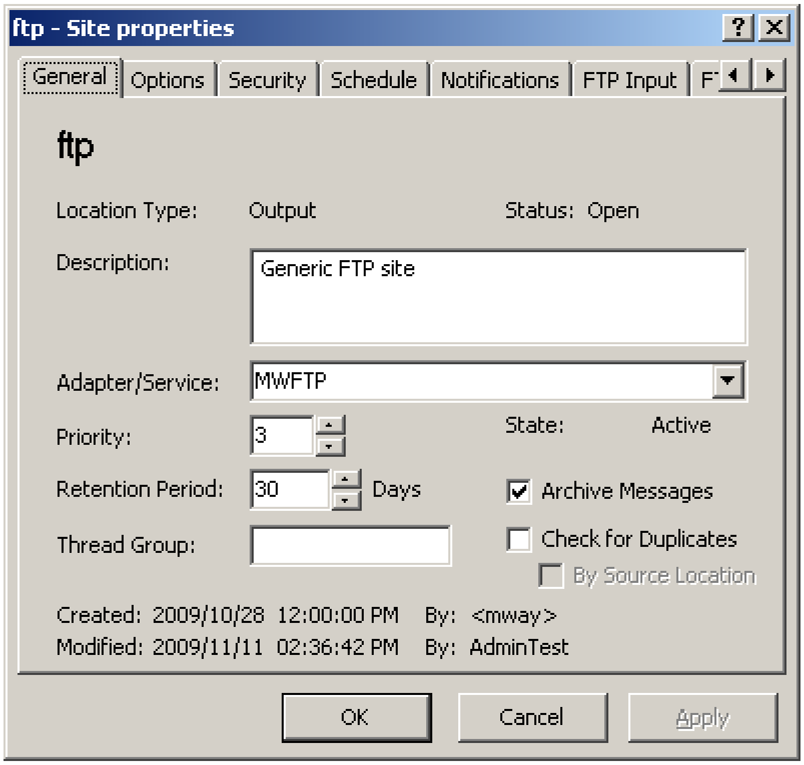


Enter new Location Name

Name: ftp

2 Type a description indicating the purpose of the location, such as, **Generic FTP site**.

3 Select the FTP adapter for this location.



ftp

Location Type: Output

Status: Open

Description: Generic FTP site

Adapter/Service: MWFTP

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

□ Check for Duplicates

□ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

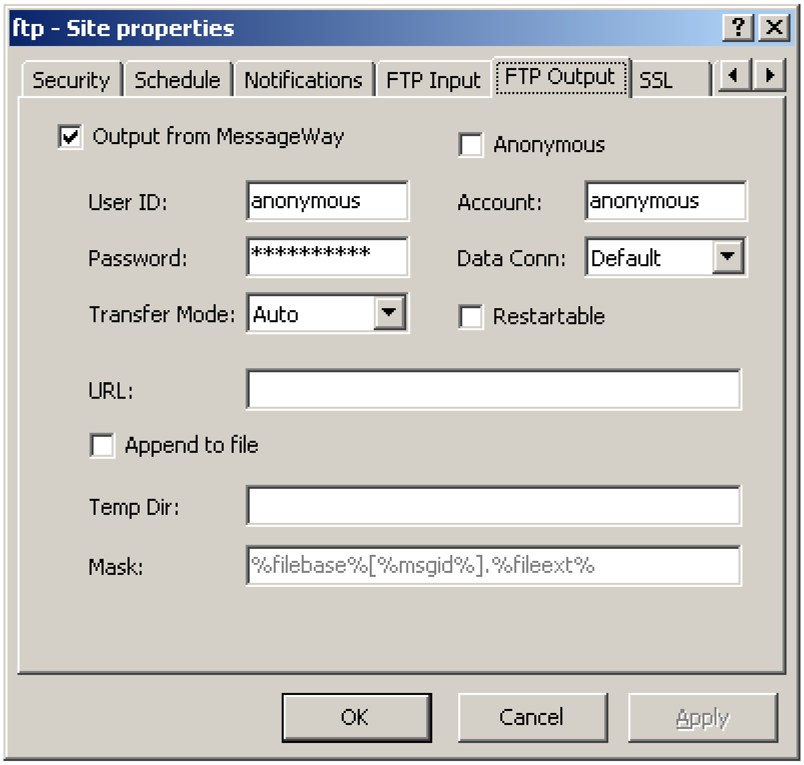
Modified: 2009/11/11 02:36:42 PM By: AdminTest

4 On the **Schedule** page, use the default schedule, **Open**.

5 On the **FTP Output** page:

a) Check the box, **Output from MessageWay**.

b) To override a default mask inherited from the FTP adapter configuration, ***enter a mask*** (on page 1137) to create a file name for the output file(s). A dimmed mask value indicates it is inherited. Leave the URL blank to send any invalid messages to the system mailbox, {Unknown}.



ftp - Site properties

☑ Output from MessageWay

☐ Anonymous

User ID: anonymous

Account: anonymous

Password: ***********

Data Conn: Default

Transfer Mode: Auto

☐ Restartable

URL:

☐ Append to file

Temp Dir:

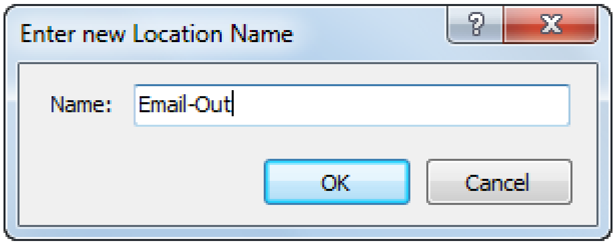
Mask: %filebase%[%msgid%].%fileext%

6 Select **Apply** or **OK** to save your configurations.

How to Configure a Generic E-mail Site

1 Create a location whose name is generic.

For instructions to create a location, refer to the topic, ***How to Create a Location*** (on page 461).

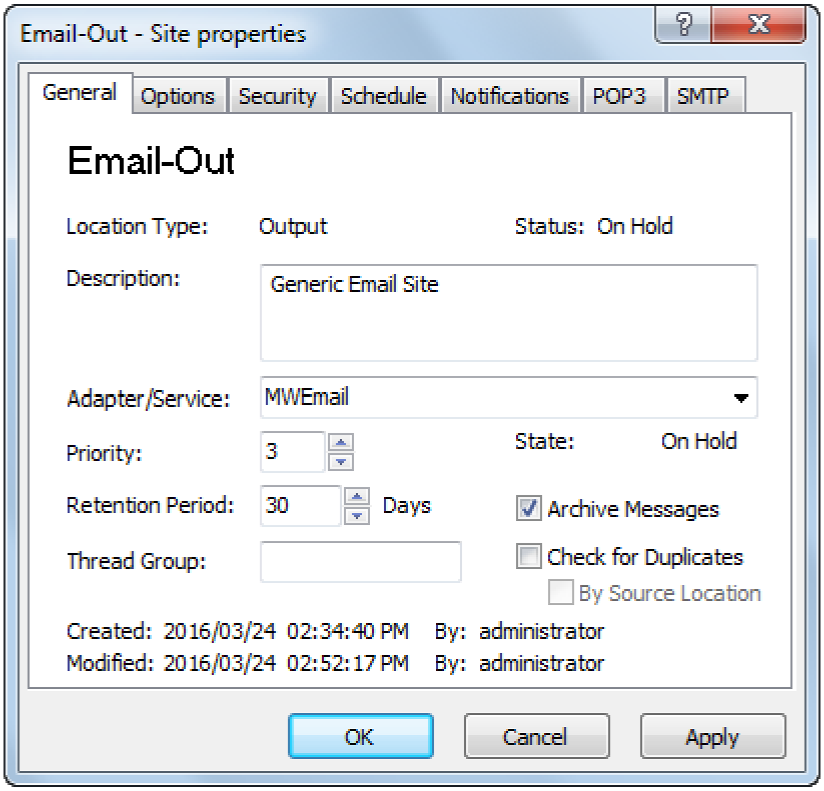


Enter new Location Name

Name: Email-Out

2 Type a description indicating the purpose of the location, such as, **Generic E-mail Site**.

3 Select the E-mail adapter for this location.



Email-Out

Location Type: Output

Status: On Hold

Description: Generic Email Site

Adapter/Service: MWEmail

Priority: 3

State: On Hold

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

☐ By Source Location

Created: 2016/03/24 02:34:40 PM By: administrator

Modified: 2016/03/24 02:52:17 PM By: administrator

4 On the **Schedule** page, use the default schedule, **Open**.

5 On the **SMTP** page,

a) Check the box, **Output from MessageWay**.

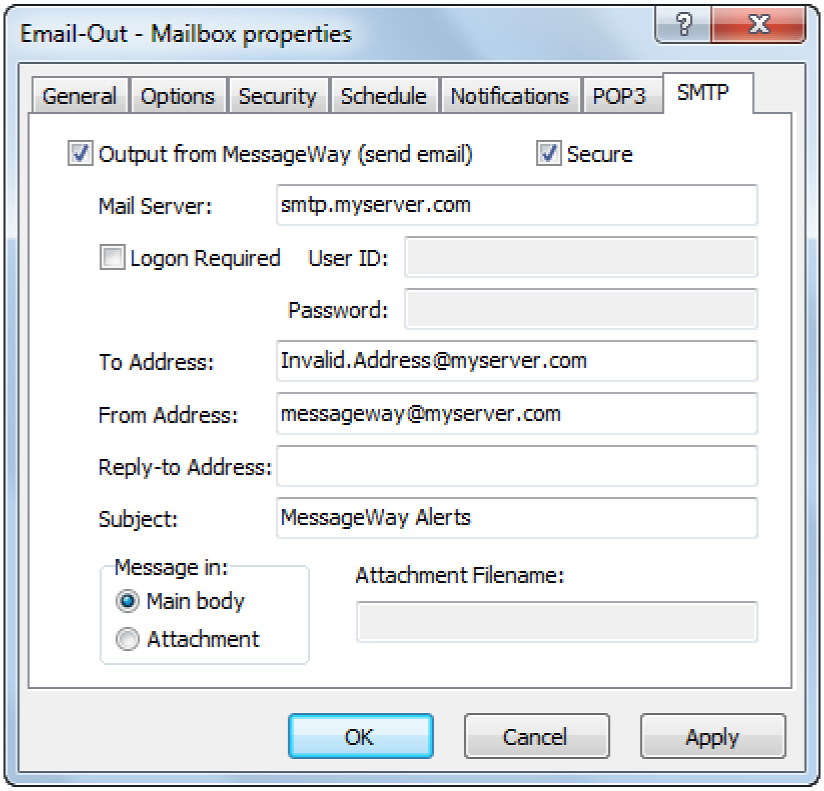
b) Check the box, **Secure**, to enable a secure SMTP connection to the e-mail server you want to connect to.

c) If required, check the **Logon Required** box, and enter a valid user ID and password.

d) In the **To Address**, type an e-mail address for a default location where you can collect problem e-mails.

e) In the **From Address** box, type a generic address that will be acceptable to your recipients.

f) Select **Main Body** for the location of the message.



Email-Out - Mailbox properties

☑ Output from MessageWay (send email) ☑ Secure

Mail Server: smtp.myserver.com

□ Logon Required User ID:

Password:

To Address: Invalid.Address@myserver.com

From Address: messageway@myserver.com

Reply-to Address:

Subject: MessageWay Alerts

Message in:
● Main body
○ Attachment

Attachment Filename:

6 Select **Apply** or **OK** to save your configurations.

Examples of Using Generic Locations

Once you have created a generic location, you may supply an external address from either an input site or from a process, such as MWTranslator.

How to Send Messages Using a Generic FTP Site

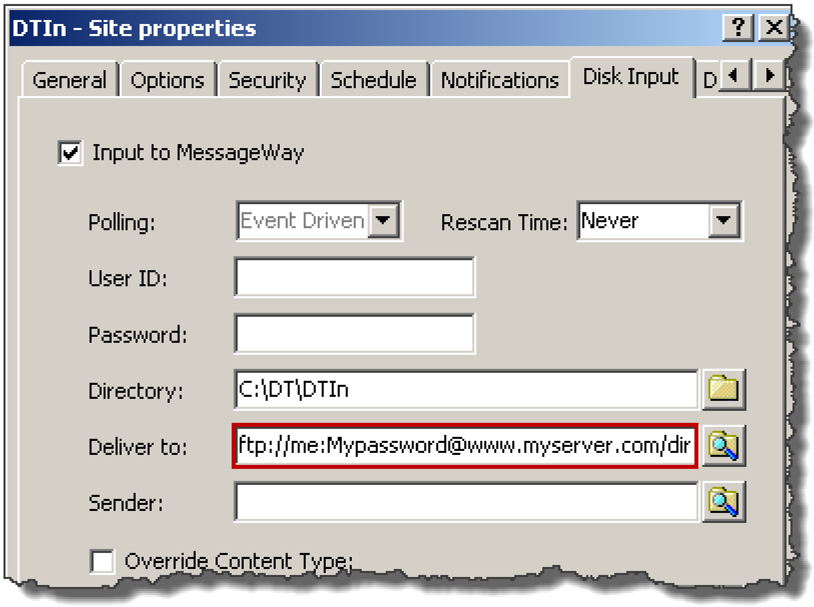
1 Make sure you have created a generic FTP site.

For instructions, refer to the topic, ***How to Create a Generic FTP Site*** (on page 663).

2 On the **Disk Input** page of the input location configuration, type an appropriate routing address in the **Deliver To** box.

- For the syntax of a MessageWay address, refer to the topic, ***Syntax for Routing Addresses*** (on page 653).

- For the syntax of an input URL, refer to the topic, ***URL (Input)*** (on page 1128).



☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

Password:

Directory: C:\DT\DTIn

Deliver to: ftp://me:Mypassword@www.myserver.com/dir

Sender:

☐ Override Content Type:

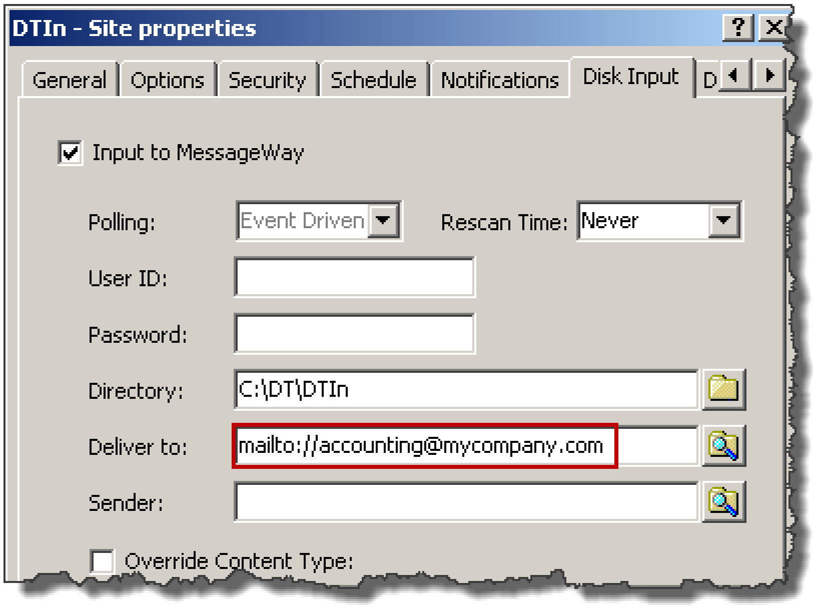
The result will be as follows:

1. The Disk Transfer adapter will deliver messages to the FTP generic site, as specified by the **ftp:** in the routing address, passing the remaining information to the FTP adapter.
2. The FTP adapter will ignore the forward slashes, **//**, in the address and attempt to connect to the server using the URL, **www.myserver.com**, logon user ID and password, **me:MyPassword**, and deposit the file in the directory, **dir**.

How to Send Messages Using a Generic E-mail Site

1. Make sure you have created a generic e-mail location. For instructions, refer to the topic, ***How to Configure a Generic E-mail Site*** (on page 665).
2. On the adapter page of the input location configuration, enter an appropriate routing address in the **Deliver To** box.
   - For the syntax of a MessageWay address, refer to the topic, ***Syntax for Routing Addresses*** (on page 653).

- For the syntax of an output e-mail address, refer to the topic, ***Email Output Options*** (on page 603).



☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

Password:

Directory: C:\DT\DTIn

Deliver to: mailto://accounting@mycompany.com

Sender:

☐ Override Content Type:

The result will be as follows:

1 The Disk Transfer adapter will deliver messages to the MAILTO generic location, as specified by the **mailto:** in the routing address, passing the remaining information to the E-mail adapter.

2 The E-mail adapter will attempt to connect to the SMTP server, **smtp.myserver.com**, provided in the MAILTO site configuration, and send the message to the e-mail address, **accounting@mycompany.com**. The From Address is provided by the MAILTO site configuration.

This page intentionally blank.

Configuring Receipt Monitor

The Receipt Monitor monitors incoming messages based on configured criteria and responds with notifications. This is useful when you expect to receive time-critical information. It includes the following configurable entities:

- Holiday Schedules, configured by the user
- Master Receipt Schedules, configured by the user
- Receipt Schedules, configured by the user

Overview of Receipt Monitor

Receipt Monitor provides users a way to monitor the number of messages received from a particular inbound address within a period of time. Receipt Monitor will log an event in the Event Log and optionally send a notification message to a location. Users may specify the period of time in a receipt schedule, the number of messages required during the period to trigger a notification event, and the type of event that will be triggered.

Understanding the Receipt Monitor Process

Receipt Monitor provides:

- Ability to monitor message traffic for an inbound address
- Ability to specify a time period for the receipt
- Ability to exempt holidays from the monitor process

Receipt Monitor uses schedules that are associated with the inbound address. The type of address depends on the adapter used to transfer the message to MessageWay. The address might be a MessageWay location, a Uniform Resource Locator (URL) for the Web, an e-mail address, or a file name.

So, consider the following:

- A receipt schedule name is not necessarily the same as a location name.
- A receipt schedule name must match the sender of a message as determined by MessageWay.
- Therefore, a sender's address does not have to be the same as the name of the input location.

Since a sender's address may be different than the name of the input location, you can set up one receipt schedule to monitor one or more input locations with various names, as long as the sender of a message as determined by MessageWay matches the sender's address. MessageWay uses various strategies to determine the sender of a message, which we explain in the following configuration information.

Configuring Receipt Monitor

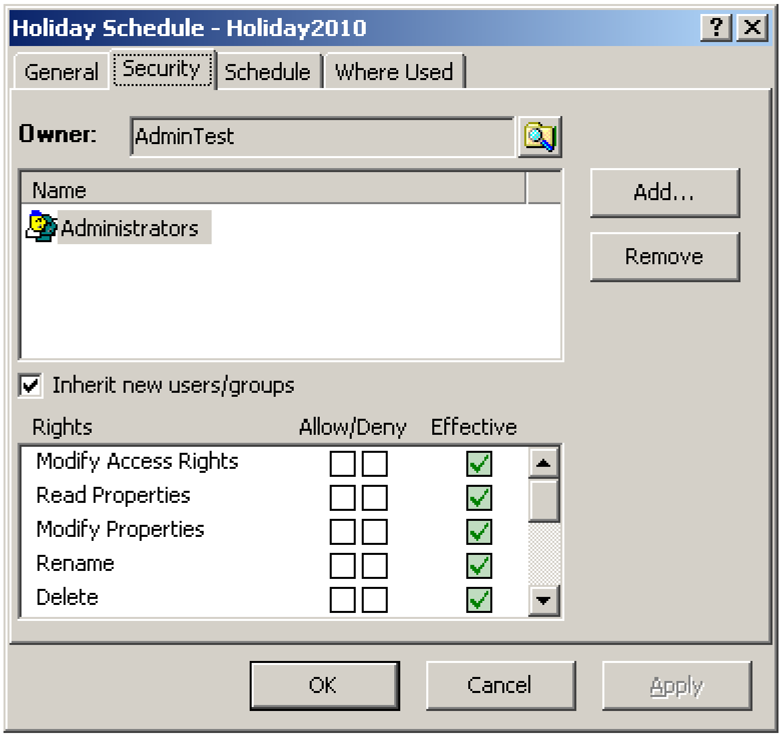
This section describes how to configure a special monitor for incoming messages, called the Receipt Monitor.

Specifying User Security for Receipt Monitor

Who is able to access the configurations and what they are able to do is shown on the **Security** page of the properties window for the schedule. Schedules reside in folders. Security settings for a schedule may be inherited from its parent folder. For basic instructions to view the properties of a folder, refer to ***How to View Properties*** (on page 1214).

Security settings for holiday schedules, master receipt schedules and receipt schedules are similar. Here we talk about security for a holiday schedule, but it is the same for master receipt schedules and receipt schedules

The following example shows the default security settings for the Holiday2010 schedule, which has inherited its rights from the **Holiday Schedules** folder. The Effective column shows what rights have been inherited, if any, and the result of any overrides.



Holiday Schedule - Holiday2010

General | Security | Schedule | Where Used

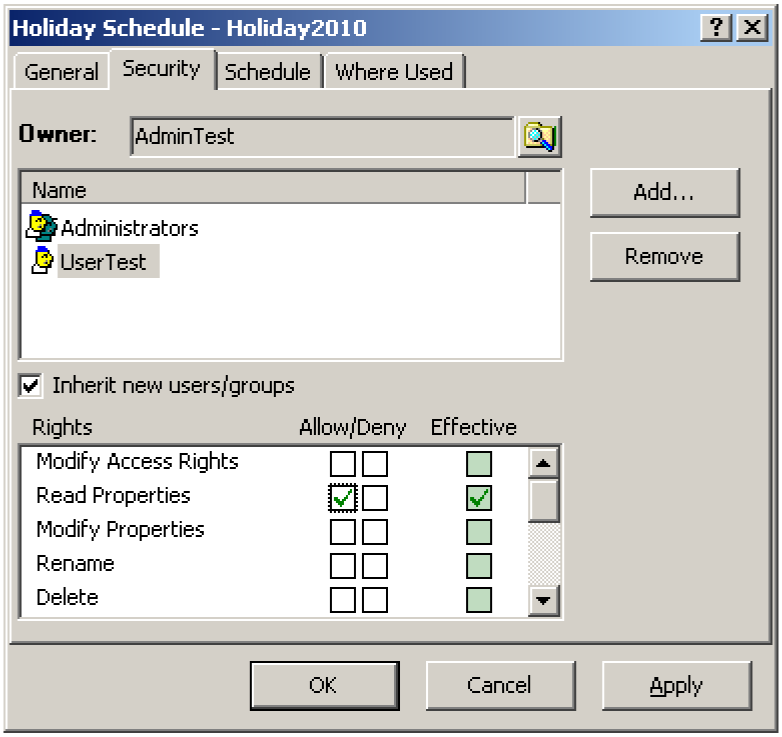
Owner: AdminTest

Name
Administrators

☑ Inherit new users/groups

Rights	Allow/Deny		Effective
Modify Access Rights	□	□	✓
Read Properties	□	□	✓
Modify Properties	□	□	✓
Rename	□	□	✓
Delete	□	□	✓

You may override the user's security settings for a schedule by checking items in the Allow/Deny boxes, whether they are inherited or not. For example, when you add a user to the Name list called UserTest, you can give this user specific rights. In this example we have given UserTest the right to Read Properties. To add a user or group to a security list, refer to ***How to Add Users or Groups to a Security Access List*** (on page 395). To add effective rights for an object, see ***How to Override Rights on a Security Access List*** (on page 395).



Owner: AdminTest

Name
Administrators
UserTest

☑ Inherit new users/groups

Rights	Allow/Deny	Effective
Modify Access Rights	□ □	🟩
Read Properties	☑ □	✓
Modify Properties	□ □	🟩
Rename	□ □	🟩
Delete	□ □	🟩

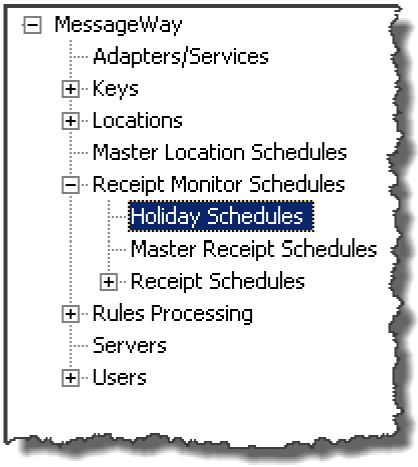
Configuring Holiday Schedules

Configuring and using holiday schedules is optional. Holiday schedules allow users to identify days when no processing should occur. You may select from all days of all months of all years, so you may create them for fiscal years or calendar years or multiples of these. Holiday schedules may be applied to a receipt schedule to exclude holidays from the schedule of events.

Creating a Holiday Schedule

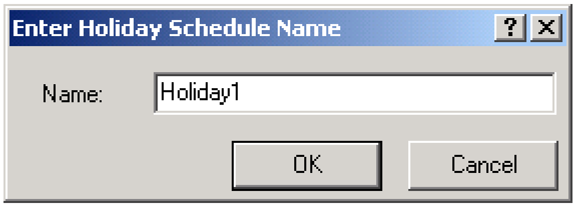
To create a holiday schedule, proceed as follows:

1 From the left pane of MessageWay Explorer, expand the **Receipt Monitor Schedules folder** and select **Holiday Schedules**.



2 From the menu bar, select the Schedules menu and then the **Add Schedule** command. The **Enter Holiday Schedule Name** dialog box appears.

3 Enter a name for the holiday schedule, and select **OK** to create the schedule and close the window.



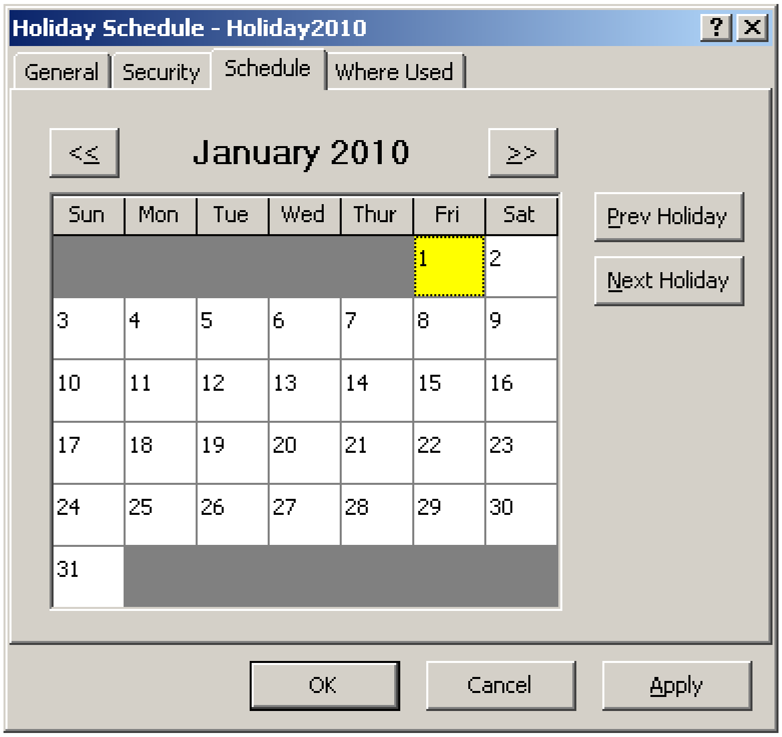
Name: Holiday1

The schedule appears in the right pane of MessageWay Explorer, and the properties window opens to configure the schedule.

Specifying a Holiday Schedule

You may create a schedule for any day of any year. To page through the months of the calendar, use the Previous button << and the Next button >>. To focus on the holiday defined before your current location, select the **Prev Holiday** button. To focus on the holiday defined after your current location, select the **Next Holiday** button.

Double-click the left button to select or deselect a day on the calendar as a holiday. Days selected as holidays appear in yellow.

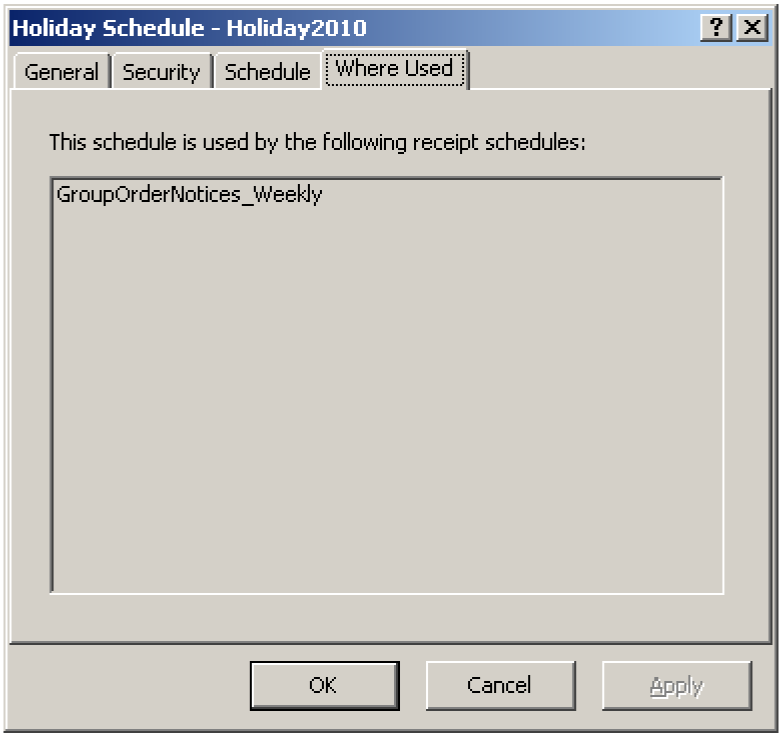


Sun	Mon	Tue	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Schedule Page (Receipt Monitor, Holiday Schedule Window)

Determining Where a Holiday Schedule Is Used

It is helpful to determine where a particular holiday schedule is used, in case you want to understand the effect of changes you make. Receipt Monitor maintains this information, and you may view it on the **Where Used** page of the Holiday Schedule window.



This schedule is used by the following receipt schedules:

GroupOrderNotices_Weekly

Where Used Page (Receipt Monitor, Holiday Schedule Window)

Configuring Master Receipt Schedules

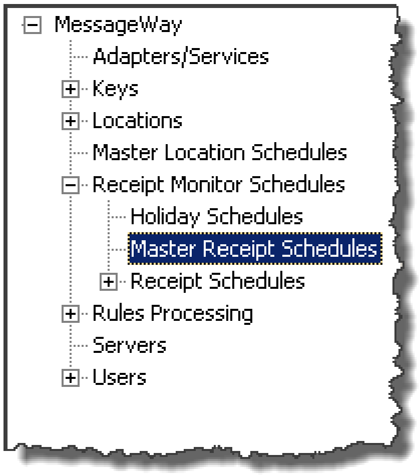
Configuring and using master schedules is optional. Master schedules allow users to specify a primary, master schedule as the basis of a receipt schedule, which then may or may not require modification.

IMPORTANT: When you customize a receipt schedule, the receipt schedule is detached from the master to allow you to make changes. Therefore, any subsequent changes made to the master schedule will not be reflected in the receipt schedule. If you decide to add a master schedule to an existing receipt schedule, all schedules will be replaced by those of the master schedule.

Creating a Master Receipt Schedule

To create a master schedule, proceed as follows:

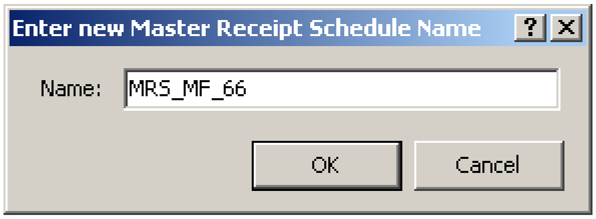
1 From the left pane of MessageWay Explorer, expand the **Receipt Monitor Schedules** folder and select **Master Receipt Schedules**.



2 From the menu bar, select the **Schedules** menu and then the **Add Schedule** command.

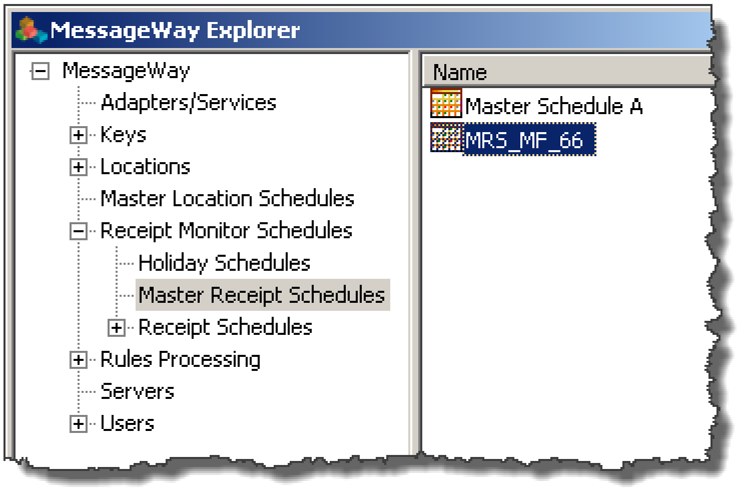
The **Enter Master Receipt Schedule Name** dialog box appears.

3 Enter a name for the master receipt schedule, and select **OK** to create the schedule and close the window.


Enter new Master Receipt Schedule Name

Name: MRS_MF_66

The schedule appears in the right pane of MessageWay Explorer.



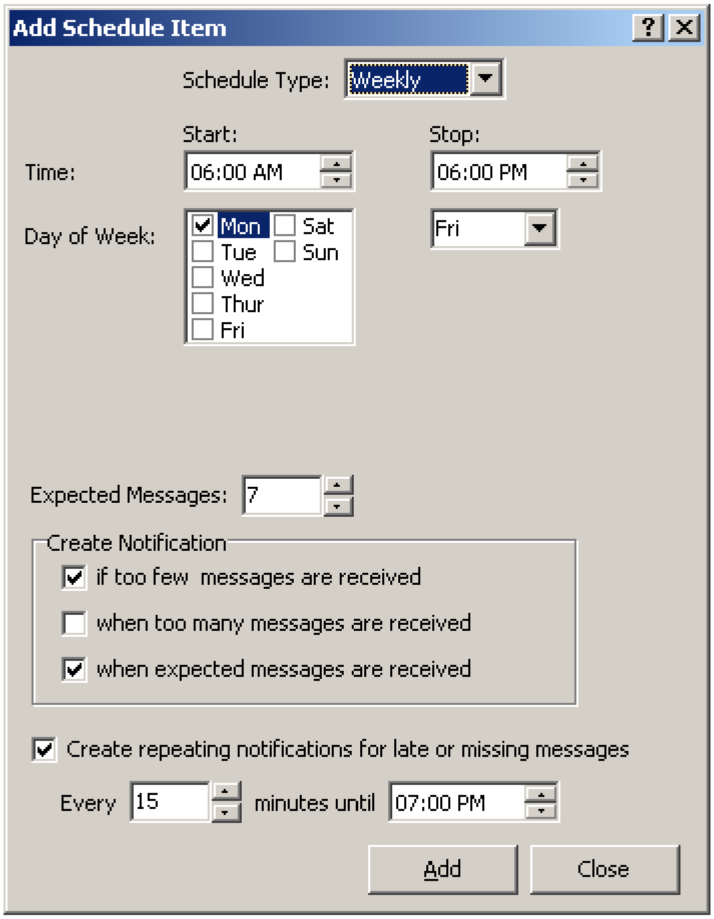
4 To open the schedule, double-click it.

To Create a Schedule Item

To create a master receipt schedule, you specify one or more schedule items, and then select a criterion to generate the notification.

1. From the Master Receipt Schedule window, on the **Schedule** tab, click **Add**.

   The Add Schedule Item window appears.
2. For Schedule Type, click the down arrow, and from the menu select **Daily**, **Weekly**, **Monthly**, **Yearly** or **Absolute**.
3. Type or select the date and time the period starts.
4. Type or select the date and time the period ends.
5. Type the number of messages that will trigger an event when they are received.
6. Select the type of notification required from the following options:
   - **If too few messages are received**
   - **When too many messages are received**
   - **When expected messages are received**
7. To receive repeating notifications for late or missing messages, check the box and specify an interval and final time for such notifications.



Schedule Type: Weekly

Time: Start: 06:00 AM Stop: 06:00 PM

Day of Week: ☑ Mon ☐ Sat ☐ Tue ☐ Sun ☐ Wed ☐ Thur ☐ Fri Fri

Expected Messages: 7

Create Notification

☑ if too few messages are received

☐ when too many messages are received

☑ when expected messages are received

☑ Create repeating notifications for late or missing messages

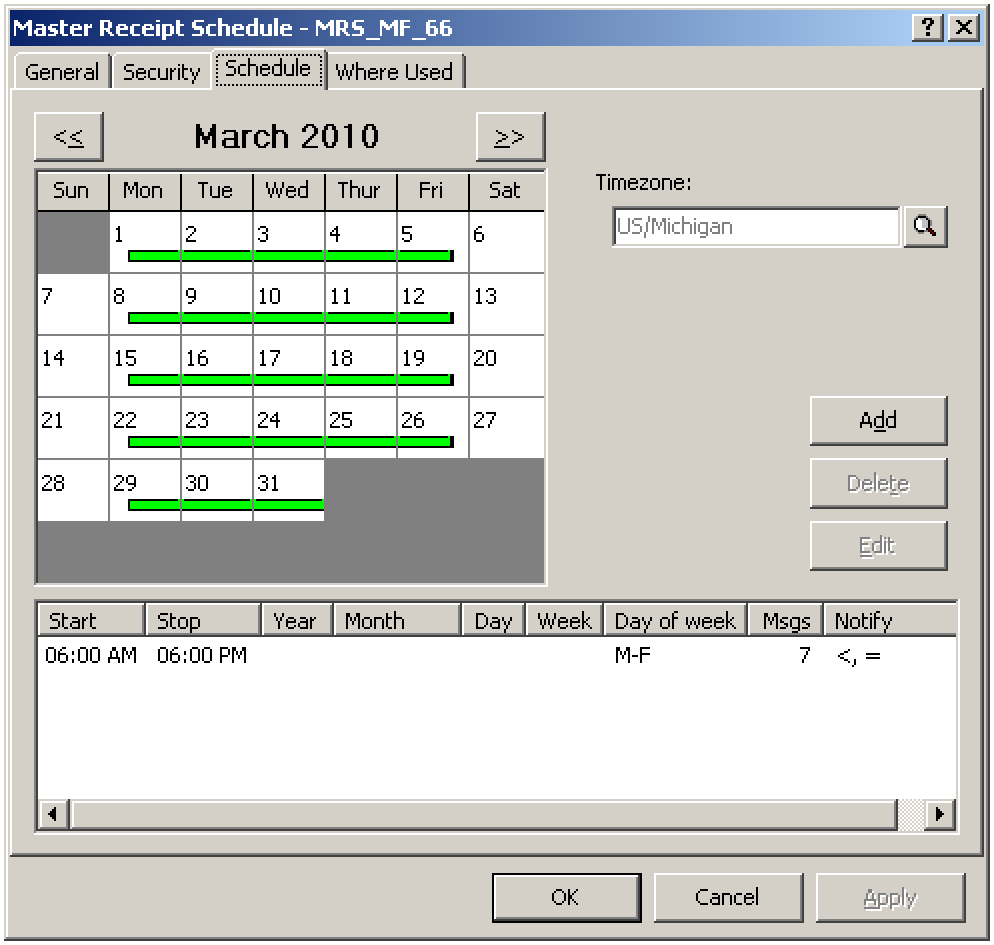
Every 15 minutes until 07:00 PM

8 Click **Add** to add the item to the schedule.

The item appears in the Schedule list, and a rectangular bar appears in the calendar as a visual aid.

9 To add another schedule item to the master receipt schedule, repeat steps 1 through 8.

10 Click **Close** to close the window and return to the Master Receipt Schedule window.



March 2010

Sun	Mon	Tue	Wed	Thur	Fri	Sat
	1 🟩	2 🟩	3 🟩	4 🟩	5 🟩	6
7	8 🟩	9 🟩	10 🟩	11 🟩	12 🟩	13
14	15 🟩	16 🟩	17 🟩	18 🟩	19 🟩	20
21	22 🟩	23 🟩	24 🟩	25 🟩	26 🟩	27
28	29 🟩	30 🟩	31 🟩			

Timezone: US/Michigan

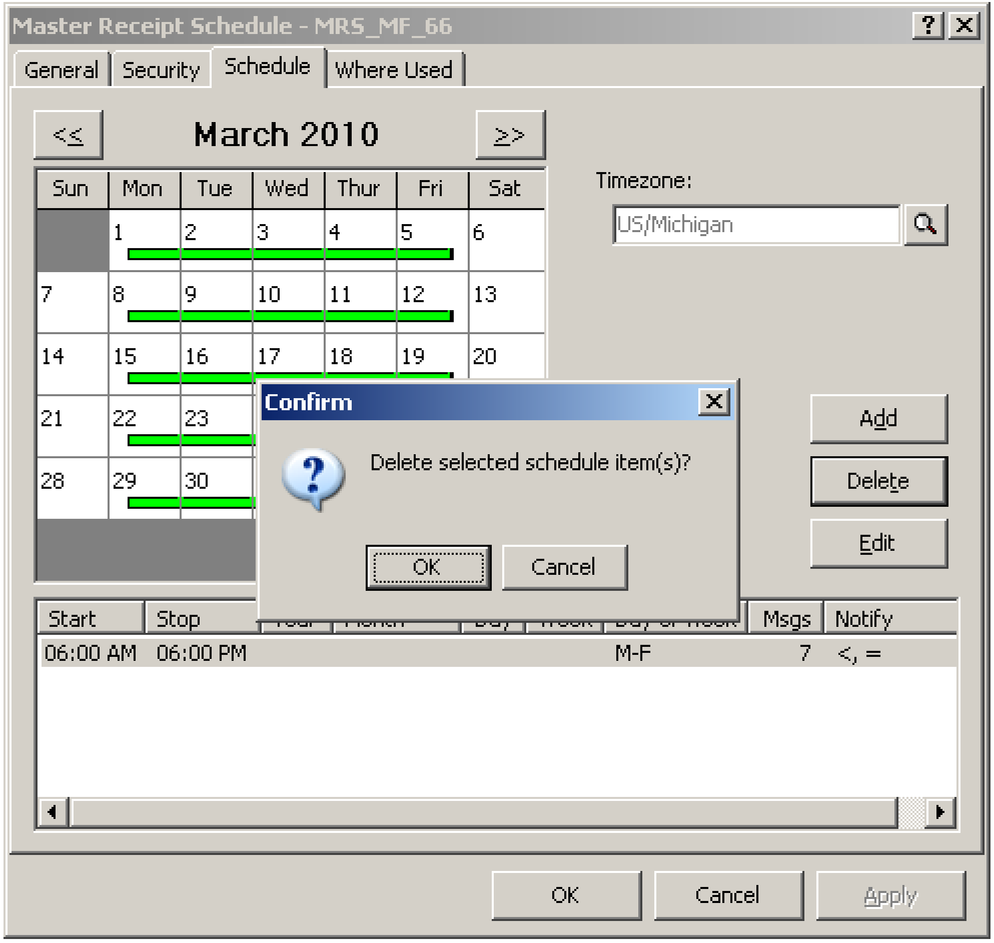
Start	Stop	Year	Month	Day	Week	Day of week	Msgs	Notify
06:00 AM	06:00 PM					M-F	7	<, =

To Delete Schedule Items

To delete one or more schedule items from the list, proceed as follows:

1 From the Schedule list, select one or more schedule items you want to delete.

2 Click the **Delete** button, and when a confirmation dialog box appears, click **OK** to confirm the delete.



Timezone: US/Michigan

Delete selected schedule item(s)?

Start	Stop	Day of Week	Msgs	Notify
06:00 AM	06:00 PM	M-F	7	<, =

To Edit a Schedule Item

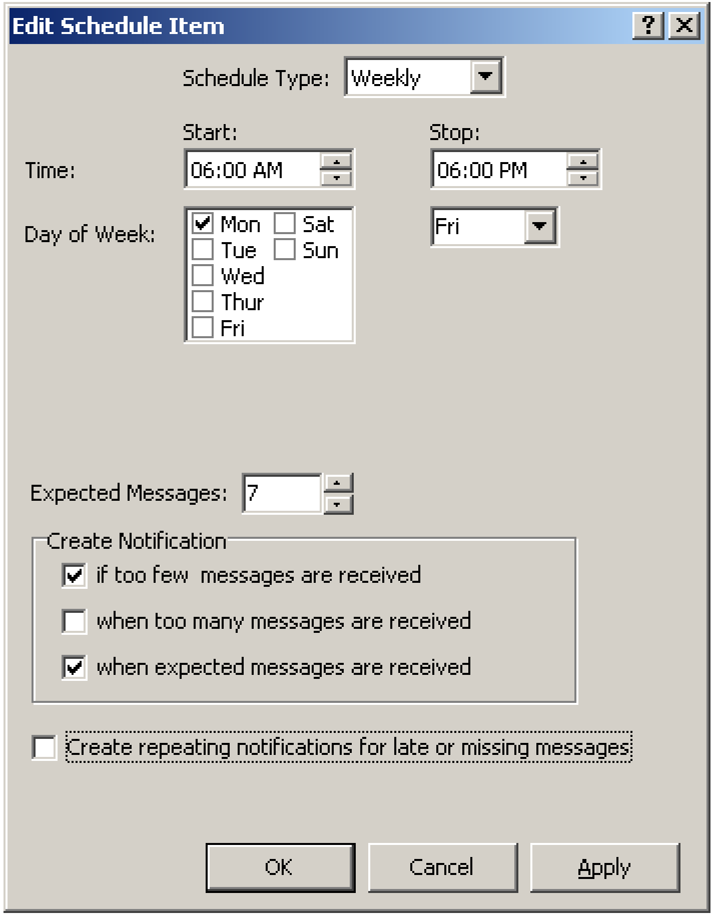
You may edit one schedule item from the list.

1 From the list, select the schedule item you want to edit, and click the **Edit** button.

The Edit Schedule Item window appears with the current settings.

2 Change the settings as required.

When you make changes, the **Apply** button becomes active.



Schedule Type: Weekly

Time: Start: 06:00 AM Stop: 06:00 PM

Day of Week: ☑ Mon ☐ Tue ☐ Wed ☐ Thur ☐ Fri ☐ Sat ☐ Sun — Fri

Expected Messages: 7

Create Notification

☑ if too few messages are received

☐ when too many messages are received

☑ when expected messages are received

☐ Create repeating notifications for late or missing messages

3 Click the **OK** button to save the changes and close the window.

The Master Receipt Schedule window appears.

Configuring Receipt Schedules

To generate a Receipt Monitor event, you must create a receipt schedule. A receipt schedule represents an inbound address, such as an e-mail address or a MessageWay input location. You may base a receipt schedule on a master schedule. You may also associate it with a holiday schedule. To organize your receipt schedules, group them in folders.

Creating a Receipt Schedule

A receipt schedule is used when the sender of a message matches the name of the receipt schedule. The sender of the message is determined within MessageWay based on the type of adapter or service that the input location uses. Therefore, before you create a receipt schedule, you must determine the sender.

To Determine a Receipt Schedule Name

When you create a receipt schedule, the receipt schedule name must be the same as the message sender. The message sender is determined by MessageWay as follows:

Source of Message	**Message Sender**
Disk Transfer, FTP locations	▪ Input site that retrieves the file ▪ Optional value in Sender field overrides input site
E-mail location	▪ In a POP3 header, the **Reply To** address of an e-mail message or **Sender** address, in that order ▪ Optional value in Sender field overrides POP3 header value
MWTranslator	▪ Sending location as determined by MWTranslator, shown on the Message List and Message Properties windows
CustomIO or CustomProc	▪ If you do not use a status file, the sender address is associated with the original MessageWay input location that uses a compound address to deliver the message ▪ If you are using a status file that specifies the source of the input, then that source value is used as the sender

For more information about locations and their properties, refer to the topic, ***Configuring Locations*** (on page 453).

To determine the name of a receipt schedule, follow these steps:

1. Find a message in MessageWay that has the same message sender for which you want to invoke Receipt Monitor.
2. From the Message List window, find the value in the Sender column

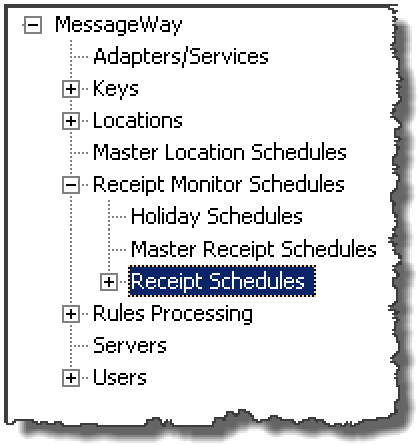
   - or -

   From the Message Properties window, find the value in the Sender field.
3. Use the message sender value as the name of the receipt schedule you want to create.

To Create a Receipt Schedule

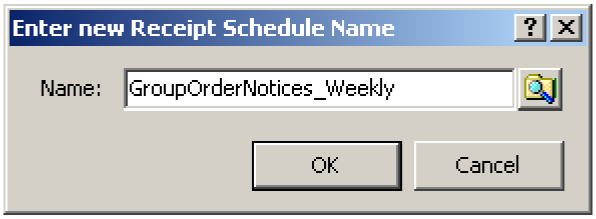
To create a receipt schedule, proceed as follows:

1. From the left pane of MessageWay Explorer, expand the **Receipt Monitor Schedules** folder, and select **Receipt Schedules**.



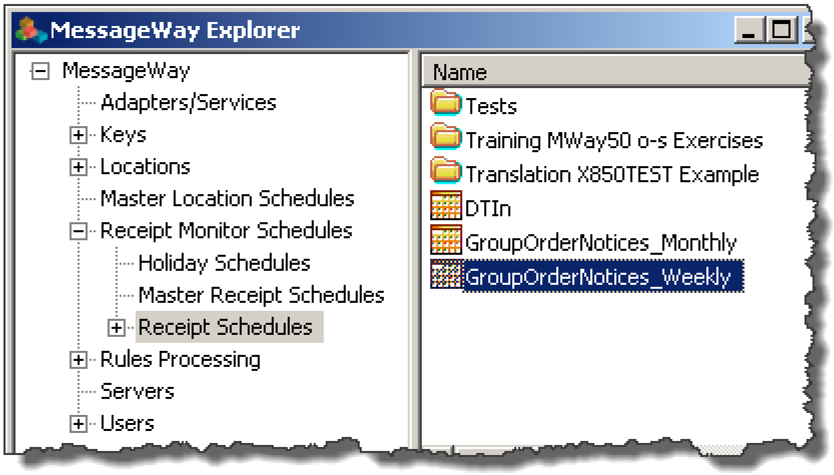
2 From the menu bar, select the **Schedules** menu and then the **Add Schedule** command. The **Enter Receipt Schedule Name** dialog box appears.

3 Type a name for the receipt schedule, and click **OK** to create the schedule and close the window.


Enter new Receipt Schedule Name

Name: GroupOrderNotices_Weekly

The schedule appears in the right pane of MessageWay Explorer.



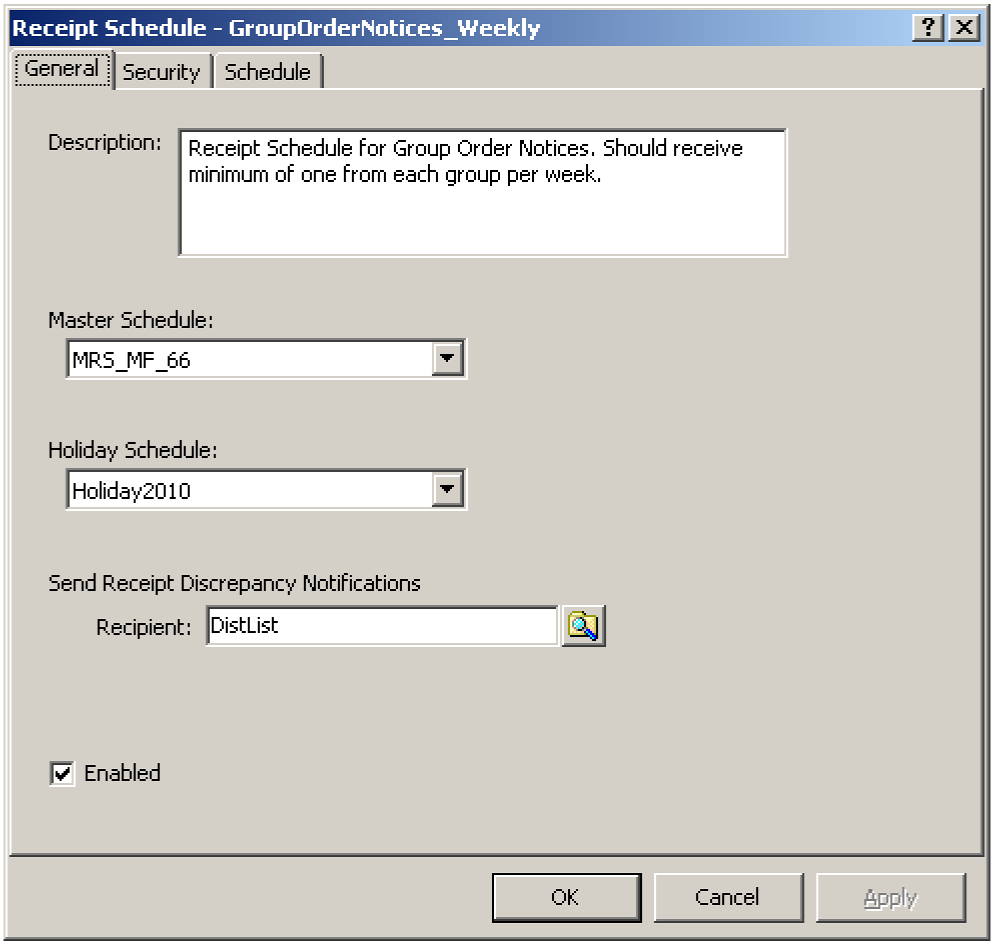
4 To open the schedule, double-click it.

Specifying Master Receipt and Holiday Schedules and Notifications

You may base this receipt schedule on a master schedule. You may also specify a holiday schedule to exclude days from notification events by selecting a defined schedule from the Holiday Schedule drop-down list. Depending on your needs, you may never use holiday schedules.

Specify a destination location to which you send notification messages.

IMPORTANT: In the event that a notification is generated, and no location is defined on a receipt schedule, the notification will go to the MessageWay system mailbox, {Unknown}.



Description: Receipt Schedule for Group Order Notices. Should receive minimum of one from each group per week.

Master Schedule: MRS_MF_66

Holiday Schedule: Holiday2010

Send Receipt Discrepancy Notifications

Recipient: DistList

☑ Enabled

Receipt Schedule with Master Schedule Example (Receipt Monitor, Receipt Schedule Window, General Page)

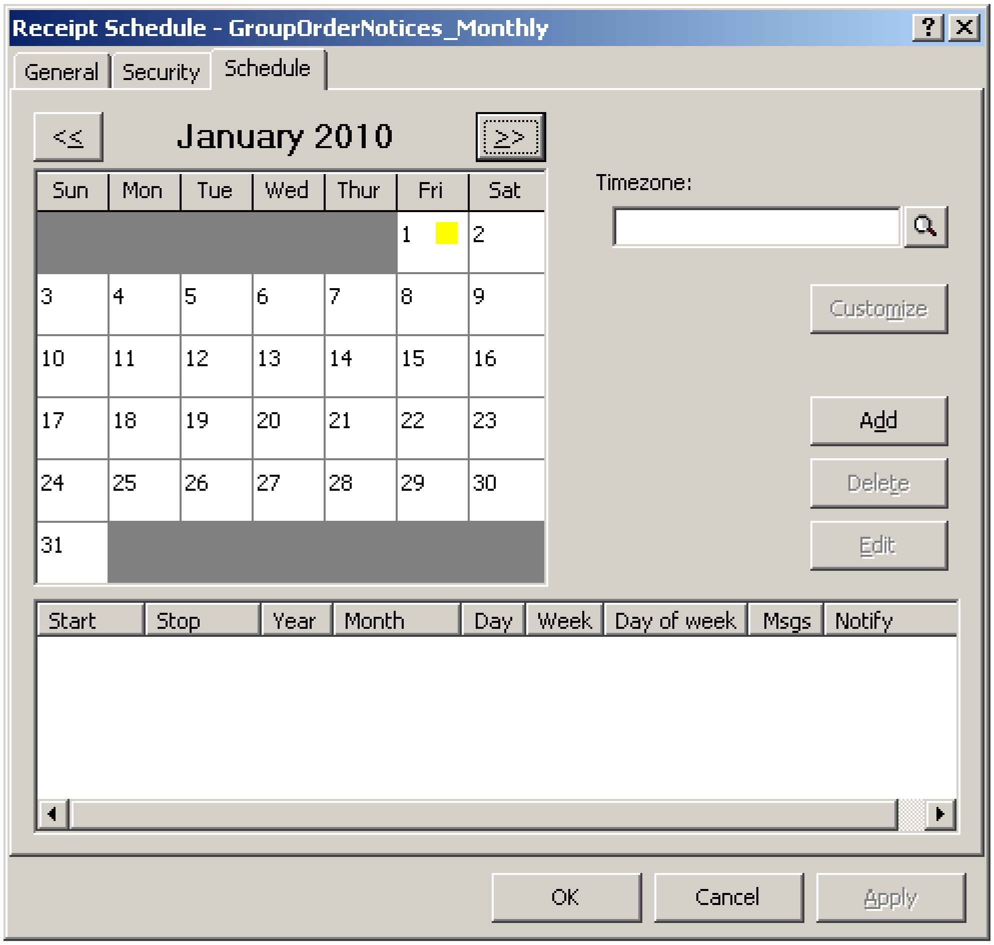
Specifying Schedule Items

Once created, a receipt schedule that is not based on a master schedule defaults to values that will never generate an event. To generate events, you must modify the values on the **Schedule** page of the Receipt

Schedule window. Notice that the holidays on the holiday schedule are designated as small squares. The squares are yellow when they do not fall on a date with a schedule item and red when they do.

The following window shows the **Schedule** page when the receipt schedule does not use a master receipt schedule. No schedule items are defined.

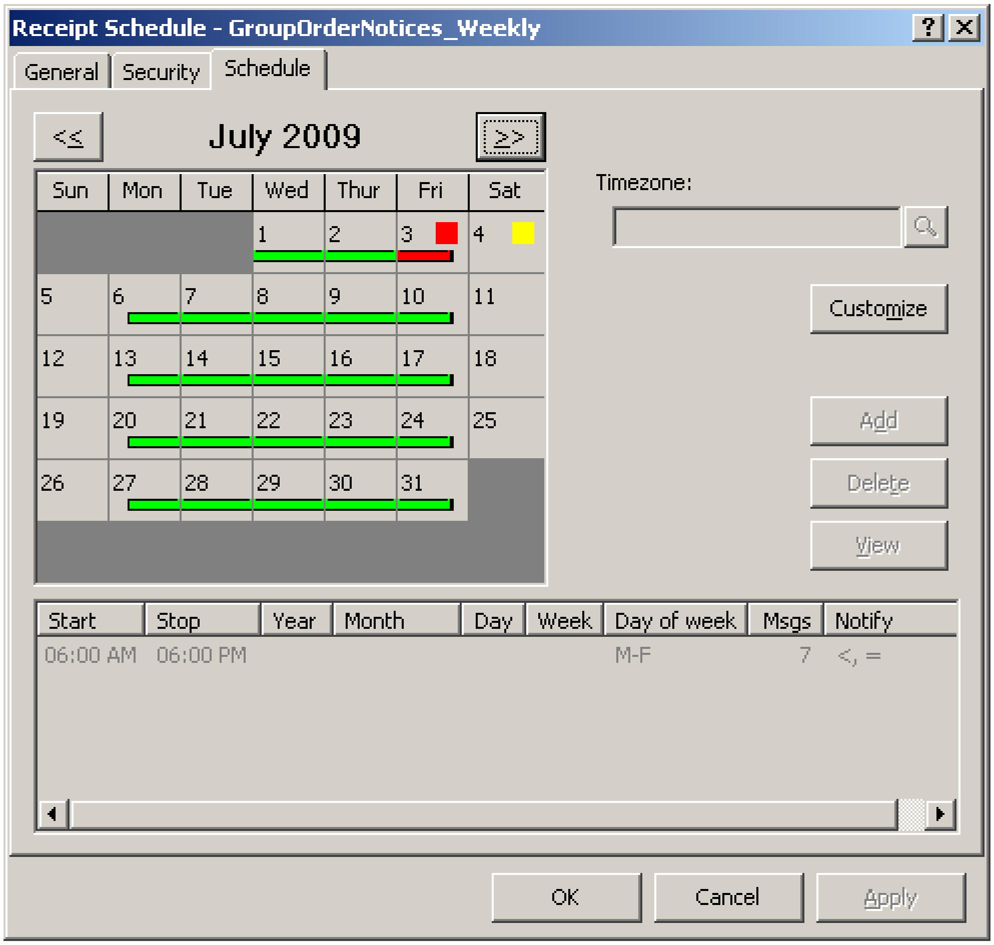
This receipt schedule uses a holiday schedule that shows one holiday on January 1.



Example without Master Schedule (Receipt Monitor, Receipt Schedule Window, Schedule Page)

The following window shows the **Schedule** page when the receipt schedule does use a master receipt schedule. Schedule items are defined. To make changes to this receipt schedule you select the **Customize** button.

IMPORTANT: When you customize a receipt schedule, the receipt schedule is detached from the master to allow you to make changes. Therefore, any subsequent changes made to the master schedule will not be reflected in the receipt schedule. If you decide to add a master schedule to an existing receipt schedule, all schedules will be replaced by those of the master schedule.



Sun	Mon	Tue	Wed	Thur	Fri	Sat
			1	2	3 🟥	4 🟨
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Start	Stop	Year	Month	Day	Week	Day of week	Msgs	Notify
06:00 AM	06:00 PM					M-F	7	<, =

Example with Master Schedule (Receipt Monitor, Receipt Schedule Window, Schedule Page)

The procedures you use to specify receipt schedule items are the same as those you would use to specify master receipt schedule items.

Refer to the following topics described for master receipt schedule items:

- ***To Create a Schedule Item*** (on page 678)
- To Delete Schedule Item(s) for One Or More Days Using the Calendar
- ***To Edit a Schedule Item*** (on page 681)

Toolbar Commands

The following tables describe the menus and commands specific to Receipt Monitor, with an explanation of what the commands do and any associated icons for specific tasks that you might be able to choose from the toolbar.

Schedules Menu Commands

The following commands appear on the **Schedules** menu, which appears when users select Receipt Monitor Schedules options: Holiday Schedules, Master Receipt Schedules, or Receipt Schedules.

Command	Description
Add Schedule	Add a holiday schedule, master receipt schedule or receipt schedule definition.
Add Folder	Create a folder to organize your receipt schedule definitions. You may only add folders for receipt schedules. The schedule names must be unique within the Receipt Schedules folder, ignoring any subfolders.

The following commands appear on the task bar.

Command	Shortcut	Icon	Description
Cut	**Ctrl+X**	✂	Copy and then delete the selected definition to move it to a new location by using a subsequent Paste command.
Copy	**Ctrl+C**	⎘	Copy the selected definition to the clipboard.
Paste	**Ctrl+V**	📋	Paste the definition on the clipboard.

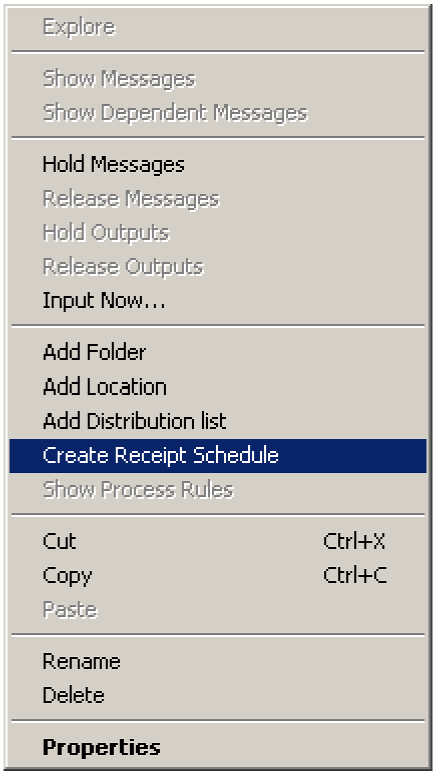
Task Bar

The following commands appear on the task bar.

Command	Shortcut	Icon	Description
Cut	**Ctrl+X**	✂	Copy and then delete the selected definition to move it to a new location by using a subsequent Paste command.
Copy	**Ctrl+C**	⎘	Copy the selected definition to the clipboard.
Paste	**Ctrl+V**	📋	Paste the definition on the clipboard.

Location Pop-up Menu

An input location may also be used as a receipt schedule address. To access the receipt schedule(s) defined for that location, right-click the location in the right pane of MessageWay Explorer to display a menu. From that menu, select the command, **Create Receipt Schedule**.



Receipt Monitor Pop-up Menu

Different menus appear when you select some entity of Receipt Monitor in the left pane of MessageWay Explorer and then right-click in the right pane. The following table explains the commands.

Command	Selected Item	Description
Explore	Folders	Displays the contents of a folder.
Add Schedule	Folders	Creates a new schedule.
Add Folder	Receipt Schedules Folder only	Creates a new folder. This folder is synchronized with folders that are created under the Locations and Rules Processing folders.
Show Location	Receipt schedule definition	Opens the location properties window when a receipt schedule uses the same name as a location.

Command	Selected Item	Description
Cut	Receipt schedule definition	Copies a schedule to the clipboard and then deletes it. This is useful for receipt schedules you want to move to a group, because they must have unique names within MessageWay.
Copy	Schedule definitions	Copies a schedule to the clipboard without deleting the original.
Paste	Schedule definitions	Pastes a cut or copied item in the right pane for the folder selected in the left pane.
Rename	Schedule definitions	Renames the selected entity.
Delete	Schedule definitions	Deletes a definition from the right pane.
Properties	Folders, schedule definitions	Displays the properties window for the item selected.

Monitoring System Activity

This section describes how to monitor message activity for adapters and locations as well as activities initiated through the Manager, which are captured in audit files.

Overview of Monitoring System Activity

The MessageWay Manager allows operators to easily monitor system activity. The Manager provides operators the following information:

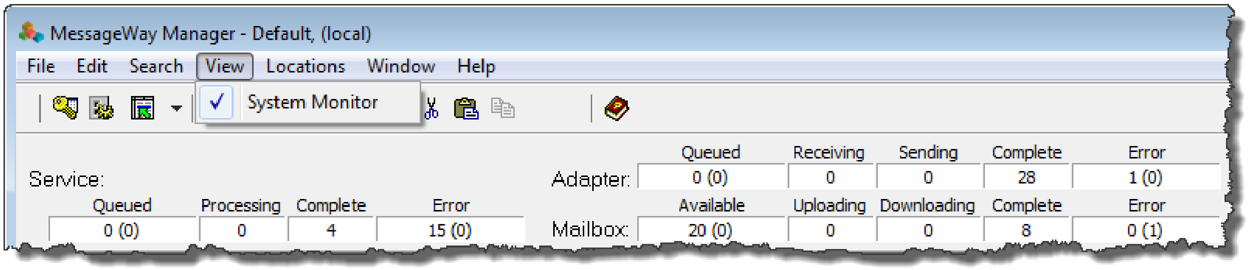
- Consolidated system activity for adapters, services and mailboxes
- Activity for each adapter or service
- Status of each location
- Output state of each service

Monitoring Consolidated System Activity

The MessageWay Manager provides a system monitor that displays consolidated statistics for all messaging activity for from one to four MessageWay server systems within an environment. Users may configure more than one environment, but the Manager connects to one environment at a time. It displays activity for services and adapters, as well as activity in mailboxes, which are locations not associated with a service or adapter. This information is updated dynamically. You can update it manually using **SHIFT+F5**.

The system monitor appears just below the toolbar. Users may display or hide the System Monitor by selecting or de-selecting the option from the **View** menu.

When you monitor a single-system environment, the name of the environment and the server appear in the header of the MessageWay Manager. The statistics reflect activity for all adapters, services and mailboxes for the one system in the environment.

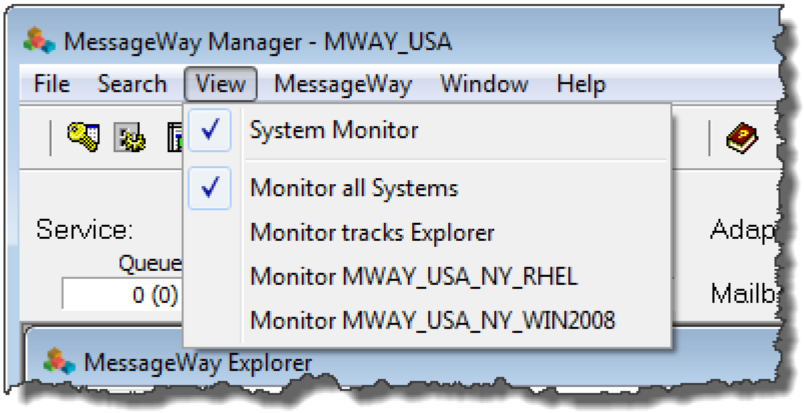


Service:	Queued	Processing	Complete	Error
	0 (0)	0	4	15 (0)

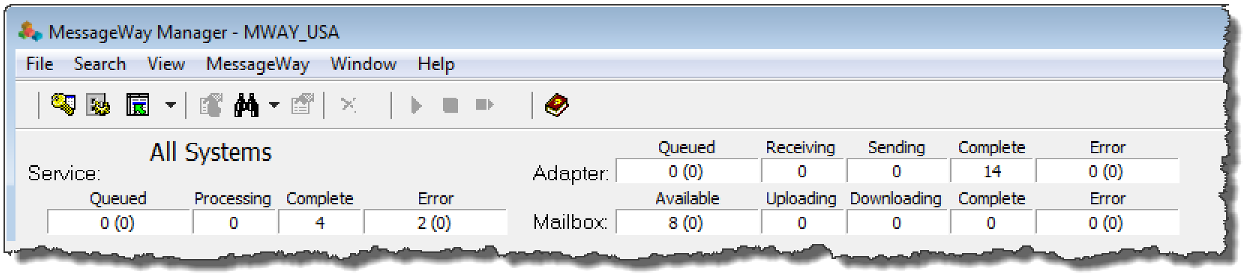
Adapter:	Queued	Receiving	Sending	Complete	Error
	0 (0)	0	0	28	1 (0)

Mailbox:	Available	Uploading	Downloading	Complete	Error
	20 (0)	0	0	8	0 (1)

When you monitor a multi-system environment, you can choose which of the servers you want to monitor, one or all.



If you monitor all systems, the name of the environment displays in the header of the MessageWay Manager, and *All Systems* appears on the System Monitor. The statistics reflect activity for all adapters, services and mailboxes for all systems in the environment and to which you are connected (logged on).



All Systems

Service:	Queued	Processing	Complete	Error
	0 (0)	0	4	2 (0)

Adapter:	Queued	Receiving	Sending	Complete	Error
	0 (0)	0	0	14	0 (0)

Mailbox:	Available	Uploading	Downloading	Complete	Error
	8 (0)	0	0	0	0 (0)

Service Statistics

The following consolidated status information appears on the **System Monitor** bar for all services.

Category	Description
Queued ( )	Displays the total number of messages awaiting processing. Numbers in parentheses show the total number of messages awaiting processing that are currently on hold, which includes the message states of **Hold**, **Hold Output** and **Schedule Wait**.
Processing	Displays the total number of messages currently being processed.
Complete	Displays the total number of messages that have been delivered.
Error ( )	Displays the total number of messages that have an error status. Numbers in parentheses show the total number of messages that have been canceled. Operators may cancel any messages that do not have the state of **Receiving**, **Complete** or **Error**.

Adapter Statistics

The following consolidated status information appears on the **System Monitor** bar for all adapters.

Category	Description
Queued ( )	Displays the total number of messages that are awaiting delivery. Numbers in parentheses show the total number of messages awaiting delivery that are currently on hold, which includes the message states of **Hold**, **Hold Output** and **Schedule Wait**.
Receiving	Displays the total number of messages currently being received into MessageWay.
Sending	Displays the total number of messages currently being sent to their destination.
Complete	Displays the total number of messages that have been sent to their destination.
Error ( )	Displays the total number of messages that have an error status and are not yet delivered. Messages in the {Unknown} mailbox are not included in the count of any of the individual adapters. Numbers in parentheses show the total number of messages that have been canceled. Operators may cancel any messages that do not have the status of **Receiving**, **Complete** or **Error**.

Mailbox Statistics

The following consolidated status information appears on the **System Monitor** bar for messages that are not associated with an adapter or service, which includes messages in the system mailboxes, {Unknown} and {Quarantine}, and pickup mailboxes.

NOTE: The optional content validation feature uses the {Quarantine} system mailbox.

Users access pickup mailboxes through optional services, such as the FTP Server, SFTP Server and Web Client. Mailboxes allow users to collect their messages from MessageWay, rather than having MessageWay deliver them automatically.

Category	Description
Available ( )	Displays the total number of messages that are awaiting pickup from a pickup mailbox. Numbers in parentheses indicate the total number of messages awaiting pickup that are currently on hold, which includes the message states of **Hold**, **Hold Output** and **Schedule Wait**.
Uploading	Displays the total number of messages currently being received into MessageWay.
Downloading	Displays the total number of messages currently being sent to their destination.
Complete	Displays the total number of messages that have been sent to their destination.

Category	Description
Error ( )	Displays the total number of messages that have an error status and are not yet delivered or that have not yet been picked up. Numbers in parentheses show the total number of messages that have been canceled. Operators may cancel any messages that do not have the status of **Receiving**, **Complete** or **Error**.

Monitoring Environments

Operators may monitor other MessageWay environments from the MessageWay Manager, which is the MessageWay client. For information about installing a Manager, refer to the separate document, *MessageWay 6.1.0 Installation Guide*.

Operators create an environment that points to from one to four servers in order to monitor that environment. For more information about configuring environments, refer to the section, ***Configuring Remote Access*** (on page 443).

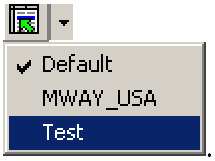
When you are monitoring and configuring environments, there are three pieces of information that you define when you configure an environment that you should distinguish:

- Environment Name of the MessageWay system or systems
- System Name of one MessageWay Server including its database and associated servers. In a single-system environment, this is typically the same as the name of the environment.
- Server IP address or name used to connect to the MessageWay system

Selecting an Environment to Monitor

You monitor MessageWay traffic by environment. Once an environment has been created and tested, operators may select the environment they wish to monitor, as follows:

1 From the toolbar, click the **Select Environment** drop-down list button.



.

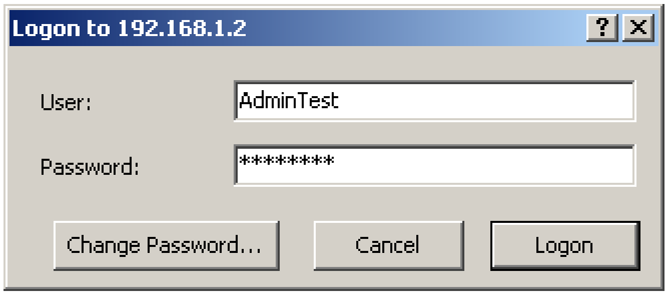
A list of configured environments appears. A check mark indicates which environment is currently selected.

2 From the list, select the remote environment you want to monitor, such as **Test**.

MessageWay attempts to connect to the database. When it connects, a logon window appears.

3 The next step is to log on, which varies depending on whether you are accessing a single-system or multi-system environment:

- For single-system environments, type your MessageWay user ID and password to log on to that system.



Logon to 192.168.1.2

User: AdminTest

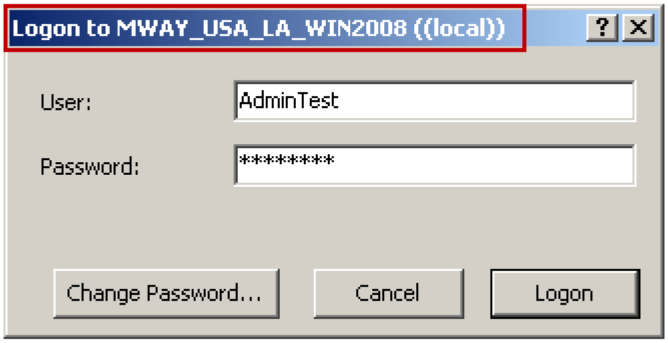
Password: *********

The environment name and the IP address or server name appear on the title bar of the MessageWay Manager.

- or -

- For multi-system environments, a logon window appears each system in your environment. If your systems all have the same user ID and password configured, click **Logon**, since MessageWay retains the user ID and password for the next system logon.

Type a valid user ID and password for the first system. The system and server to which you are connecting appears in the title bar. When your server is on the same system as the Manager, the server by default is called *(local)*.



Logon to MWAY_USA_LA_WIN2008 ((local))

User: AdminTest

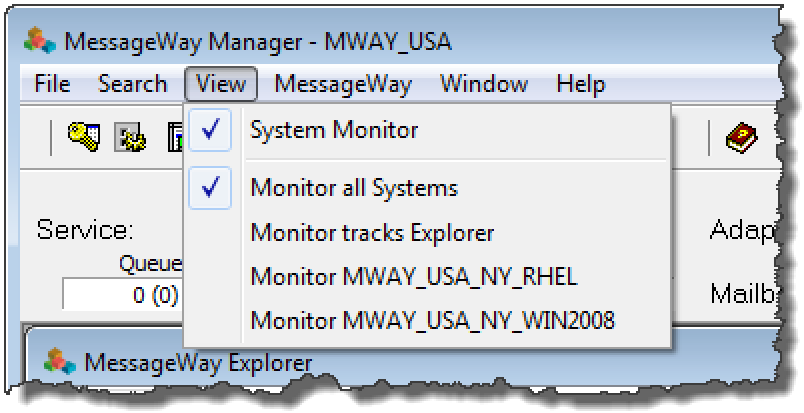
Password: *********

Initially, only the environment name appears in the title bar of the MessageWay Manager.

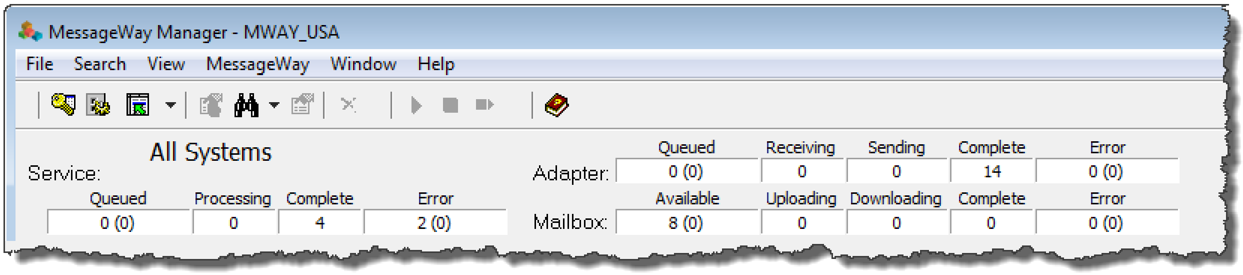
After you actually select an environment from MessageWay Explorer, the server IP address or name will appear also.

Selecting Systems to Monitor in a Multi-system Environment

In environments that include more than one system, users can configure the MessageWay Manager to monitor one or more of the systems. You select what to monitor from the **View** menu:



Your selection appears on the system monitor:



All Systems

Service:

Queued	Processing	Complete	Error
0 (0)	0	4	2 (0)

	Queued	Receiving	Sending	Complete	Error
Adapter:	0 (0)	0	0	14	0 (0)

	Available	Uploading	Downloading	Complete	Error
Mailbox:	8 (0)	0	0	0	0 (0)

Your choice affects:

- ***Numbers you see in the System Monitor*** (on page 691)
- ***What is returned when you use the Find options*** (on page 733)

To choose which systems to monitor, from the **View** menu:

- To monitor all systems in your environment, click **Monitor all Systems**.
- To monitor the system or systems selected in MessageWay Explorer, click **Monitor tracks Explorer**.

NOTE: Typically, you select only one system at a time in MessageWay Explorer. However, if you click MessageWay in the left pane, it automatically selects all systems.

- To monitor a single system, select **Monitor** and the system name.

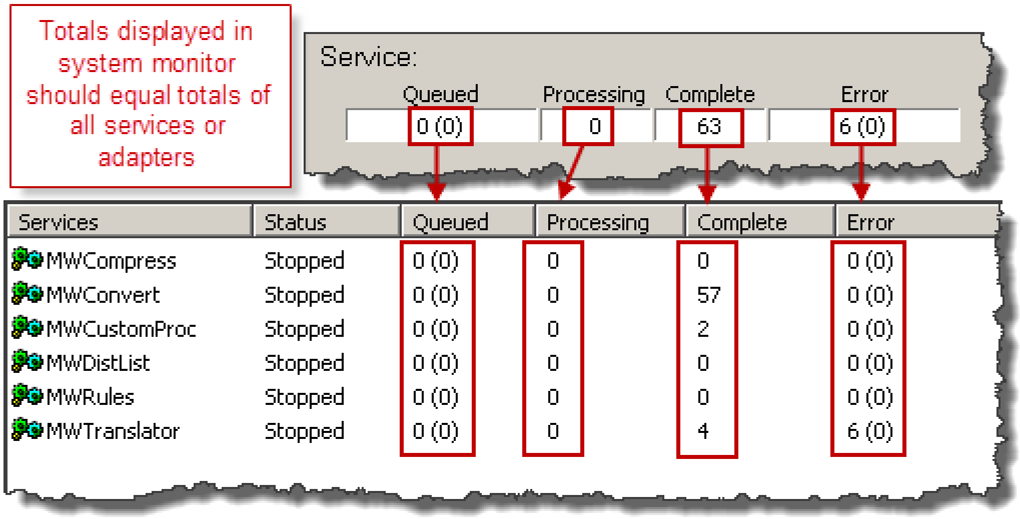
Monitoring Multiple Environments

You can only monitor one environment at a time, which may have up to 4 systems associated with it. To monitor multiple environments simultaneously, run multiple instances of the Manager. It helps to have a large viewing device when you do this.

Monitoring Individual Adapter and Service Status and Activity

Operators may monitor statuses and statistics for each of the adapters or services for one environment by selecting **Adapters/Services** from the left pane of the MessageWay Explorer. The MessageWay Server updates these statistics periodically. Users may update the statistics manually by selecting **SHIFT+F5**.

The totals of the columns' statistics for a single-system environment for services and adapters should equal the statistics in the System Monitor for services and adapters, respectively.



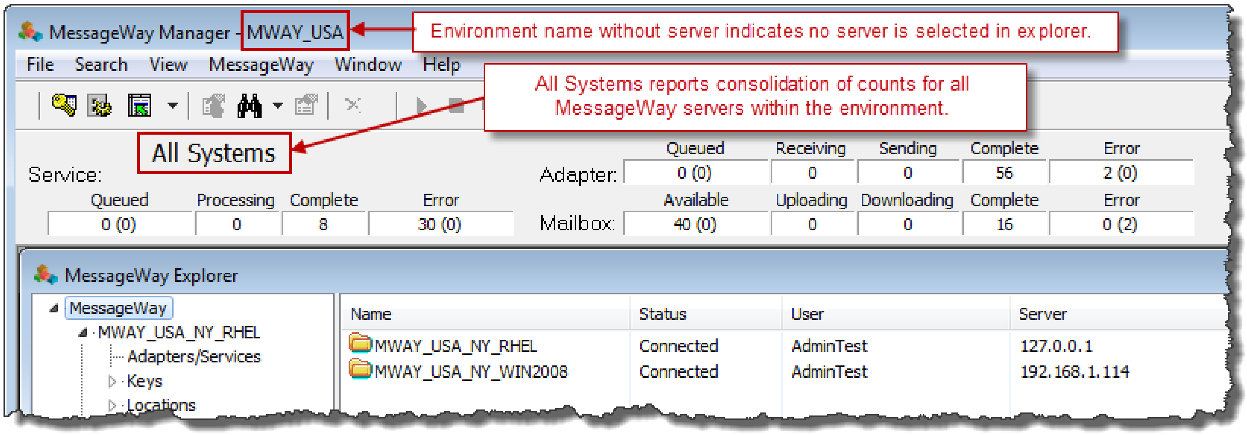
Totals displayed in system monitor should equal totals of all services or adapters

Service:

Queued	Processing	Complete	Error
0 (0)	0	63	6 (0)

Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	57	0 (0)
MWCustomProc	Stopped	0 (0)	0	2	0 (0)
MWDistList	Stopped	0 (0)	0	0	0 (0)
MWRules	Stopped	0 (0)	0	0	0 (0)
MWTranslator	Stopped	0 (0)	0	4	6 (0)

The totals of the columns' statistics for a multi-system environment for services and adapters should equal the statistics in the System Monitor for services and adapters of all the systems in the environment that you are monitoring from the System Monitor, one of them or all of them. Remember that the MessageWay Explorer pane, which is below the System Monitor pane, shows all systems in the environment in the left pane.



Environment name without server indicates no server is selected in explorer.

All Systems reports consolidation of counts for all MessageWay servers within the environment.

Service:

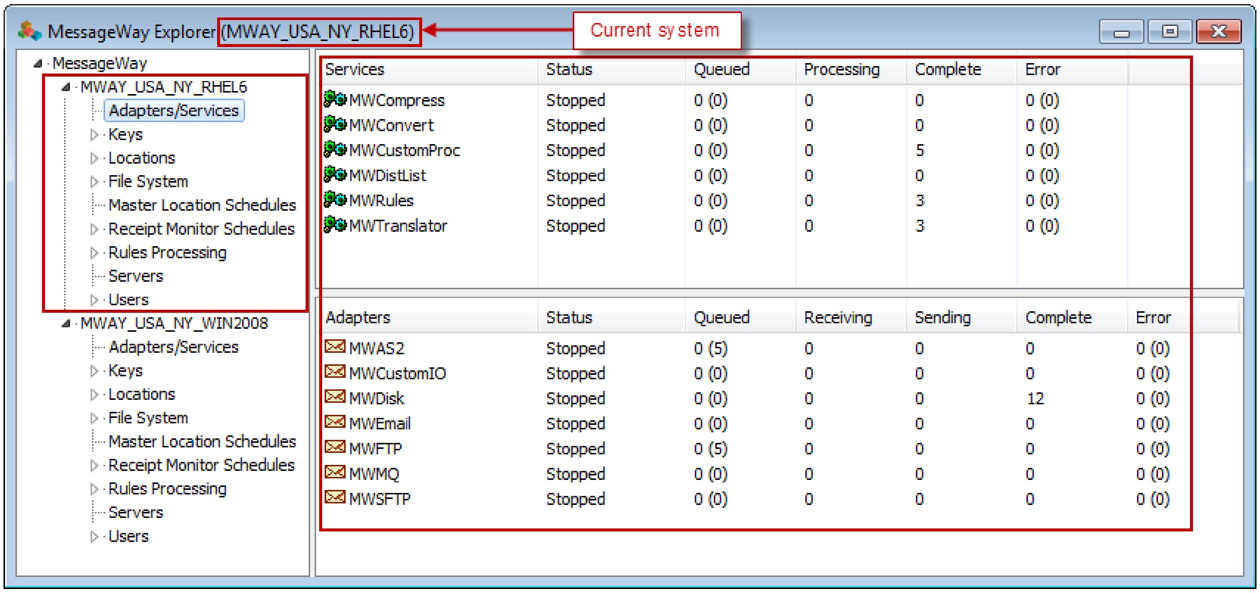
Queued	Processing	Complete	Error
0 (0)	0	8	30 (0)

	Queued	Receiving	Sending	Complete	Error
Adapter:	0 (0)	0	0	56	2 (0)

	Available	Uploading	Downloading	Complete	Error
Mailbox:	40 (0)	0	0	16	0 (2)

Name	Status	User	Server
MWAY_USA_NY_RHEL	Connected	AdminTest	127.0.0.1
MWAY_USA_NY_WIN2008	Connected	AdminTest	192.168.1.114

However, you can only select one system at a time in MessageWay Explorer, which shows the numbers for each adapter and service for that one system in the Explorer panes.



Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0	5	0 (0)
MWDistList	Stopped	0 (0)	0	0	0 (0)
MWRules	Stopped	0 (0)	0	3	0 (0)
MWTranslator	Stopped	0 (0)	0	3	0 (0)

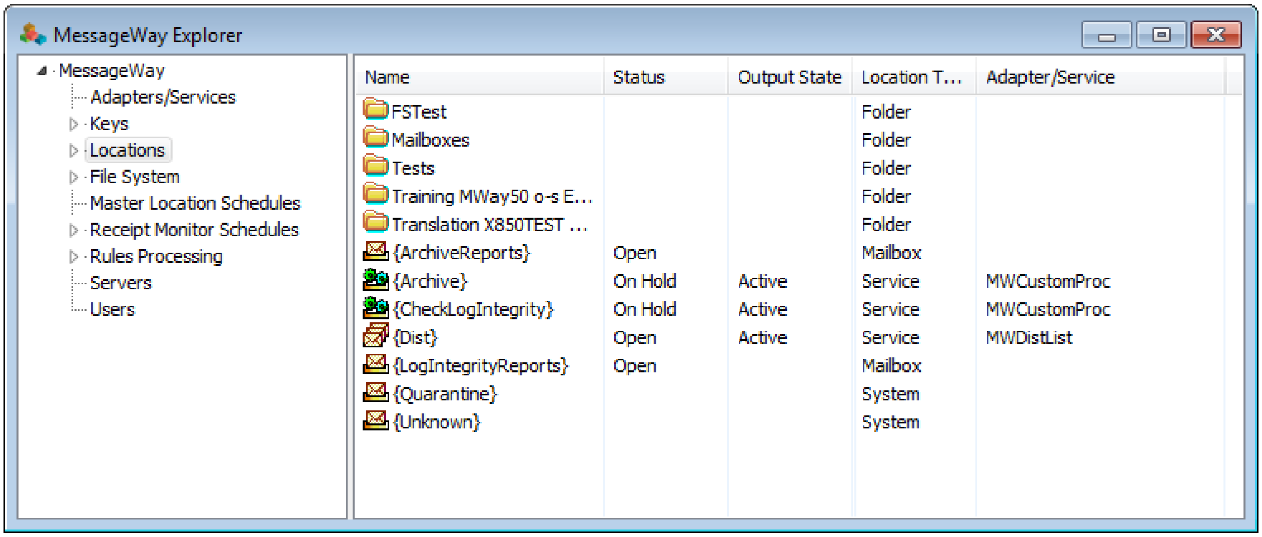
Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWAS2	Stopped	0 (5)	0	0	0	0 (0)
MWCustomIO	Stopped	0 (0)	0	0	0	0 (0)
MWDisk	Stopped	0 (0)	0	0	12	0 (0)
MWEmail	Stopped	0 (0)	0	0	0	0 (0)
MWFTP	Stopped	0 (5)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

Monitoring Location Status

Operators may monitor the status of all locations by selecting **Locations** for a system from the left pane of the MessageWay Explorer. To update the information, users must press **SHIFT+F5**. The information is *not* updated automatically.

It is important that periodically operators be able to check the statuses of the locations to see which ones have the status of Active or On Hold and which schedules are open, closed or using threshold release.

When locations are on hold, they will not deliver new messages. When schedules are closed, they will not deliver messages either.



Name	Status	Output State	Location T...	Adapter/Service
FSTest			Folder	
Mailboxes			Folder	
Tests			Folder	
Training MWay50 o-s E...			Folder	
Translation X850TEST ...			Folder	
{ArchiveReports}	Open		Mailbox	
{Archive}	On Hold	Active	Service	MWCustomProc
{CheckLogIntegrity}	On Hold	Active	Service	MWCustomProc
{Dist}	Open	Active	Service	MWDistList
{LogIntegrityReports}	Open		Mailbox	
{Quarantine}			System	
{Unknown}			System	

Some users organize their locations within a series of folders. In this case, they can view only the locations in a selected folder. To find a specific location, use the ***search options*** (on page 763).

Viewing MessageWay Manager Audit Information

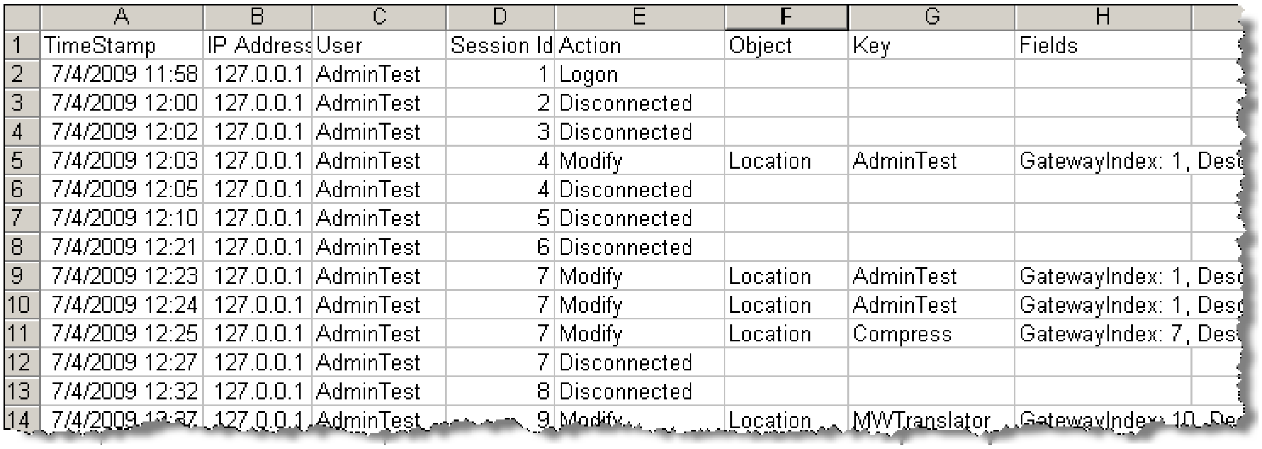
MessageWay also has audit files that log information about the activities of the MessageWay Manager. By default, audit records are written to the AuditTable in the MessageWay database.

To view audit records that have been logged to the database, use the ***Search, Find Logs, Audit Logs*** (on page 774) feature.

Audit records can also be written to files. The default location of the audit files varies depending on the operating system, as follows:

Operating System	Default Location of Audit Files
Windows	c:\MessageWay\audit
UNIX/Linux	/var/opt/messageway/audit

For each new session of the MessageWay Manager, MessageWay checks to see if an audit file exists for that day. If not, it creates one. MessageWay creates .csv files and assigns file names using the date prefixed with the word audit, for example, audit20070704. To view the contents of an audit file, open it with any program capable of reading .csv files.



	A	B	C	D	E	F	G	H	
1	TimeStamp	IP Address	User	Session Id	Action	Object	Key	Fields	
2	7/4/2009 11:58	127.0.0.1	AdminTest	1	Logon				
3	7/4/2009 12:00	127.0.0.1	AdminTest	2	Disconnected				
4	7/4/2009 12:02	127.0.0.1	AdminTest	3	Disconnected				
5	7/4/2009 12:03	127.0.0.1	AdminTest	4	Modify	Location	AdminTest	GatewayIndex: 1, Desc	
6	7/4/2009 12:05	127.0.0.1	AdminTest	4	Disconnected				
7	7/4/2009 12:10	127.0.0.1	AdminTest	5	Disconnected				
8	7/4/2009 12:21	127.0.0.1	AdminTest	6	Disconnected				
9	7/4/2009 12:23	127.0.0.1	AdminTest	7	Modify	Location	AdminTest	GatewayIndex: 1, Desc	
10	7/4/2009 12:24	127.0.0.1	AdminTest	7	Modify	Location	AdminTest	GatewayIndex: 1, Desc	
11	7/4/2009 12:25	127.0.0.1	AdminTest	7	Modify	Location	Compress	GatewayIndex: 7, Desc	
12	7/4/2009 12:27	127.0.0.1	AdminTest	7	Disconnected				
13	7/4/2009 12:32	127.0.0.1	AdminTest	8	Disconnected				
14	7/4/2009 12:37	127.0.0.1	AdminTest	9	Modify	Location	MWTranslator	GatewayIndex: 10, Des	

Controlling Message Traffic

This section describes how to control messages as they travel through MessageWay.

Overview of Controlling Message Traffic

The purpose of MessageWay is to give users a mechanism to control message traffic, providing security, accountability, and fast service. User security configurations control the tasks users can perform.

There are two types of messaging monitors: the System Monitor provides consolidated information and the Adapters and Services monitors provides the same information by adapter or service.

NOTE: If you are currently monitoring multiple systems in an environment, you will be able to search for locations and messages across all the systems. You will also be able to select locations or messages from the returned list that belong to different systems and issue commands, such as hold and release commands.

The purpose of the MessageWay monitors is to allow operators to spot potential trouble. Operators must be able to handle the exceptions efficiently. Often this includes controlling the message traffic while problems are diagnosed and fixed. Other than taking the drastic step of stopping the entire MessageWay system, operators may control the flow of messages at three levels, using various commands, as shown in the following table:

Control Level	Commands
Adapter/service	Start, Stop, Restart, Suspend, Resume
Location	Hold Messages, Release Messages (Service location only) Hold Outputs, Release Outputs
Message	Resubmit Message, Redirect Message, Release Message, Restart Receive Message, Cancel Message (Input site only) Input now (Service location only) Execute now

Operators may execute the commands using the toolbar buttons, menu selections, or by right-clicking an entity, such as an adapter, service, location or message.

IMPORTANT: When a system failure occurs while an adapter or service is processing a message, the automatic recovery process within MessageWay will attempt to reprocess the message for input or output, based on the Error Action settings on the **Options** page for the location in question. MessageWay repeats its attempt from the beginning of the message, unless check-point restart is available. Currently, FTP and SFTP adapter transfers support restart. On the inbound side, failed receives may leave a partial file in the

Message Store, but the retry will overlay partial files. On the outbound side, after an e-mail has been sent by the E-mail adapter but not yet marked delivered by MessageWay, and the process is interrupted, the E-mail adapter will resend the entire message. This may result in sending duplicate messages to the recipient.

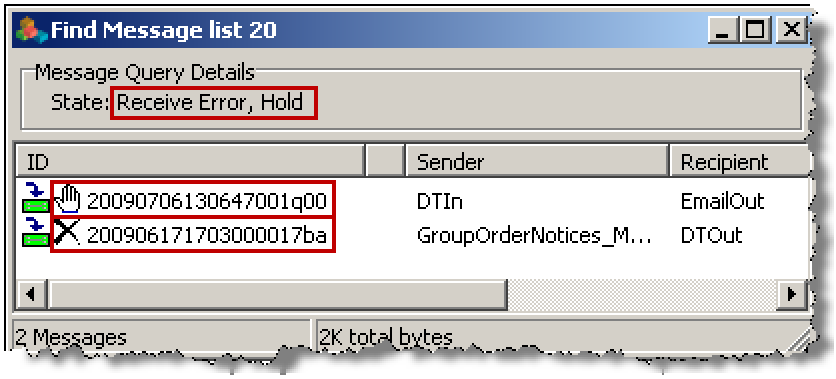
Understanding Message States

Message states are important diagnostic tools. Descriptions of the various states of messages, their associated icons and what might cause the message to have that state are shown in the following table:

Message State	Icon	Description	Possible Cause
Available for Download	☝	The message is waiting in a pickup type location for a user to collect it.	Normal processing for locations not associated with an adapter or service. User must collect messages through the optional services, such as the FTP Server, SFTP Server, AS2 interface or Web Client.
Canceled	⊘	This message is canceled.	Operator has canceled the message.
Complete	✓	This message has been delivered or picked up/collected.	Normal processing for all locations.
Downloading	⬇	A user is receiving the message from MessageWay through the AS2 interface, FTP Server, SFTP Server or Web Client.	The message is being downloaded by one of the MessageWay perimeter servers.
Error	✗	The message has not been delivered from MessageWay, because it has an error.	▪ Invalid output location ▪ (Translator) Translation abort ▪ (Rules Processing) Reject or abort
Hold, Hold Output, Schedule Wait	✋	This message is currently on hold or waiting for a closed schedule to open, and will be processed when it is released.	▪ Destination location is on hold ▪ Service Location is holding its outputs ▪ Schedule is closed; may use threshold release
Receive Error	✕	Adapter was not able to complete input of message in Message Store. This may contain partial data.	▪ Protocol problems with connecting site ▪ Adapter or service was stopped during transfer

Message State	Icon	Description	Possible Cause
Sending	⚙	An adapter or service is in the process of sending the message	Normal processing.
Queued	⌛	The message is queued awaiting delivery to a process or out from MessageWay.	▪ Adapter or service is busy processing other messages ▪ Adapter or service is stopped or suspended
Uploading	⬆	A user is sending the message to MessageWay through the AS2 interface, FTP Server, SFTP Server or Web Client.	The message is being uploaded by one of the MessageWay perimeter servers.

The icons appear on Message List windows, as shown in this example. To display messages on a Message List window, refer to the topic ***Searching for Message Information*** (on page 742).

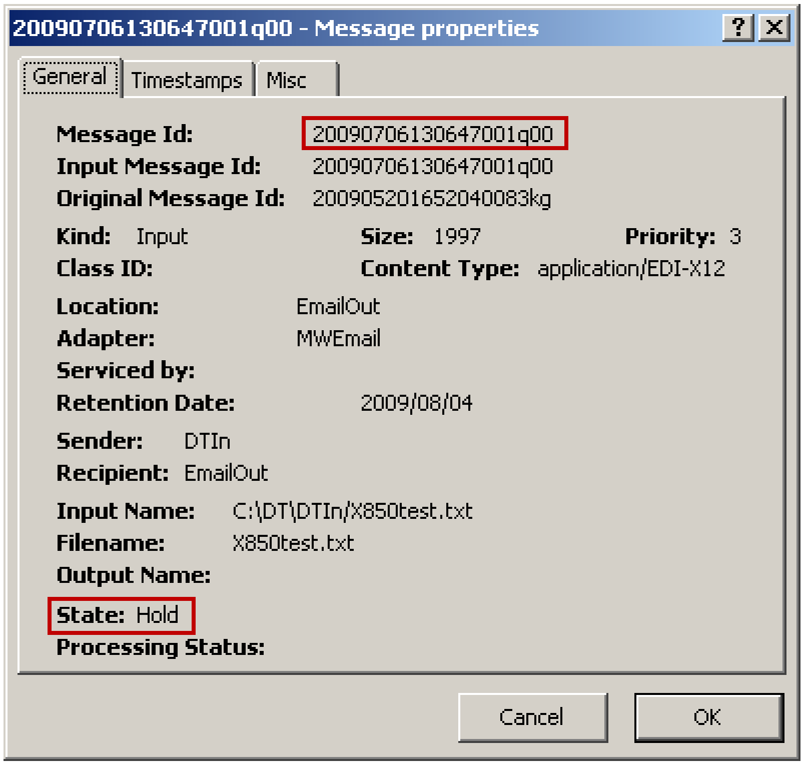

Find Message list 20

Message Query Details
State: Receive Error, Hold

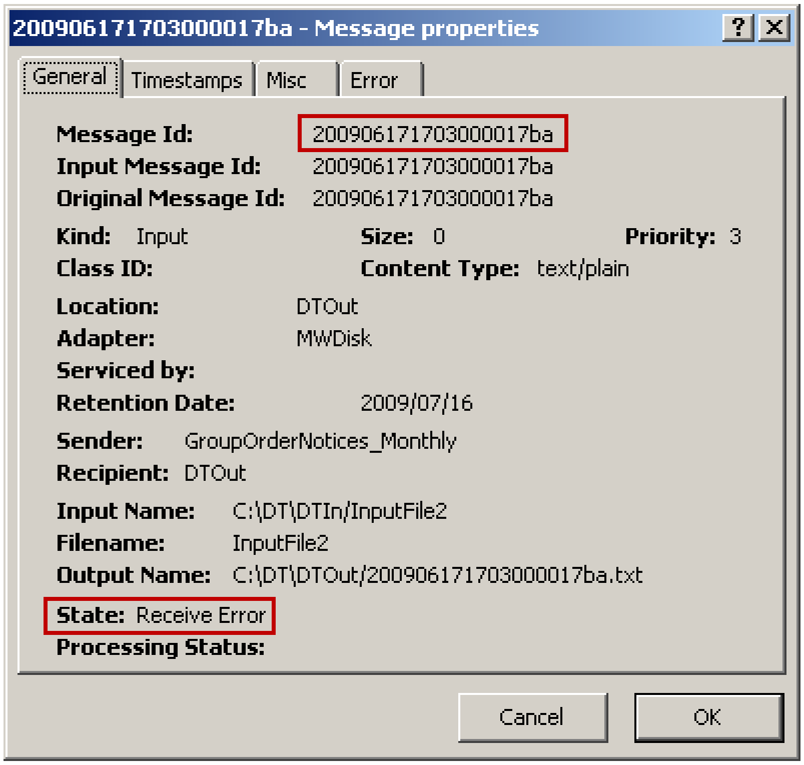
ID	Sender	Recipient
20090706130647001q00	DTIn	EmailOut
200906171703000017ba	GroupOrderNotices_M...	DTOut

2 Messages | 2K total bytes

The message state appears on the Message Properties window, which you can relate to the items on the Message List window using the Message ID, as show in the following examples:



Message Id: 20090706130647001q00
Input Message Id: 20090706130647001q00
Original Message Id: 20090520165204083kg
Kind: Input **Size:** 1997 **Priority:** 3
Class ID: **Content Type:** application/EDI-X12
Location: EmailOut
Adapter: MWEmail
Serviced by:
Retention Date: 2009/08/04
Sender: DTIn
Recipient: EmailOut
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.txt
Output Name:
State: Hold
Processing Status:



Message Id: 20090617170300017ba
Input Message Id: 20090617170300017ba
Original Message Id: 20090617170300017ba
Kind: Input **Size:** 0 **Priority:** 3
Class ID: **Content Type:** text/plain
Location: DTOut
Adapter: MWDisk
Serviced by:
Retention Date: 2009/07/16
Sender: GroupOrderNotices_Monthly
Recipient: DTOut
Input Name: C:\DT\DTIn/InputFile2
Filename: InputFile2
Output Name: C:\DT\DTOut/20090617170300017ba.txt
State: Receive Error
Processing Status:

Controlling Adapter and Service Activity

Operators may start and stop or suspend and resume adapters and services to control message activity. Adapters provide connections between MessageWay and the outside world. Starting and stopping adapters prevents messages from entering or leaving MessageWay, depending on the configurations of the locations associated with them. Services provide access to services within MessageWay, such as rules processing and distribution lists.

IMPORTANT: When a system failure occurs while an adapter or service is processing a message, the automatic recovery process within MessageWay will attempt to reprocess the message for input or output, based on the Error Action settings on the **Options** page for the location in question. MessageWay repeats its attempt from the beginning of the message, unless check-point restart is available. Currently, FTP and SFTP adapter transfers support restart. On the inbound side, failed receives may leave a partial file in the Message Store, but the retry will overlay partial files. On the outbound side, after an e-mail has been sent by the E-mail adapter but not yet marked delivered by MessageWay, and the process is interrupted, the E-mail adapter will resend the entire message. This may result in sending duplicate messages to the recipient.

How to Stop and Start Adapters and Services

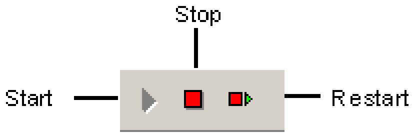
Operators have the option to start and stop adapters and services as needed. When users make changes to the configuration of an adapter or service that is running, operators must restart the adapter or service to make the changes take effect.

CAUTION: To stop an adapter or service that is running and processing messages, you should first allow the traffic to clear. To do this, ***use suspend*** (on page 706) to clear the traffic, and then restart. Suspend allows all traffic to clear before the adapter or service is stopped. Restart will reread the configuration files if changes have been made. Resume will not reread configuration files.

To stop or start an adapter or service when you don't need to first let message traffic clear:

1 Select the adapter or service from MessageWay Explorer.

2 If there is no traffic for the adapter or service, select the button on the toolbar for the appropriate action.

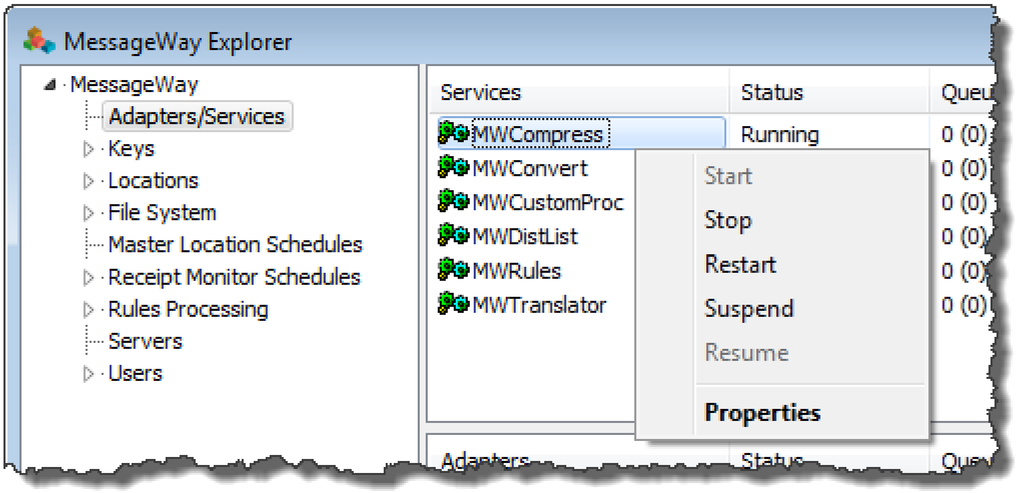


How to Suspend and Resume Adapters and Services

When an adapter or service is running, operators have the option to suspend and resume activity as needed. This allows all messaging traffic to clear before the adapter or service stops. To suspend or resume an adapter or service:

1 Select the adapter or service from MessageWay Explorer.

2 Right click, and select **Suspend** or **Resume**.



- or -

From the Adapters/Services menu, select **Suspend** or **Resume**.

When you suspend an adapter or service, the status should change to **Suspended**. When you resume an adapter or service, the status should change to **Resuming** and then **Running**.

IMPORTANT: If you have made changes to configurations, and you have suspended the adapter or service, issue a restart command to reread the configuration files. The resume command does not reread configuration files.

Effect on Messages of Starting and Stopping Adapters and Services

When an adapter or service is stopped, messages queue to the adapter or service. The number of queued messages appears under the Queued columns in the System Monitor and in the Adapters/Services monitor.

The behavior of the start, stop, suspend and resume commands is as follows:

Stop
- Adapter does not poll locations or send messages
- Service does not receive or send messages
- Message transfers or processing that are in progress are allowed a couple of minutes to finish, after which time they are aborted. Messages in error must be resubmitted manually.

Start
- Adapter and service configurations are reloaded, implementing any changes
- Adapter polls locations and sends messages

- Service receives and sends messages

Suspend
- Adapter does not poll locations or send messages
- Service does not receive or send messages
- Message transfers or processing that are in progress are allowed to finish

Resume
- Adapter and service configurations are *not* reloaded.
- Adapter polls locations and sends messages
- Service receives and sends messages

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

The effect of adapter and service commands on their status is as follows:

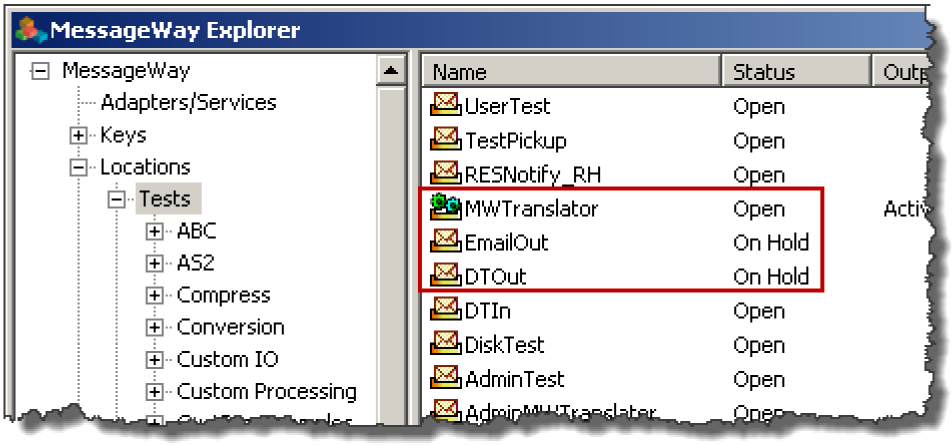
Command	Effect on Adapter or Service Status
Start	Running
Stop	Stopped
Restart	Stopped then Running
Suspend	Suspended
Resume	Running

The following figure shows messages queued for both an adapter and a service.

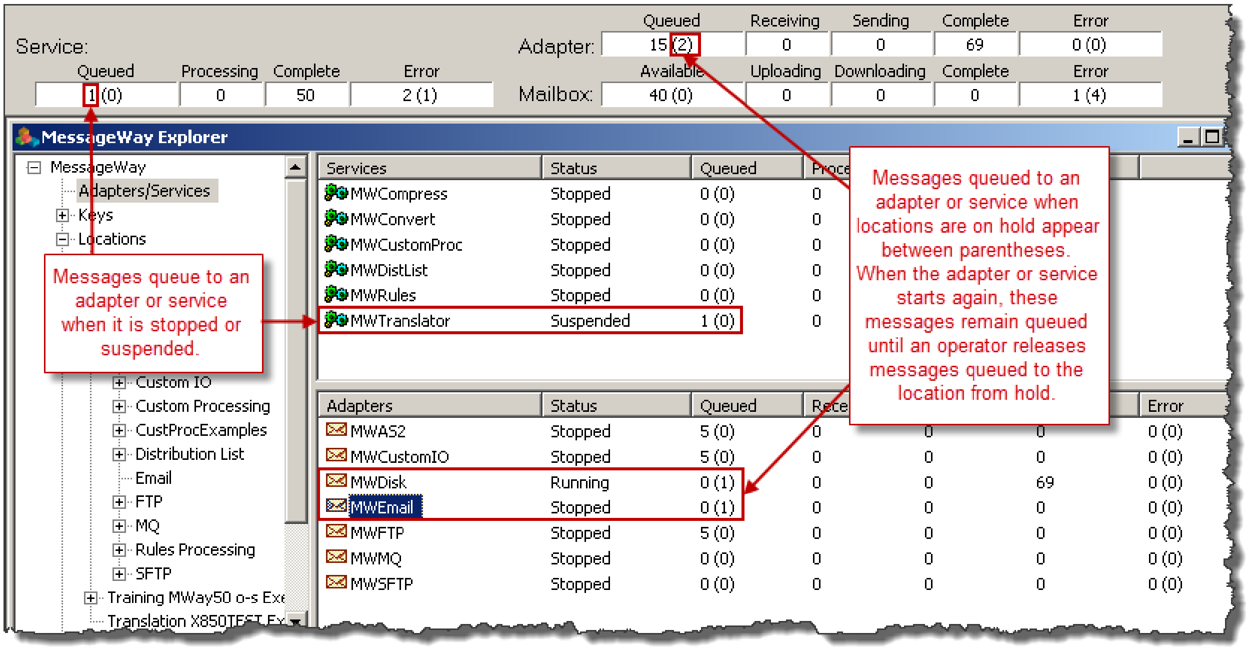
The status of a location takes precedence over the status of an adapter or service, which determines where the numbers appear in the monitors. When an output location is on hold, the messages queued to it appear in the Queued column within parentheses, regardless of the status of the adapter or service. When the location is Open and the adapter or service is stopped or suspended, the messages appear in the Queued column before the parentheses.

Note the status of the following locations:

- MWTranslator is Open/Active
- DTOut is On Hold
- EmailOut is On Hold



Name	Status	Outp
UserTest	Open	
TestPickup	Open	
RESNotify_RH	Open	
MWTranslator	Open	Acti
EmailOut	On Hold	
DTOut	On Hold	
DTIn	Open	
DiskTest	Open	
AdminTest	Open	
AdminMWTranslator	Open	



Service:

Queued	Processing	Complete	Error
1 (0)	0	50	2 (1)

	Queued	Receiving	Sending	Complete	Error
Adapter:	15 (2)	0	0	69	0 (0)
	Available	Uploading	Downloading	Complete	Error
Mailbox:	40 (0)	0	0	0	1 (4)

Services	Status	Queued	Proce
MWCompress	Stopped	0 (0)	0
MWConvert	Stopped	0 (0)	0
MWCustomProc	Stopped	0 (0)	0
MWDistList	Stopped	0 (0)	0
MWRules	Stopped	0 (0)	0
MWTranslator	Suspended	1 (0)	0

Adapters	Status	Queued	Rece			Error
MWAS2	Stopped	5 (0)	0	0	0	0 (0)
MWCustomIO	Stopped	5 (0)	0	0	0	0 (0)
MWDisk	Running	0 (1)	0	0	69	0 (0)
MWEmail	Stopped	0 (1)	0	0	0	0 (0)
MWFTP	Stopped	5 (0)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

Messages queue to an adapter or service when it is stopped or suspended.

Messages queued to an adapter or service when locations are on hold appear between parentheses. When the adapter or service starts again, these messages remain queued until an operator releases messages queued to the location from hold.

An operator can release messages from hold in two ways:

- ***Release all messages for the location*** (on page 710)
- ***Release individual messages*** (on page 716)

Holding and Releasing Locations

To stop delivery to and from a location, operators may put the location on hold.

NOTE: If you are currently monitoring all systems in a multi-system environment, you can perform actions on multiple locations or messages across systems. The command menu will display only commands allowed for *all* the selected items.

The effect on message traffic of putting locations on hold depends on the type of location. The following table describes the expected behavior:

Location Type	Effect of Hold Messages Command
Input site	Messages that are currently being transferred to the Message Store will complete, but no new messages will be received.
Output site	Messages that are currently being transferred from the Message Store will complete, but no new messages will be delivered.
I/O site	Messages that are currently being transferred to or from the Message Store will complete, but no new messages will be received or sent.
Service location	Messages that are currently being received by the service, such as Rules Processing, will complete, but no new messages will be processed. They will be queued to the location in *Hold* status.
Pickup mailbox	Messages that are currently being transferred to or from the Message Store by a user using the Web Client, FTP Perimeter Server or SFTP Perimeter Server will complete, but no new messages may be picked up or sent.
System mailbox	Not applicable

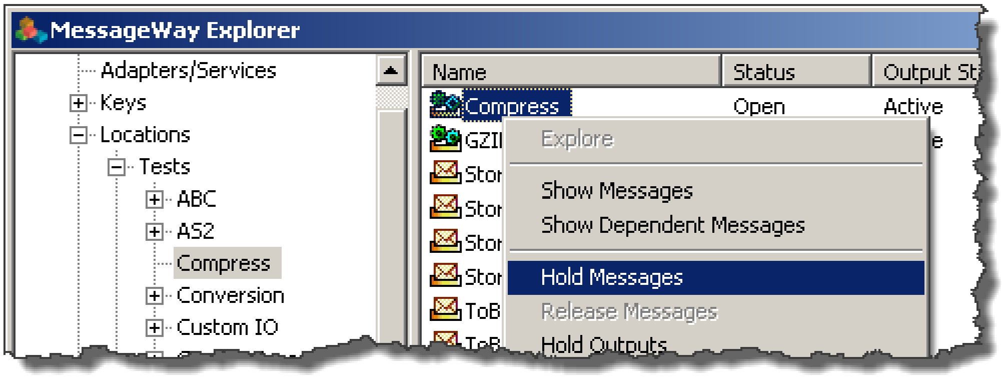
How to Hold All Messages for Locations

To stop the adapter or service from processing messages queued to a location, you can put the location on hold, as follows:

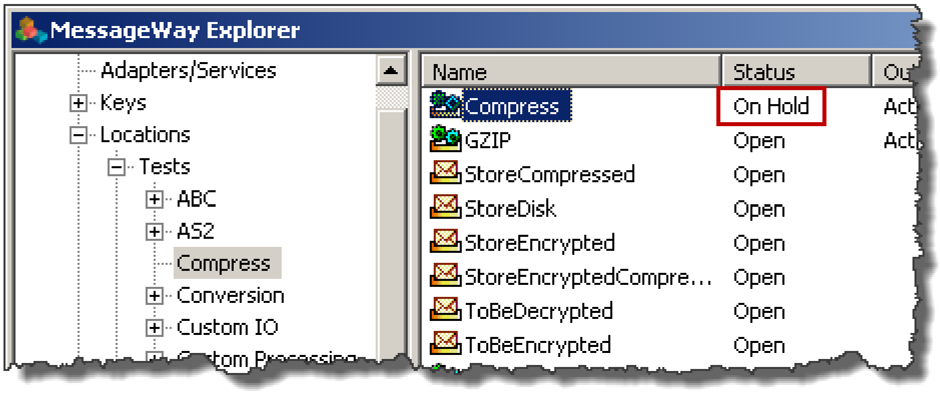
1 From the **Locations** folder in MessageWay Explorer, select one or more locations.

TIP: To change the status of a group of objects such as locations, they must all have the same status. For example, to change the status of locations to *On Hold*, you must only select locations that are currently *Open*. To select a group of objects, rather than select each one separately, click the column header *Status* to sort the objects by status. Then you can easily select a block of objects and then right-click to select the appropriate command to change the status of all selected objects.

2 Right-click, and select **Hold Messages**.



When the command is executed, the status of the location changes to **On Hold**.



Name	Status	Ou
Compress	On Hold	Act
GZIP	Open	Act
StoreCompressed	Open	
StoreDisk	Open	
StoreEncrypted	Open	
StoreEncryptedCompre...	Open	
ToBeDecrypted	Open	
ToBeEncrypted	Open	

CAUTION: When you use the ***copy utility command*** (on page 837), mwimp, to import a location definition, by default, the command places any locations that it is to replace and that have changes, to be put on hold before it overwrites the location definition. As a result, users must manually release the location from hold. However, an option in the command allows it to override the current status of a location definition with the status contained in the saved definition file. This may cause problems if the location is already on hold for some reason and the saved definition has a status of *Open* for the location, then it will change the current status of the location to *Open*.

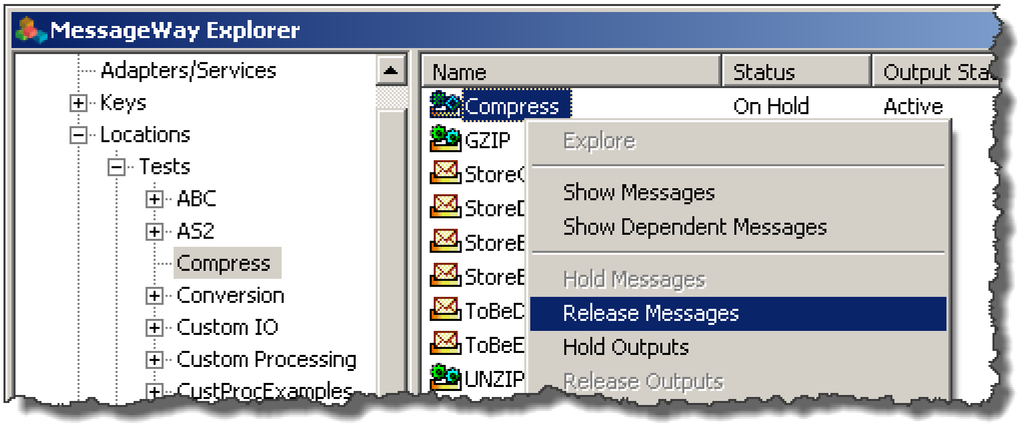
How to Release All Messages for Locations

When you want to allow the adapter or service to continue processing messages queued for a location, you release the location from hold as follows:

1 From the Locations folder in MessageWay Explorer, select one or more locations with a status of *On Hold*.

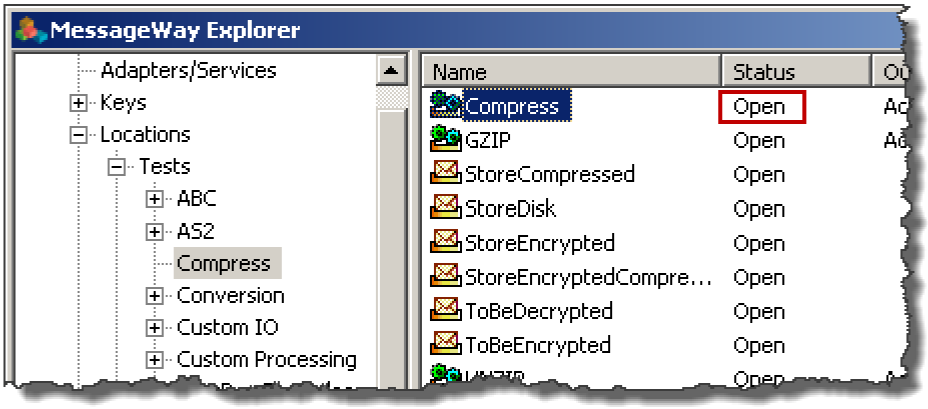
TIP: To change the status of a group of objects such as locations, they must all have the same status. For example, to change the status of locations to *On Hold*, you must only select locations that are currently *Open*. To select a group of objects, rather than select each one separately, click the column header *Status* to sort the objects by status. Then you can easily select a block of objects and then right-click to select the appropriate command to change the status of all selected objects.

2 Right-click, and select the option, **Release Messages**.



Name	Status	Output Sta
Compress	On Hold	Active
GZIP		
StoreC		
StoreD		
StoreE		
StoreE		
ToBeD		
ToBeE		
UNZIP		

When the command is executed, the status of the location changes to **Open**.



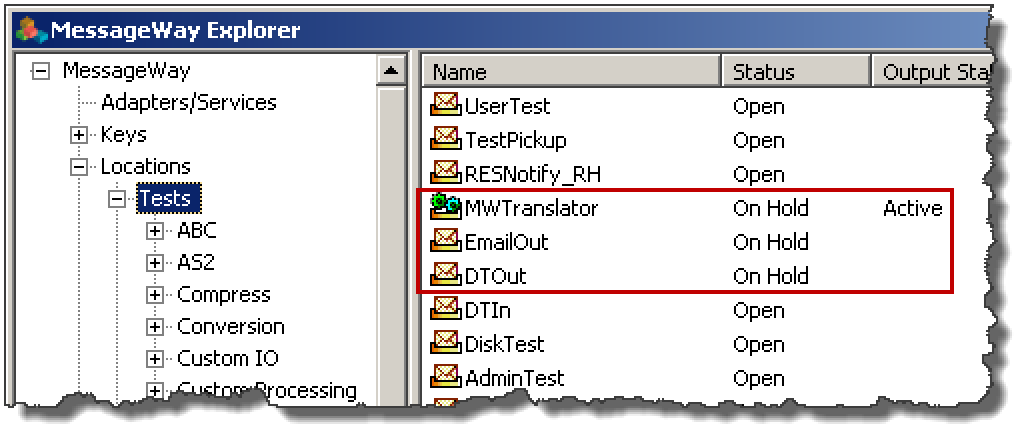
Name	Status	Ou
Compress	Open	Ac
GZIP	Open	Ac
StoreCompressed	Open	
StoreDisk	Open	
StoreEncrypted	Open	
StoreEncryptedCompre...	Open	
ToBeDecrypted	Open	
ToBeEncrypted	Open	
UNZIP	Open	

Effect on Messages of Holding and Releasing Locations

When an input location is on hold, there is no visible effect in the counts of MessageWay monitors, because the input messages have not yet entered MessageWay. For adapters capable of polling, they do not poll locations on hold. When the location is released from hold, all waiting input messages will be processed, typically during the next polling cycle.

When an output site, that is one with a type of Output or I/O, is on hold, messages are queued with a state of *Hold* to the adapter associated with the site. In the following example, notice what happens to the counts in the System Monitor and adapter and services monitors after a message is submitted to an output location that has a status *On Hold*.

The following figure shows the output sites and service that are on hold.

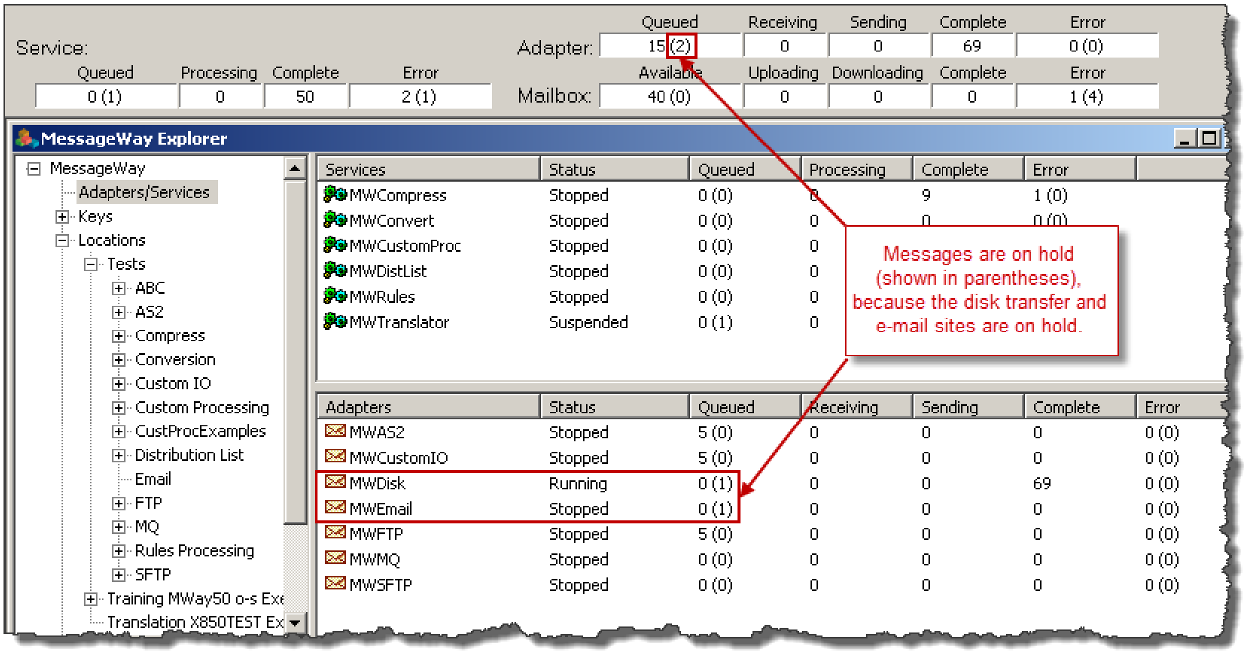


MessageWay Explorer

- MessageWay
  - Adapters/Services
  - Keys
  - Locations
    - Tests
      - ABC
      - AS2
      - Compress
      - Conversion
      - Custom IO
      - Custom Processing

Name	Status	Output Sta
UserTest	Open	
TestPickup	Open	
RESNotify_RH	Open	
MWTranslator	On Hold	Active
EmailOut	On Hold	
DTOut	On Hold	
DTIn	Open	
DiskTest	Open	
AdminTest	Open	

In the monitors, the number of messages on hold appears within parentheses under the **Queued** column. Notice that whether the adapter is running (MWDisk) or stopped (MWEmail), messages held for a location are not processed.



Service:

Queued	Processing	Complete	Error
0 (1)	0	50	2 (1)

Adapter:

Queued	Receiving	Sending	Complete	Error
15 (2)	0	0	69	0 (0)

Mailbox:

Available	Uploading	Downloading	Complete	Error
40 (0)	0	0	0	1 (4)

MessageWay Explorer

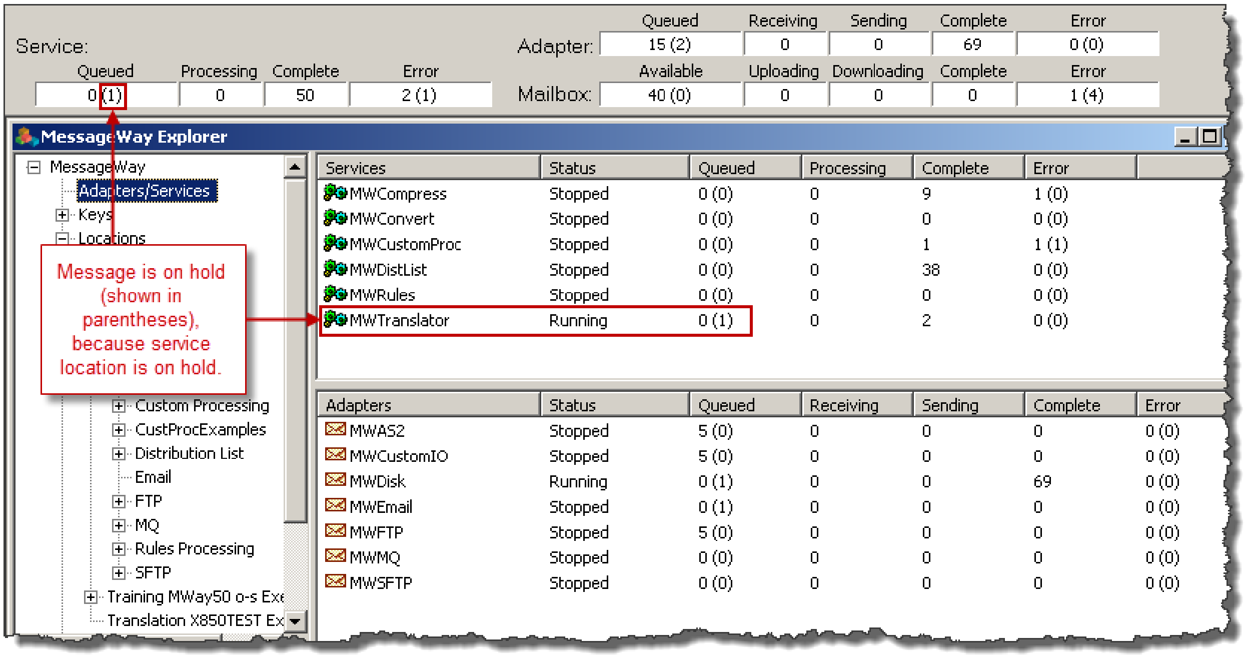
- MessageWay
  - Adapters/Services
  - Keys
  - Locations
    - Tests
      - ABC
      - AS2
      - Compress
      - Conversion
      - Custom IO
      - Custom Processing
      - CustProcExamples
      - Distribution List
      - Email
      - FTP
      - MQ
      - Rules Processing
      - SFTP
    - Training MWay50 o-s Exe
    - Translation X850TEST Ex

Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	9	1 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0		
MWDistList	Stopped	0 (0)	0		
MWRules	Stopped	0 (0)	0		
MWTranslator	Suspended	0 (1)	0		

Messages are on hold (shown in parentheses), because the disk transfer and e-mail sites are on hold.

Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWAS2	Stopped	5 (0)	0	0	0	0 (0)
MWCustomIO	Stopped	5 (0)	0	0	0	0 (0)
MWDisk	Running	0 (1)	0	0	69	0 (0)
MWEmail	Stopped	0 (1)	0	0	0	0 (0)
MWFTP	Stopped	5 (0)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

When a service location is on hold, messages appear in the Queued column for that service. In the following example, notice what happens to the counts in the System Monitor and Services Monitor after a message is submitted to a service location that is on hold. The number of messages on hold appears within parentheses under the Queued column.



Service:

Queued	Processing	Complete	Error
0 (1)	0	50	2 (1)

	Queued	Receiving	Sending	Complete	Error
Adapter:	15 (2)	0	0	69	0 (0)

	Available	Uploading	Downloading	Complete	Error
Mailbox:	40 (0)	0	0	0	1 (4)

Message is on hold (shown in parentheses), because service location is on hold.

Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	9	1 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0	1	1 (1)
MWDistList	Stopped	0 (0)	0	38	0 (0)
MWRules	Stopped	0 (0)	0	0	0 (0)
MWTranslator	Running	0 (1)	0	2	0 (0)

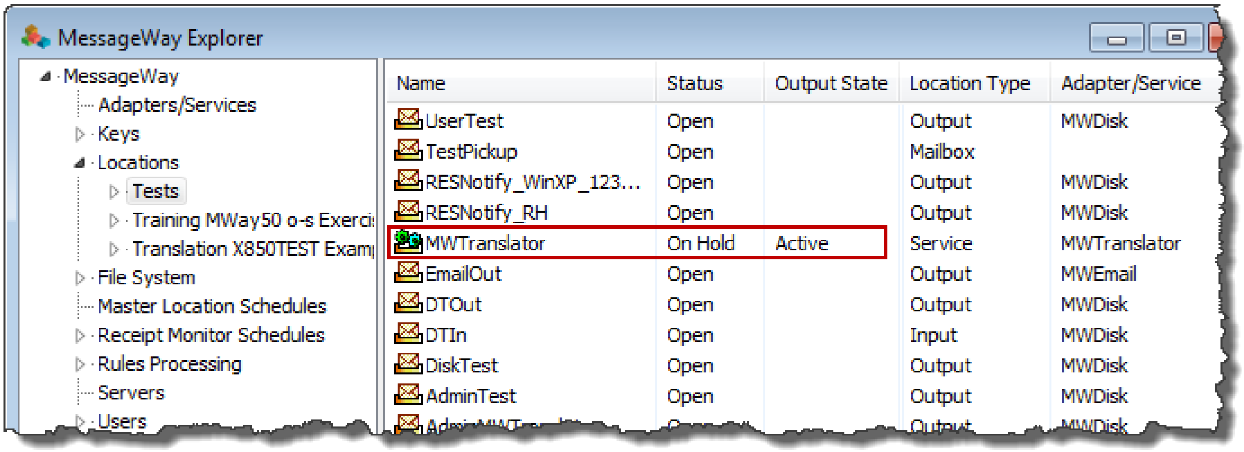
Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWAS2	Stopped	5 (0)	0	0	0	0 (0)
MWCustomIO	Stopped	5 (0)	0	0	0	0 (0)
MWDisk	Running	0 (1)	0	0	69	0 (0)
MWEmail	Stopped	0 (1)	0	0	0	0 (0)
MWFTP	Stopped	5 (0)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

Holding and Releasing Outputs for Service Locations

Releasing the MWTranslator service location from hold, as described in the previous topic ***Holding and Releasing Locations*** (on page 709), will allow MWTranslator to then process the message.

NOTE: If you are currently monitoring all systems in a multi-system environment, you can perform actions on multiple locations or messages across systems. The command menu will display only commands allowed for *all* the selected items.

Let us stop the message at the next point, which is delivery from MWTranslator to its destination location, but before final delivery. Assume that you have already put MWTranslator on hold (Hold Messages). The statuses of MWTranslator would look like the following picture.



Name	Status	Output State	Location Type	Adapter/Service
UserTest	Open		Output	MWDisk
TestPickup	Open		Mailbox	
RESNotify_WinXP_123...	Open		Output	MWDisk
RESNotify_RH	Open		Output	MWDisk
MWTranslator	On Hold	Active	Service	MWTranslator
EmailOut	Open		Output	MWEmail
DTOut	Open		Output	MWDisk
DTIn	Open		Input	MWDisk
DiskTest	Open		Output	MWDisk
AdminTest	Open		Output	MWDisk
AdminMWT	Open		Output	MWDisk

To stop MWTranslator from delivering the outputs to the destination locations:

1 Before you issue the Release command, right-click the service location MWTranslator.

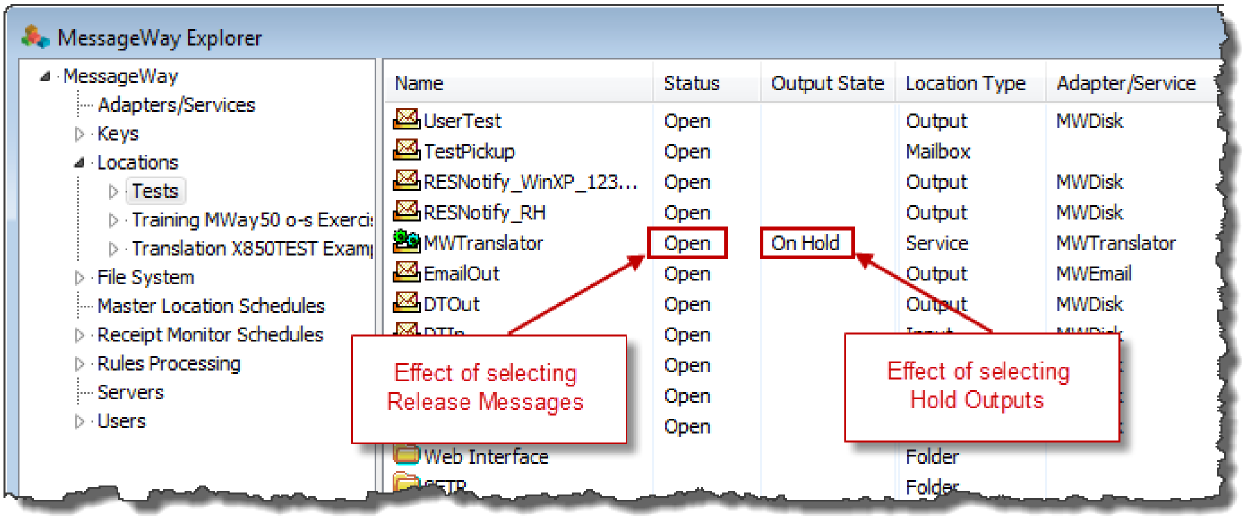
2 From the pop-up menu, click **Hold Outputs**.

The *output state* changes to *On Hold*.

3 Right-click the service location MWTranslator again, and click **Release Messages**.

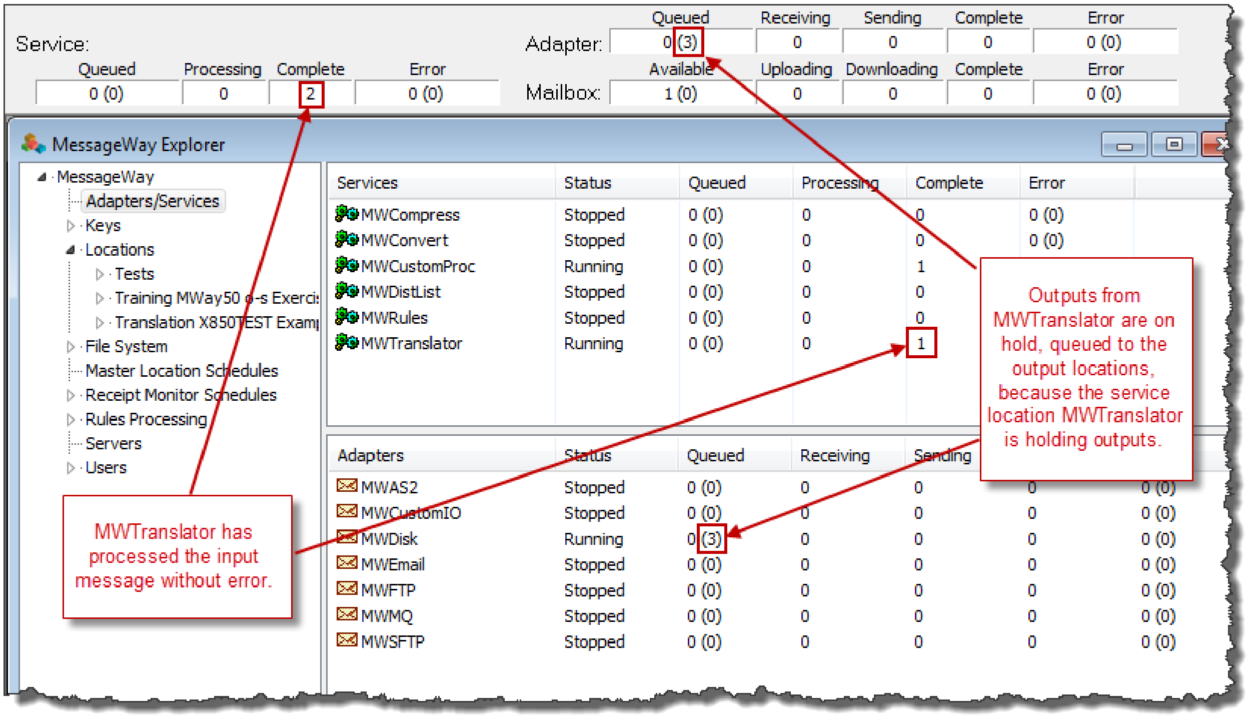
The location *status* changes to *Open*, and MWTranslator will process the message.

The following partial window shows the result of these commands on the status and output state of the MWTranslator service location.


MessageWay Explorer
MessageWay
Adapters/Services
Keys
Locations
Tests
Training MWay50 o-s Exerci
Translation X850TEST Exam
File System
Master Location Schedules
Receipt Monitor Schedules
Rules Processing
Servers
Users
Effect of selecting Release Messages
Effect of selecting Hold Outputs

Name	Status	Output State	Location Type	Adapter/Service
UserTest	Open		Output	MWDisk
TestPickup	Open		Mailbox	
RESNotify_WinXP_123...	Open		Output	MWDisk
RESNotify_RH	Open		Output	MWDisk
MWTranslator	Open	On Hold	Service	MWTranslator
EmailOut	Open		Output	MWEmail
DTOut	Open		Output	MWDisk
DTIn	Open		Input	MWDisk
	Open			
	Open			
	Open			
Web Interface			Folder	
SFTP			Folder	

When the operator issues the **Release Messages** command for the MWTranslator service location, MWTranslator processes the message and the outputs appear in a *Hold* status for the destination adapters and output locations. In this example, all outputs are to be delivered by the Disk Transfer adapter.



Service:

Queued	Processing	Complete	Error
0 (0)	0	2	0 (0)

	Queued	Receiving	Sending	Complete	Error
Adapter:	0 (3)	0	0	0	0 (0)

	Available	Uploading	Downloading	Complete	Error
Mailbox:	1 (0)	0	0	0	0 (0)

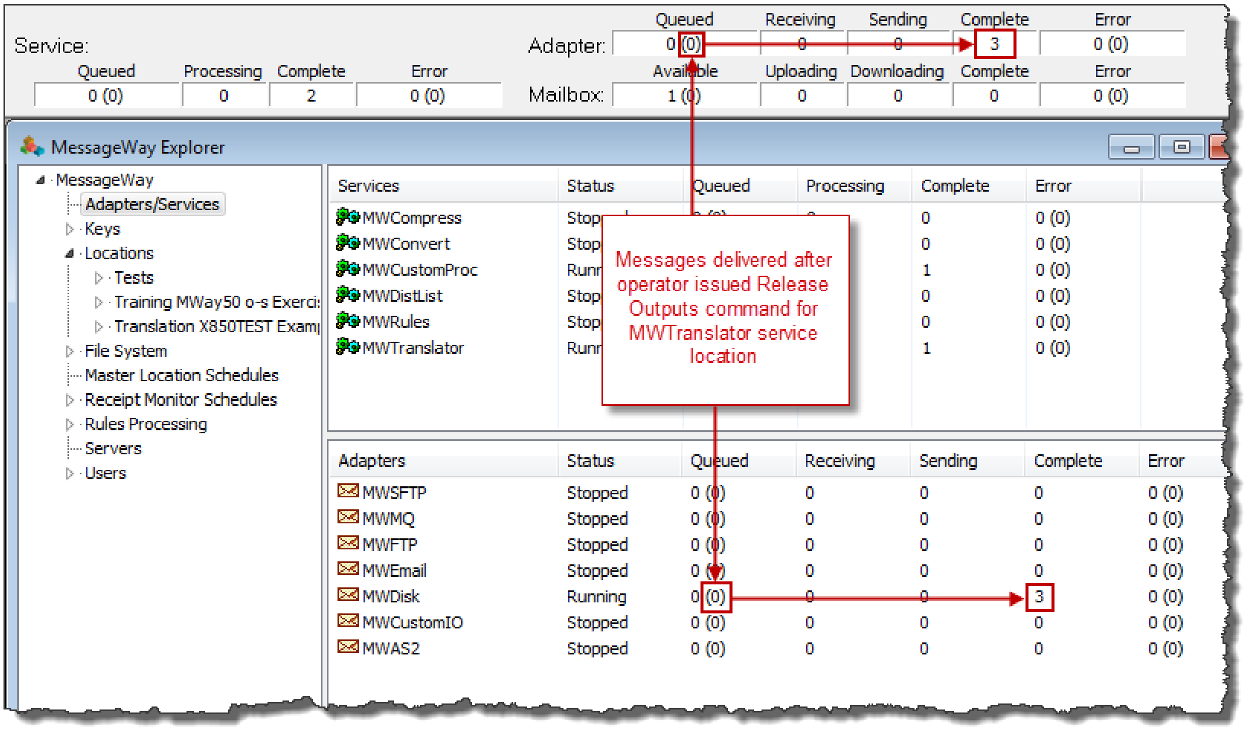
Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Running	0 (0)	0	1	
MWDistList	Stopped	0 (0)	0	0	
MWRules	Stopped	0 (0)	0	0	
MWTranslator	Running	0 (0)	0	1	

Adapters	Status	Queued	Receiving	Sending		
MWAS2	Stopped	0 (0)	0	0	0	0 (0)
MWCustomIO	Stopped	0 (0)	0	0	0	0 (0)
MWDisk	Running	0 (3)	0	0	0	0 (0)
MWEmail	Stopped	0 (0)	0	0	0	0 (0)
MWFTP	Stopped	0 (0)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

MWTranslator has processed the input message without error.

Outputs from MWTranslator are on hold, queued to the output locations, because the service location MWTranslator is holding outputs.

When the operator selects **Release Outputs** for the MWTranslator service location, the adapter associated with the output locations, MWDisk, delivers the messages.



Service:

Queued	Processing	Complete	Error
0 (0)	0	2	0 (0)

	Queued	Receiving	Sending	Complete	Error
Adapter:	0 (0)	0	0	3	0 (0)

	Available	Uploading	Downloading	Complete	Error
Mailbox:	1 (0)	0	0	0	0 (0)

Services	Status	Queued	Processing	Complete	Error
MWCompress	Stop			0	0 (0)
MWConvert	Stop			0	0 (0)
MWCustomProc	Runn			1	0 (0)
MWDistList	Stop			0	0 (0)
MWRules	Stop			0	0 (0)
MWTranslator	Runn			1	0 (0)

Messages delivered after operator issued Release Outputs command for MWTranslator service location

Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWFTP	Stopped	0 (0)	0	0	0	0 (0)
MWEmail	Stopped	0 (0)	0	0	0	0 (0)
MWDisk	Running	0 (0)	0	0	3	0 (0)
MWCustomIO	Stopped	0 (0)	0	0	0	0 (0)
MWAS2	Stopped	0 (0)	0	0	0	0 (0)

Releasing Individual Messages from Hold

Operators cannot put specific messages on hold. They may put locations on hold, which applies a *Hold* state for each message queued to that location at that time. However, operators may release individual messages from hold.

NOTE: If you are currently monitoring all systems in a multi-system environment, you can perform actions on multiple locations or messages across systems. The command menu will display only commands allowed for *all* the selected items.

To release specific messages:

1 Select a message or group of messages from a message list.

TIP: To select a group of messages, rather than select each one separately, click the column header *Status* to sort the messages by status, and then you can select a block of messages at once.

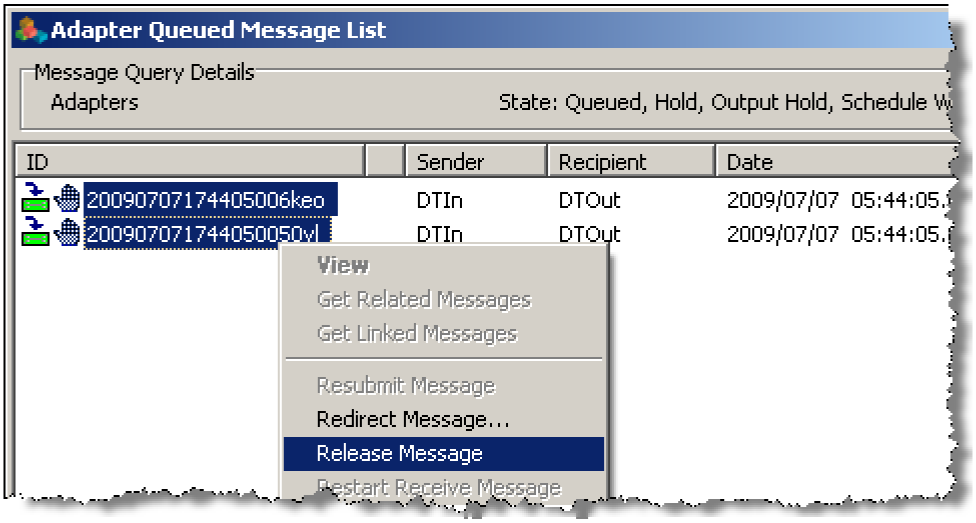
2 From the **Messages** menu, select **Release Message**.

- or -

Right-click one or more messages, and from the pop-up menu, select **Release Message**.

This command overrides the states of *Hold*, *Output Hold* and *Schedule Wait*, and allows the messages to be delivered.

IMPORTANT: The **Release Messages** command will not override a state of *Queued*, which results from a busy or stopped adapter or service. To complete the release process, the adapters or services that deliver the messages must be running.



Adapter Queued Message List

Message Query Details

Adapters State: Queued, Hold, Output Hold, Schedule W

ID		Sender	Recipient	Date
20090707174405006keo		DTIn	DTOut	2009/07/07 05:44:05.
20090707174405005ovl		DTIn	DTOut	2009/07/07 05:44:05.

Canceling Messages

The **Cancel** command allows operators to interrupt the transfer process of a message or group of messages. Operators may cancel messages with any status except **Receiving**, **Complete**, or **Error**. For example, the following message is on hold, as indicated by the icon ✋, and may be canceled.

NOTE: If you are currently monitoring all systems in a multi-system environment, you can perform actions on multiple locations or messages across systems. The command menu will display only commands allowed for *all* the selected items.

To cancel messages:

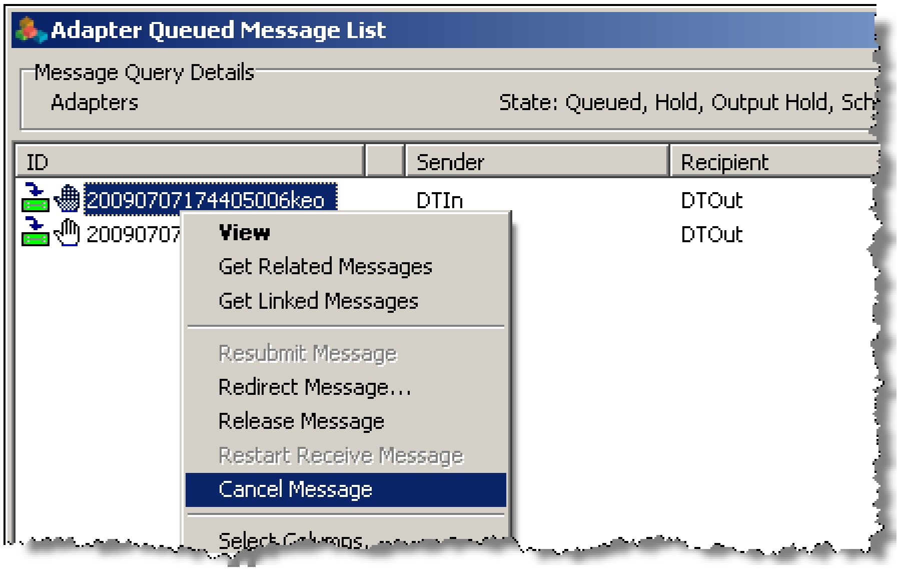
1 ***Select the message or group of messages from a message list*** (on page 733).

TIP: To select a group of messages, rather than select each one separately, click the column header *Status* to sort the messages by status, and then you can select a block of messages at once.

2 From the **Messages** menu, select **Cancel Message**.

- or -

Right-click one or more messages, and from the pop-up menu, select **Cancel Message**.



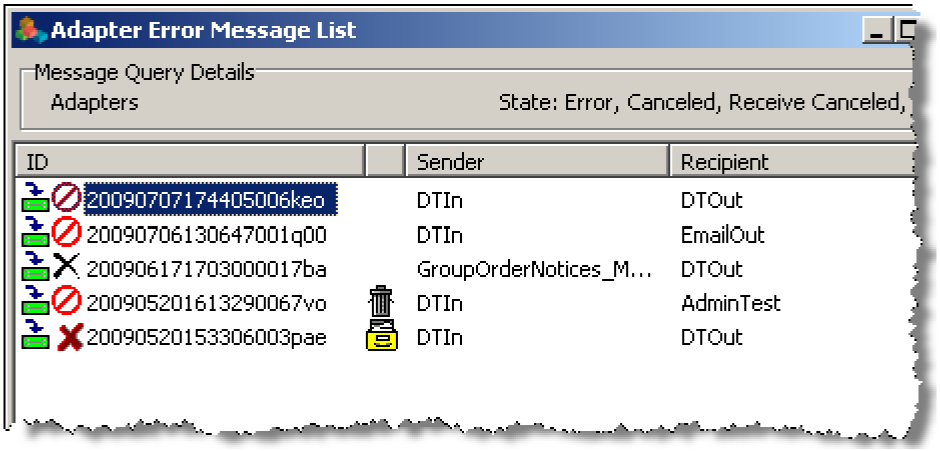
Adapter Queued Message List

Message Query Details
Adapters
State: Queued, Hold, Output Hold, Sch

ID		Sender	Recipient
20090707174405006keo		DTIn	DTOut
20090707			DTOut

Message with Status of Hold (Message List Window)

When a message is canceled, it will have the state of canceled, indicated by the icon ⊘.

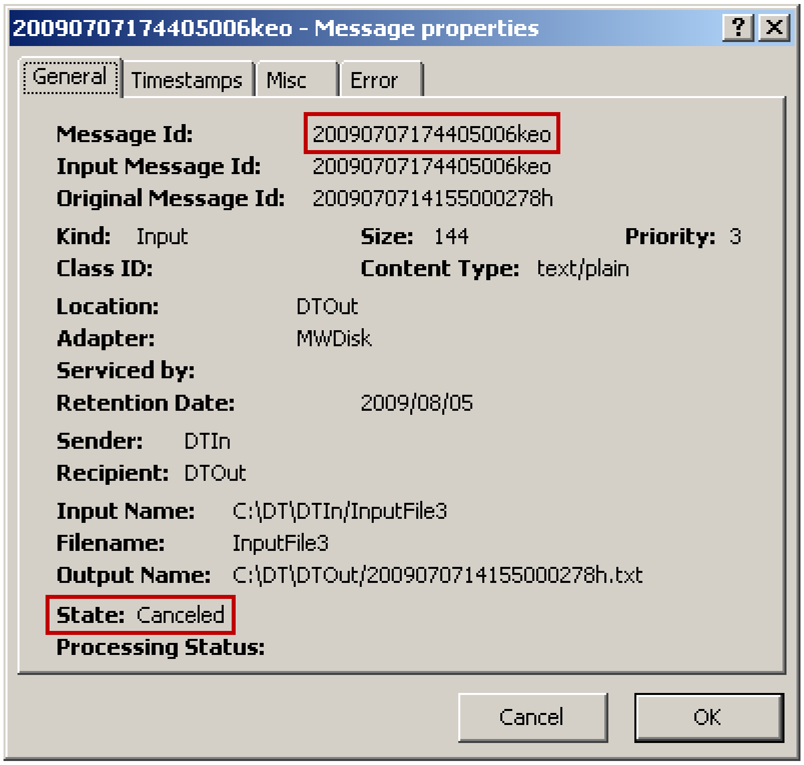


Message Query Details
Adapters State: Error, Canceled, Receive Canceled,

ID		Sender	Recipient
20090707174405006keo		DTIn	DTOut
20090706130647001q00		DTIn	EmailOut
20090617170300017ba		GroupOrderNotices_M...	DTOut
200905201613290067vo		DTIn	AdminTest
20090520153306003pae		DTIn	DTOut

Canceled Message (Message List Window)

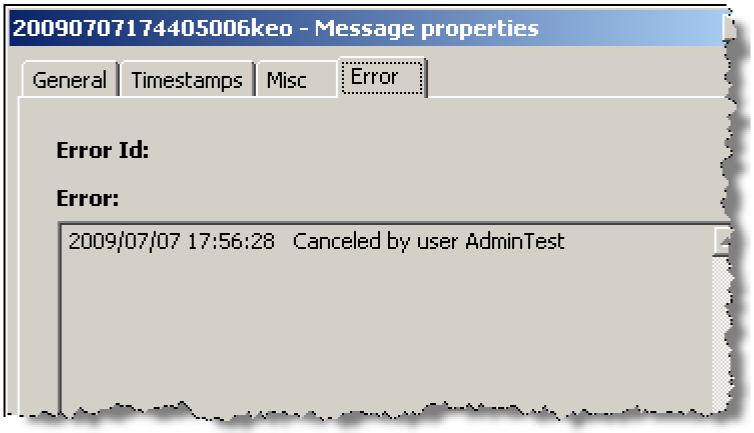
The state *Canceled* also appears on the **General** page of the Message Properties window.



Message Id: 20090707174405006keo
Input Message Id: 20090707174405006keo
Original Message Id: 20090707141550000278h
Kind: Input **Size:** 144 **Priority:** 3
Class ID: **Content Type:** text/plain
Location: DTOut
Adapter: MWDisk
Serviced by:
Retention Date: 2009/08/05
Sender: DTIn
Recipient: DTOut
Input Name: C:\DT\DTIn/InputFile3
Filename: InputFile3
Output Name: C:\DT\DTOut/20090707141550000278h.txt
State: Canceled
Processing Status:

Error Message Canceled by User (General Page, Message Properties Window)

The error text on the **Error** page of the Message Properties window names the user that canceled the message.



Error Id:

Error:

2009/07/07 17:56:28 Canceled by user AdminTest

Error Message Canceled by User (Error Page, Message Properties Window)

Resubmitting and Redirecting Received Messages

To reprocess a message that has already been received in MessageWay, operators may resubmit or redirect messages that have states of *Error*, *Complete* or *Canceled*. Operators may also redirect messages that have additional states of *Available*, *Hold* or *Queued*.

NOTE: If you are currently monitoring all systems in a multi-system environment, you can perform actions on multiple locations or messages across systems. The command menu will display only commands allowed for *all* the selected items.

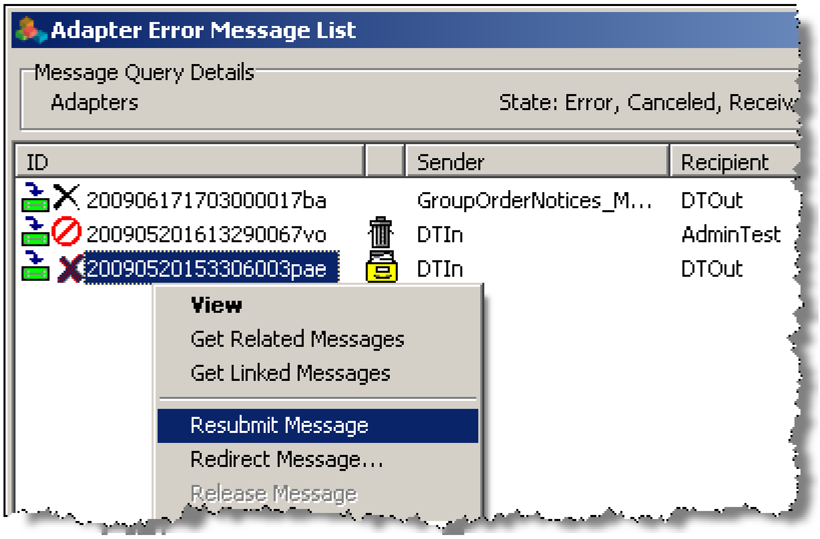
How to Resubmit and Redirect Messages

To resubmit a message that has a state of *Error*, *Complete* or *Canceled*:

1. Select a message or group of messages from the Message List window.
2. From the **Messages** menu, select the command **Resubmit Message**.

   - or -

Right-click, and select **Resubmit Message** from the menu.



ID		Sender	Recipient
200906171703000017ba		GroupOrderNotices_M...	DTOut
200905201613290067vo		DTIn	AdminTest
200905201533060003pae		DTIn	DTOut

NOTE: If you are monitoring all systems in a multi-system environment, remember that *all* the messages you select must have one of the allowed states, *Error*, *Complete* or *Canceled*. When any one of the messages has some other state, such as hold, the resubmit command is not available.

To redirect a message that has a state of *Error*, *Complete*, *Canceled*, *Available*, *Hold* or *Queued*:

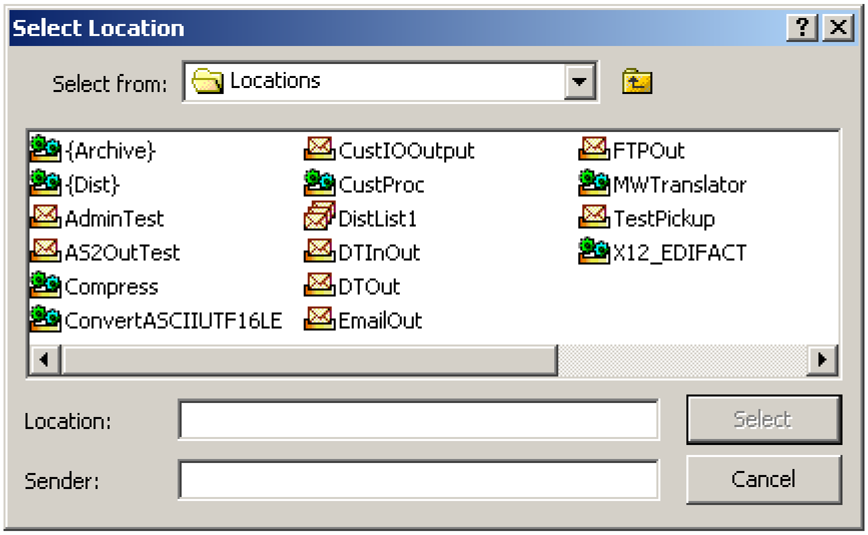
1 Select a message or group of messages from the Message List window.

2 From the **Messages** menu, select the command **Redirect Message**.

- or -

Right-click, and select **Redirect Message** from the menu.

The **Select Location** dialog box appears.



CAUTION: If you are monitoring all systems in a multi-system environment, remember that you can only redirect messages within the system where the message resides. When you select multiple messages that belong to different systems, the Select Location window shows only the first system. If the destination location does not exist on a particular system, the message is sent to the {Unknown} system mailbox.

3 Optionally, in the **Select from** box, change the folder from which to choose a location. The default folder is **Locations**.

4 From the list of locations, choose a location to which you want to send the message.

- or -

In the **Location** box, type the name of a destination location.

5 Optionally, to specify a sender location different from the original one, in the **Sender** box, type the new sender location.

6 Click **Select** to send the message to this different location.

Effect on Messages of Resubmit and Redirect Commands

The content of messages that have been resubmitted or redirected is not duplicated. All such messages share the same content file, and all such messages have the same Original Message ID. However, when the original state of the message is **Error** or **Canceled**, MessageWay updates the information about the message in the current detail record. When the original state of the message is **Complete**, MessageWay creates a new detail record with a new message ID, creating a second message that is related to the first by common content and the same Original Message ID.

Resubmitted and redirected messages that had an original state of **Error** or **Canceled** have the following common characteristics, which are visible on various pages of the Message Properties window.

On the **General** page:

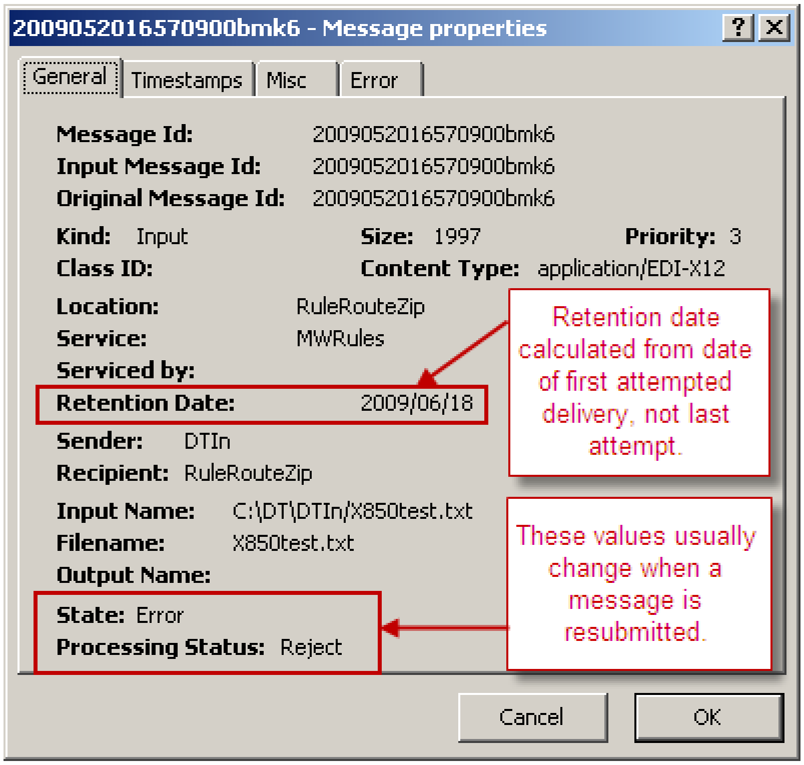
- Original Message ID does not change
- Retention Date of message is based on the date and time the message was originally submitted
- State is updated to reflect the result of the last time message was sent

On the **Timestamps** page

- Time Sent or Received is updated to last time message was sent
- Inbound (IB) date and time stamps reflect the first time the message was sent
- Outbound (OB) date and time stamps reflect the last time the message was sent

NOTE: The priority of a message that has been resubmitted or redirected will retain the priority of the original message. Use the ***Change Priority command*** (on page 729) to change the priority of the message before using the Resubmit or Redirect commands.

The following input message, which had an error, was resubmitted. The **General** page of the Message Properties window shows a retention date of thirty days from the date the message was originally sent. On the **Timestamps** page, the outbound date and time sent were updated to reflect the latest attempt to send the message. The message still has a state of Error, because the problem was not corrected to allow normal delivery.



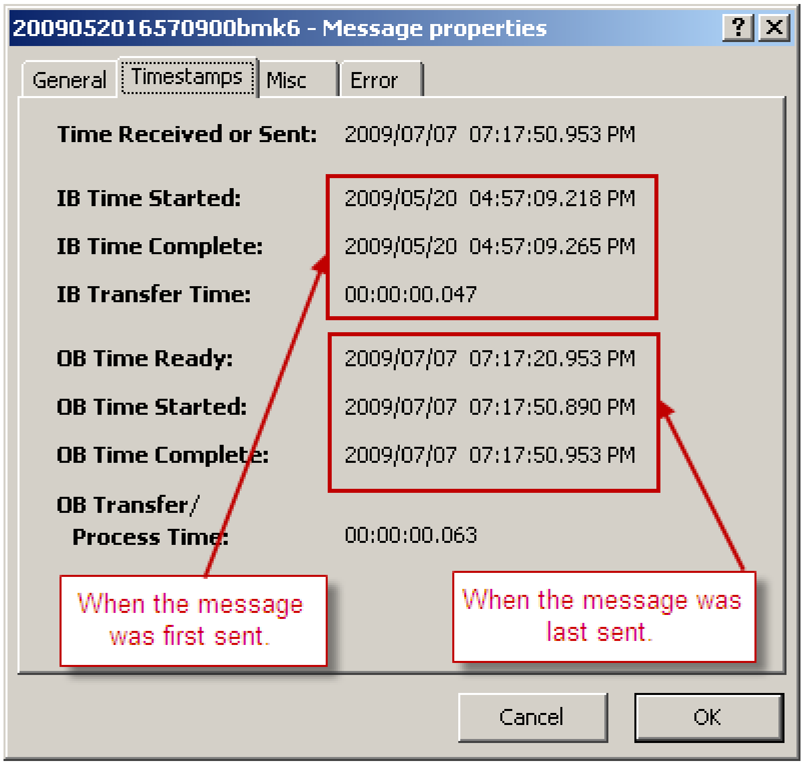
Message Id: 2009052016570900bmk6
Input Message Id: 2009052016570900bmk6
Original Message Id: 2009052016570900bmk6
Kind: Input **Size:** 1997 **Priority:** 3
Class ID: **Content Type:** application/EDI-X12
Location: RuleRouteZip
Service: MWRules
Serviced by:
Retention Date: 2009/06/18
Sender: DTIn
Recipient: RuleRouteZip
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.txt
Output Name:
State: Error
Processing Status: Reject

Retention date calculated from date of first attempted delivery, not last attempt.

These values usually change when a message is resubmitted.

Effect of Resubmit Command on Message Properties Window (General Page)

The **Timestamps** page shows the date and time the message was sent originally and the date and time the message was last sent.



Time Received or Sent: 2009/07/07 07:17:50.953 PM

IB Time Started: 2009/05/20 04:57:09.218 PM

IB Time Complete: 2009/05/20 04:57:09.265 PM

IB Transfer Time: 00:00:00.047

OB Time Ready: 2009/07/07 07:17:20.953 PM

OB Time Started: 2009/07/07 07:17:50.890 PM

OB Time Complete: 2009/07/07 07:17:50.953 PM

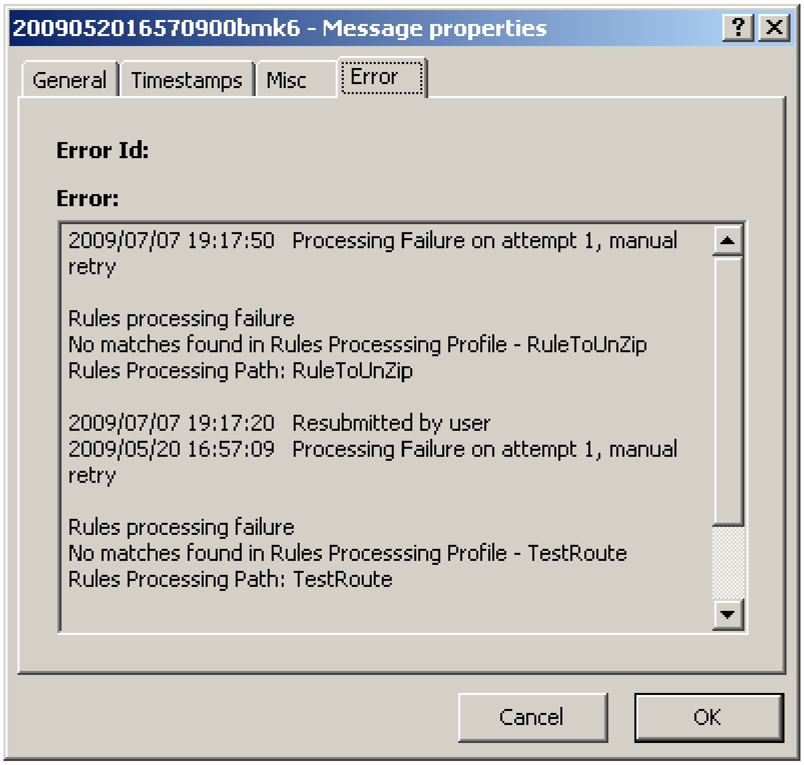
OB Transfer/ Process Time: 00:00:00.063

When the message was first sent.

When the message was last sent.

Effect of Resubmit Command on Message Properties Window (Timestamps Page)

The **Error** page shows some history about the resubmitted message.

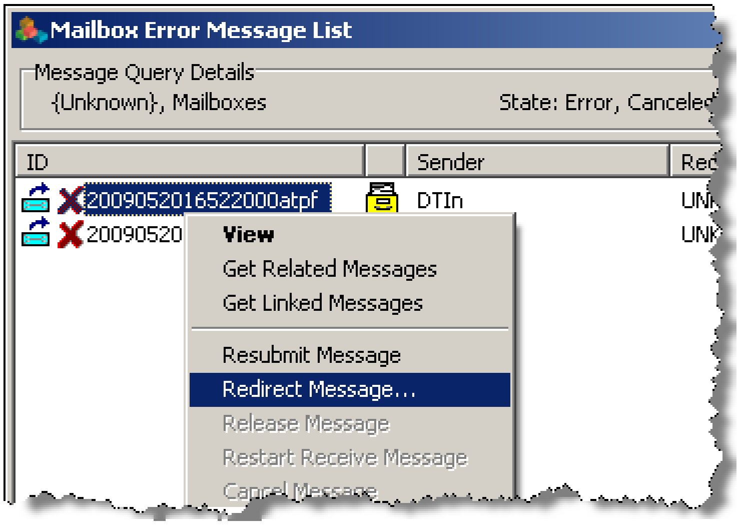


Error Id:

Error:

```
2009/07/07 19:17:50   Processing Failure on attempt 1, manual
retry

Rules processing failure
No matches found in Rules Processsing Profile - RuleToUnZip
Rules Processing Path: RuleToUnZip

2009/07/07 19:17:20   Resubmitted by user
2009/05/20 16:57:09   Processing Failure on attempt 1, manual
retry

Rules processing failure
No matches found in Rules Processsing Profile - TestRoute
Rules Processing Path: TestRoute
```

The following message will be redirected from the {Unknown} system mailbox to a different location, because the original location did not exist. The **General** page of the Message Properties window shows a retention date of thirty days from the date the message was originally sent. The *Location* and *Recipient* values were updated to show the latest location to which the message was delivered. On the **Timestamps** page, the outbound date and time sent will be updated to reflect the latest attempt to send the message. The state of the message was updated to Complete.

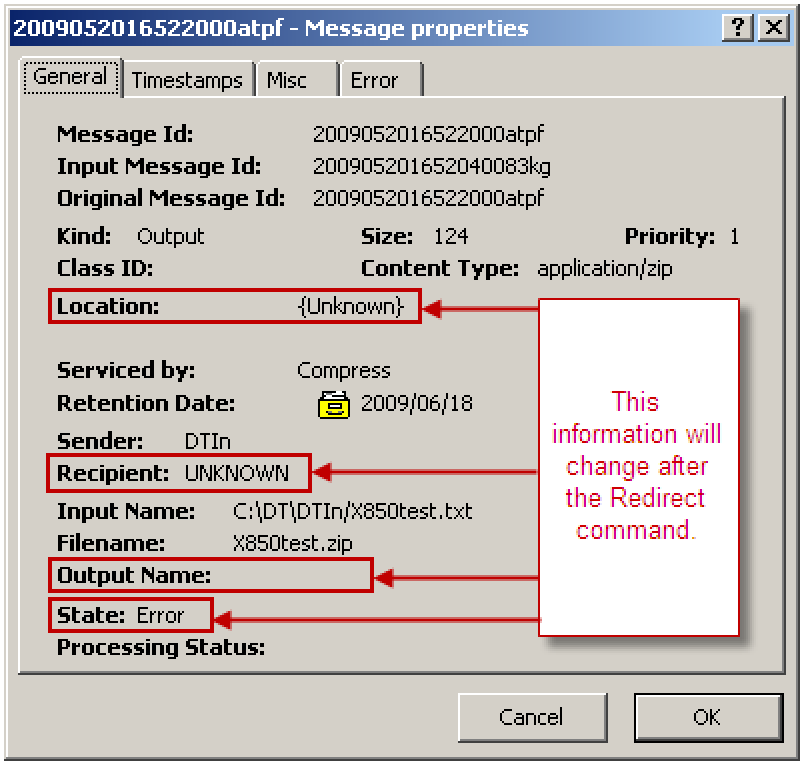


Message Query Details
{Unknown}, Mailboxes State: Error, Canceled

ID		Sender	Rec
2009052016522000atpf		DTIn	UNI
20090520			UNK

Result of Redirect Command Shown on Message List Window

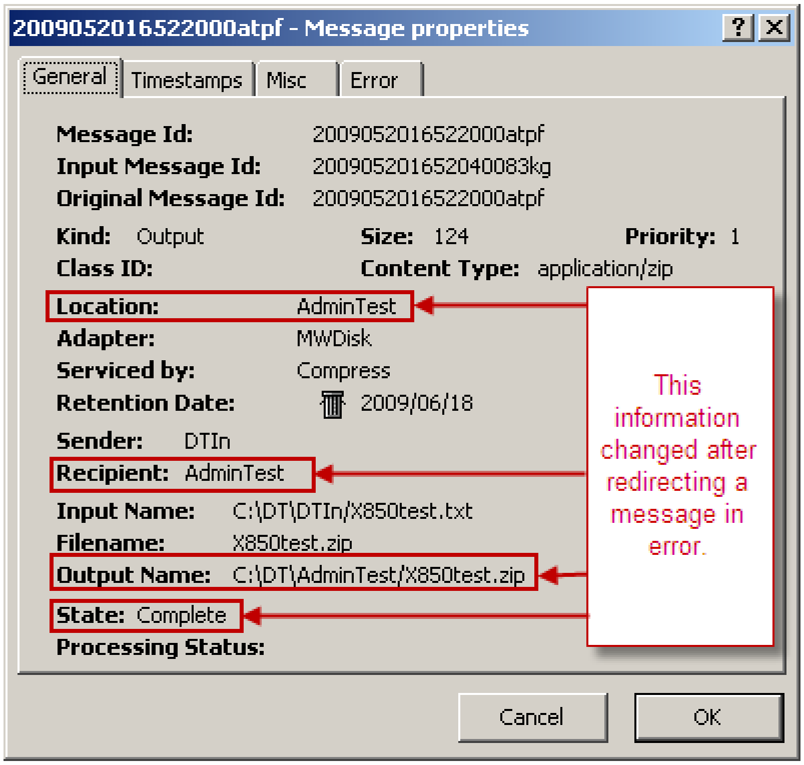
The following before and after versions of the **General** page for the message show what information has changed for the original message that was in error after using the **Redirect Messages** command.



Message Id: 2009052016522000atpf
Input Message Id: 2009052016520400083kg
Original Message Id: 2009052016522000atpf
Kind: Output
Size: 124
Priority: 1
Class ID:
Content Type: application/zip
Location: {Unknown}
Serviced by: Compress
Retention Date: 2009/06/18
Sender: DTIn
Recipient: UNKNOWN
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.zip
Output Name:
State: Error
Processing Status:

This information will change after the Redirect command.

Before Effect of Redirect Command on Message Properties Window (General Page)



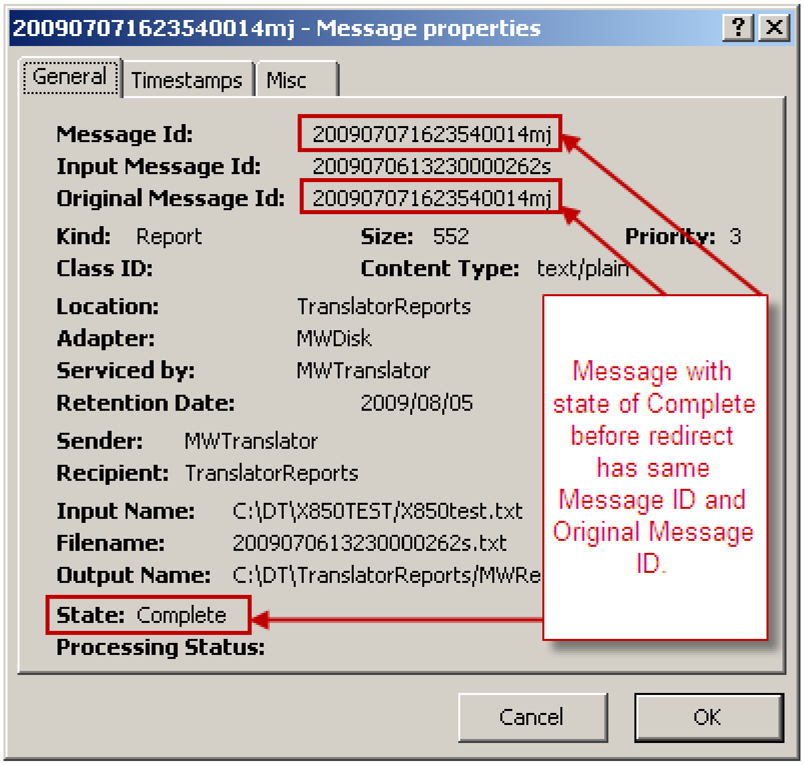
Message Id: 2009052016522000atpf
Input Message Id: 200905201652040083kg
Original Message Id: 2009052016522000atpf
Kind: Output
Size: 124
Priority: 1
Class ID:
Content Type: application/zip
Location: AdminTest
Adapter: MWDisk
Serviced by: Compress
Retention Date: 2009/06/18
Sender: DTIn
Recipient: AdminTest
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.zip
Output Name: C:\DT\AdminTest/X850test.zip
State: Complete
Processing Status:

This information changed after redirecting a message in error.

Effect of Redirect Command on Message Properties Window (General Page)

The following example shows a message that has been redirected, that had an original state of Complete. Notice that MessageWay has created a second detail record for the message.

Here is the original message before issuing the **Redirect Message** command.

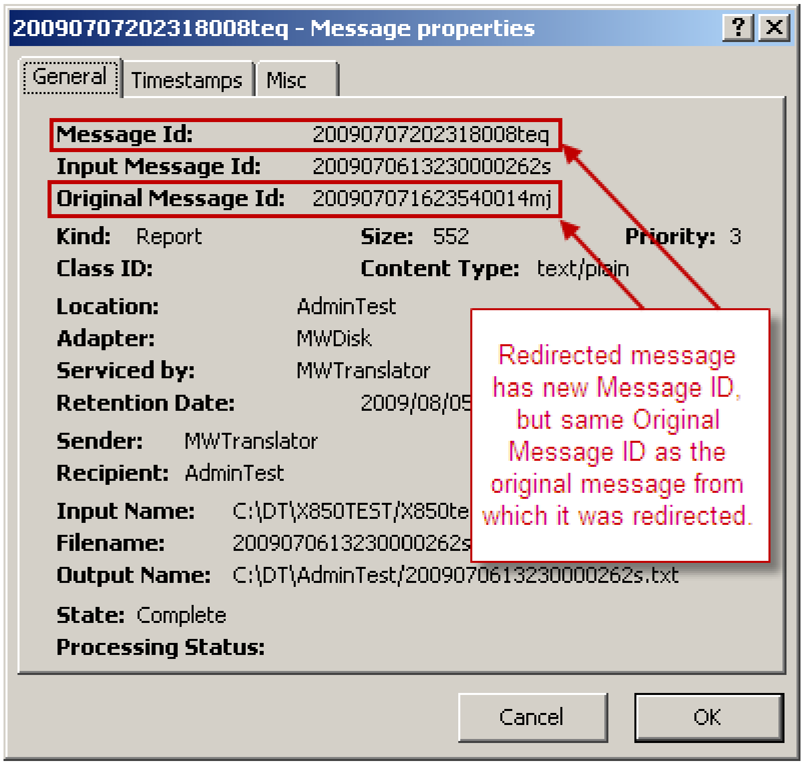


Message Id: 200907071623540014mj
Input Message Id: 2009070613230000262s
Original Message Id: 200907071623540014mj
Kind: Report Size: 552 Priority: 3
Class ID: Content Type: text/plain
Location: TranslatorReports
Adapter: MWDisk
Serviced by: MWTranslator
Retention Date: 2009/08/05
Sender: MWTranslator
Recipient: TranslatorReports
Input Name: C:\DT\X850TEST/X850test.txt
Filename: 2009070613230000262s.txt
Output Name: C:\DT\TranslatorReports/MWRe
State: Complete
Processing Status:

Message with state of Complete before redirect has same Message ID and Original Message ID.

Original Message Information on Message Properties Window before Redirect Command

Here is the information for the new message after it was redirected to a different location. Typically a Redirect Message command would identify a different output location than the original message, but this is not mandatory.



20090707202318008teq - Message properties

Message Id: 20090707202318008teq
Input Message Id: 20090706132300002625s
Original Message Id: 20090707162354001 4mj
Kind: Report
Size: 552
Priority: 3
Class ID:
Content Type: text/plain
Location: AdminTest
Adapter: MWDisk
Serviced by: MWTranslator
Retention Date: 2009/08/05
Sender: MWTranslator
Recipient: AdminTest
Input Name: C:\DT\X850TEST/X850te
Filename: 20090706132300002625s
Output Name: C:\DT\AdminTest/20090706132300002625s.txt
State: Complete
Processing Status:

Redirected message has new Message ID, but same Original Message ID as the original message from which it was redirected.

Original Message Information on Message Properties Window after Redirect Command

IMPORTANT: For those messages whose content is stored on disk rather than in the database, the content of messages that have been resubmitted or redirected remains where it was placed in the Message Store directory under the subdirectory for the first or original destination location.To find the message content on disk in the Message Store, you should search in the **msgstore** data directory by Message ID or by Original Message ID. The message will reside in a subdirectory of the same name as the original location to which it was delivered. If the original location was invalid, the message will be under the **{Unknown}** subdirectory. If you don't find the message here, use **Find Archive Messages** if you have used the MessageWay Archive program.

Retrying Failed Message Receipt

MessageWay queues and logs messages for receipt into MessageWay. It assigns them a message ID and other properties before it starts reading the data.

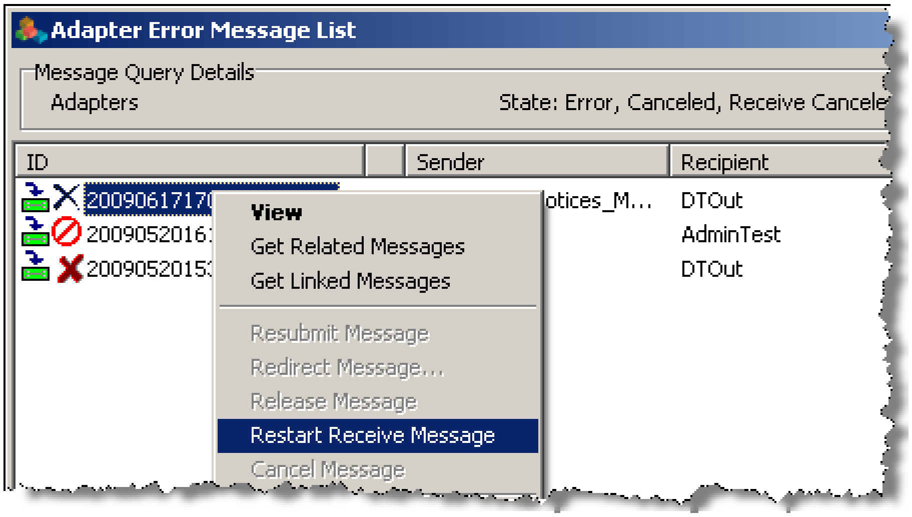
IMPORTANT: For input locations, users should specify an Error Action. For input messages that go to an error state because they are not properly received, MessageWay will only attempt to input the message again when an error action is configured for the input location or when the adapter is restarted.

When the adapter starts the receive process and there is an error, it will execute the **Error Action** strategy specified on the **Options** page of the Site Properties window of the input location.

NOTE: For retries, the adapter attempts to read the data from the beginning of the message. Another option, restartable, is available for the FTP and SFTP adapters. When the adapter connects to a server that supports check-point restart and the **Restartable** box is checked on the input page of the site properties window, MessageWay will attempt to restart receiving the data from the last check-point.

Messages that fail receipt have a state of *Receive Error*. Users may manually try to receive the message again, as follow:

1. From the Message List, right-click the message, which should have the Receive Error icon, ✕, next to it.
2. From the pop-up menu, select **Restart Receive Message**.



Adapter Error Message List

Message Query Details
Adapters State: Error, Canceled, Receive Cancele

ID		Sender	Recipient
20090617170		otices_M...	DTOut
2009052016			AdminTest
2009052015			DTOut

MessageWay will attempt to reread the file, overlaying any partial data that it may already have stored.

IMPORTANT: In the event that retry attempts fail to receive the message successfully, partial files may be stored in MessageWay. Also, MessageWay must clear the file name from the queue before it will be able to receive any new files that use the same file name. To clear the file name from the queue, users may restart the adapter.

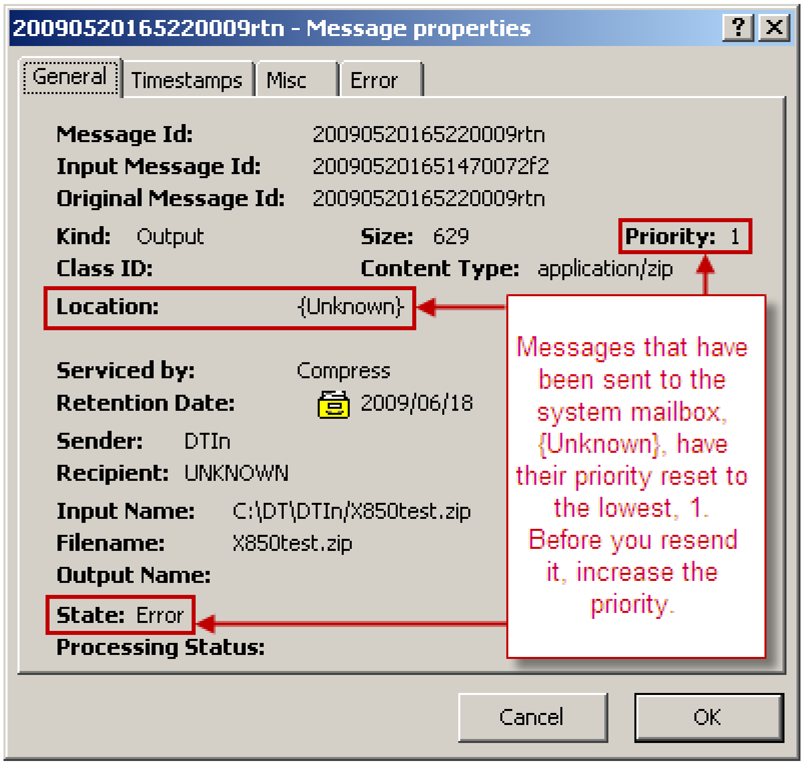
Changing Message Priority

Operators may also affect how messages are processed by changing the priority of a message. Priority is typically assigned by location configuration. For more information about message priorities, refer to the topic in the reference section, ***Priority*** (on page 1047).

NOTE: If you are currently monitoring all systems in a multi-system environment, you can perform actions on multiple locations or messages across systems. The command menu will display only commands allowed for *all* the selected items.

To change the priority of messages:

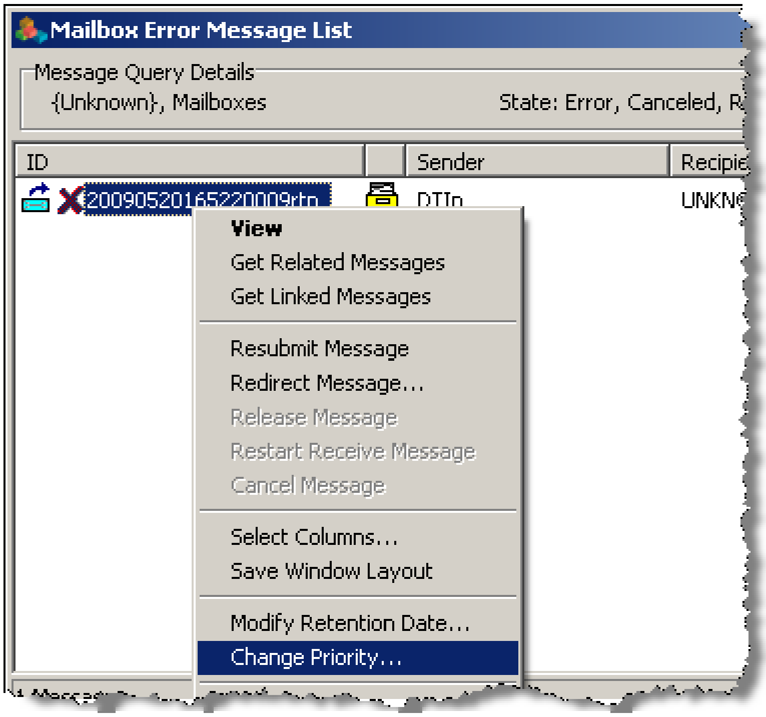
1. ***Select the message or group of messages from a message list*** (on page 733).
2. (Optional) To view the original priority of the message, right-click the message, and select **Properties** from the pop-up menu.



Message Id: 20090520165220009rtn
Input Message Id: 20090520165147007 2f2
Original Message Id: 20090520165220009rtn
Kind: Output **Size:** 629 **Priority:** 1
Class ID: **Content Type:** application/zip
Location: {Unknown}
Serviced by: Compress
Retention Date: 2009/06/18
Sender: DTIn
Recipient: UNKNOWN
Input Name: C:\DT\DTIn/X850test.zip
Filename: X850test.zip
Output Name:
State: Error
Processing Status:

Messages that have been sent to the system mailbox, {Unknown}, have their priority reset to the lowest, 1. Before you resend it, increase the priority.

3 From the **Messages** menu or with a right-click from the pop-up menu, select **Change Priority**.

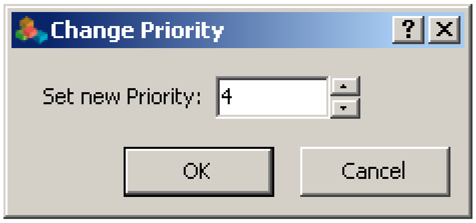


Message Query Details
{Unknown}, Mailboxes State: Error, Canceled, R

ID		Sender	Recipie
2009052016522009rtn		DTIn	UNKN

The **Change Priority** dialog box appears.

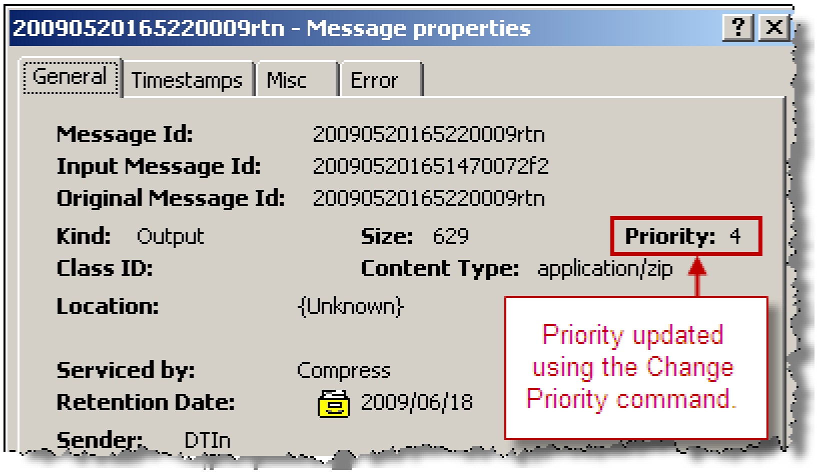
4 Select or type a new priority from 1 (lowest) to 5 (highest).



Set new Priority: 4

NOTE: This updated priority is used for subsequent steps in a process or commands, such as *Redirect Message* or *Resubmit Message*.

5 (Optional) To review the changed priority, right-click the message, and select **Properties** from the pop-up menu.



Message Id: 20090520165220009rtn
Input Message Id: 200905201651470072f2
Original Message Id: 20090520165220009rtn
Kind: Output
Size: 629
Priority: 4
Class ID:
Content Type: application/zip
Location: {Unknown}
Serviced by: Compress
Retention Date: 2009/06/18
Sender: DTIn

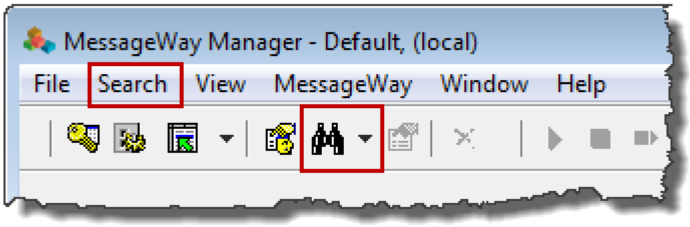
Priority updated using the Change Priority command.

Finding Configurations and Messages

This section describes how to use the search options in MessageWay to find messages and various configurations in any of the monitored systems in the environment.

Basic Search Strategies

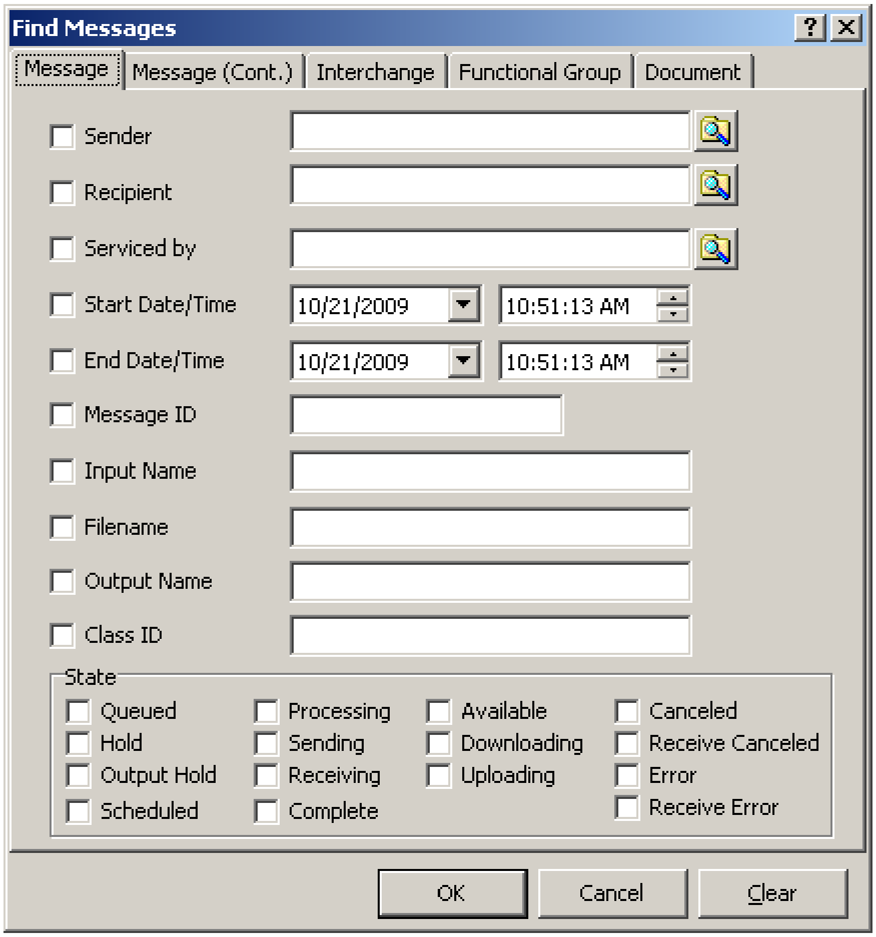
Search options are available from the **Search** menu on the toolbar and the **Search** button on the task bar, as shown in the following figure:



Users may search for the following:

- Messages
- Archive messages
- Locations
- Location schedules
- Receipt schedules
- Rules profiles
- Keys
- Users
- Sessions
- Logs

A dialog box appears with search options.



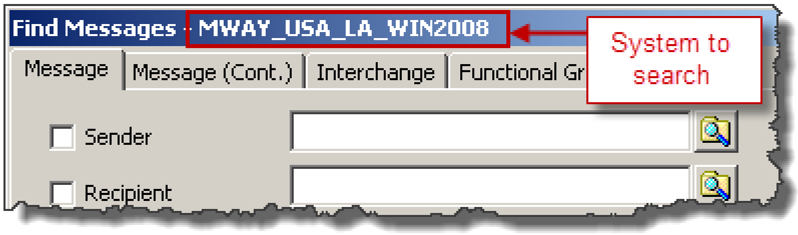
□ Start Date/Time 10/21/2009 10:51:13 AM

□ End Date/Time 10/21/2009 10:51:13 AM

When you monitor all systems in a multi-system environment, MessageWay searches those environments that you are monitoring and to which you are connected and logged on. When you monitor only one system, MessageWay searches that system. The systems searched appears in the window header of the find window and the item list.

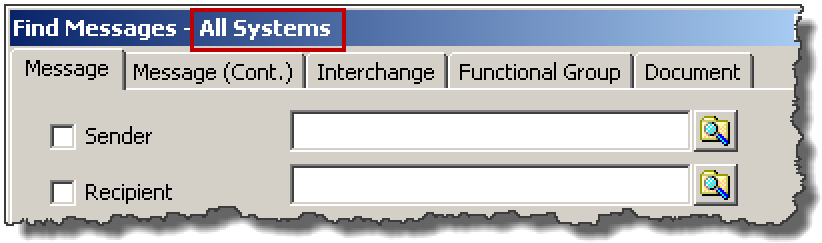
For location and message lists, users may perform commands on items that belong to different systems. For example, they can select locations from system A and system B and put them on hold. Or, they can select messages from system A and system B with a state of Complete and resubmit them. However, *all* items selected from the list must allow the command, or the command will not be available.

The following Find Messages window shows that the search will be for the system listed:



System to search

This Find Messages window shows that the search will be for all systems:



In most fields on the Find windows, you can search using the wild cards before or after a text string, but not within a string. You can use an asterisk, *, for any number of unknown characters and a question mark, ?, for one or more unknown characters.

Finding Messages

When users are trying to resolve problems, they must know what kind of information is available about messages and how to find that information. The information that is available for all messages is stored in the Message Store. Additional information about actions on messages is stored in the ***audit files*** (on page 699).

Additional information may be available for messages that have been processed by a service, such as MessageWay Translator or Custom Processing. For example, for MessageWay Translator, the processing reports may be sent as messages to locations dictated by its location configurations. There may also be logging and reconciliation information in the MessageWay database when users have these features enabled. To query this translation logging and reconciliation information, operators must use the MW Translator Operator Program. For more information, refer to the online help for the program, or the documentation, *MW Translator Operator Guide and Reference*.

Overview of Finding Message Information

The focus here is to help operators understand and find information in the Message Store.

Understanding the Message Store

The Message Store has two parts: details about the message and message content itself. Physically, the content files may be configured to be stored in different places, based on the configuration of the destination location of a message. The setting is on the **Options** tab of the destination location. For more information about this location, refer to the reference topic, ***Options (Location Properties)*** (on page 1051).

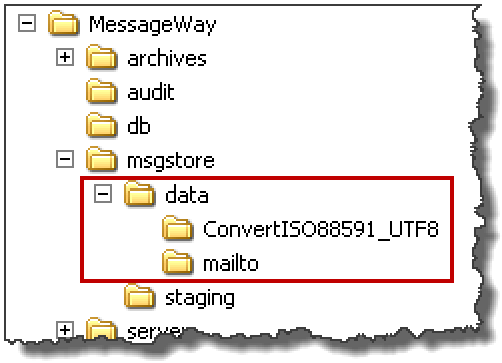
The following table describes the options available to store messages:

Message Information	Storage Location
Message detail	MessageWay database
Message content	▪ Disk on local file system - or - ▪ MessageWay database

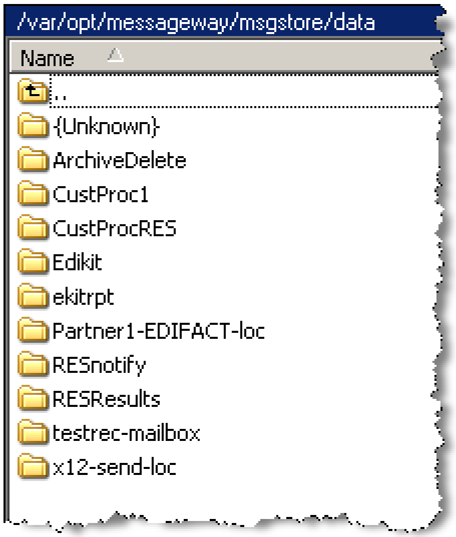
Message content is always associated with the original destination location. When content files are stored on disk, MessageWay creates a directory structure and places the files in subdirectories with the same name as the destination location. The default location of the structure varies depending on the operating system, as shown in the following table:

System	Default Directory for Message Content Files
Window	c:\MessageWay\msgstore\data
UNIX/Linux	/var/opt/messageway/msgstore/data

The subdirectories of the **data** directory contain the content files. MessageWay stores the data in these subdirectories using the names of the original destination locations. For Windows, the directory structure looks as follows:



For UNIX and Linux, the default directory structure looks as follows:



/var/opt/messageway/msgstore/data

Name

..
{Unknown}
ArchiveDelete
CustProc1
CustProcRES
Edikit
ekitrpt
Partner1-EDIFACT-loc
RESnotify
RESResults
testrec-mailbox
x12-send-loc

The files are stored as **.msg** files, whose name is the same as the Message ID that you see on a message list in the Manager, except that the disk file is prefixed with an **M**.

NOTE: There will typically be more messages in the disk subdirectory for a given destination location than appear on a message list for the same location when you choose **Show Messages** in the Manager. This is because all contents remain in the original destination location, even though they may have been subsequently sent elsewhere, as when you redirect a message.

Understanding Message IDs

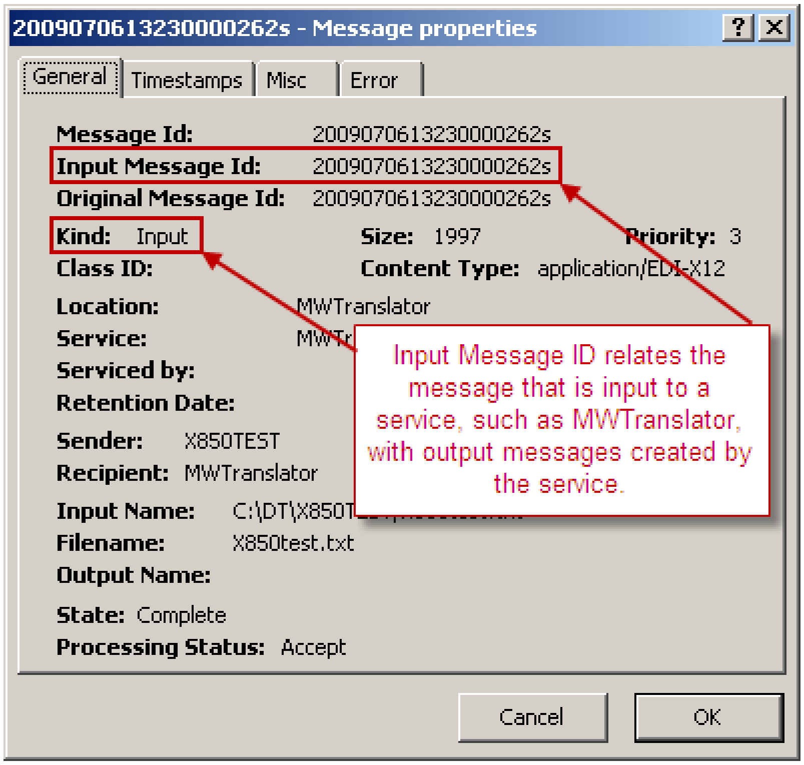
Each message is assigned a Message ID, unique within the system. There are three message IDs that the Message Store has for each message: Message ID, Input Message ID, and Original Message ID. MessageWay uses these IDs to track and relate the messages as they progress through the system. The following table describes their use:

ID Type	Description
Message ID	The Message ID is a unique message identifier assigned by the MessageWay Server.
Input Message ID	The Input Message ID is the link to the input message. For messages received or sent by adapters or rules processing, this is the same as the message ID. For messages sent from services other than Rules Processing, this relates generated outputs with the original input message. To view all related messages, select one of the messages from a message list, right-click, and then choose **Get Related Messages**.

ID Type	Description
Original Message ID	This is the same as the Message ID, unless this message was created by resubmitting or redirecting a completed message. All messages that have the same original message ID share the same message content file. To view all messages that share the same content, select one of the messages from a message list, right-click, and then select **Get Linked Messages**.

The message IDs are listed on the Message Properties window.

The following two messages are related, because the first is an input to a service and the second is one of the outputs of the service. These messages share the same *Input Message ID*.



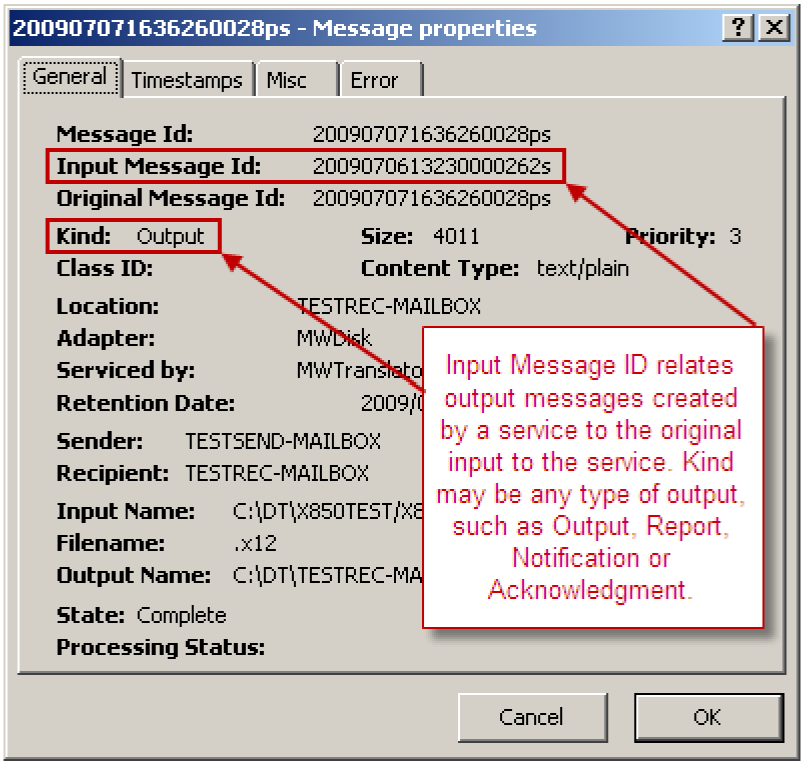
20090706132300002622s - Message properties

Message Id: 20090706132300002622s
Input Message Id: 20090706132300002622s
Original Message Id: 20090706132300002622s
Kind: Input
Size: 1997
Priority: 3
Class ID:
Content Type: application/EDI-X12
Location: MWTranslator
Service: MWTr
Serviced by:
Retention Date:
Sender: X850TEST
Recipient: MWTranslator
Input Name: C:\DT\X850T
Filename: X850test.txt
Output Name:
State: Complete
Processing Status: Accept

Input Message ID relates the message that is input to a service, such as MWTranslator, with output messages created by the service.

Input Message ID on Message Properties Window

The process creates output with a new Message ID and relates it to the first message with the *Input Message ID*.

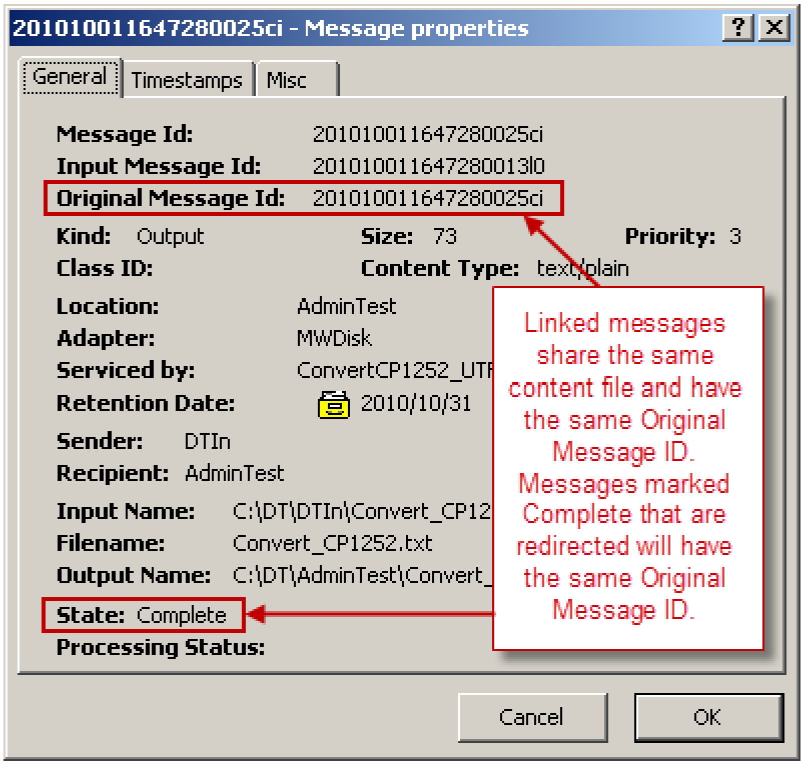


Message Id: 200907071636260028ps
Input Message Id: 200907061323000262s
Original Message Id: 200907071636260028ps
Kind: Output
Size: 4011
Priority: 3
Class ID:
Content Type: text/plain
Location: TESTREC-MAILBOX
Adapter: MWDisk
Serviced by: MWTranslato
Retention Date: 2009/0
Sender: TESTSEND-MAILBOX
Recipient: TESTREC-MAILBOX
Input Name: C:\DT\X850TEST/X8
Filename: .x12
Output Name: C:\DT\TESTREC-MA
State: Complete
Processing Status:

Input Message ID relates output messages created by a service to the original input to the service. Kind may be any type of output, such as Output, Report, Notification or Acknowledgment.

Input Message Related to Output Message on Message Properties Window

The following two messages are linked, because the first was delivered (marked *Complete*) and later sent to a different location using the Redirect Message command. Although they are considered separate messages, each with its own Message ID, they share the same content, so the Original Message IDs are the same.

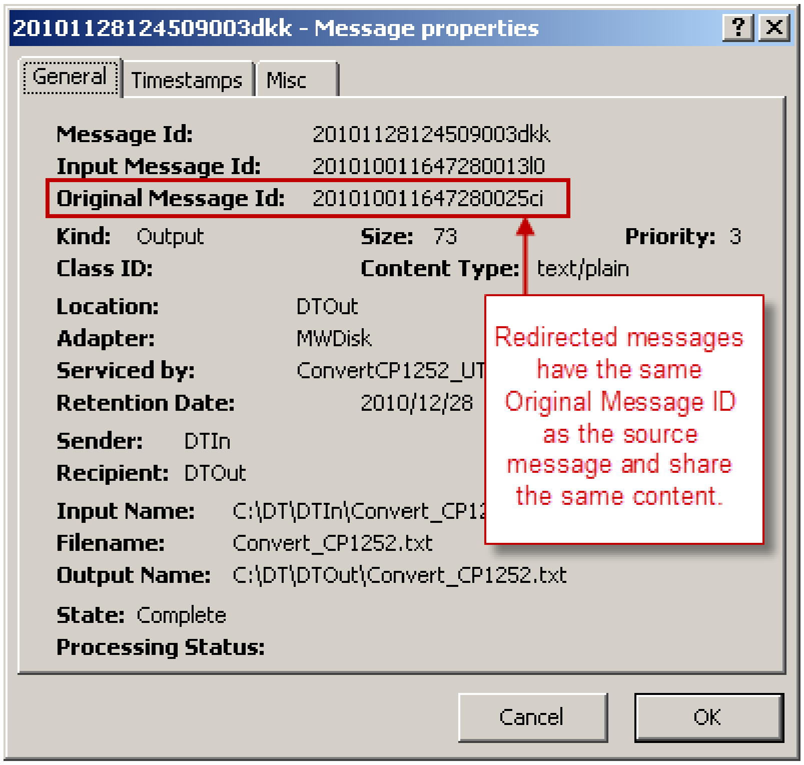


Message Id: 201010011647280025ci
Input Message Id: 20101001164728001310
Original Message Id: 201010011647280025ci
Kind: Output Size: 73 Priority: 3
Class ID: Content Type: text/plain
Location: AdminTest
Adapter: MWDisk
Serviced by: ConvertCP1252_UTF
Retention Date: 2010/10/31
Sender: DTIn
Recipient: AdminTest
Input Name: C:\DT\DTIn\Convert_CP12
Filename: Convert_CP1252.txt
Output Name: C:\DT\AdminTest\Convert_
State: Complete
Processing Status:

Linked messages share the same content file and have the same Original Message ID. Messages marked Complete that are redirected will have the same Original Message ID.

Example of Linked Messages with Same Original Message ID

Because the original message had a state of Complete, MessageWay creates a new message detail record with a new Message ID and relates it to the first message with the Original Message ID. This new message shares that same content file as the original message.



Message Id: 20101128124509003dkk
Input Message Id: 201010011647280013l0
Original Message Id: 20101001164728025ci
Kind: Output
Size: 73
Priority: 3
Class ID:
Content Type: text/plain
Location: DTOut
Adapter: MWDisk
Serviced by: ConvertCP1252_UT
Retention Date: 2010/12/28
Sender: DTIn
Recipient: DTOut
Input Name: C:\DT\DTIn\Convert_CP12
Filename: Convert_CP1252.txt
Output Name: C:\DT\DTOut\Convert_CP1252.txt
State: Complete
Processing Status:

Redirected messages have the same Original Message ID as the source message and share the same content.

Example of Linked Messages with Same Original Message ID

Controlling the Number of Returned Messages

The User Server configuration controls the number of messages that MessageWay returns in response to a query. Use this setting to limit resource usage. Encourage users to search using criteria that return selected items rather than attempting to return all items.

CAUTION: This process requires that you restart the MessageWay User Server, which will disconnect all users.

To change this number:

1 From the left pane of MessageWay Explorer, click **Servers**.

2 From the right pane, double-click **MWUser**.

The MWUser Server Properties window appears.

3 On the **MWUser** tab:

a) In the **Max Find Message Rows**, type the number of messages you will allow the user server to return in response to a **Find Messages** or **Find Archive Messages** query.

b) In the **Max Message Rows**, type the number of messages you will allow users to view in a window.

4 Restart the MessageWay User Server.

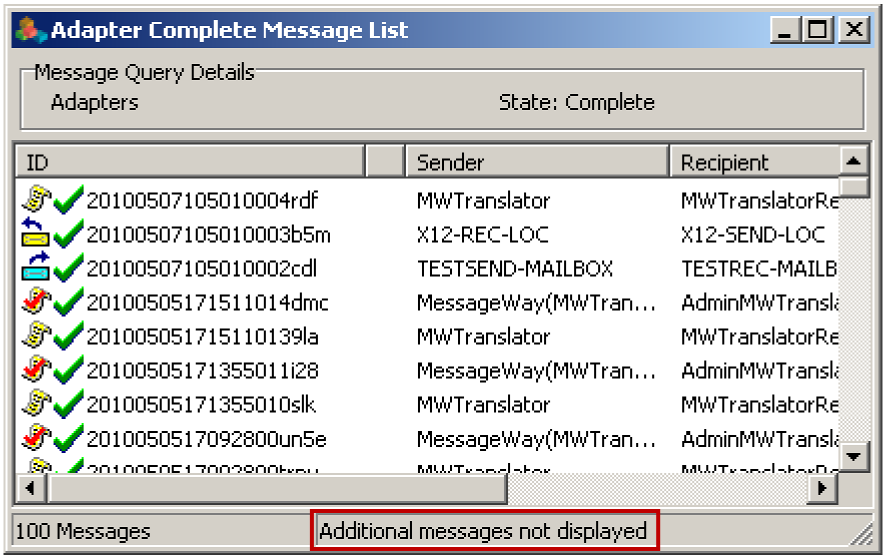
NOTE: The number of rows returned by the user server is hard coded to 10,000 in response to a **Find Locations**, **Find Rules** or **Find Users** query.

Searching for Message Information

There are basically three ways to search the Message Store from the MessageWay Manager. These methods all display a Message List window:

- Double-click one of the statistics columns in the System Monitor or the Service or Adapters Monitors
- Select a location that contains output, which will be all location types except *Input*, and select **Show Messages** from the **Locations** menu or with a right click from the pop-up menu
- Use the Find Messages window to enter search criteria, which searches the message detail records for information about the message

When more messages are returned than can be displayed, a message appears at the bottom of the window: *Additional messages not displayed*. In this case, you should narrow your search.



Adapter Complete Message List

Message Query Details
Adapters State: Complete

ID		Sender	Recipient
✓ 20100507105010004rdf		MWTranslator	MWTranslatorRe
✓ 20100507105010003b5m		X12-REC-LOC	X12-SEND-LOC
✓ 20100507105010002cdl		TESTSEND-MAILBOX	TESTREC-MAILB
✓ 20100505171511014dmc		MessageWay(MWTran...	AdminMWTransl
✓ 201005051715110139la		MWTranslator	MWTranslatorRe
✓ 20100505171355011i28		MessageWay(MWTran...	AdminMWTransl
✓ 20100505171355010slk		MWTranslator	MWTranslatorRe
✓ 2010050517092800un5e		MessageWay(MWTran...	AdminMWTransl

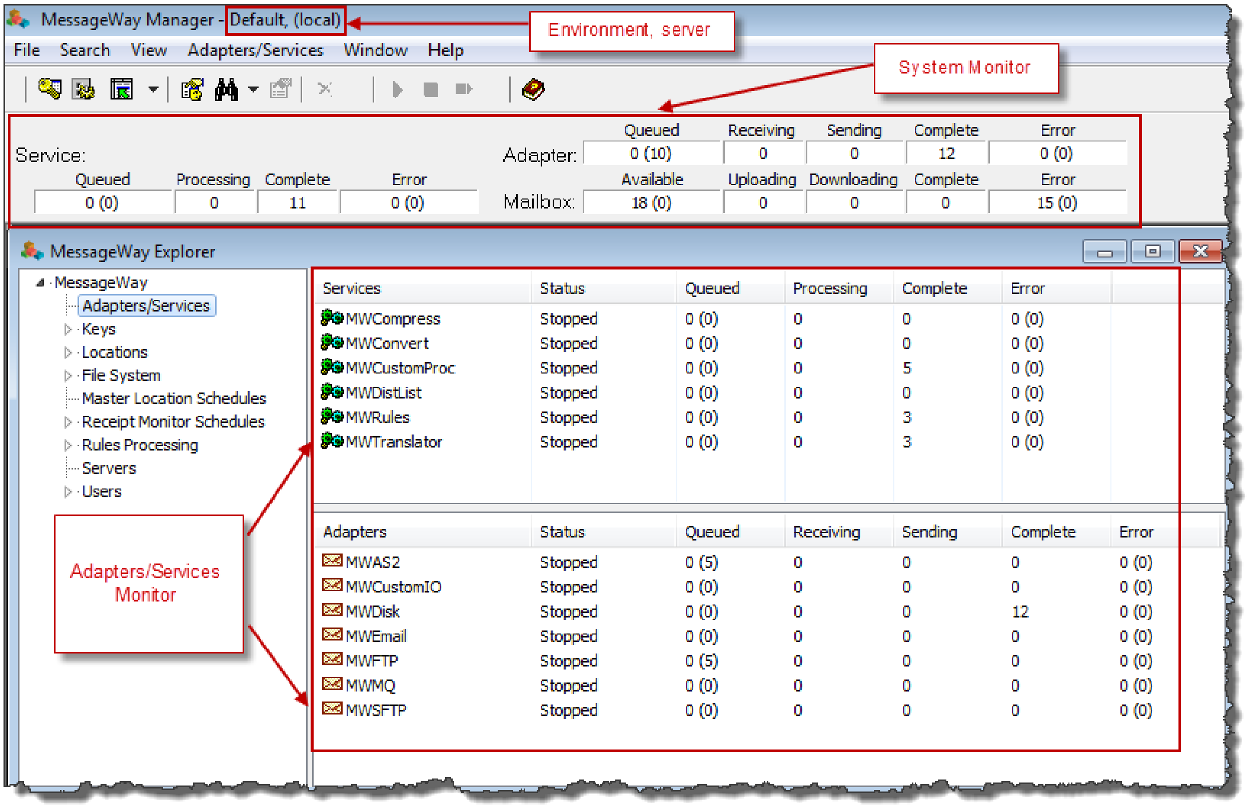
100 Messages | Additional messages not displayed

Selecting Messages From Monitor Columns

There are two types of monitors available to operators that show the current status of the messaging process: the System Monitor and the Services and Adapters monitors.

The System Monitor shows consolidated activity along the various processing points of messages, separated into three categories: Service, Adapter and Mailbox. Mailboxes include statistics for messages in locations that are not associated with an adapter or service, such as those in the system mailbox {Unknown} and those associated with a pickup mailbox. For more information about the System Monitor, refer to the topic, ***System Monitor Bar*** (on page 1332).

The Adapters and Services monitor shows statistics by individual service and adapter. The totals of the numbers in the columns for Services and Adapters should equal the numbers shown in the System Monitor.



Environment, server

System Monitor

Adapters/Services Monitor

Service:

Queued	Processing	Complete	Error
0 (0)	0	11	0 (0)

Adapter:

Queued	Receiving	Sending	Complete	Error
0 (10)	0	0	12	0 (0)

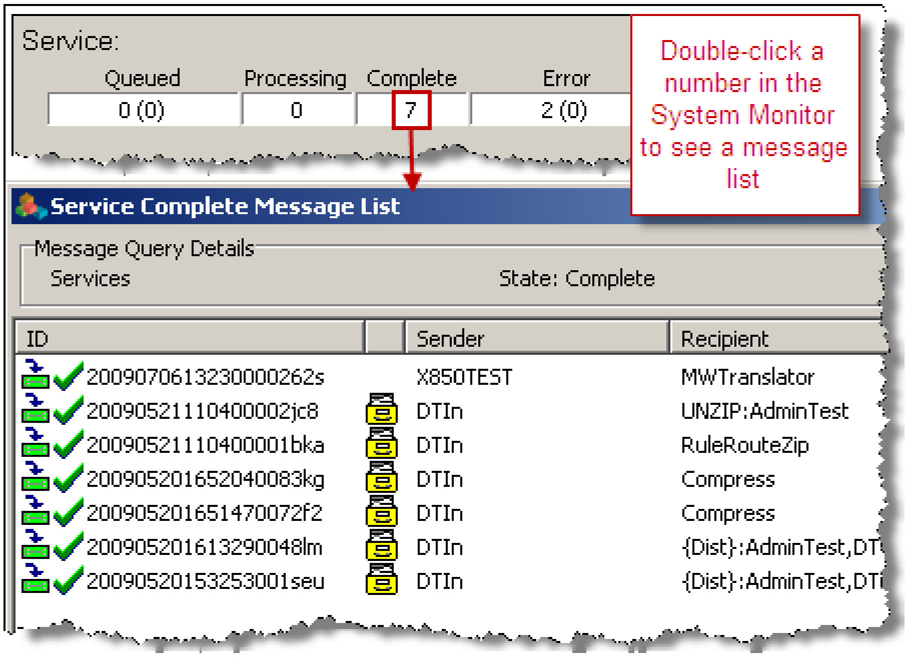
Mailbox:

Available	Uploading	Downloading	Complete	Error
18 (0)	0	0	0	15 (0)

Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0	5	0 (0)
MWDistList	Stopped	0 (0)	0	0	0 (0)
MWRules	Stopped	0 (0)	0	3	0 (0)
MWTranslator	Stopped	0 (0)	0	3	0 (0)

Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWAS2	Stopped	0 (5)	0	0	0	0 (0)
MWCustomIO	Stopped	0 (0)	0	0	0	0 (0)
MWDisk	Stopped	0 (0)	0	0	12	0 (0)
MWEmail	Stopped	0 (0)	0	0	0	0 (0)
MWFTP	Stopped	0 (5)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

To view a list of messages associated with a particular category, double-click the number in a table cell. For example, to see the messages for all services that have been delivered, double-click the *Complete* box on the System Monitor, which displays a Message List window.



Service:

Queued	Processing	Complete	Error
0 (0)	0	7	2 (0)

Double-click a number in the System Monitor to see a message list

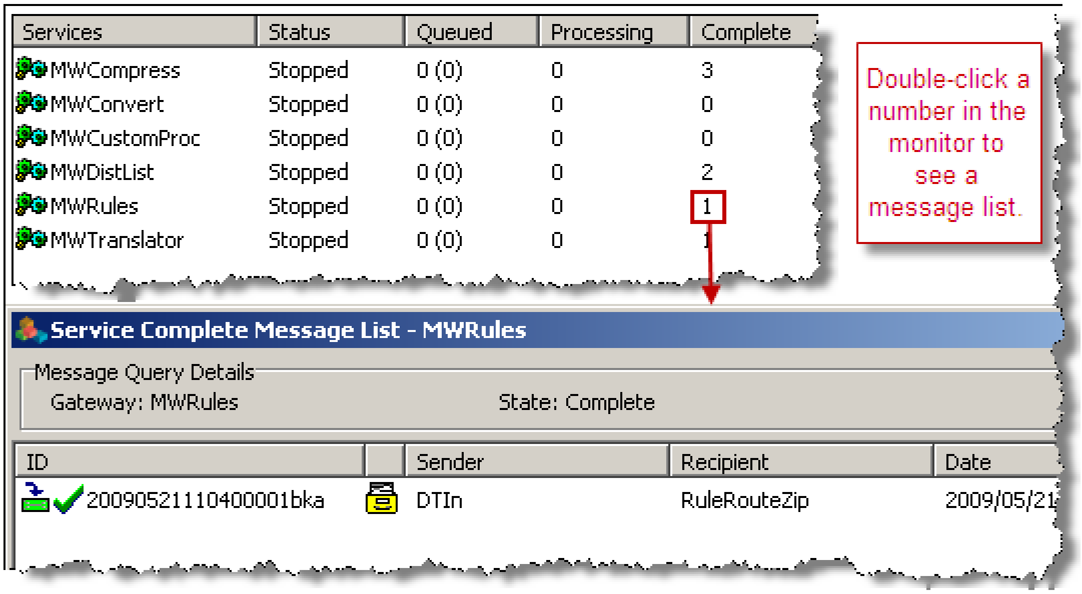
Service Complete Message List

Message Query Details
Services State: Complete

ID		Sender	Recipient
✓ 20090706132300002625		X850TEST	MWTranslator
✓ 20090521110400002jc8		DTIn	UNZIP:AdminTest
✓ 20090521110400001bka		DTIn	RuleRouteZip
✓ 200905201652040083kg		DTIn	Compress
✓ 200905201651470072f2		DTIn	Compress
✓ 200905201613290048lm		DTIn	{Dist}:AdminTest,DT
✓ 20090520153253001seu		DTIn	{Dist}:AdminTest,DT

Message List Result of double-clicking on System Monitor, Processing Complete

To see the messages for the Rules Processing Service that have been delivered, double-click the *Complete* category on the Services monitor, which displays a Message List window.



Services	Status	Queued	Processing	Complete
MWCompress	Stopped	0 (0)	0	3
MWConvert	Stopped	0 (0)	0	0
MWCustomProc	Stopped	0 (0)	0	0
MWDistList	Stopped	0 (0)	0	2
MWRules	Stopped	0 (0)	0	1
MWTranslator	Stopped	0 (0)	0	1

Double-click a number in the monitor to see a message list.

Service Complete Message List - MWRules

Message Query Details
Gateway: MWRules State: Complete

ID		Sender	Recipient	Date
✓ 20090521110400001bka		DTIn	RuleRouteZip	2009/05/21

Message List Result of double-clicking on Services Monitor, MWRules Complete

Selecting Messages for Specific Location

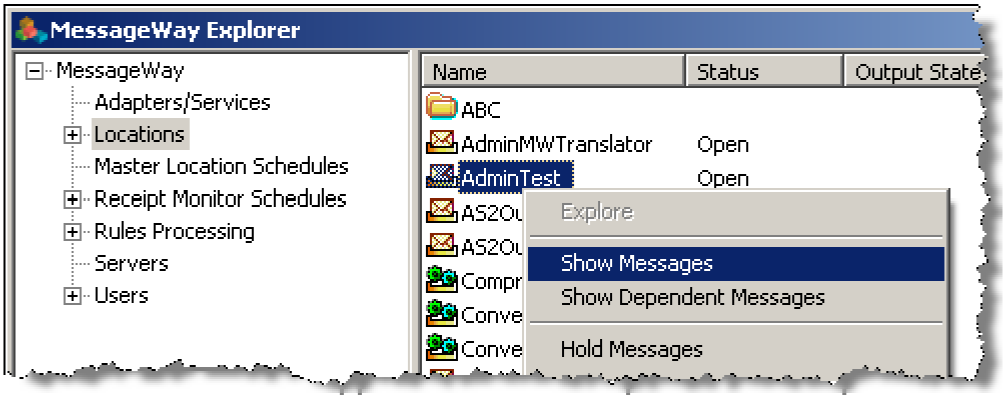
To look at a list of messages that have been delivered to a specific location:

1 From the **Locations** folder of MessageWay Explorer, select the location.

2 From the **Locations** menu, click **Show Messages**.

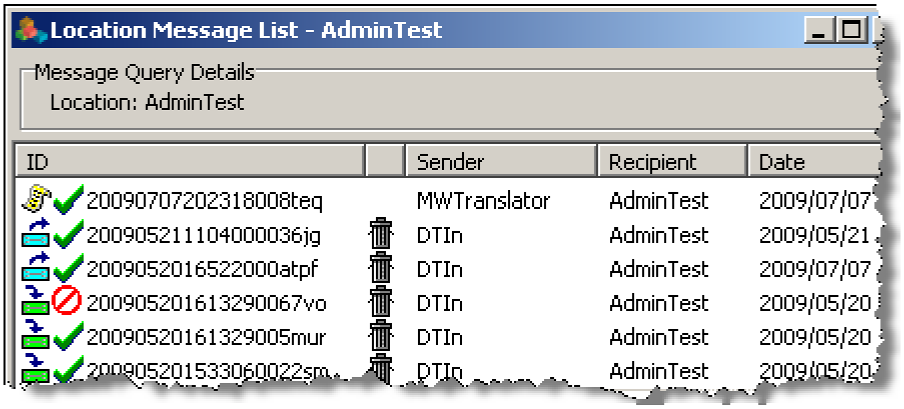
- or -

Right click the location, and select **Show Messages** from the pop-up menu.



Name	Status	Output State
ABC		
AdminMWTranslator	Open	
AdminTest	Open	
AS2Ou		
AS2Ou		
Compr		
Conve		
Conve		

Example of Show Messages Command



Message Query Details
Location: AdminTest

ID		Sender	Recipient	Date
✓ 20090707202318008teq		MWTranslator	AdminTest	2009/07/07
✓ 20090521110400036jg		DTIn	AdminTest	2009/05/21
✓ 20090520165220000atpf		DTIn	AdminTest	2009/07/07
200905201613290067vo		DTIn	AdminTest	2009/05/20
✓ 20090520161329005mur		DTIn	AdminTest	2009/05/20
✓ 200905201533060022sm		DTIn	AdminTest	2009/05/20

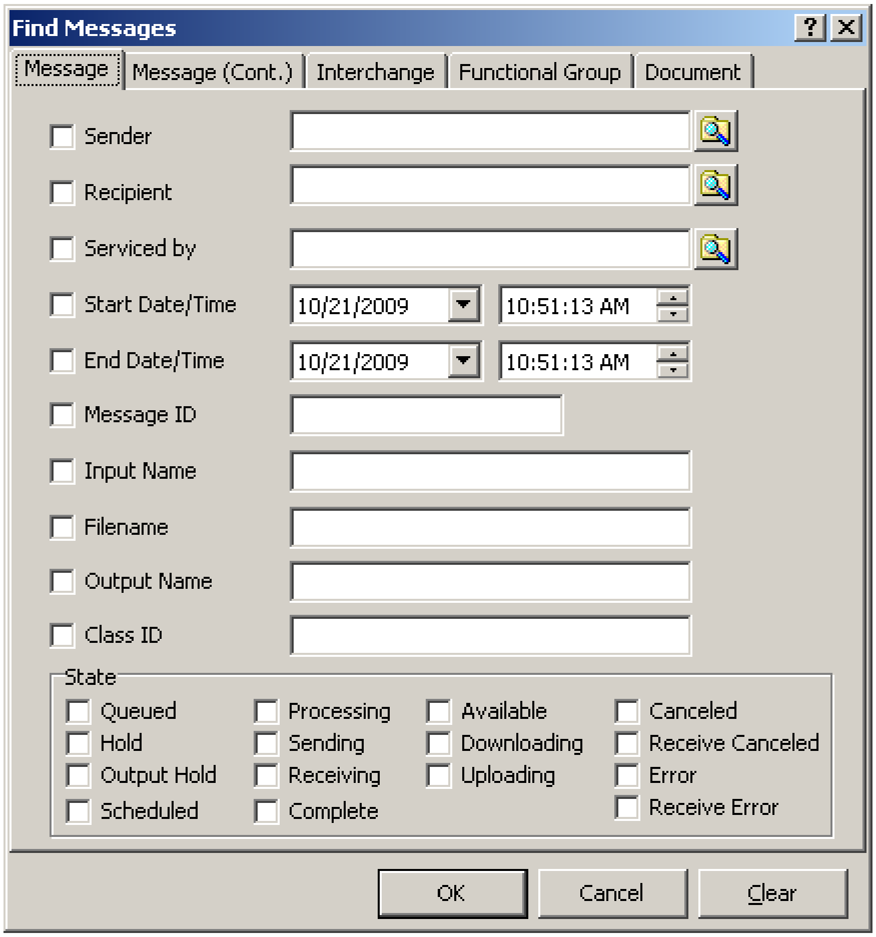
Message List Result of Selecting a Location and then Show Messages

Finding Messages Using Search Criteria

When users want to search the Message Store based on certain criteria, they may use the Find Messages window, by selecting the **Search** menu or button on the toolbar.

TIP: An effective way to view input messages is by using the Find Messages window. Output messages are associated with the destination location. The **Show Messages** command is only available for output type locations.

Note that MessageWay does not support input filenames that contain backslashes, \. For operating systems, such as UNIX, that allow backslashes in filenames, the filename property will be whatever follows the final backslash.

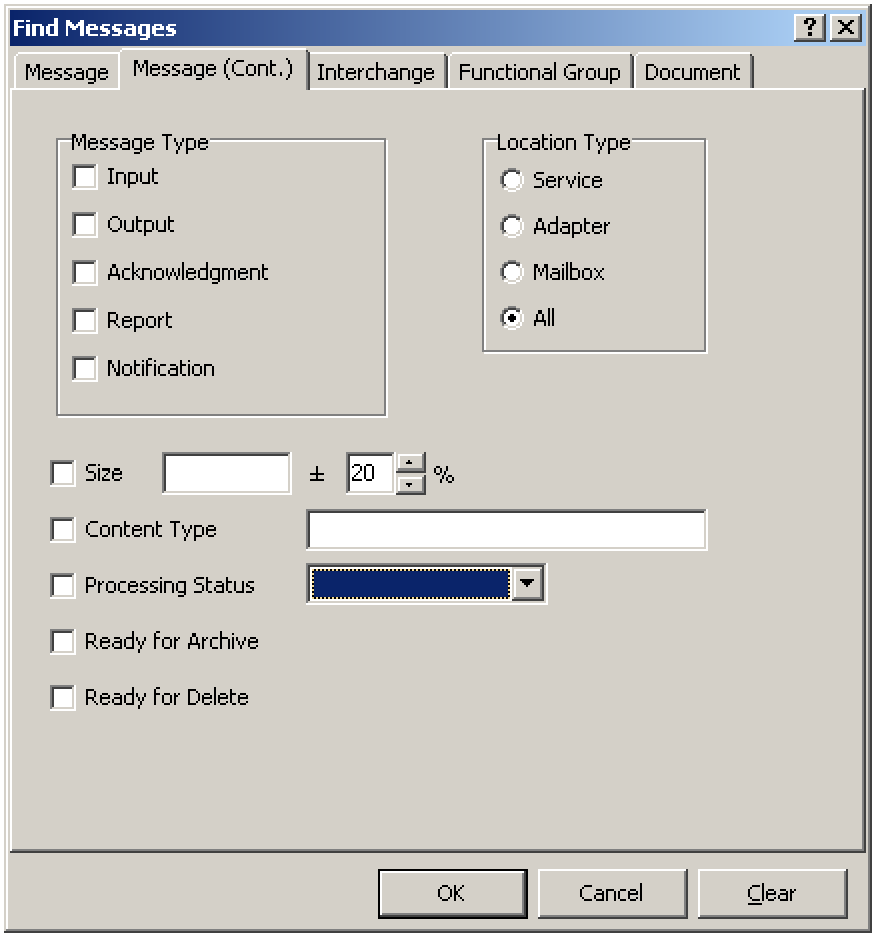

Find Messages

□ Sender
□ Recipient
□ Serviced by
□ Start Date/Time 10/21/2009 10:51:13 AM
□ End Date/Time 10/21/2009 10:51:13 AM
□ Message ID
□ Input Name
□ Filename
□ Output Name
□ Class ID

State

□ Queued
□ Hold
□ Output Hold
□ Scheduled
□ Processing
□ Sending
□ Receiving
□ Complete
□ Available
□ Downloading
□ Uploading
□ Canceled
□ Receive Canceled
□ Error
□ Receive Error

Search Criteria on Find Messages Window (Message page)



Message Type
- □ Input
- □ Output
- □ Acknowledgment
- □ Report
- □ Notification

Location Type
- ○ Service
- ○ Adapter
- ○ Mailbox
- ● All

□ Size ± 20 %

□ Content Type

□ Processing Status

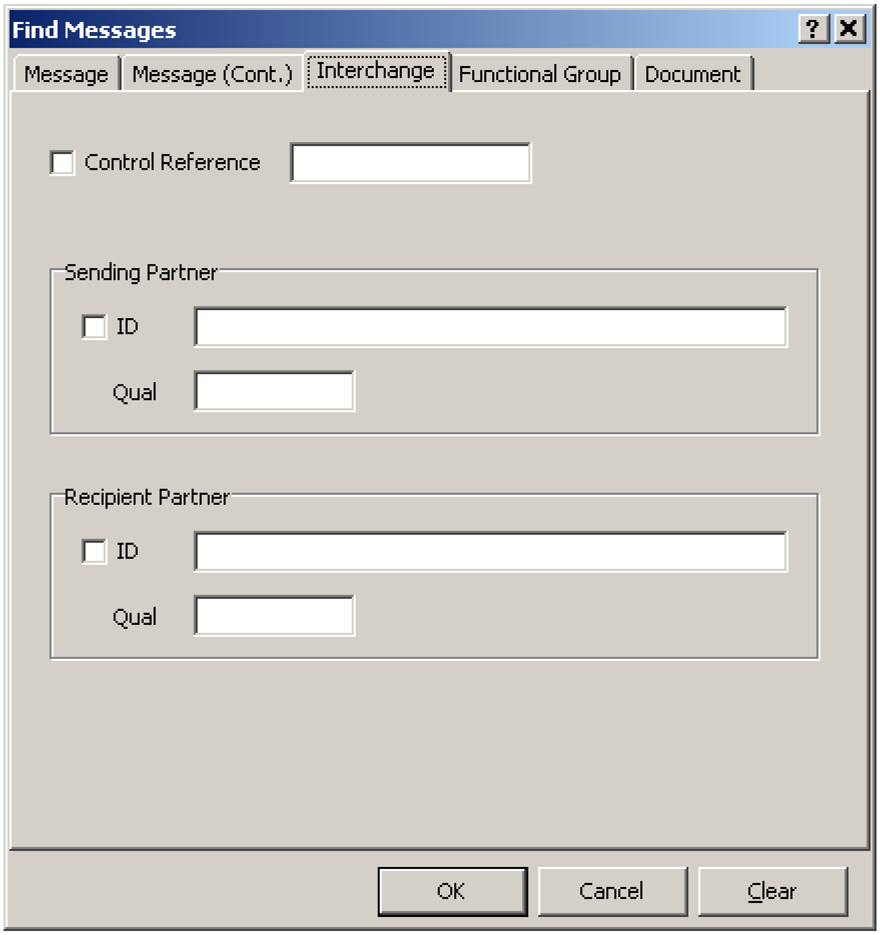
□ Ready for Archive

□ Ready for Delete

Search Criteria on Find Messages Window (Message (Cont.) page)

When users know information based on MWTranslator processing, they may search by those criteria also.

IMPORTANT: To search for messages processed by MWTranslator, you must first start the Logging Server. The MWTranslator service creates audit records, *.aud files, that accumulate in the /MessageWay/server/MWTranslator/temp directory until the Logging Server adds them to the database where they are available for searches. Information about logging is also available in this topic, ***Logging and Reconciliation of Acknowledgments*** (on page 910). For complete information about audit logging and reconciliation, refer to the topic "Using Audit and Reconciliation" in the M*W Translator Operator* Guide and Reference.



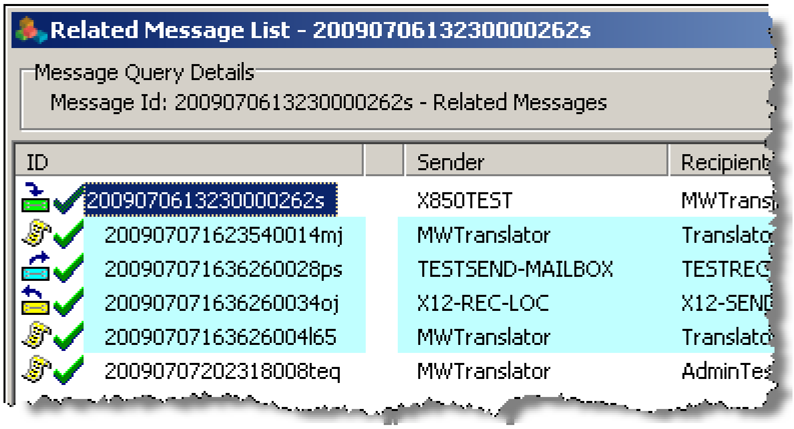
MWTranslator Search Criteria on Find Messages Window

IMPORTANT: When you leave all values blank, the list shows all messages in the Message Store. Users should always select some criteria to limit the number of messages on the list. You can set system-wide limits for total messages returned and total displayed in a window on the **MWUser** tab of the ***Server Properties window*** (on page 1313).

Finding Related and Linked Messages

Each message has a unique message identification comprising a message ID and the destination location. On the Message Properties window, the value in **Message Id** is the primary key to the Messages table. The value in **Location** is the name of the destination location where the message logically resides. In cases where the destination location does not exist, the message resides in the system mailbox {Unknown}.

The **Input Message Id** allows the system to display messages related by a service, such as MWTranslator that does translation processing, which all have the same **Input Message Id**. The **Get Related Messages** command displays all messages related to the one that is currently selected. Input messages have a blue background and output messages have a yellow background. When you select an input message, all of its related outputs will be highlighted in blue. When you select an output message, its related input will be highlighted in yellow. Output messages are visually offset from the input messages.



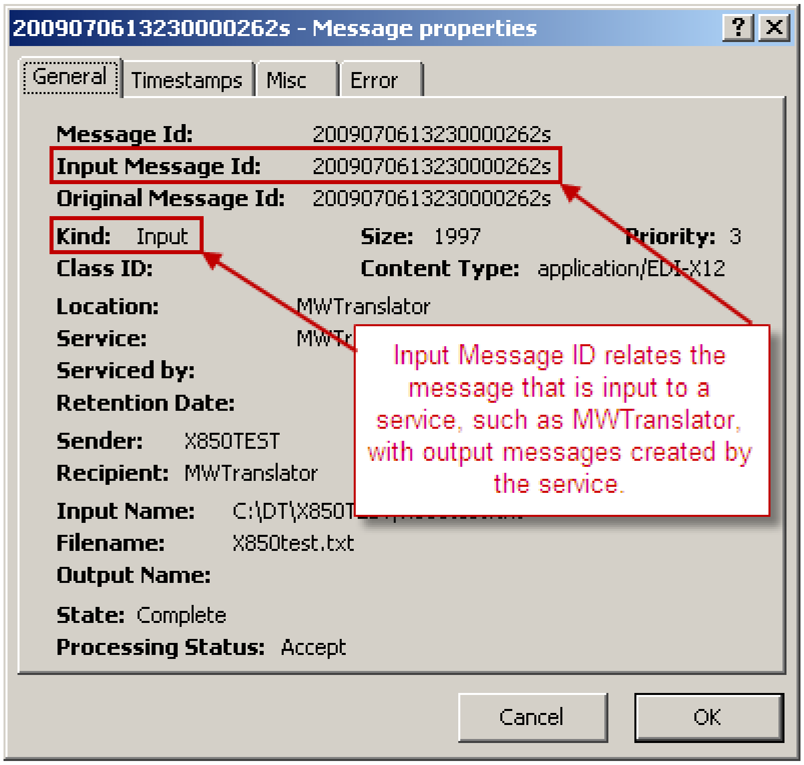
Related Message List - 2009070613230000262s

Message Query Details
Message Id: 2009070613230000262s - Related Messages

ID		Sender	Recipient
2009070613230000262s		X850TEST	MWTrans
200907071623540014mj		MWTranslator	Translato
200907071636260028ps		TESTSEND-MAILBOX	TESTREC
200907071636260034oj		X12-REC-LOC	X12-SEND
20090707163626004l65		MWTranslator	Translato
20090707202318008teq		MWTranslator	AdminTes

Result of Get Related Messages Command, Input Selected

Compare the Input Message Id value for the following 2 messages, which represent the input to an MWTranslator process and one of the outputs, an acknowledgment, from the same MWTranslator process. Note that the **Input Message Id** values are the same, and they both appear on the list of related messages.

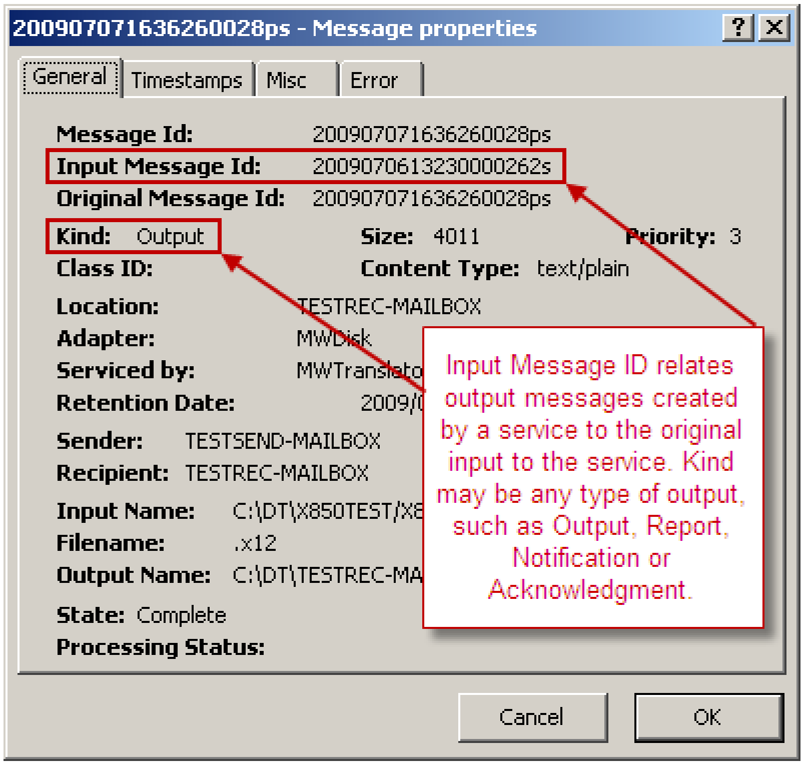


2009070613230000262s - Message properties

Message Id: 2009070613230000262s
Input Message Id: 2009070613230000262s
Original Message Id: 2009070613230000262s
Kind: Input **Size:** 1997 **Priority:** 3
Class ID: **Content Type:** application/EDI-X12
Location: MWTranslator
Service: MWTr
Serviced by:
Retention Date:
Sender: X850TEST
Recipient: MWTranslator
Input Name: C:\DT\X850T
Filename: X850test.txt
Output Name:
State: Complete
Processing Status: Accept

Input Message ID relates the message that is input to a service, such as MWTranslator, with output messages created by the service.

Related Input Message Id for MWTranslator Input in the Message Properties Window



200907071636260028ps - Message properties

Message Id: 200907071636260028ps
Input Message Id: 2009070613230000262s
Original Message Id: 200907071636260028ps
Kind: Output **Size:** 4011 **Priority:** 3
Class ID: **Content Type:** text/plain
Location: TESTREC-MAILBOX
Adapter: MWDisk
Serviced by: MWTranslato
Retention Date: 2009/(
Sender: TESTSEND-MAILBOX
Recipient: TESTREC-MAILBOX
Input Name: C:\DT\X850TEST/X8
Filename: .x12
Output Name: C:\DT\TESTREC-MA
State: Complete
Processing Status:

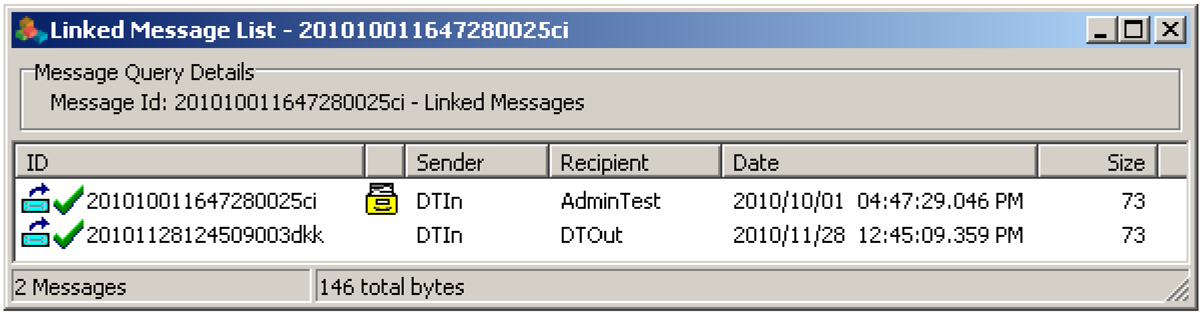
Input Message ID relates output messages created by a service to the original input to the service. Kind may be any type of output, such as Output, Report, Notification or Acknowledgment.

Related Input Message Id for MWTranslator Output in the Message Properties Window

The **Original Message Id** allows the system to display messages linked for one of the following reasons:

- Copies of reports sent by MWTranslator
- Messages resent using the **Resubmit** or **Redirect** commands
- Messages processed by the Distribution List service
- Messages processed by the Rules Processing service

Such messages all have the same original message ID and they all share the same content file. The **Get Linked Messages** command displays all messages linked to the one that is currently selected.



Linked Message List - 201010011647280025ci

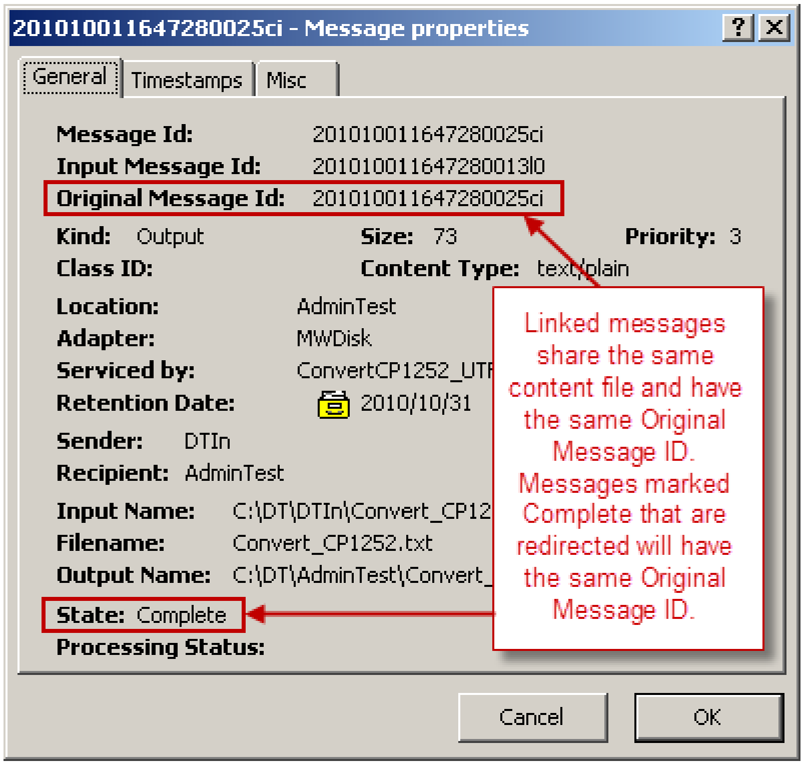
Message Query Details
Message Id: 201010011647280025ci - Linked Messages

ID		Sender	Recipient	Date	Size
✓ 201010011647280025ci	▤	DTIn	AdminTest	2010/10/01 04:47:29.046 PM	73
✓ 20101128124509003dkk		DTIn	DTOut	2010/11/28 12:45:09.359 PM	73

2 Messages | 146 total bytes

Result of Get Linked Messages Command

Compare the **Original Message Id** value for the following 2 messages. The first is the original message, and the second is the result of a **Redirect Message** command.

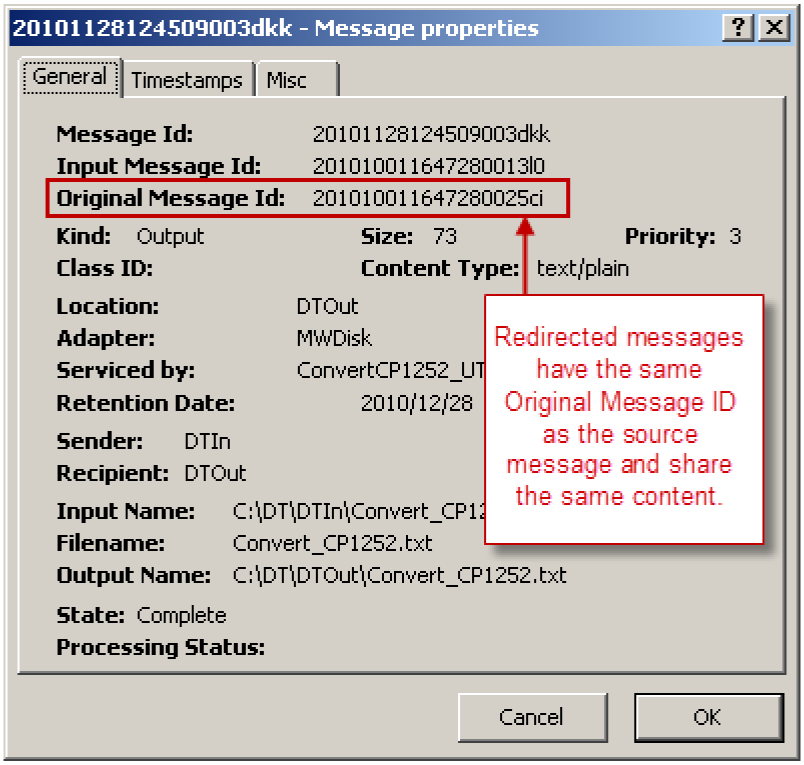


20101001164728025ci - Message properties

Message Id: 2010100116472800025ci
Input Message Id: 2010100116472800013l0
Original Message Id: 2010100116472800025ci
Kind: Output
Size: 73
Priority: 3
Class ID:
Content Type: text/plain
Location: AdminTest
Adapter: MWDisk
Serviced by: ConvertCP1252_UTF
Retention Date: 2010/10/31
Sender: DTIn
Recipient: AdminTest
Input Name: C:\DT\DTIn\Convert_CP12
Filename: Convert_CP1252.txt
Output Name: C:\DT\AdminTest\Convert_
State: Complete
Processing Status:

Linked messages share the same content file and have the same Original Message ID. Messages marked Complete that are redirected will have the same Original Message ID.

Linked Message 1 with Same Original Message ID (Input to Redirect Message Command)

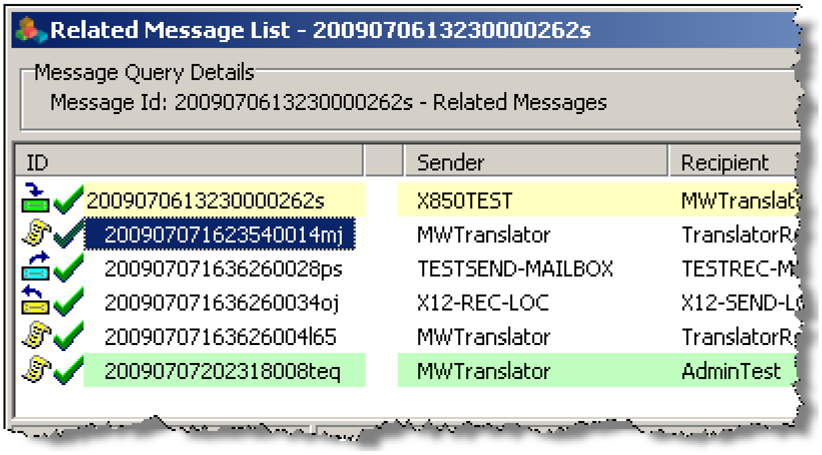


Message Id: 20101128124509003dkk
Input Message Id: 201010011647280013l0
Original Message Id: 201010011647280025ci
Kind: Output Size: 73 Priority: 3
Class ID: Content Type: text/plain
Location: DTOut
Adapter: MWDisk
Serviced by: ConvertCP1252_UT
Retention Date: 2010/12/28
Sender: DTIn
Recipient: DTOut
Input Name: C:\DT\DTIn\Convert_CP12
Filename: Convert_CP1252.txt
Output Name: C:\DT\DTOut\Convert_CP1252.txt
State: Complete
Processing Status:

Redirected messages have the same Original Message ID as the source message and share the same content.

Linked Message 2 with Same Original Message ID (Output from Redirect Message Command)

Notice that some messages are both linked and related, as in the following example, where a report from MWTranslator was sent to another location using the **Redirect** command. Therefore, the input message ID are both the same, making them related, and the original message IDs are the same since they share the same content, making them linked. When you select a linked message that is included in a related messages list, the message to which it is linked is highlighted in green, as shown here.

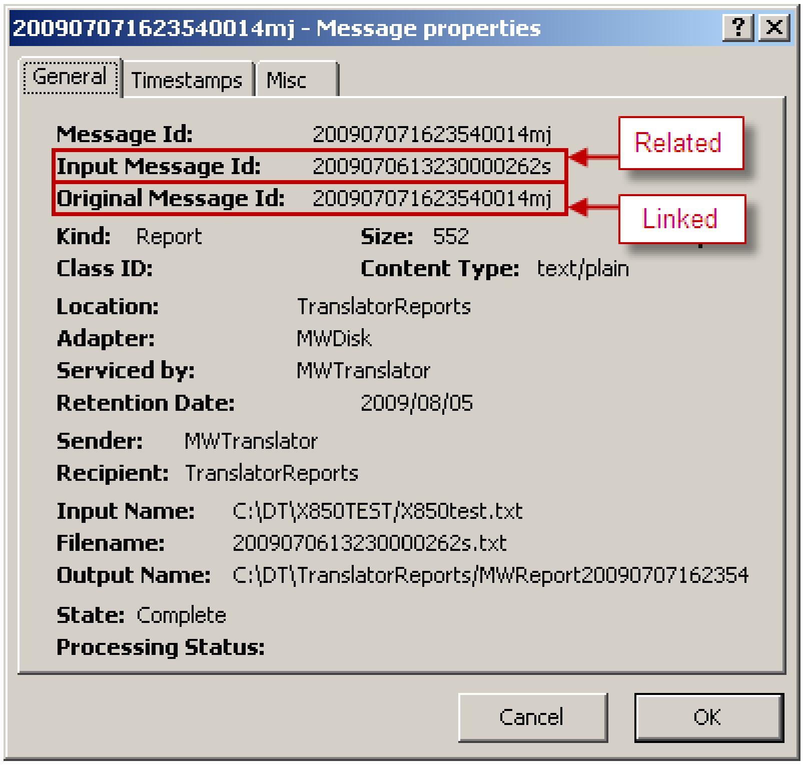


Message Query Details
Message Id: 20090706132300002625 - Related Messages

ID	Sender	Recipient
20090706132300002625	X850TEST	MWTranslat
20090707162354001 4mj	MWTranslator	TranslatorR
20090707163626002 8ps	TESTSEND-MAILBOX	TESTREC-M
20090707163626003 4oj	X12-REC-LOC	X12-SEND-L
20090707163626004l65	MWTranslator	TranslatorR
20090707202318008teq	MWTranslator	AdminTest

Messages That Are Both Linked and Related

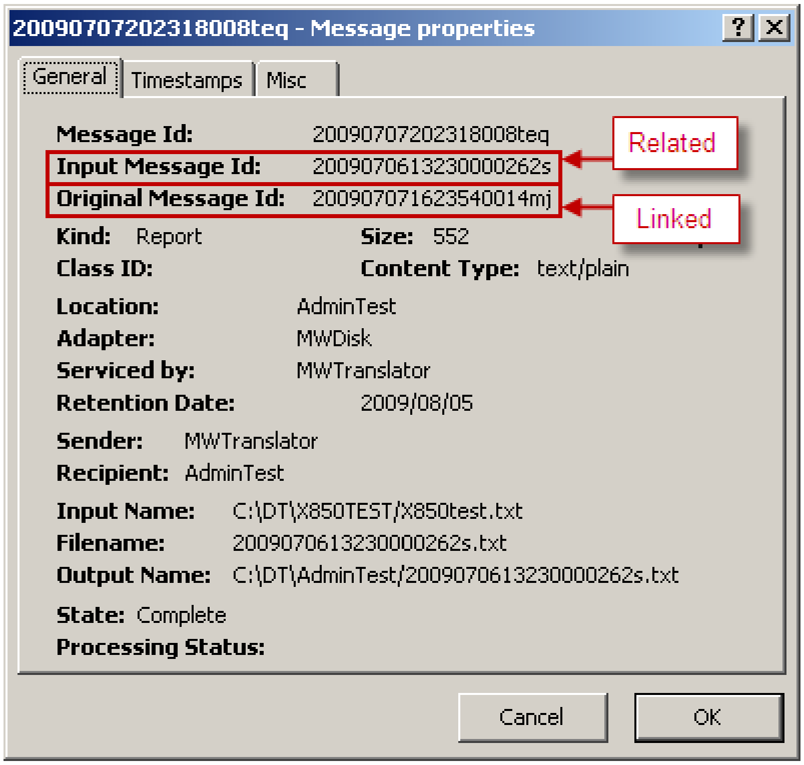
These are the message properties of the original report created by MWTranslator.



Message Id: 200907071623540014mj
Input Message Id: 2009070613230000262s
Original Message Id: 200907071623540014mj
Kind: Report
Size: 552
Class ID:
Content Type: text/plain
Location: TranslatorReports
Adapter: MWDisk
Serviced by: MWTranslator
Retention Date: 2009/08/05
Sender: MWTranslator
Recipient: TranslatorReports
Input Name: C:\DT\X850TEST/X850test.txt
Filename: 2009070613230000262s.txt
Output Name: C:\DT\TranslatorReports/MWReport20090707162354
State: Complete
Processing Status:

Linked and Related Message 1

These are the message properties of the copy of the MWTranslator report that was redirected to a different location.



Message Id: 20090707202318008teq
Input Message Id: 20090706132300002625
Original Message Id: 200907071623540014mj
Kind: Report
Size: 552
Class ID:
Content Type: text/plain
Location: AdminTest
Adapter: MWDisk
Serviced by: MWTranslator
Retention Date: 2009/08/05
Sender: MWTranslator
Recipient: AdminTest
Input Name: C:\DT\X850TEST/X850test.txt
Filename: 20090706132300002625.txt
Output Name: C:\DT\AdminTest/20090706132300002625.txt
State: Complete
Processing Status:

Linked and Related Message 2

Viewing Message Information

Once operators find a message they want to explore further, they may look at its processing information on the Message Properties window or they may look at the content on the message on the Message window. Operators may display many of the properties on the Message List window without having to view the Message Properties window. Operators may also use the audit files to find a trace for actions on messages. For more information about audit files, refer to the topic ***Viewing Audit Information*** (on page 699).

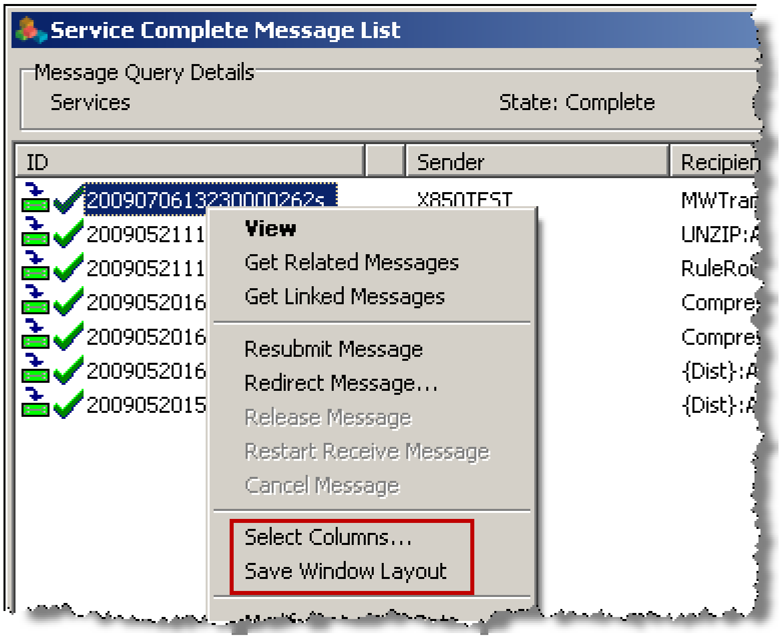
TIP: When you see a message at the bottom of the Message List window that says *Additional messages not displayed*, you should narrow your search criteria.

Displaying More Properties in a Message List Window

Users may display additional properties directly in the Message List window, allowing an overview of the properties of many items at once.

To display more columns of information in the Message List window:

1 Right click in the detail area of the message list.



Message Query Details
Services State: Complete

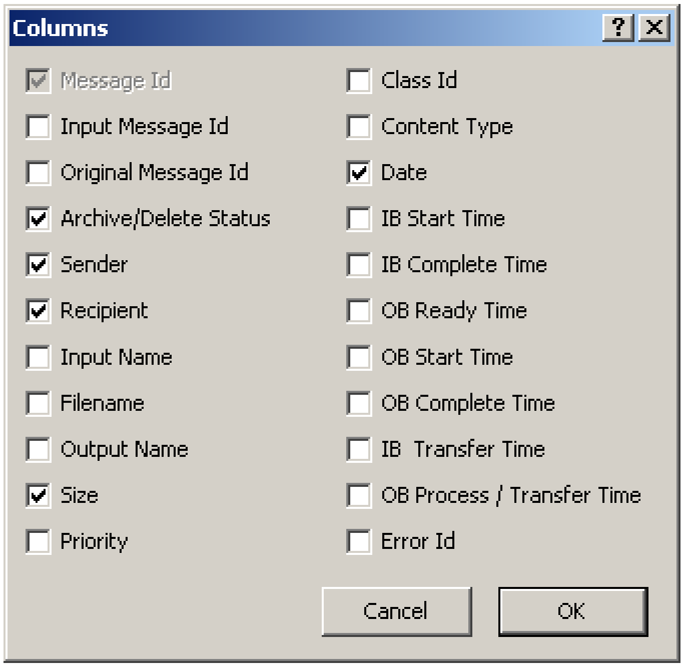
ID		Sender	Recipien
2009070613230000262s		X850TEST	MWTrar
2009052111			UNZIP:A
2009052111			RuleRou
2009052016			Compre
2009052016			Compre
2009052016			{Dist}:A
2009052015			{Dist}:A

2 From the menu, click **Select Columns**.

The **Columns** dialog box appears.

3 Check or uncheck the boxes as required and click **OK**.

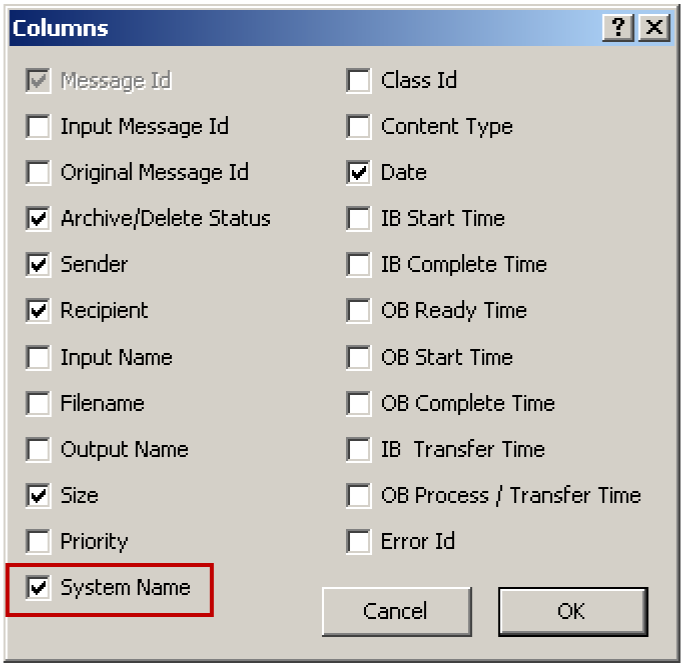
You may uncheck any boxes but Message ID. The columns of additional information appear after the original default columns, **Message ID**, **Archive/Delete**, **Sender**, **Recipient**, **Size** and **Date**.



☑ Message Id
☐ Input Message Id
☐ Original Message Id
☑ Archive/Delete Status
☑ Sender
☑ Recipient
☐ Input Name
☐ Filename
☐ Output Name
☑ Size
☐ Priority

☐ Class Id
☐ Content Type
☑ Date
☐ IB Start Time
☐ IB Complete Time
☐ OB Ready Time
☐ OB Start Time
☐ OB Complete Time
☐ IB Transfer Time
☐ OB Process / Transfer Time
☐ Error Id

For multi-system environments, another column is available, *System Name*, so you know to which system the message belongs.



☑ Message Id
□ Input Message Id
□ Original Message Id
☑ Archive/Delete Status
☑ Sender
☑ Recipient
□ Input Name
□ Filename
□ Output Name
☑ Size
□ Priority
☑ System Name

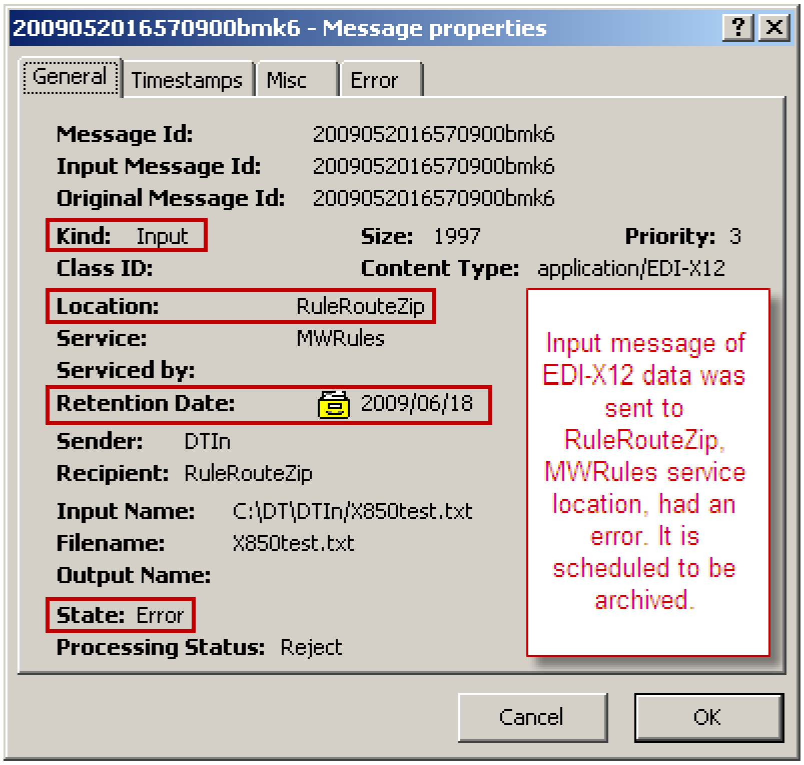
□ Class Id
□ Content Type
☑ Date
□ IB Start Time
□ IB Complete Time
□ OB Ready Time
□ OB Start Time
□ OB Complete Time
□ IB Transfer Time
□ OB Process / Transfer Time
□ Error Id

4 To save your settings for future queries, from the menu, click **Save Window Layout**.

Viewing Information about a Message

To view the message properties of a message, right click the message from a message list and choose **Properties** from the pop-up menu.

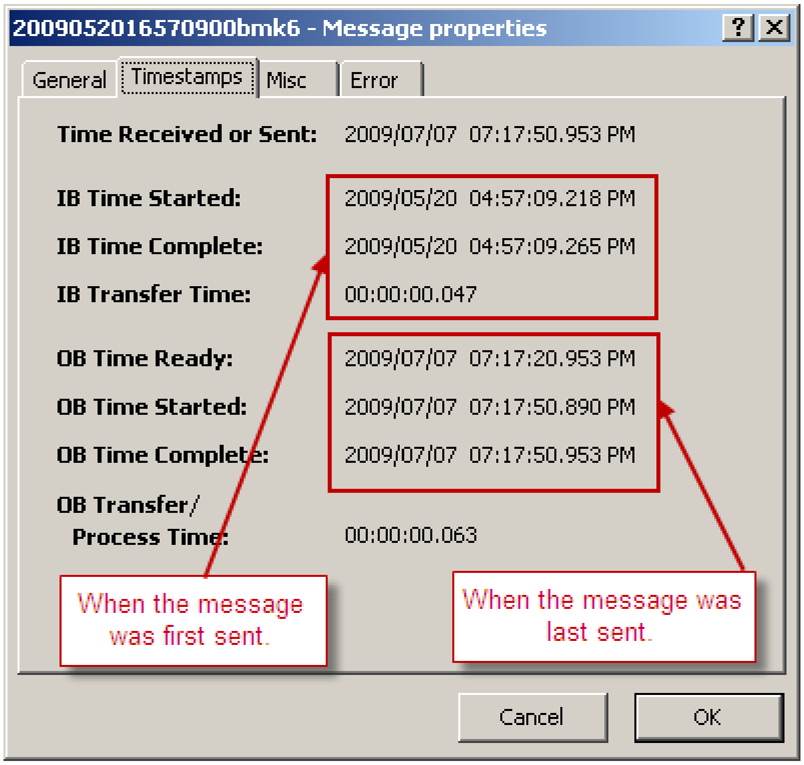
In the following example, the message shown has an error to show the additional pages available for such messages.



Message Id: 2009052016570900bmk6
Input Message Id: 2009052016570900bmk6
Original Message Id: 2009052016570900bmk6
Kind: Input
Size: 1997
Priority: 3
Class ID:
Content Type: application/EDI-X12
Location: RuleRouteZip
Service: MWRules
Serviced by:
Retention Date: 2009/06/18
Sender: DTIn
Recipient: RuleRouteZip
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.txt
Output Name:
State: Error
Processing Status: Reject

Input message of EDI-X12 data was sent to RuleRouteZip, MWRules service location, had an error. It is scheduled to be archived.

Viewing Processing Information about a Message (Message Properties Window, General Page)



20090520165709000bmk6 - Message properties

Time Received or Sent: 2009/07/07 07:17:50.953 PM

IB Time Started: 2009/05/20 04:57:09.218 PM

IB Time Complete: 2009/05/20 04:57:09.265 PM

IB Transfer Time: 00:00:00.047

OB Time Ready: 2009/07/07 07:17:20.953 PM

OB Time Started: 2009/07/07 07:17:50.890 PM

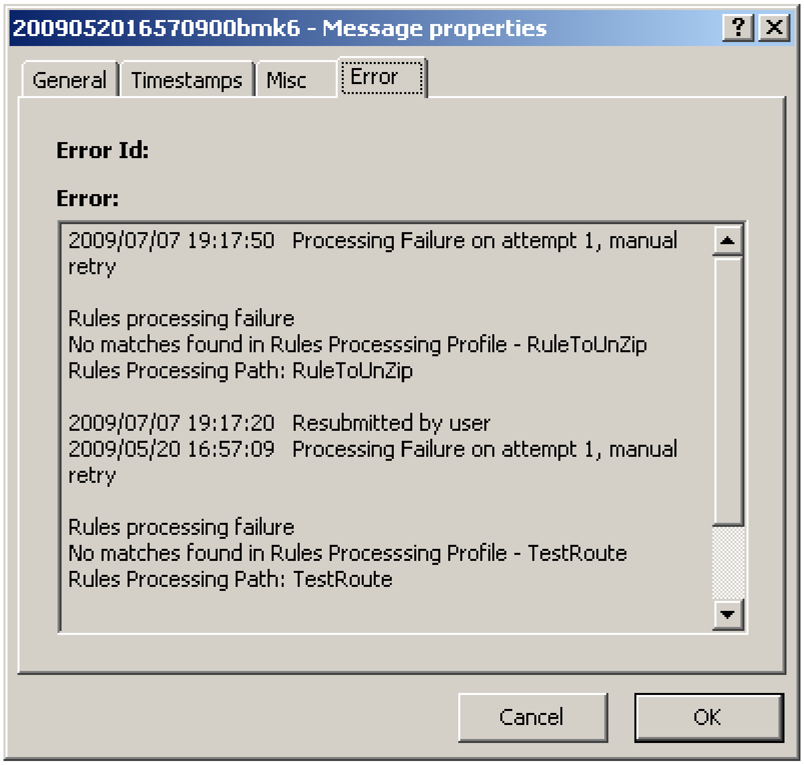
OB Time Complete: 2009/07/07 07:17:50.953 PM

OB Transfer/ Process Time: 00:00:00.063

When the message was first sent.

When the message was last sent.

Viewing Processing Information about a Message (Message Properties Window, Timestamps Page)



Error Id:

Error:

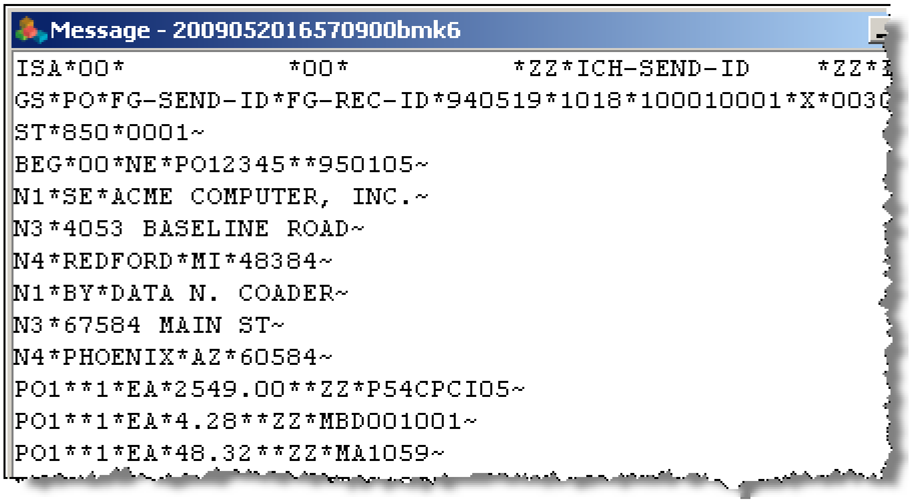
```
2009/07/07 19:17:50   Processing Failure on attempt 1, manual
retry

Rules processing failure
No matches found in Rules Processsing Profile - RuleToUnZip
Rules Processing Path: RuleToUnZip

2009/07/07 19:17:20   Resubmitted by user
2009/05/20 16:57:09   Processing Failure on attempt 1, manual
retry

Rules processing failure
No matches found in Rules Processsing Profile - TestRoute
Rules Processing Path: TestRoute
```

Viewing Processing Information about a Message (Message Properties Window, Error Page)

Viewing the Content of a Message

Operators may view the content of a message by right clicking the message from a Message List window and choosing **View** from the pop-up menu. When you view the content of a message, you have the option of one of several types of view, which you may select from the toolbar as follows:

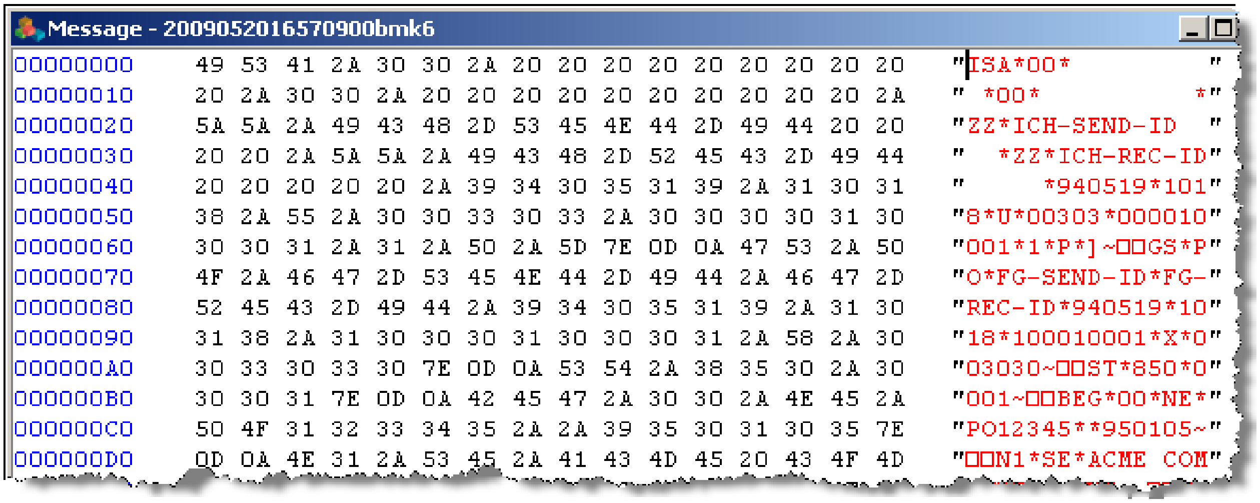
- **Text** button , displays text using CR/LF as line breaks.
- **Hex** button , displays text as hexadecimal values and ASCII text.
- **EDI** button EDI, displays text.
- **Fixed** button , displays text a column width of 80 characters.
- **Find** button , allows you to enter text that you want to find in the displayed message.
- **Search Again** button , finds the next occurrence of the data entered in the **Find** dialog box.



Message - 2009052016570900bmk6

```
ISA*00*          *00*          *ZZ*ICH-SEND-ID    *ZZ*I
GS*PO*FG-SEND-ID*FG-REC-ID*940519*1018*100010001*X*0030
ST*850*0001~
BEG*00*NE*PO12345**950105~
N1*SE*ACME COMPUTER, INC.~
N3*4053 BASELINE ROAD~
N4*REDFORD*MI*48384~
N1*BY*DATA N. COADER~
N3*67584 MAIN ST~
N4*PHOENIX*AZ*60584~
PO1**1*EA*2549.00**ZZ*P54CPCI05~
PO1**1*EA*4.28**ZZ*MBD001001~
PO1**1*EA*48.32**ZZ*MA1059~
```

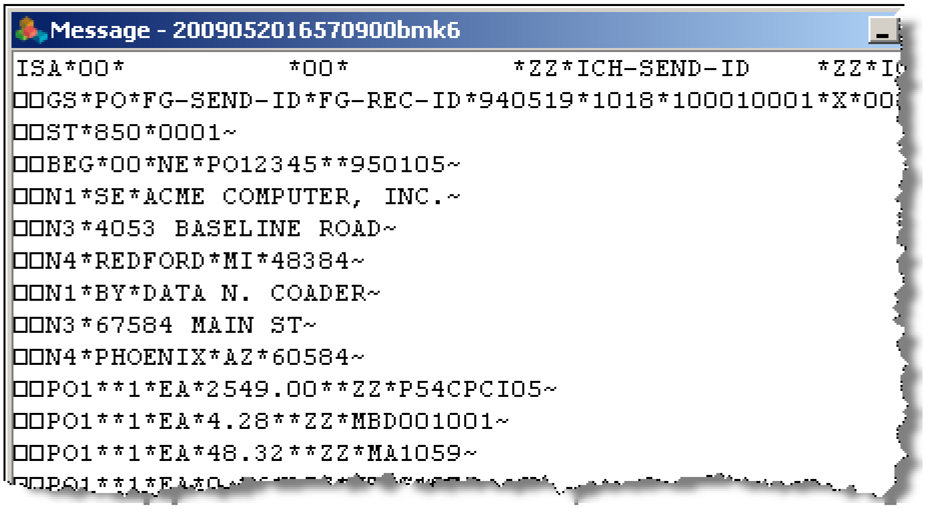
Viewing the Content of a Message (Message Window, Text View)



Message - 2009052016570900bmk6

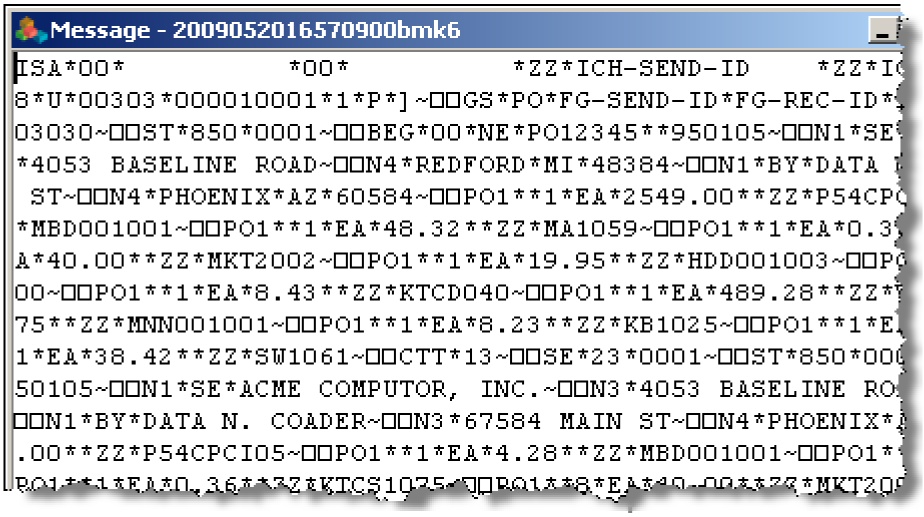
```
00000000    49 53 41 2A 30 30 2A 20 20 20 20 20 20 20 20 20    "ISA*00*         "
00000010    20 2A 30 30 2A 20 20 20 20 20 20 20 20 20 20 2A    " *00*          *"
00000020    5A 5A 2A 49 43 48 2D 53 45 4E 44 2D 49 44 20 20    "ZZ*ICH-SEND-ID  "
00000030    20 20 2A 5A 5A 2A 49 43 48 2D 52 45 43 2D 49 44    "  *ZZ*ICH-REC-ID"
00000040    20 20 20 20 20 2A 39 34 30 35 31 39 2A 31 30 31    "     *940519*101"
00000050    38 2A 55 2A 30 30 33 30 33 2A 30 30 30 30 31 30    "8*U*00303*000010"
00000060    30 30 31 2A 31 2A 50 2A 5D 7E 0D 0A 47 53 2A 50    "001*1*P*]~□□GS*P"
00000070    4F 2A 46 47 2D 53 45 4E 44 2D 49 44 2A 46 47 2D    "O*FG-SEND-ID*FG-"
00000080    52 45 43 2D 49 44 2A 39 34 30 35 31 39 2A 31 30    "REC-ID*940519*10"
00000090    31 38 2A 31 30 30 30 31 30 30 30 31 2A 58 2A 30    "18*100010001*X*0"
000000A0    30 33 30 33 30 7E 0D 0A 53 54 2A 38 35 30 2A 30    "03030~□□ST*850*0"
000000B0    30 30 31 7E 0D 0A 42 45 47 2A 30 30 2A 4E 45 2A    "001~□□BEG*00*NE*"
000000C0    50 4F 31 32 33 34 35 2A 2A 39 35 30 31 30 35 7E    "PO12345**950105~"
000000D0    0D 0A 4E 31 2A 53 45 2A 41 43 4D 45 20 43 4F 4D    "□□N1*SE*ACME COM"
```

Viewing the Content of a Message (Message Window, Hex View)



```
ISA*00*          *00*          *ZZ*ICH-SEND-ID    *ZZ*I
□□GS*PO*FG-SEND-ID*FG-REC-ID*940519*1018*100010001*X*00
□□ST*850*0001~
□□BEG*00*NE*PO12345**950105~
□□N1*SE*ACME COMPUTER, INC.~
□□N3*4053 BASELINE ROAD~
□□N4*REDFORD*MI*48384~
□□N1*BY*DATA N. COADER~
□□N3*67584 MAIN ST~
□□N4*PHOENIX*AZ*60584~
□□PO1**1*EA*2549.00**ZZ*P54CPCI05~
□□PO1**1*EA*4.28**ZZ*MBD001001~
□□PO1**1*EA*48.32**ZZ*MA1059~
□□PO1**1*EA*0.
```

Viewing the Content of a Message (Message Window, EDI View)



```
ISA*00*          *00*          *ZZ*ICH-SEND-ID    *ZZ*I
8*U*00303*000010001*1*P*]~□□GS*PO*FG-SEND-ID*FG-REC-ID*
03030~□□ST*850*0001~□□BEG*00*NE*PO12345**950105~□□N1*SE
*4053 BASELINE ROAD~□□N4*REDFORD*MI*48384~□□N1*BY*DATA
 ST~□□N4*PHOENIX*AZ*60584~□□PO1**1*EA*2549.00**ZZ*P54CP
*MBD001001~□□PO1**1*EA*48.32**ZZ*MA1059~□□PO1**1*EA*0.3
A*40.00**ZZ*MKT2002~□□PO1**1*EA*19.95**ZZ*HDD001003~□□P
00~□□PO1**1*EA*8.43**ZZ*KTCD040~□□PO1**1*EA*489.28**ZZ*
75**ZZ*MNN001001~□□PO1**1*EA*8.23**ZZ*KB1025~□□PO1**1*E
1*EA*38.42**ZZ*SW1061~□□CTT*13~□□SE*23*0001~□□ST*850*00
50105~□□N1*SE*ACME COMPUTOR, INC.~□□N3*4053 BASELINE RO
□□N1*BY*DATA N. COADER~□□N3*67584 MAIN ST~□□N4*PHOENIX*
.00**ZZ*P54CPCI05~□□PO1**1*EA*4.28**ZZ*MBD001001~□□PO1*
PO1**1*EA*0.36**ZZ*KTCS1075~□□PO1**8*EA*40.00**ZZ*MKT20
```

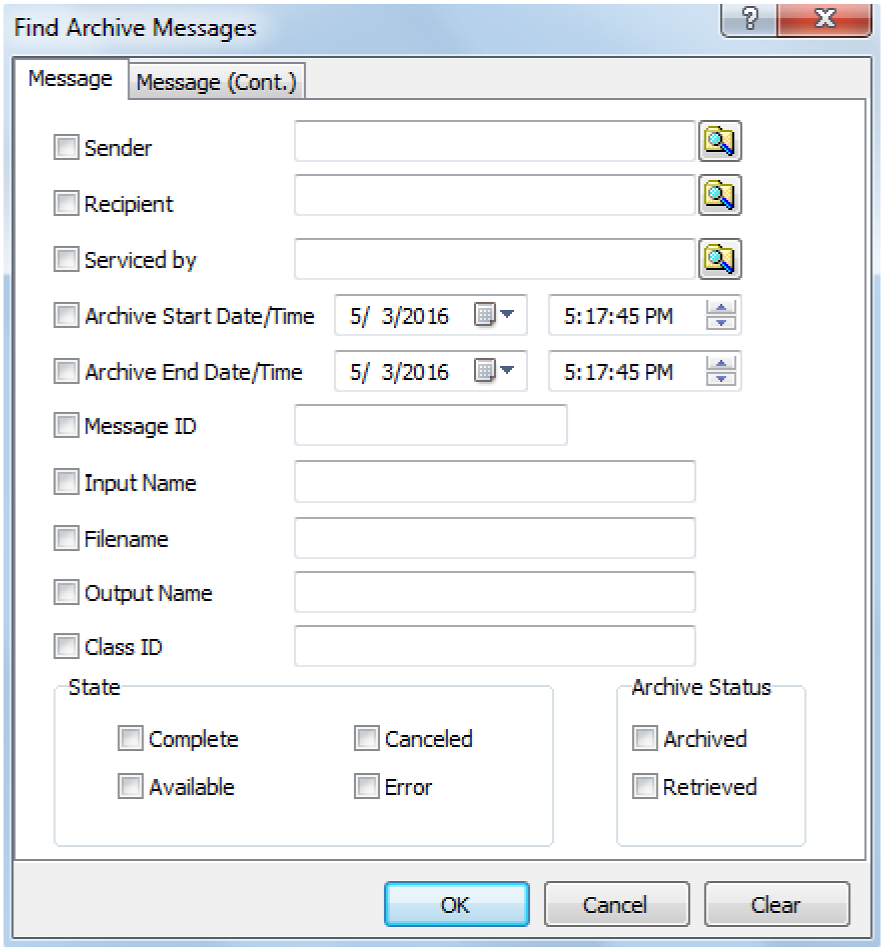
Viewing the Content of a Message (Message Window, Fixed View)

NOTE: Unicode characters will be displayed as non-printable characters and replaced with periods.

Finding Archive Messages

When users want to find messages that have been archived, they must use the **Find Archive Messages** window by selecting the **Search** menu or button on the toolbar.

Note that MessageWay does not support input filenames that contain backslashes, \. For operating systems, such as UNIX, that allow backslashes in filenames, the filename property will be whatever follows the final backslash.



Find Archive Messages

Message | Message (Cont.)

□ Sender

□ Recipient

□ Serviced by

□ Archive Start Date/Time 5/ 3/2016 5:17:45 PM

□ Archive End Date/Time 5/ 3/2016 5:17:45 PM

□ Message ID

□ Input Name

□ Filename

□ Output Name

□ Class ID

State

□ Complete □ Canceled

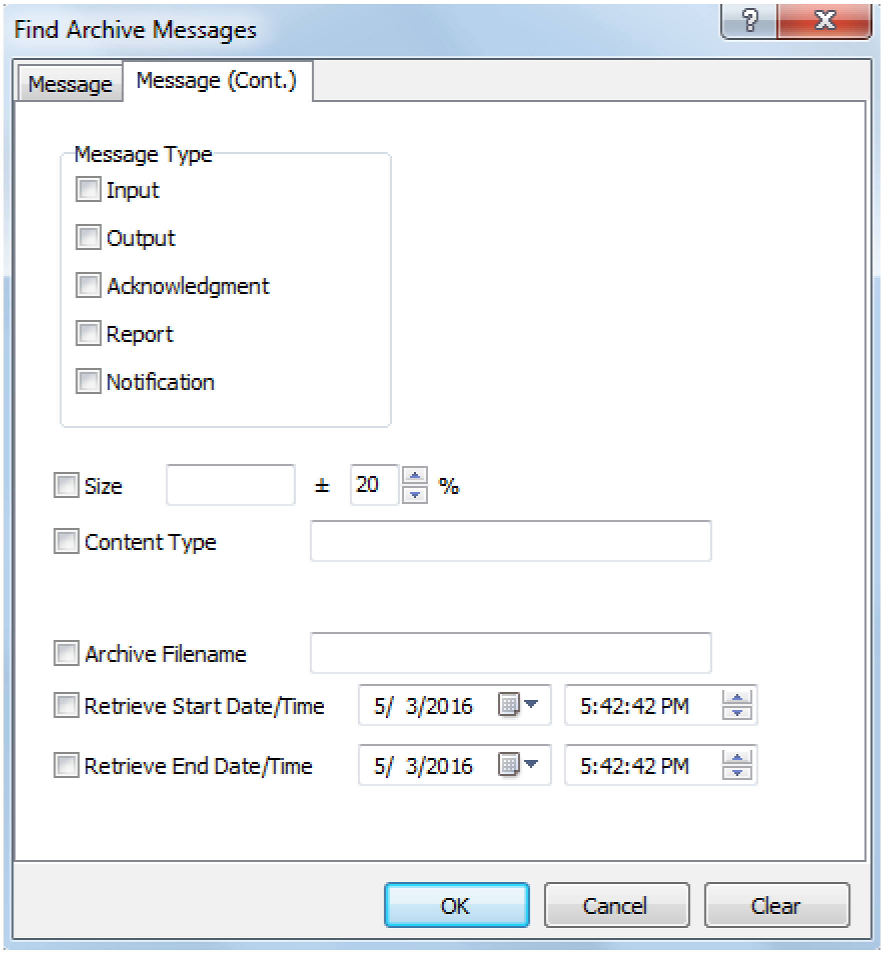
□ Available □ Error

Archive Status

□ Archived

□ Retrieved

Search Criteria on Find Archive Messages Window (Message page)



Message Type

□ Input

□ Output

□ Acknowledgment

□ Report

□ Notification

□ Size ± 20 %

□ Content Type

□ Archive Filename

□ Retrieve Start Date/Time 5/ 3/2016 5:42:42 PM

□ Retrieve End Date/Time 5/ 3/2016 5:42:42 PM

Search Criteria on Find Archive Messages Window (Message (Cont.) page)

IMPORTANT: When you leave all values blank, the list shows all messages in the archive. Users should always select some criteria to limit the number of archive messages on the list. You can set system-wide limits for total messages returned and total displayed in a window on the **MWUser** tab of the ***Server Properties window*** (on page 1313).

Finding Locations

Use the Search option to find locations based on their properties. For more information about the fields, refer to the reference topic, ***Find Locations Window*** (on page 980).

To find a location, from the MessageWay Manager:

1 From the menu bar, select **Search**.

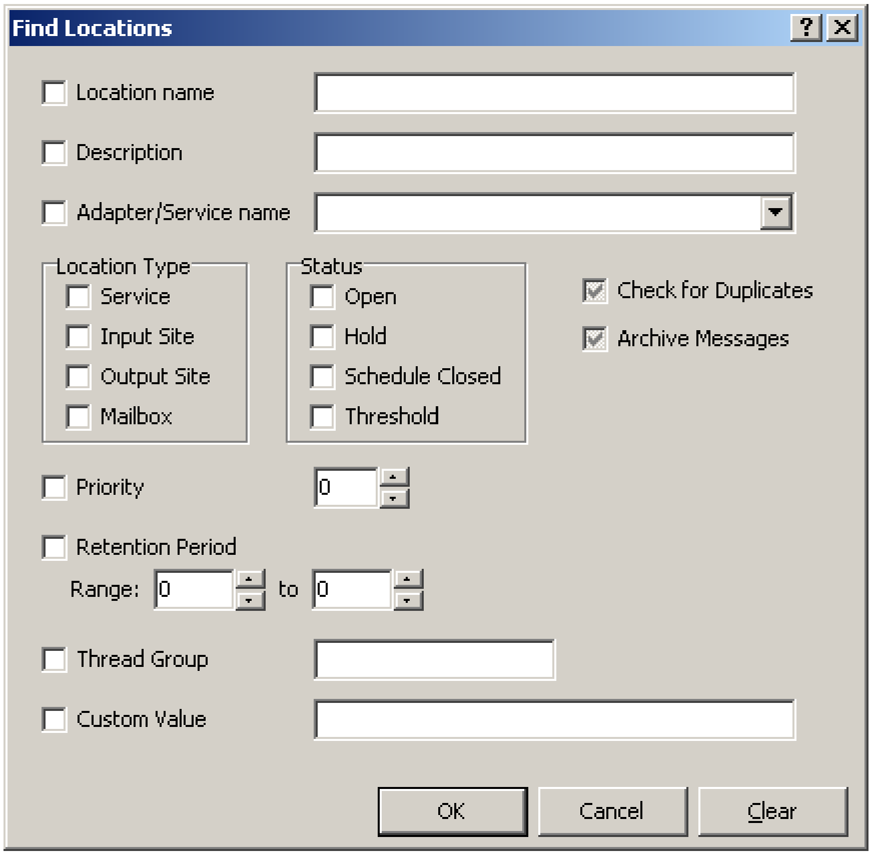
- or -

From the task bar, click the **Search** button.

2 Select **Find Locations**.

The Find Locations window appears.

3 Enter the information to search for a location. Leave all fields blank to return all configurations.



Find Locations

☐ Location name

☐ Description

☐ Adapter/Service name

Location Type
☐ Service
☐ Input Site
☐ Output Site
☐ Mailbox

Status
☐ Open
☐ Hold
☐ Schedule Closed
☐ Threshold

☑ Check for Duplicates

☑ Archive Messages

☐ Priority 0

☐ Retention Period

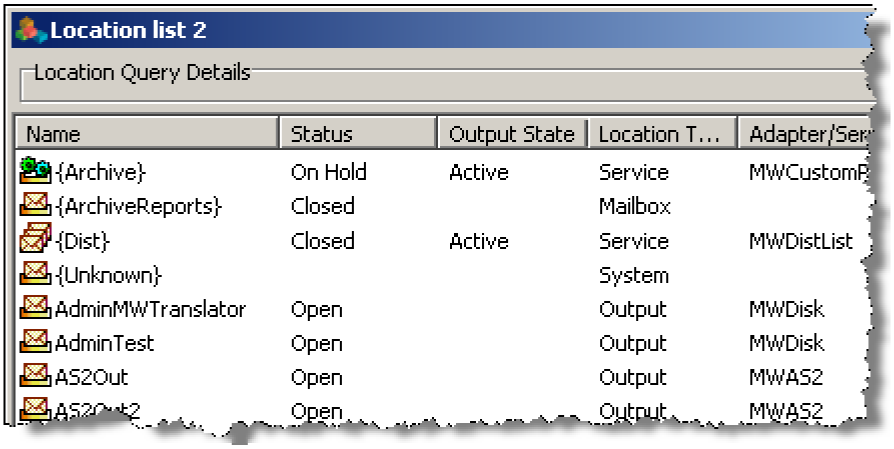
Range: 0 to 0

☐ Thread Group

☐ Custom Value

4 Click **OK.**

A location list appears.

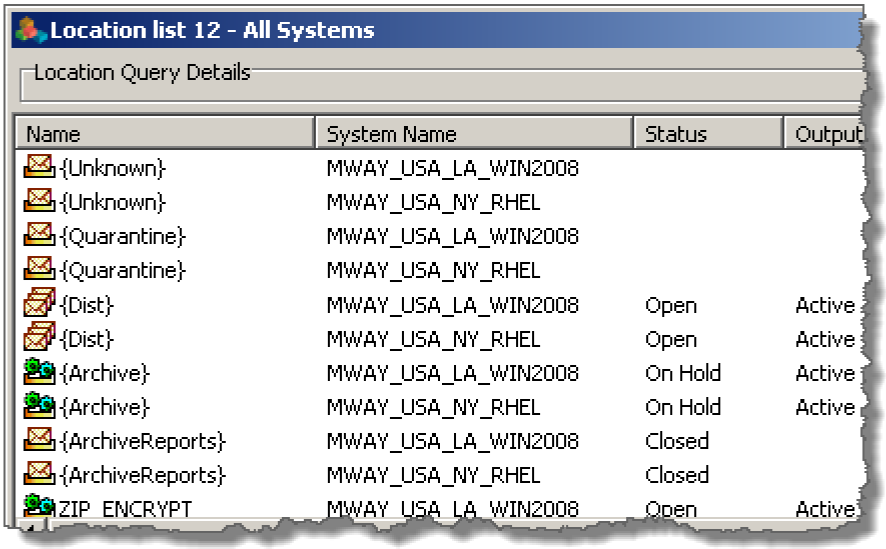


Location list 2

Location Query Details

Name	Status	Output State	Location T...	Adapter/Ser
{Archive}	On Hold	Active	Service	MWCustomP
{ArchiveReports}	Closed		Mailbox	
{Dist}	Closed	Active	Service	MWDistList
{Unknown}			System	
AdminMWTranslator	Open		Output	MWDisk
AdminTest	Open		Output	MWDisk
AS2Out	Open		Output	MWAS2
AS2Out2	Open		Output	MWAS2

When you search through multi-system environments, a System Name column also appears.



Name	System Name	Status	Output
{Unknown}	MWAY_USA_LA_WIN2008		
{Unknown}	MWAY_USA_NY_RHEL		
{Quarantine}	MWAY_USA_LA_WIN2008		
{Quarantine}	MWAY_USA_NY_RHEL		
{Dist}	MWAY_USA_LA_WIN2008	Open	Active
{Dist}	MWAY_USA_NY_RHEL	Open	Active
{Archive}	MWAY_USA_LA_WIN2008	On Hold	Active
{Archive}	MWAY_USA_NY_RHEL	On Hold	Active
{ArchiveReports}	MWAY_USA_LA_WIN2008	Closed	
{ArchiveReports}	MWAY_USA_NY_RHEL	Closed	
ZIP_ENCRYPT	MWAY_USA_LA_WIN2008	Open	Active

Finding Location Schedules

All location schedules, master and local, are used for automated receipt and delivery of messages. Master location schedules may be shared by multiple locations. Local schedules are specific to a location. Use the Search option to find location schedules based on their properties. For more information about the fields, refer to the reference topic, ***Find Location Schedules Window*** (on page 983).

To find a location schedule, from the MessageWay Manager:

1 From the menu bar, select **Search**.

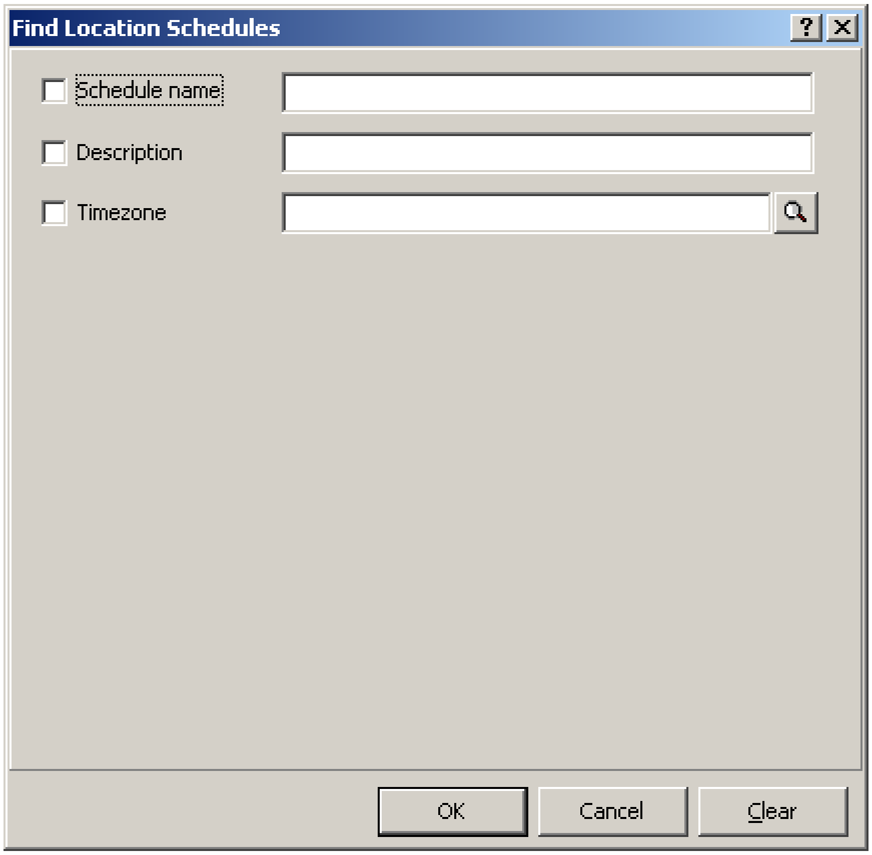
   - or -

   From the task bar, click the **Search** button.

2 Select **Find Location Schedules**.

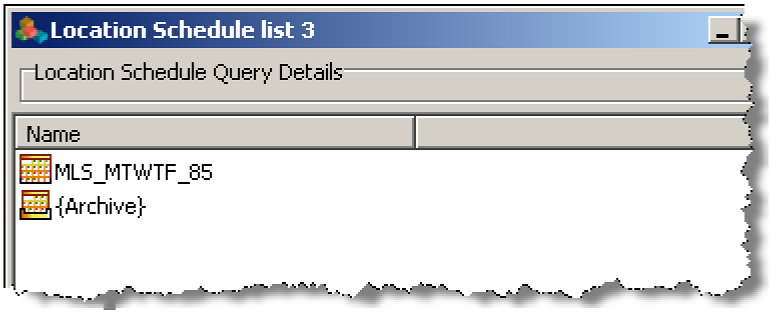
   The Find Location Schedules window appears.

3 Enter the information to search for a location schedule. Leave all fields blank to return all configurations.



4 Click **OK**.

A location schedule list appears.



When you search through multi-system environments, a System Name column also appears.

The list uses different icons for master location schedules and local location schedules, as follows:

Icon	Schedule Type
▦	Master location schedule

Icon	Schedule Type
📅	Local location schedule

Finding Receipt Schedules

Receipt Monitor uses schedules to monitor input addresses for message arrivals. Use the Search option to find a receipt schedule based on its properties. For more information about the fields, refer to the reference topic, ***Find Receipt Schedules Window*** (on page 1006).

To find a receipt schedule, from the MessageWay Manager:

1. From the menu bar, select **Search**.

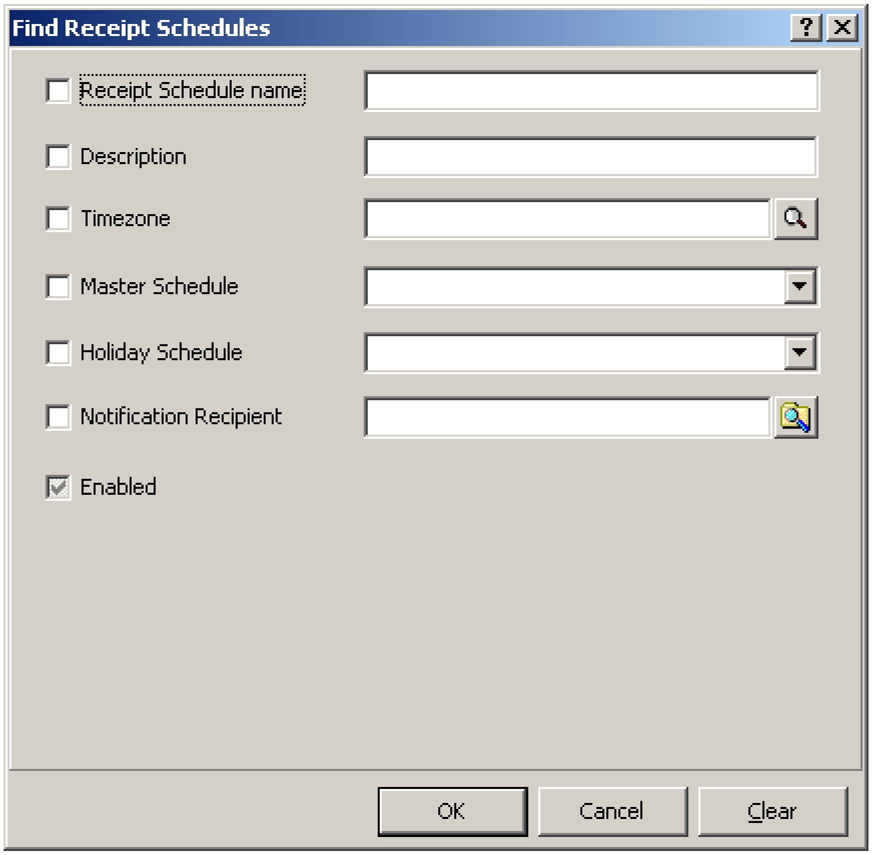
   - or -

   From the task bar, click the **Search** button.

2. Select **Find Receipt Schedules**.

   The Find Receipt Schedules window appears.

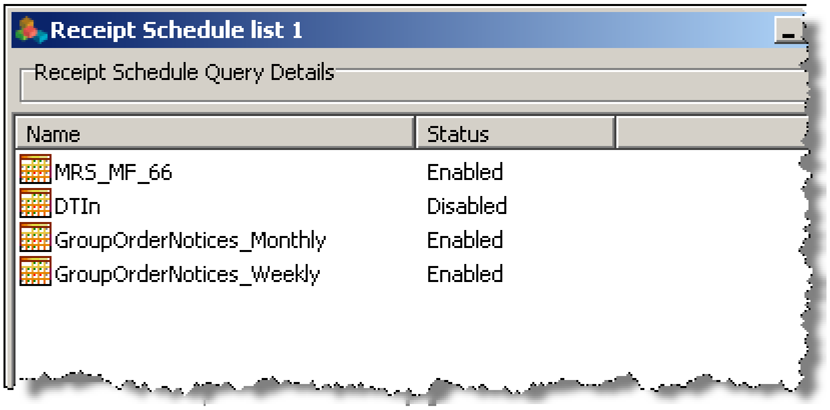
3 Enter the information to search for a receipt schedule. Leave all fields blank to return all configurations.



□ Receipt Schedule name	
□ Description	
□ Timezone	
□ Master Schedule	
□ Holiday Schedule	
□ Notification Recipient	
☑ Enabled	

4 Click **OK**.

A receipt schedule list appears.



Name	Status
MRS_MF_66	Enabled
DTIn	Disabled
GroupOrderNotices_Monthly	Enabled
GroupOrderNotices_Weekly	Enabled

When you search through multi-system environments, a System Name column also appears.

Finding Rules Processing Profiles

Rules Processing is a service that routes messages based on message properties or content. Users create Rules Processing Profiles that the service uses to route messages. Use the Search option to find a rules processing profile based on its properties. For more information about the fields, refer to the reference topic, ***Find Rules Processing Window*** (on page 1008).

To find a rules processing profile, from the MessageWay Manager:

1 From the menu bar, select **Search**.

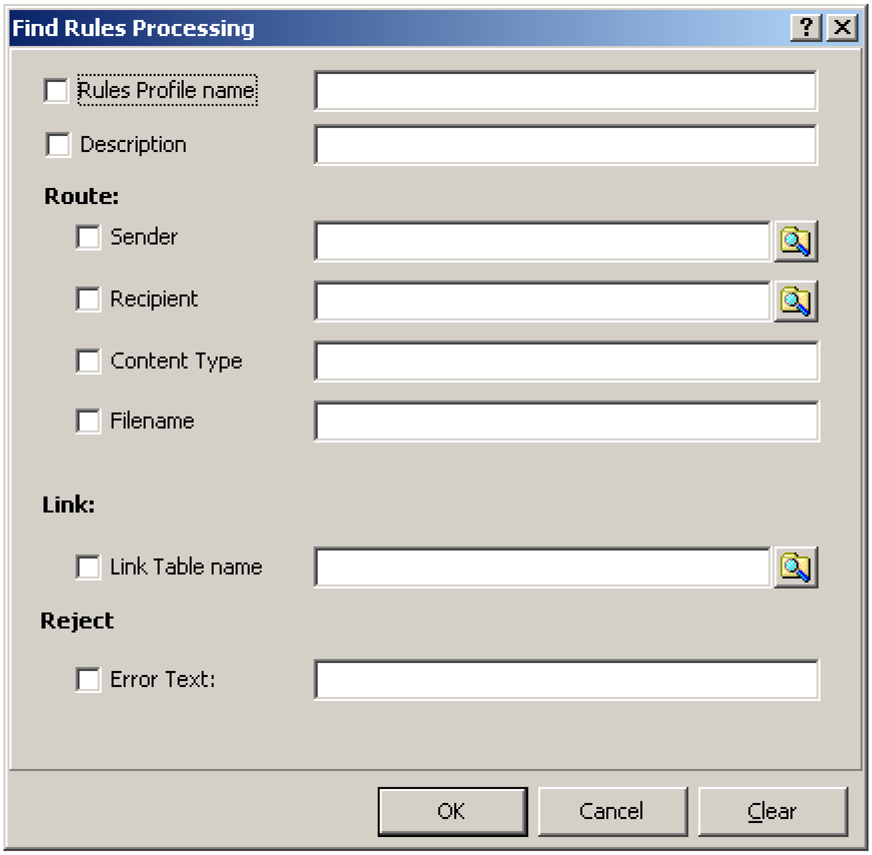
- or -

From the task bar, click the **Search** button.

2 Select **Find Rules Processing**.

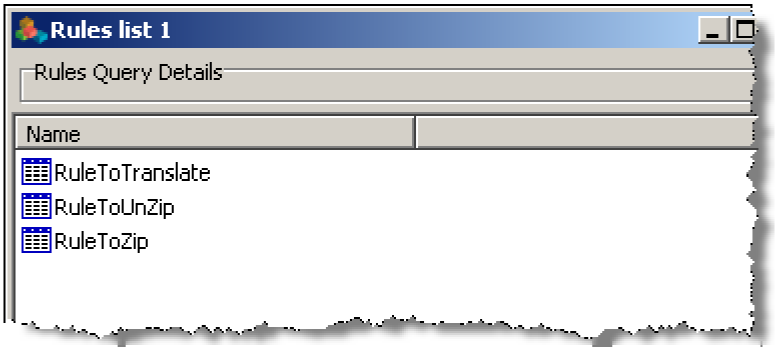
The Find Rules Processing window appears.

3 Enter the information to search for a rules processing profile. Leave all fields blank to return all configurations.



4 Click **OK**.

A rules list appears.



RuleToTranslate
RuleToUnZip
RuleToZip

When you search through multi-system environments, a System Name column also appears.

Finding Keys

Use the Search option to find a MessageWay client key based on its properties. For more information about the fields, refer to the reference topic, ***Find Keys Window*** (on page 979).

To find a client key, from the MessageWay Manager:

1 From the menu bar, select **Search**.

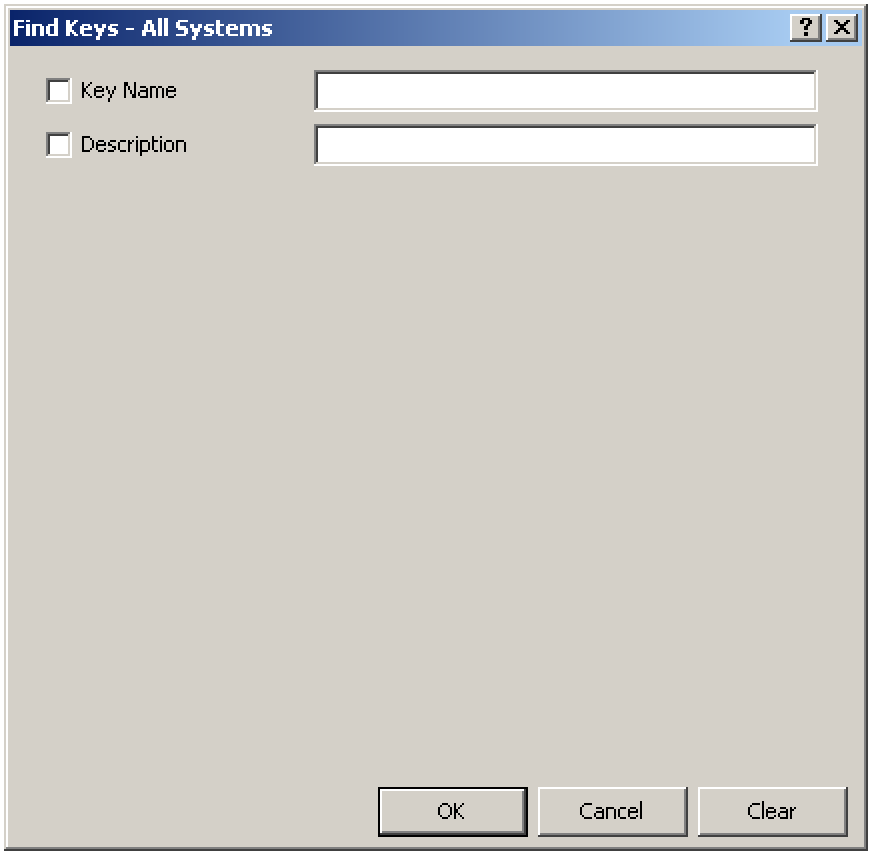
- or -

From the task bar, click the **Search** button.

2 Select **Find Keys**.

The Find Keys window appears.

3 Enter the information to search for a user. Leave all fields blank to return all configurations.



Find Keys - All Systems

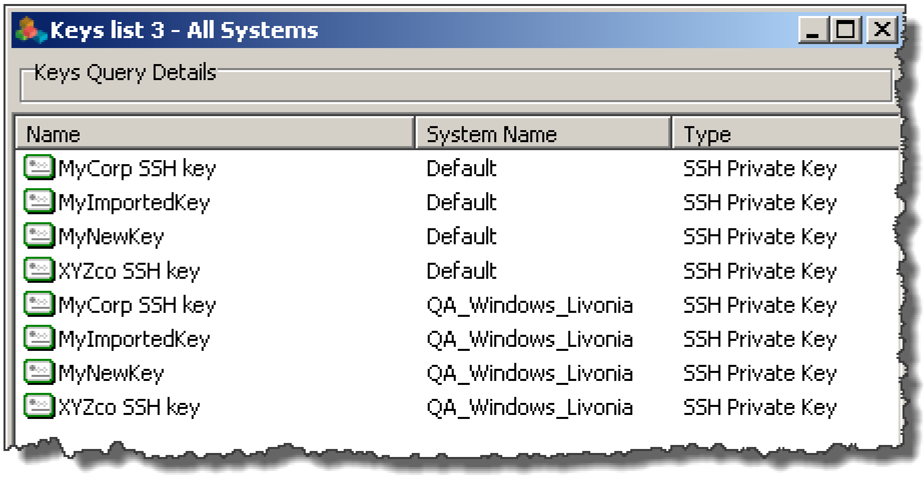
☐ Key Name

☐ Description

4 Click **OK**.

A keys list appears.

NOTE: When you monitor multiple MessageWay systems, this list returns the keys from all systems you are currently monitoring.



Keys list 3 - All Systems

Name	System Name	Type
MyCorp SSH key	Default	SSH Private Key
MyImportedKey	Default	SSH Private Key
MyNewKey	Default	SSH Private Key
XYZco SSH key	Default	SSH Private Key
MyCorp SSH key	QA_Windows_Livonia	SSH Private Key
MyImportedKey	QA_Windows_Livonia	SSH Private Key
MyNewKey	QA_Windows_Livonia	SSH Private Key
XYZco SSH key	QA_Windows_Livonia	SSH Private Key

Finding Users

Use the Search option to find a MessageWay user based on its properties. For more information about the fields, refer to the reference topic, ***Find Users Window*** (on page 1020).

To find a user, from the MessageWay Manager:

1 From the menu bar, select **Search**.

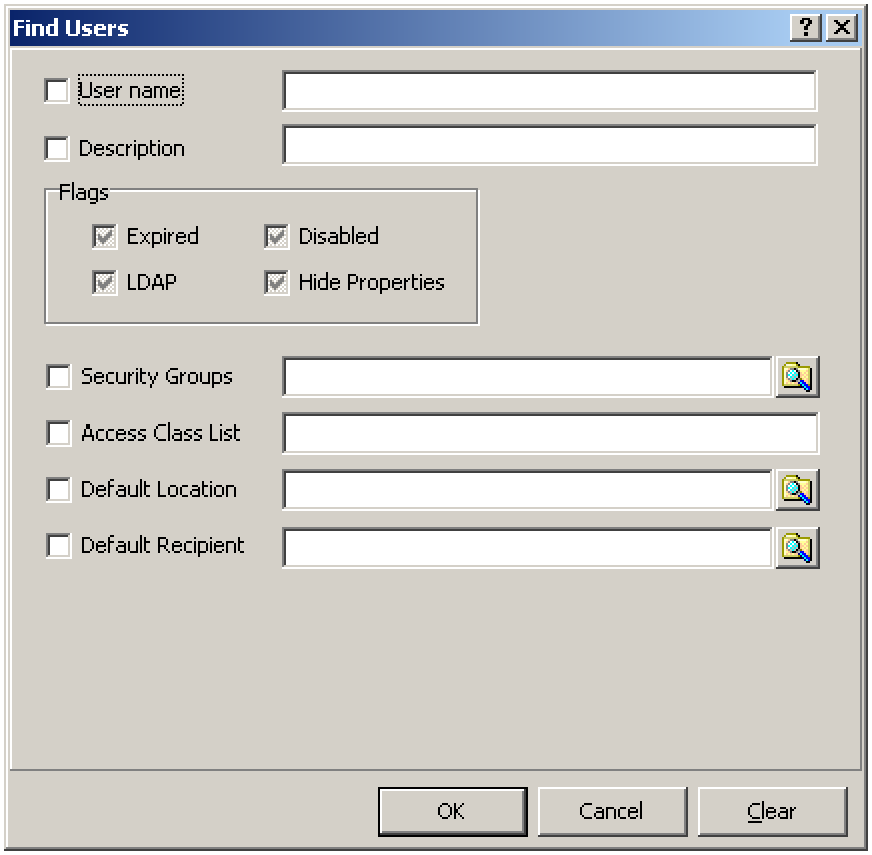
- or -

From the task bar, click the **Search** button.

2 Select **Find Users**.

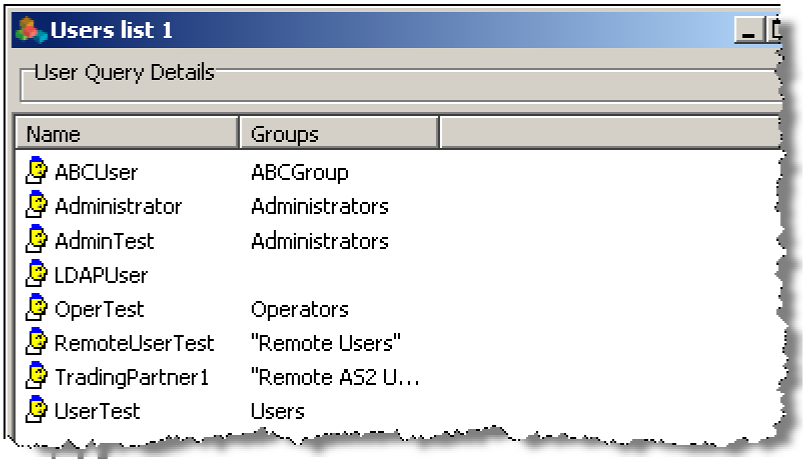
The Find Users window appears.

3 Enter the information to search for a user. Leave all fields blank to return all configurations.



4 Click **OK**.

A user list appears.



Name	Groups
ABCUser	ABCGroup
Administrator	Administrators
AdminTest	Administrators
LDAPUser	
OperTest	Operators
RemoteUserTest	"Remote Users"
TradingPartner1	"Remote AS2 U...
UserTest	Users

When you search through multi-system environments, a System Name column also appears.

Finding Sessions

Use the Search option to find active sessions for users who are connected to MessageWay.

IMPORTANT: A session remains active until the user logs off or the session times out, which is determined by the configurations for the entity that makes the connection. However, orphaned sessions, typically the result of physical connections that are not maintained, may still appear on a Find Sessions message list. The Scheduling Server deletes these orphaned sessions based on the *Logon Idle Lifetime* setting in the User Policies Properties window. If you change the setting, you must restart the User Server, the Service Interface and the Scheduling Server for the change to take effect as expected.

For more information about the fields, refer to the reference topic, ***Find Sessions Window*** (on page 1011).

To find a session, from the MessageWay Manager:

1 From the menu bar, select **Search**.

- or -

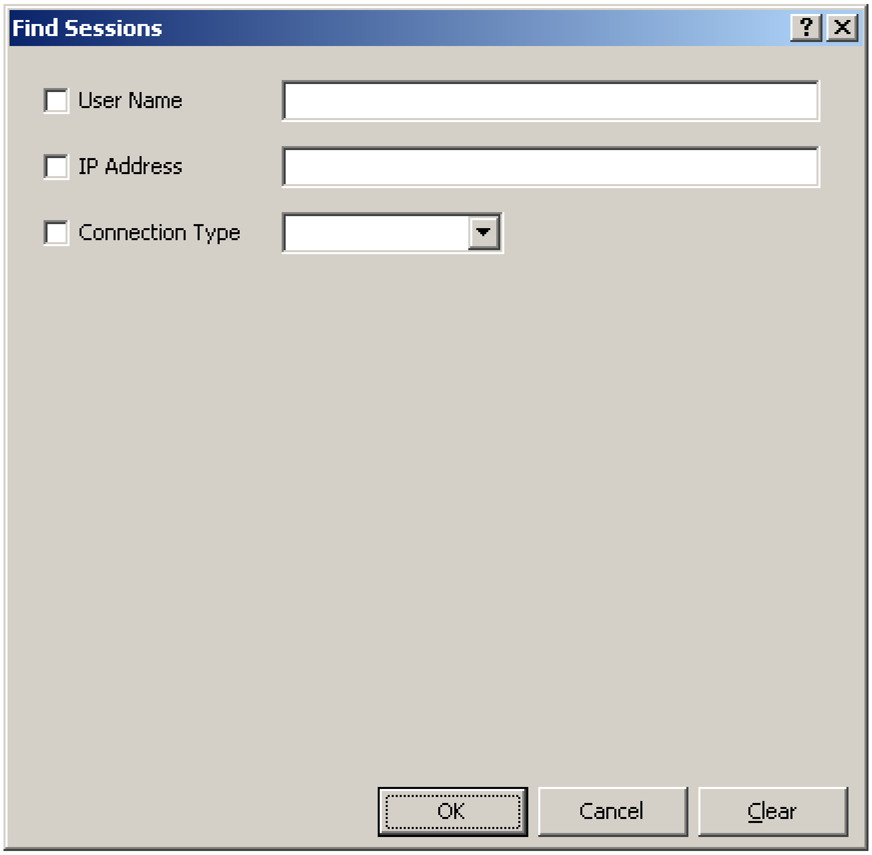
From the task bar, click the **Search** button.

2 Select **Find Sessions**.

The Find Sessions window appears.

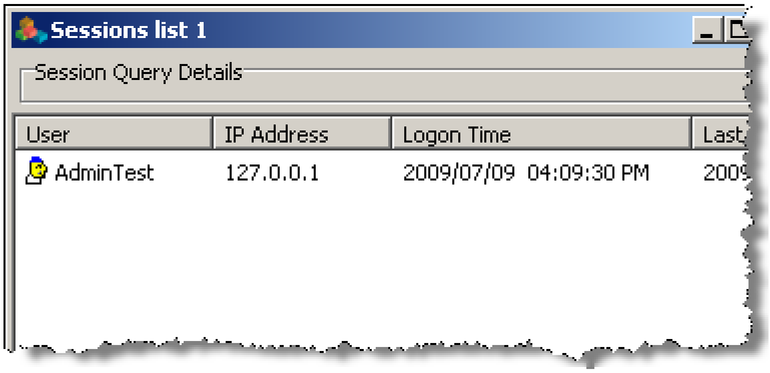
3 Type the name of a MessageWay user and/or IP address of a client and/or select or type a connection type to search for a session. Leave all fields blank to return all connected sessions.

NOTE: The drop-down list may not show all connection types. If you type a Connection Type rather than select one from the list, it must match the name recognized by MessageWay, for example **WEB**. The names are case-insensitive.



4 Click **OK**.

A sessions list appears.



User	IP Address	Logon Time	Last
AdminTest	127.0.0.1	2009/07/09 04:09:30 PM	200

When you search through multi-system environments, a System Name column also appears.

Finding Audit Logs

Use the Search option to find audit log entries in the MessageWay database based on the log entry date and other properties. For more information about the fields, refer to the reference topic, ***Find Audit Logs Window*** (on page 1013).

NOTE: User access right **View Logs** is required to find and view audit logs.

To find an audit log entry, from the MessageWay Manager:

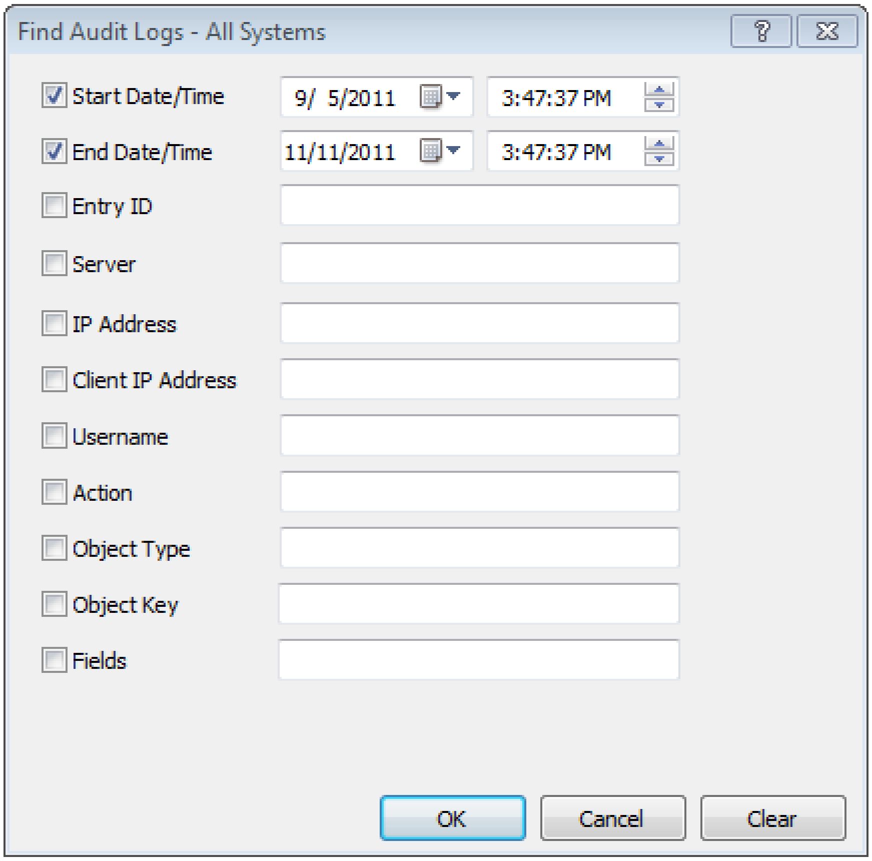
1 From the menu bar, select **Search**.

- or -

From the task bar, click the **Search** button.

2 Select **Find Logs, Audit Logs**.

The Find Audit Logs window appears.



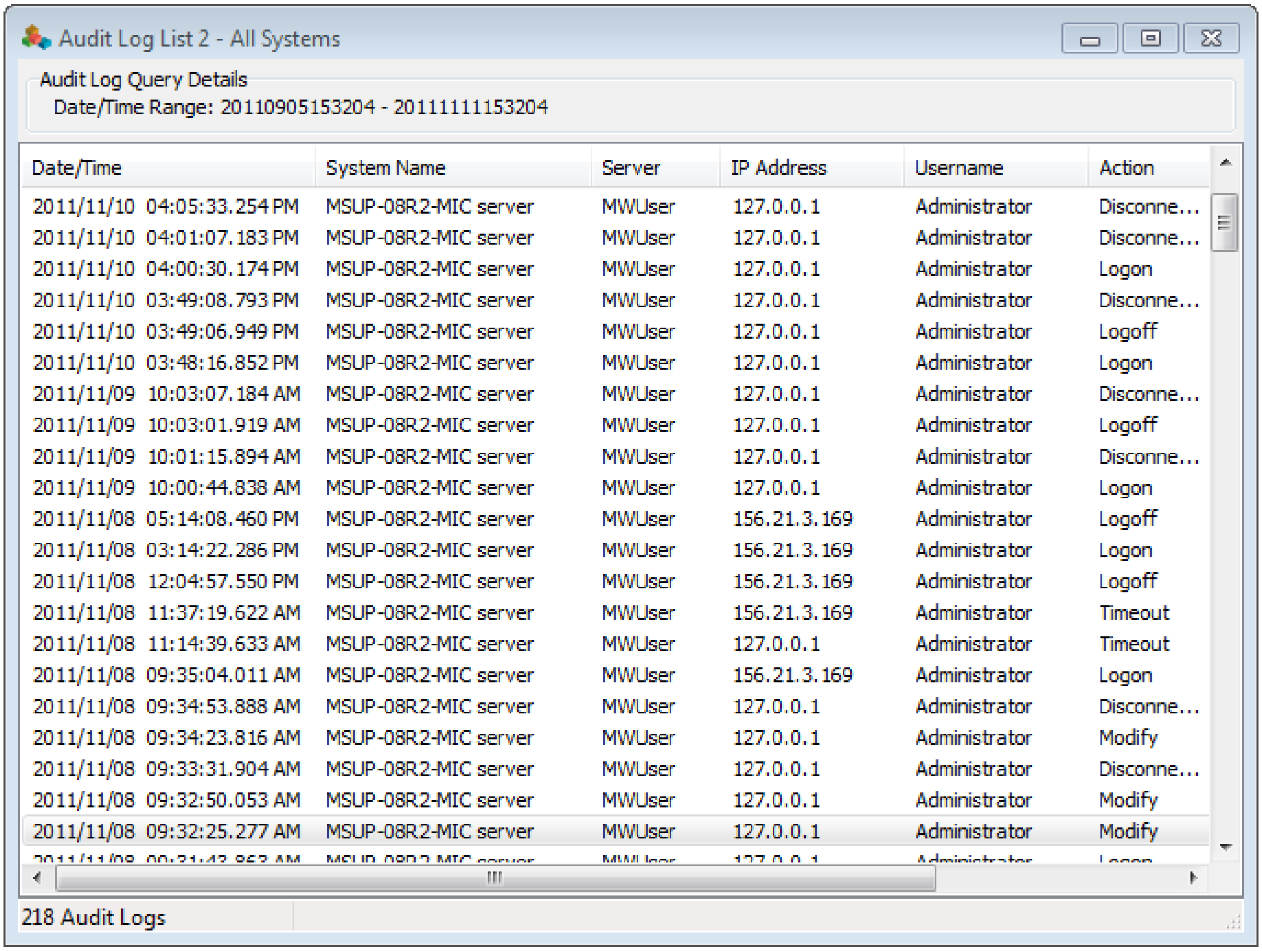
Find Audit Logs - All Systems

☑ Start Date/Time	9/ 5/2011	3:47:37 PM
☑ End Date/Time	11/11/2011	3:47:37 PM
□ Entry ID		
□ Server		
□ IP Address		
□ Client IP Address		
□ Username		
□ Action		
□ Object Type		
□ Object Key		
□ Fields		

3 Enter the information to search for a log entry.

4 Click **OK**.

An Audit Log Entry list appears.



Audit Log List 2 - All Systems

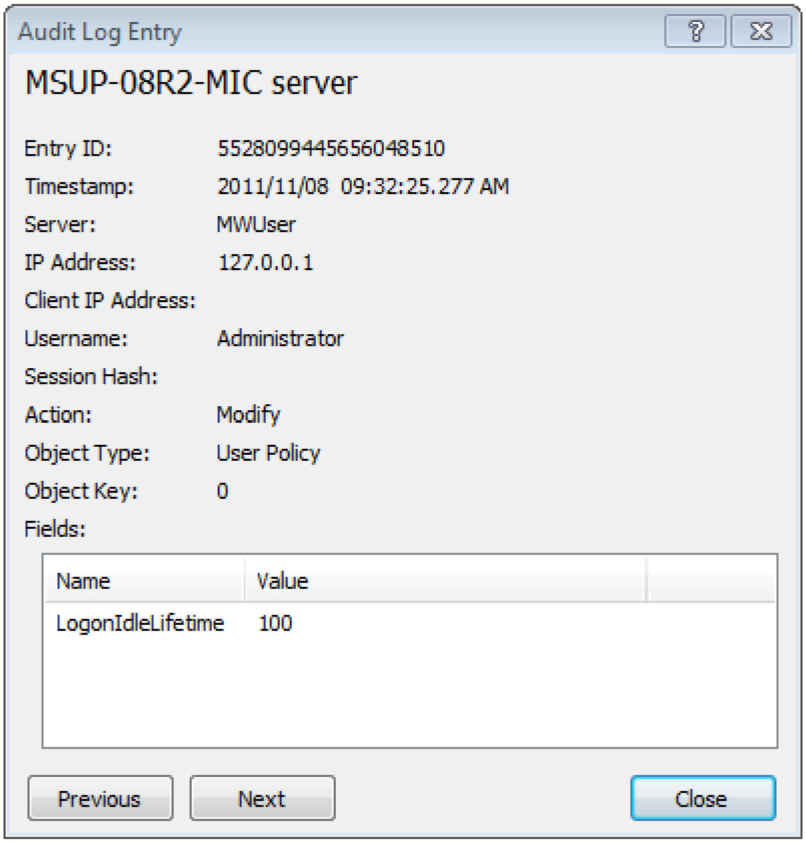
Audit Log Query Details

Date/Time Range: 20110905153204 - 20111111153204

Date/Time	System Name	Server	IP Address	Username	Action
2011/11/10 04:05:33.254 PM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Disconne…
2011/11/10 04:01:07.183 PM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Disconne…
2011/11/10 04:00:30.174 PM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Logon
2011/11/10 03:49:08.793 PM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Disconne…
2011/11/10 03:49:06.949 PM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Logoff
2011/11/10 03:48:16.852 PM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Logon
2011/11/09 10:03:07.184 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Disconne…
2011/11/09 10:03:01.919 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Logoff
2011/11/09 10:01:15.894 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Disconne…
2011/11/09 10:00:44.838 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Logon
2011/11/08 05:14:08.460 PM	MSUP-08R2-MIC server	MWUser	156.21.3.169	Administrator	Logoff
2011/11/08 03:14:22.286 PM	MSUP-08R2-MIC server	MWUser	156.21.3.169	Administrator	Logon
2011/11/08 12:04:57.550 PM	MSUP-08R2-MIC server	MWUser	156.21.3.169	Administrator	Logoff
2011/11/08 11:37:19.622 AM	MSUP-08R2-MIC server	MWUser	156.21.3.169	Administrator	Timeout
2011/11/08 11:14:39.633 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Timeout
2011/11/08 09:35:04.011 AM	MSUP-08R2-MIC server	MWUser	156.21.3.169	Administrator	Logon
2011/11/08 09:34:53.888 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Disconne…
2011/11/08 09:34:23.816 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Modify
2011/11/08 09:33:31.904 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Disconne…
2011/11/08 09:32:50.053 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Modify
2011/11/08 09:32:25.277 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Modify
2011/11/08 09:31:43.863 AM	MSUP-08R2-MIC server	MWUser	127.0.0.1	Administrator	Logon

218 Audit Logs

5 Double-click an entry to view the associated data.



Entry ID: 5528099445656048510
Timestamp: 2011/11/08 09:32:25.277 AM
Server: MWUser
IP Address: 127.0.0.1
Client IP Address:
Username: Administrator
Session Hash:
Action: Modify
Object Type: User Policy
Object Key: 0
Fields:

Name	Value
LogonIdleLifetime	100

This window shows the data for a log entry. This includes the settings that show the state of the object when the action was logged. The Fields show the detail data, which changes depending on the type of log entry. Use the Next and Previous buttons to view the details for other log entries.

Finding Event Logs

Use the Search option to find event log entries in the MessageWay database based on the log entry date and other properties. For more information about the fields, refer to the reference topic, ***Find Event Logs Window*** (on page 1016).

NOTE: User access right **View Logs** is required to find and view event logs.

To find an event log entry, from the MessageWay Manager:

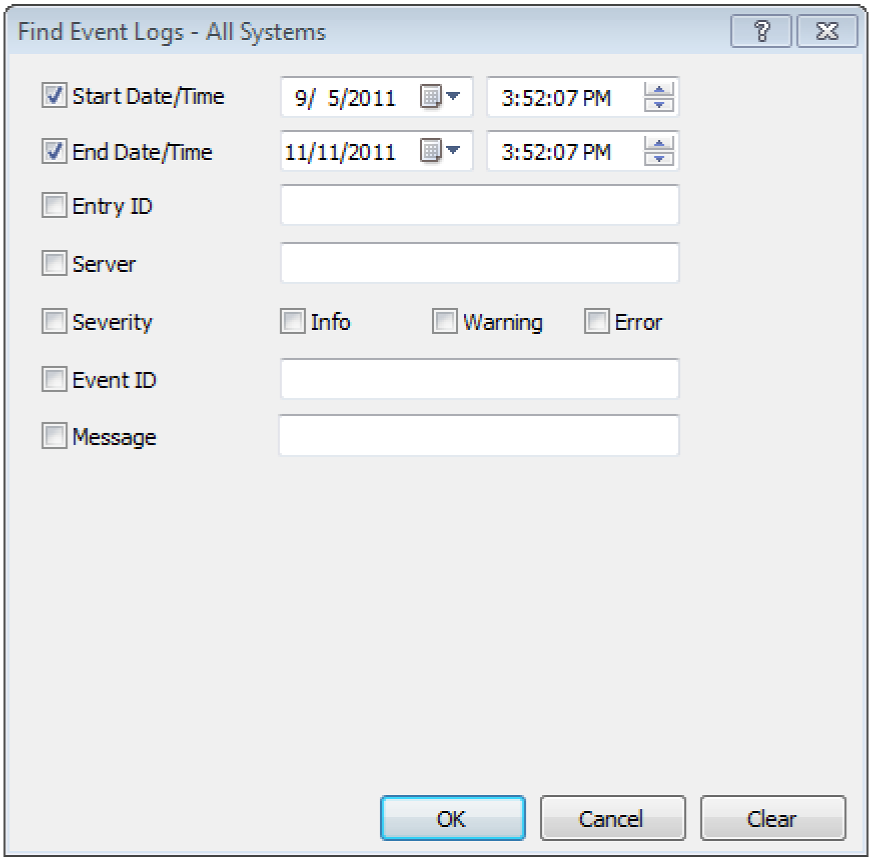
1 From the menu bar, select **Search**.

- or -

From the task bar, click the **Search** button.

2 Select **Find Logs, Event Logs**.

The Find Event Logs window appears.



☑ Start Date/Time 9/ 5/2011 3:52:07 PM

☑ End Date/Time 11/11/2011 3:52:07 PM

□ Entry ID

□ Server

□ Severity □ Info □ Warning □ Error

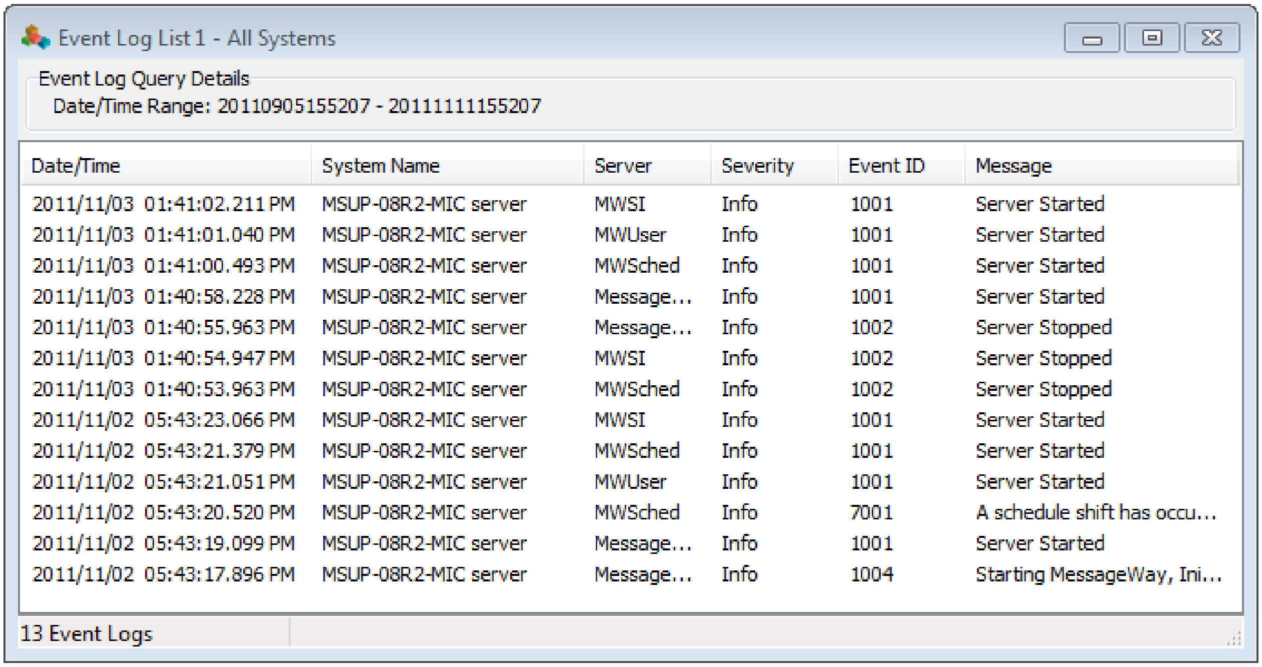
□ Event ID

□ Message

3 Enter the information to search for a log entry.

4 Click **OK**.

An Event Log Entry list appears.



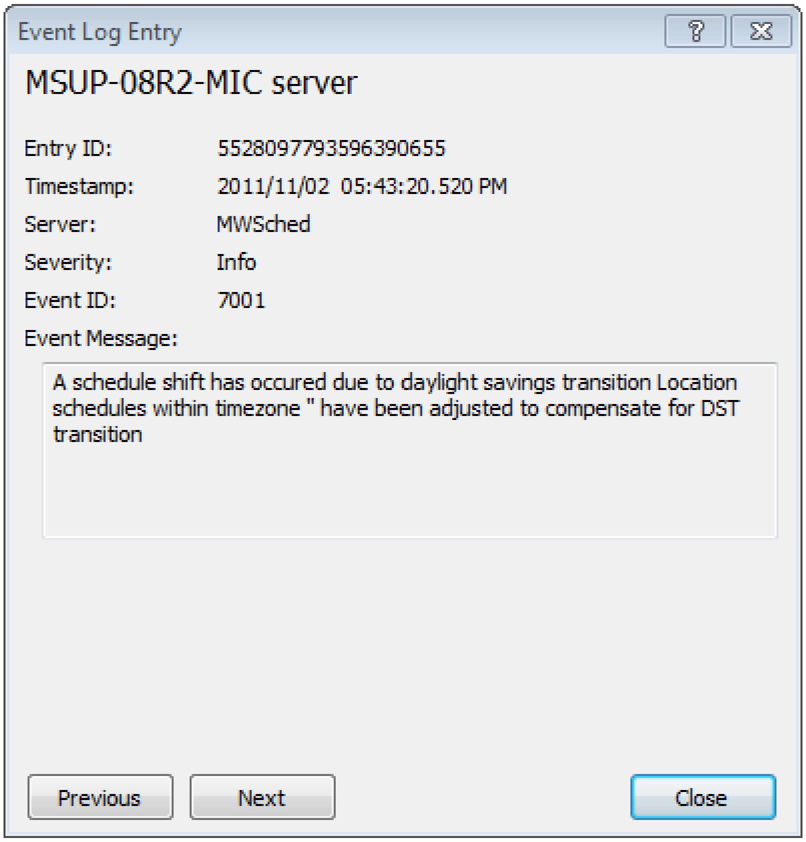
Event Log Query Details

Date/Time Range: 20110905155207 - 20111111155207

Date/Time	System Name	Server	Severity	Event ID	Message
2011/11/03 01:41:02.211 PM	MSUP-08R2-MIC server	MWSI	Info	1001	Server Started
2011/11/03 01:41:01.040 PM	MSUP-08R2-MIC server	MWUser	Info	1001	Server Started
2011/11/03 01:41:00.493 PM	MSUP-08R2-MIC server	MWSched	Info	1001	Server Started
2011/11/03 01:40:58.228 PM	MSUP-08R2-MIC server	Message…	Info	1001	Server Started
2011/11/03 01:40:55.963 PM	MSUP-08R2-MIC server	Message…	Info	1002	Server Stopped
2011/11/03 01:40:54.947 PM	MSUP-08R2-MIC server	MWSI	Info	1002	Server Stopped
2011/11/03 01:40:53.963 PM	MSUP-08R2-MIC server	MWSched	Info	1002	Server Stopped
2011/11/02 05:43:23.066 PM	MSUP-08R2-MIC server	MWSI	Info	1001	Server Started
2011/11/02 05:43:21.379 PM	MSUP-08R2-MIC server	MWSched	Info	1001	Server Started
2011/11/02 05:43:21.051 PM	MSUP-08R2-MIC server	MWUser	Info	1001	Server Started
2011/11/02 05:43:20.520 PM	MSUP-08R2-MIC server	MWSched	Info	7001	A schedule shift has occu…
2011/11/02 05:43:19.099 PM	MSUP-08R2-MIC server	Message…	Info	1001	Server Started
2011/11/02 05:43:17.896 PM	MSUP-08R2-MIC server	Message…	Info	1004	Starting MessageWay, Ini…

13 Event Logs

5 Double-click an entry to view the associated data.



MSUP-08R2-MIC server

Entry ID: 5528097793596390655

Timestamp: 2011/11/02 05:43:20.520 PM

Server: MWSched

Severity: Info

Event ID: 7001

Event Message:

A schedule shift has occured due to daylight savings transition Location schedules within timezone '' have been adjusted to compensate for DST transition

This window shows the data associated with this entry. The Event Message shows the detail data, which changes depending on the type of log entry. Use the Next and Previous buttons to view the details for other log entries.

Finding Trace Logs

Use the Search option to find trace log entries in the MessageWay database based on the log entry date and other properties. For more information about the fields, refer to the reference topic, ***Find Trace Logs Window*** (on page 1018).

NOTE: User access right **View Logs** is required to find and view trace logs.

To find a trace log entry, from the MessageWay Manager:

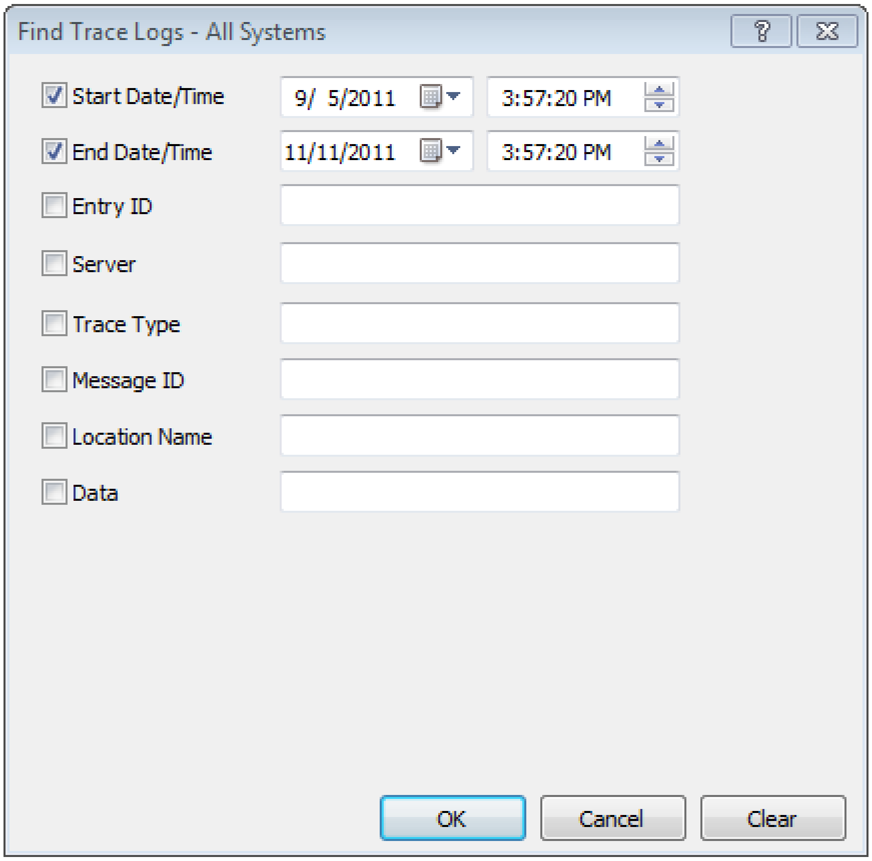
1 From the menu bar, select **Search**.

- or -

From the task bar, click the **Search** button.

2 Select **Find Logs, Trace Logs**.

The Find Trace Logs window appears.



Find Trace Logs - All Systems

☑ Start Date/Time 9/ 5/2011 3:57:20 PM

☑ End Date/Time 11/11/2011 3:57:20 PM

□ Entry ID

□ Server

□ Trace Type

□ Message ID

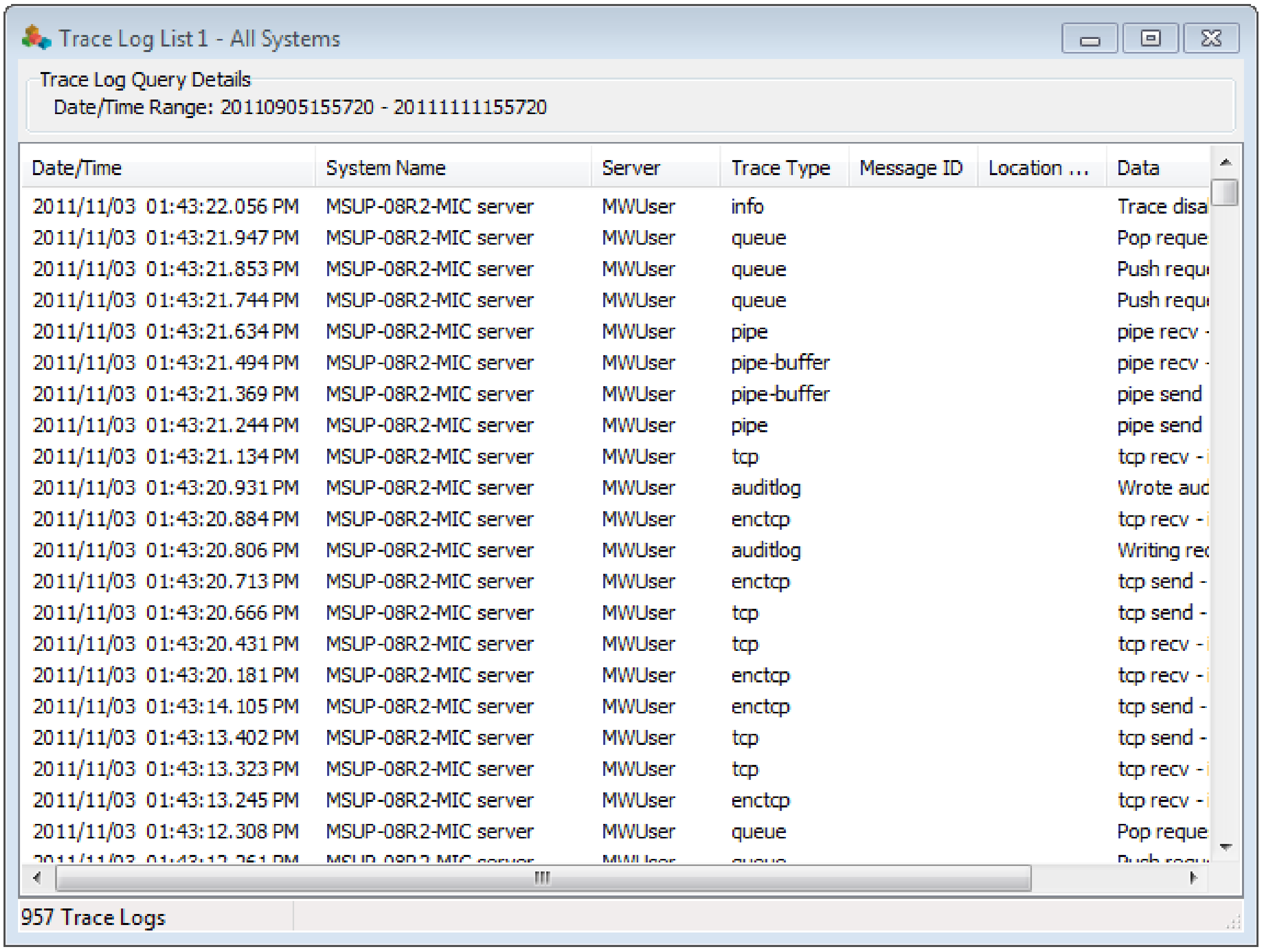
□ Location Name

□ Data

3 Enter the information to search for a log entry.

4 Click **OK**.

A Trace Log Entry list appears.



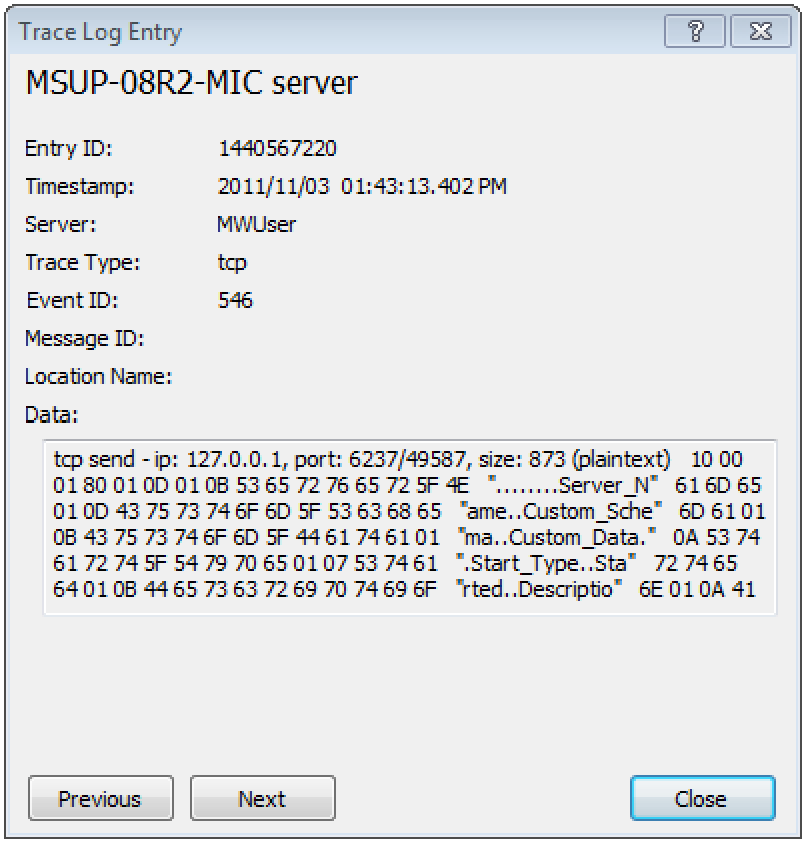
Trace Log Query Details

Date/Time Range: 20110905155720 - 20111111155720

Date/Time	System Name	Server	Trace Type	Message ID	Location ...	Data
2011/11/03 01:43:22.056 PM	MSUP-08R2-MIC server	MWUser	info			Trace disa
2011/11/03 01:43:21.947 PM	MSUP-08R2-MIC server	MWUser	queue			Pop reque
2011/11/03 01:43:21.853 PM	MSUP-08R2-MIC server	MWUser	queue			Push requ
2011/11/03 01:43:21.744 PM	MSUP-08R2-MIC server	MWUser	queue			Push requ
2011/11/03 01:43:21.634 PM	MSUP-08R2-MIC server	MWUser	pipe			pipe recv -
2011/11/03 01:43:21.494 PM	MSUP-08R2-MIC server	MWUser	pipe-buffer			pipe recv -
2011/11/03 01:43:21.369 PM	MSUP-08R2-MIC server	MWUser	pipe-buffer			pipe send
2011/11/03 01:43:21.244 PM	MSUP-08R2-MIC server	MWUser	pipe			pipe send
2011/11/03 01:43:21.134 PM	MSUP-08R2-MIC server	MWUser	tcp			tcp recv -
2011/11/03 01:43:20.931 PM	MSUP-08R2-MIC server	MWUser	auditlog			Wrote aud
2011/11/03 01:43:20.884 PM	MSUP-08R2-MIC server	MWUser	enctcp			tcp recv -
2011/11/03 01:43:20.806 PM	MSUP-08R2-MIC server	MWUser	auditlog			Writing rec
2011/11/03 01:43:20.713 PM	MSUP-08R2-MIC server	MWUser	enctcp			tcp send -
2011/11/03 01:43:20.666 PM	MSUP-08R2-MIC server	MWUser	tcp			tcp send -
2011/11/03 01:43:20.431 PM	MSUP-08R2-MIC server	MWUser	tcp			tcp recv -
2011/11/03 01:43:20.181 PM	MSUP-08R2-MIC server	MWUser	enctcp			tcp recv -
2011/11/03 01:43:14.105 PM	MSUP-08R2-MIC server	MWUser	enctcp			tcp send -
2011/11/03 01:43:13.402 PM	MSUP-08R2-MIC server	MWUser	tcp			tcp send -
2011/11/03 01:43:13.323 PM	MSUP-08R2-MIC server	MWUser	tcp			tcp recv -
2011/11/03 01:43:13.245 PM	MSUP-08R2-MIC server	MWUser	enctcp			tcp recv -
2011/11/03 01:43:12.308 PM	MSUP-08R2-MIC server	MWUser	queue			Pop reque
2011/11/03 01:43:12.261 PM	MSUP-08R2-MIC server	MWUser	queue			Push requ

957 Trace Logs

5 Double-click an entry to view the associated data.



MSUP-08R2-MIC server

Entry ID: 1440567220

Timestamp: 2011/11/03 01:43:13.402 PM

Server: MWUser

Trace Type: tcp

Event ID: 546

Message ID:

Location Name:

Data:

```
tcp send - ip: 127.0.0.1, port: 6237/49587, size: 873 (plaintext)   10 00
01 80 01 0D 01 0B 53 65 72 76 65 72 5F 4E   "........Server_N"   61 6D 65
01 0D 43 75 73 74 6F 6D 5F 53 63 68 65   "ame..Custom_Sche"   6D 61 01
0B 43 75 73 74 6F 6D 5F 44 61 74 61 01   "ma..Custom_Data."   0A 53 74
61 72 74 5F 54 79 70 65 01 07 53 74 61   ".Start_Type..Sta"   72 74 65
64 01 0B 44 65 73 63 72 69 70 74 69 6F   "rted..Descriptio"   6E 01 0A 41
```

This window shows the data associated with the entry. The Data field shows the detail data, which changes depending on the type of log entry. Use the Next and Previous buttons to view the details for other log entries.

Maintaining Message Information

This section provides information about how to maintain the various MessageWay storage directories, which include:

- For message content, the message store (either disk or database) contains message content files
- For messages retrieved from archive, the archive retrieve message store (either disk or database) contains retrieved from archive message content files
- Message archive directory contains message archive zip files and corresponding archive table entries
- Server directory contains sub-directories for adapters and services to store persistent and temporary information
- MessageWay audit directory contains:
  - Audit files, whose names begin with *audit*, that log MessageWay Manager operator actions
  - Service Interface audit files, whose names begin with *siaudit*, that log activity from remote users

Overview of Maintaining Message Information

The processes to maintain information varies depending on the type of information. The following table briefly describes how to maintain the information:

Information	Maintenance Process
Message Store	Archive program: ▪ Retention is determined by configurations for destination location and other rules ▪ Default retention options may be changed in MWArchive Server Properties window ▪ User commands *Mark for Archive* and *Mark for Delete* will override default retention
Archive Retrieve Message Store	Archive program: ▪ Retention is determined by settings in MWArchive Server Properties window ▪ User command *Delete Content...* within Find Archive Messages list allow messages retrieved from archive to be manually deleted
Archive	Archive Maintenance program: ▪ Retention is determined by settings in MWArchive Server Properties window

Information	Maintenance Process
Server	Archive program cleans temporary files in /server/temp, /server/<adapter or service>/temp and /server/<adapter or service>/tmp left during failed processes: ▪ Default retention is 30 days ▪ Retention option may be changed in MWArchive Server Properties window Manual for other files
Audit	Archive program: ▪ Default retention is 20 days ▪ Retention option may be changed in MWArchive Server Properties window

The Message Store and audit files generate the most data, which the Archive program maintains. The archive directory is maintained by the Archive Maintenance program. The other types of information listed here may be either deleted or moved offline and then deleted, so the manual process is simple.

NOTE: The MessageWay Archive program does not store encrypted data. All data is stored as raw data. To encrypt archived data, use a third-party tool.

The MessageWay Archive program archives and then deletes message content and detail information or simply deletes messages. It may be run by a MessageWay schedule, or operators may run it on demand.

The MessageWay Archive Maintenance program maintains the archive directory, which includes both archive zip files and their corresponding Archive Message table entries.   It may be run by a MessageWay schedule, or operators may run it on demand.

The destination location determines whether messages will be archived first or deleted without being archived. The default setting for all locations when they are created is that they will be archived. Once archived, the messages are deleted from the Message Store.

MessageWay archives or deletes messages depending on various message statuses. For more information about this process, refer to the topic, ***Settings to Archive or Delete Messages*** (on page 785).

When a message is a candidate to be archived or deleted, the following icons appear on the Message List and Message Properties Windows:

Archive/Delete Status	Icon	Description
Ready for Archive	🗃	Message will be a candidate for archive on the day after the associated retention date when the MessageWay Archive program runs.
	🚫	(Translator option using Reconciliation) Message is ready for archive, but it cannot be archived, because it is awaiting a return acknowledgment.

Archive/Delete Status	Icon	Description
Ready for Delete	🗑	Message will be a candidate for deletion on the day after the associated retention date when the MessageWay Archive program runs.
	🚫	(Translator option using Reconciliation) Message is ready for delete, but it cannot be deleted, because it is awaiting a return acknowledgment.

The archive files reside in the *archives* subdirectory of the MessageWay directory. Users can change the location of the archive files. For more information, refer to the topic, ***Changing the Location of the MessageWay Directories*** (on page 785).

Changing the Location of the MessageWay Directories

The installation process creates subdirectories to store data under the MessageWay directory, ../MessageWay.

Best Practice

When users process hundreds of messages a day, they should configure the archive directory to be on a different disk from the Message Store directory.

Users may change the location of the directories in the MessageWay configuration file, messageway.conf, by adding the following lines to the file before the final *</MessageWay>* tag, as needed:

<MsgStoreDir>*msgstore-dir***</MsgStoreDir>**

<ServerDir>*server-dir***</ServerDir>**

<AuditDir>*audit-dir***</AuditDir>**

<ArchiveDir>*archive-dir***</ArchiveDir>**

For more information about the MessageWay configuration file, refer to the topic, ***Configurations for An Environment*** (on page 84).

Settings to Automatically Archive or Delete Messages

By default, new output locations are initially configured to archive messages. Various criteria determine whether and when a message will be archived or deleted from the Message Store. When run, the archive program will query the MessageWay database for messages to archive or delete.

The basic process is as follows:

- Archive messages from locations configured to archive messages, and then delete the messages that have been archived

  - or -

- Delete the messages from locations *not* configured to archive messages

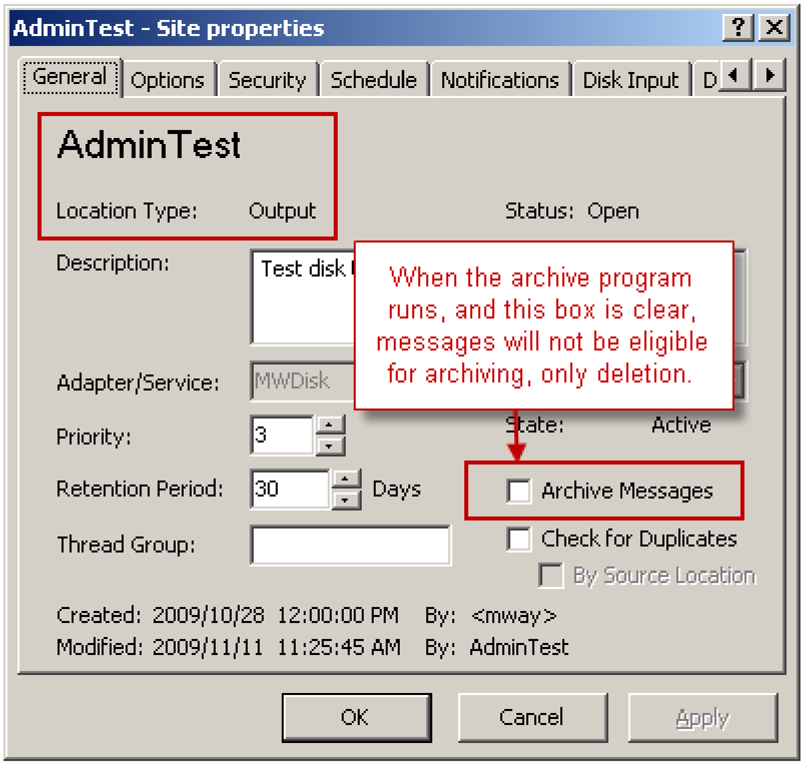
Users may modify this process by changing message properties or by specifying options on the MWArchive Server Properties window.

NOTE: Users may override this automatic process and its criteria by ***manually marking messages for archiving or deletion*** (on page 795).

Standard Criteria to Automatically Archive then Delete Messages

MessageWay first determines which messages are to be archived, and then after archiving eligible messages, it deletes those messages eligible for deletion.

CAUTION: When the archive program runs, if the destination location has the **Archive Messages** box *unchecked*, all messages queued to that site will be eligible for deletion, not archiving, whether or not they were originally marked for archive.



AdminTest - Site properties

AdminTest

Location Type: Output

Status: Open

Description: Test disk

Adapter/Service: MWDisk

Priority: 3

State: Active

Retention Period: 30 Days

☐ Archive Messages

☐ Check for Duplicates

☐ By Source Location

Thread Group:

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 11:25:45 AM By: AdminTest

When the archive program runs, and this box is clear, messages will not be eligible for archiving, only deletion.

NOTE: Linked messages have a unique Message ID but the same Original Message ID, and thus share the same content file. Linked messages typically result from the **Resubmit Message** or **Redirect Message** commands, or services that do not change the data, such as Rules Processing or Distribution List. The content file may be archived multiple times, if linked messages remain from one archive run to another.

Messages are eligible for archiving based on the following criteria:

- State of the message is *Complete*

  - and -

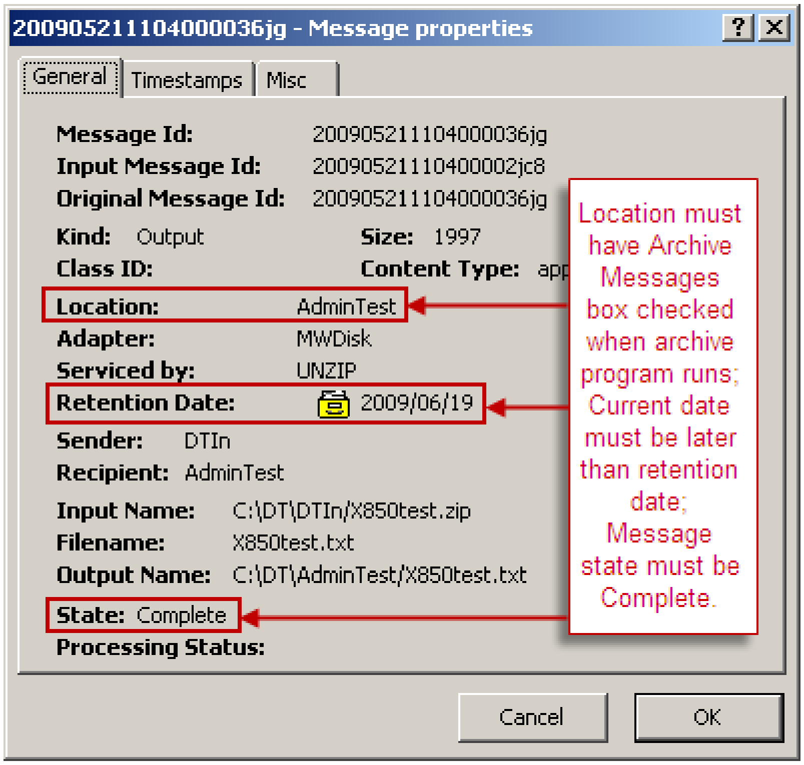
- Retention date for the message (Message Properties window, **General** tab) is less than the current system date

  - and -

- **Archive Messages** box is checked for the location (Site, Service Location, Mailbox) properties window, **General** tab) when the archive program runs

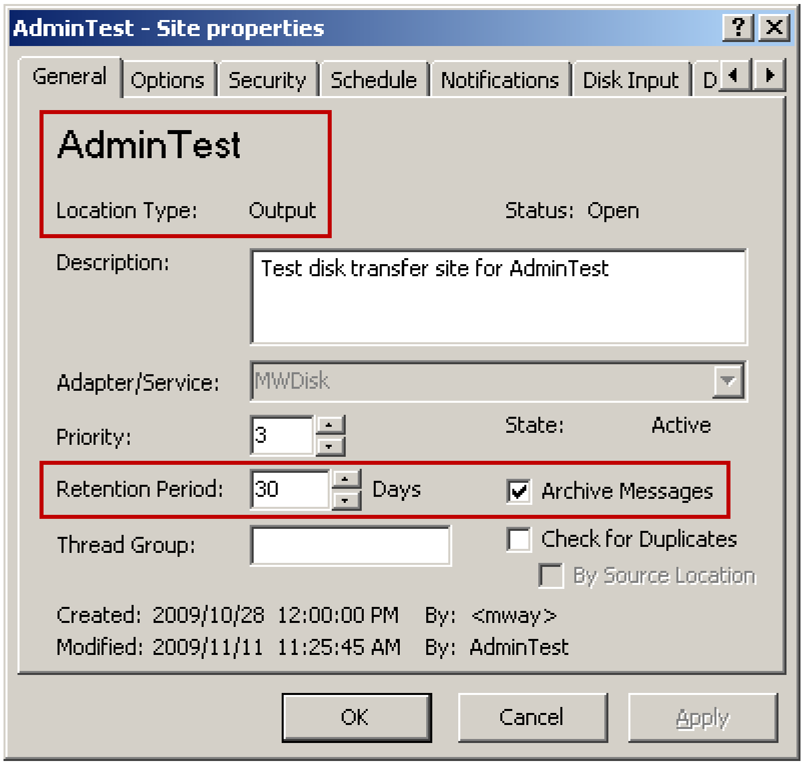
  - and -

- For MWTranslator that uses document reconciliation, no part of the message (interchange, functional group, document) has a status of *Awaiting Ack*



Message Id: 200905211104000036jg
Input Message Id: 20090521110400002jc8
Original Message Id: 200905211104000036jg
Kind: Output **Size:** 1997
Class ID: **Content Type:** app
Location: AdminTest
Adapter: MWDisk
Serviced by: UNZIP
Retention Date: 2009/06/19
Sender: DTIn
Recipient: AdminTest
Input Name: C:\DT\DTIn/X850test.zip
Filename: X850test.txt
Output Name: C:\DT\AdminTest/X850test.txt
State: Complete
Processing Status:

Location must have Archive Messages box checked when archive program runs; Current date must be later than retention date; Message state must be Complete.



AdminTest

Location Type: Output

Status: Open

Description: Test disk transfer site for AdminTest

Adapter/Service: MWDisk

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

☐ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 11:25:45 AM By: AdminTest

Messages will be deleted after archiving when:

- A message has been properly archived and has no other constraints

  - or -

- All ***linked messages*** (on page 748) have been archived or deleted

NOTE: The content file is deleted from the Message Store only when the last linked message is archived or deleted.

- or -

For MWTranslator that uses document reconciliation, no part of the message is awaiting an acknowledgment

Standard Criteria to Delete Messages

The archive program can delete messages without first archiving them. The messages must meet some of the same criteria as for archiving, but this process ignores any archiving requirements.

Messages will be deleted without being archived when:

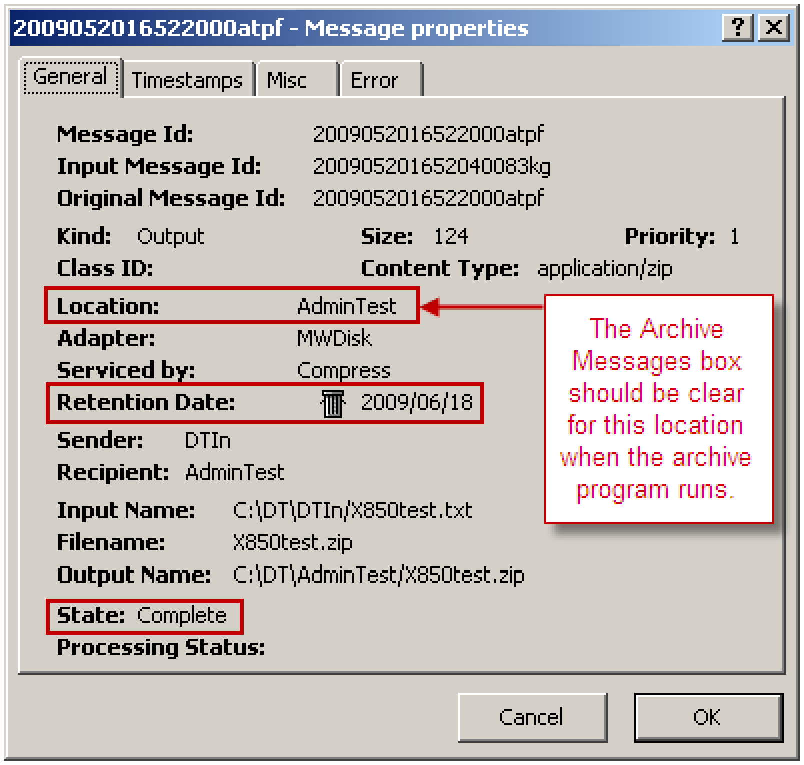
- State of message is *Complete*

  - and -

- Retention date for the message (Message Properties window, **General** tab) is less than the current system date

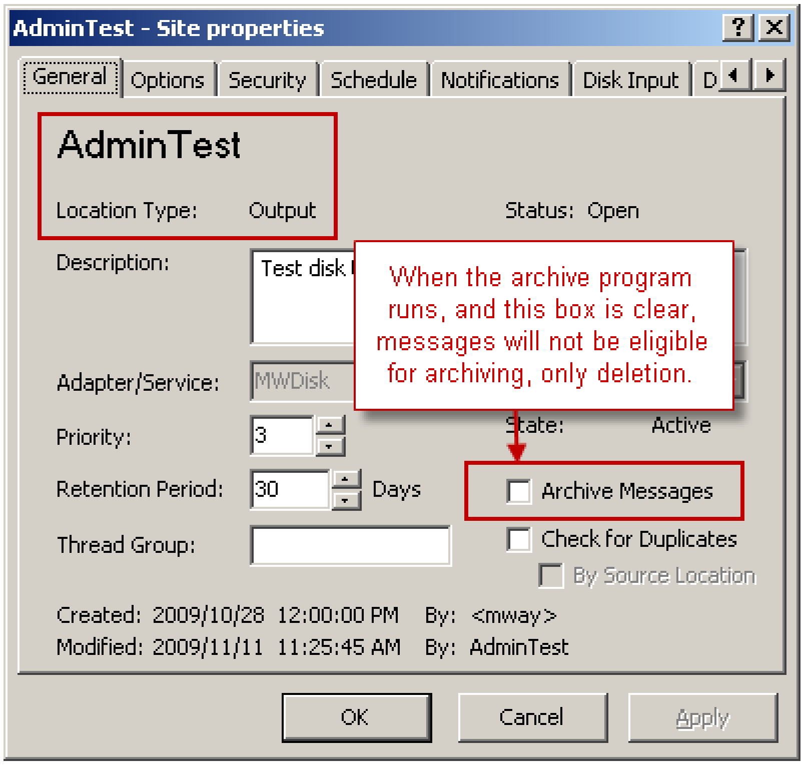
- and -

- Archive Messages box is *not* checked for the location (location properties window, **General** tab) when the archive program runs



Message Id: 2009052016522000atpf
Input Message Id: 20090520165204083kg
Original Message Id: 2009052016522000atpf
Kind: Output **Size:** 124 **Priority:** 1
Class ID: **Content Type:** application/zip
Location: AdminTest
Adapter: MWDisk
Serviced by: Compress
Retention Date: 2009/06/18
Sender: DTIn
Recipient: AdminTest
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.zip
Output Name: C:\DT\AdminTest/X850test.zip
State: Complete
Processing Status:

The Archive Messages box should be clear for this location when the archive program runs.



AdminTest

Location Type: Output

Status: Open

Description: Test disk

Adapter/Service: MWDisk

State: Active

Priority: 3

Retention Period: 30 Days

□ Archive Messages

□ Check for Duplicates

□ By Source Location

Thread Group:

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 11:25:45 AM By: AdminTest

When the archive program runs, and this box is clear, messages will not be eligible for archiving, only deletion.

Additional Settings That Affect Archiving

Users may modify the basic automatic archiving process for a particular message, for a set of messages or for all messages as follows:

For individual messages, users may do one of the following:

- ***Change the retention date*** (on page 792)
- ***Mark the message Ready for Archive*** (on page 795)
- ***Mark the message Ready for Delete*** (on page 795)

To prohibit messages already delivered to a specific location from being archived and to set new messages to *Ready for Delete* after all criteria have been met, users may:

- ***Clear the Archive Messages box on the destination location*** (on page 791)

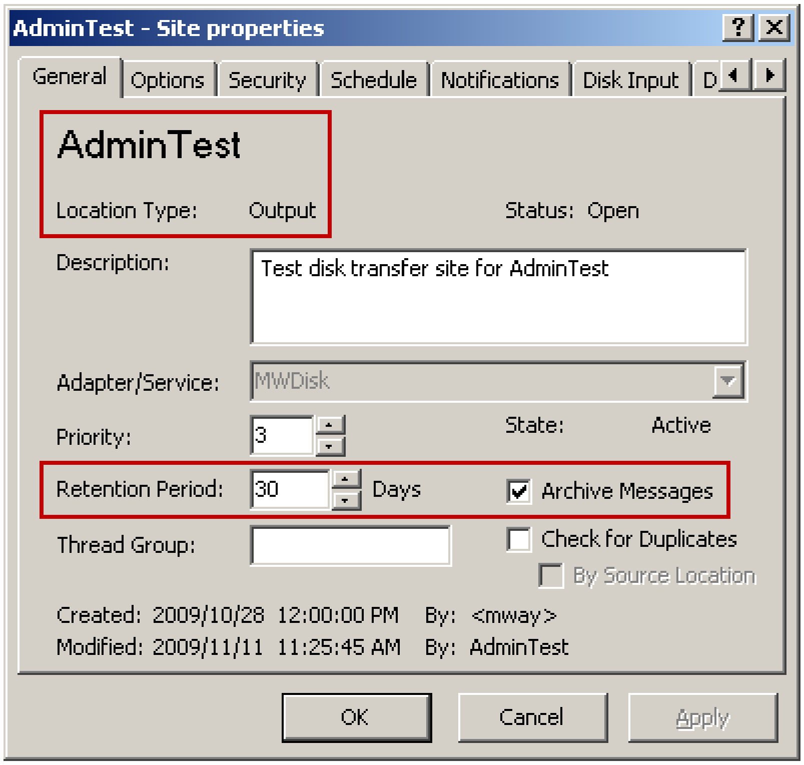
For all messages that meet the criteria, users may:

- ***Delete all messages (Do Not Archive)*** (on page 799)
- ***Archive messages with a status of Error, Available or Canceled (Force Archive)*** (on page 799)
- ***Archive messages to different files by location or location folders*** (on page 797)
- ***Archive messages to multiple files to avoid memory problem (Max Archive Messages)*** (on page 799)
- ***(MWTranslator Reconciliation) Archive messages marked Awaiting Ack (Max Ack Time)*** (on page 799)
- ***(MWTranslator Control Reference Processing) Delete records in the CTRLVAL file (CtrlVal Retention)*** (on page 799)

Configuring Locations to Archive Messages

Configurations on locations used to deliver data, that is, locations with types of *Output*, *I/O*, *Service* or *Mailbox*, determine whether a message is to be archived. By default, when you create such a location, the **Archive Messages** box is checked. Locations that allow input only cannot be configured for archiving.

IMPORTANT: Messages will be archived when the Archive program runs if the datetime stamp for the retention period has passed AND the **Archive Messages** box is currently checked on the location, assuming the other criteria for archiving have also been met.



AdminTest

Location Type: Output

Status: Open

Description: Test disk transfer site for AdminTest

Adapter/Service: MWDisk

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

☐ By Source Location

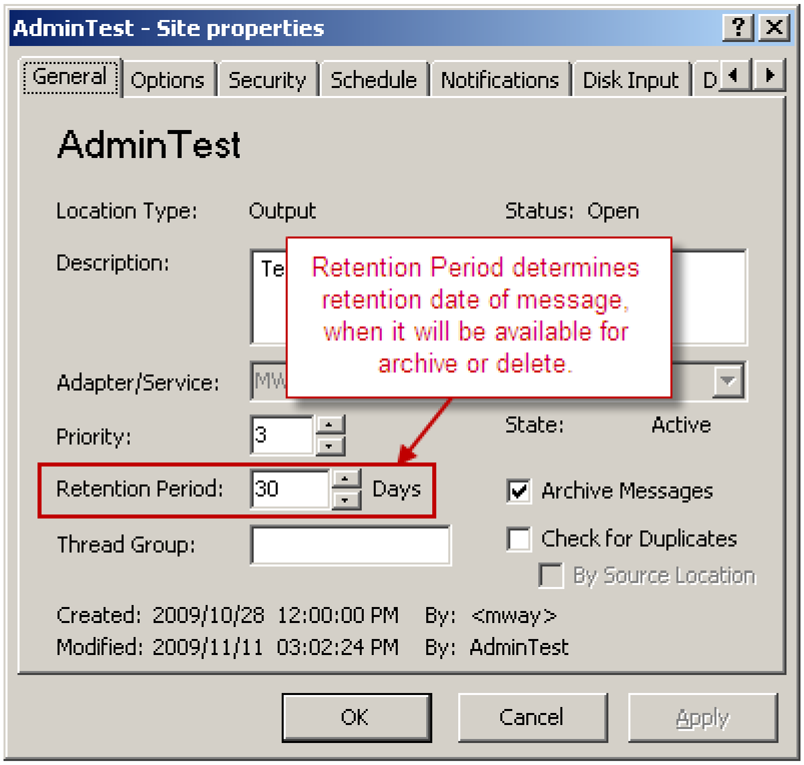
Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 11:25:45 AM By: AdminTest

Modifying the Message Retention Date for Archiving

When messages are archived or deleted depends on the setting of the *Archive Messages* option at the time of archiving and the retention date. The date appears on the **General** tab of the Message Properties window.

The retention date is set when the message first enters the system and is not changed. It is calculated from the retention period on the destination location. A message is a candidate for archiving and deletion *one day after the retention date.* The message will then be archived when the archive program runs if the **Archive Messages** box is currently checked and other criteria are met.



AdminTest - Site properties

AdminTest

Location Type: Output

Status: Open

Description: Te

Adapter/Service: MW

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

□ Check for Duplicates

□ By Source Location

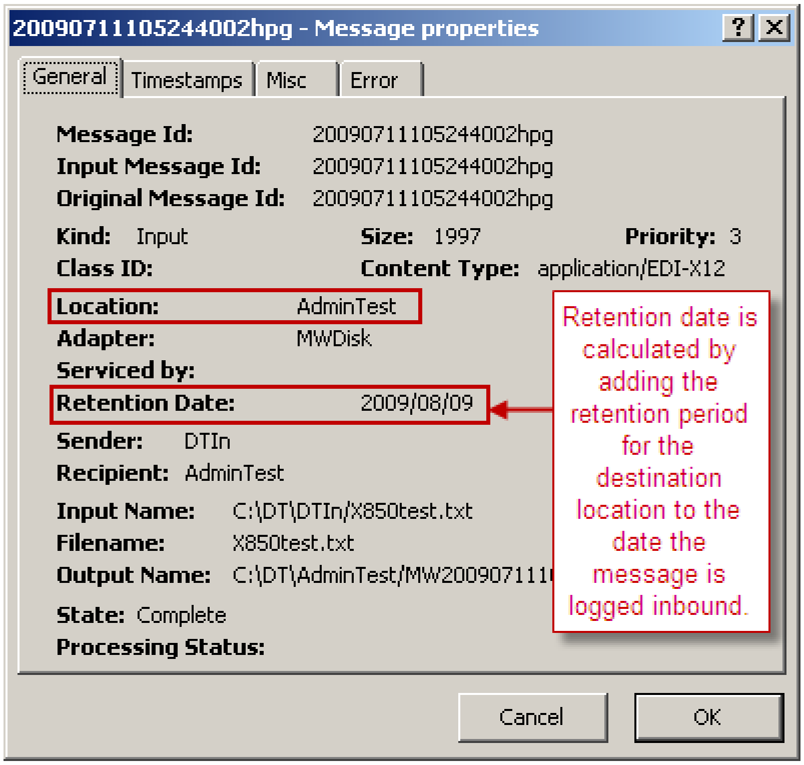
Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 03:02:24 PM By: AdminTest

Retention Period determines retention date of message, when it will be available for archive or delete.

Retention Period on Destination Location (Site Properties Window)

Note that in the following Message Properties window, the retention date of the message sent to the AdminTest site is set by the location configurations above, exactly 30 days from the date of input, visible on the **Timestamps** page. You might also be able to calculate it by looking at the Message ID, which is the date and time MessageWay logged the message.



Message Id: 20090711105244002hpg
Input Message Id: 20090711105244002hpg
Original Message Id: 20090711105244002hpg
Kind: Input Size: 1997 Priority: 3
Class ID: Content Type: application/EDI-X12
Location: AdminTest
Adapter: MWDisk
Serviced by:
Retention Date: 2009/08/09
Sender: DTIn
Recipient: AdminTest
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.txt
Output Name: C:\DT\AdminTest/MW20090711
State: Complete
Processing Status:

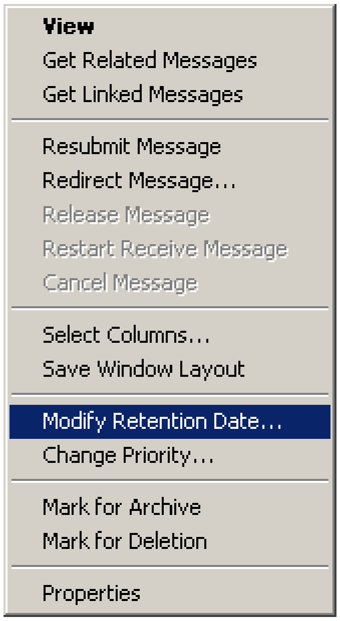
Retention date is calculated by adding the retention period for the destination location to the date the message is logged inbound.

Retention Date Calculated from Retention Period (Message Properties Window)

If we change the retention period to be less than today's date, we will be able to archive the message, since its status is **Complete**.

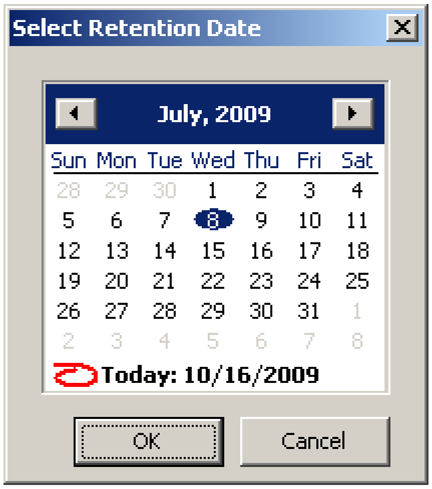
To change the retention date:

1 Select the message from a message list, right click and choose **Modify Retention Date** from the pop-up menu.

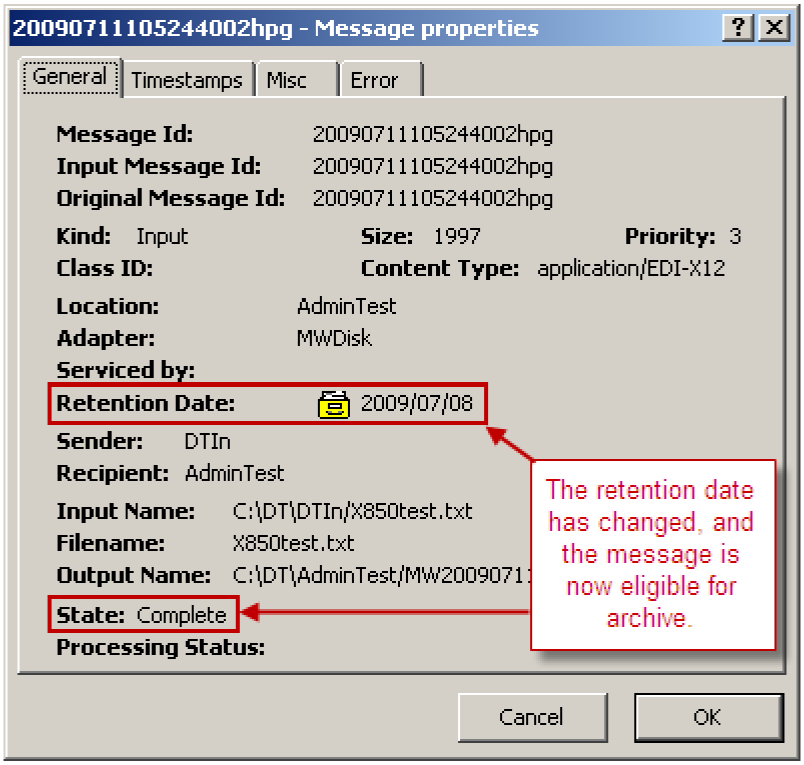


The **Select Retention Date** dialog box appears.

2 Select a date that is less than the current date, and click **OK**.



The next time the MessageWay Archive program runs, the message will be archived and then potentially deleted, assuming all other criteria for archiving have been met.



20090711105244002hpg - Message properties

Message Id: 20090711105244002hpg
Input Message Id: 20090711105244002hpg
Original Message Id: 20090711105244002hpg
Kind: Input **Size:** 1997 **Priority:** 3
Class ID: **Content Type:** application/EDI-X12
Location: AdminTest
Adapter: MWDisk
Serviced by:
Retention Date: 2009/07/08
Sender: DTIn
Recipient: AdminTest
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.txt
Output Name: C:\DT\AdminTest/MW2009071
State: Complete
Processing Status:

The retention date has changed, and the message is now eligible for archive.

Retention Date Reset Manually (Message Properties Window)

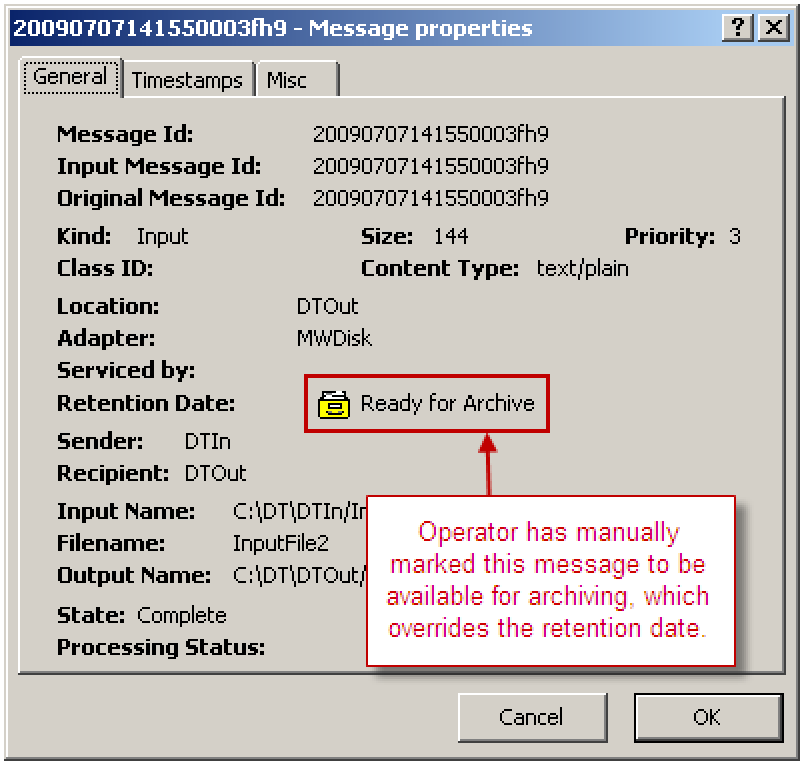
Manually Marking Messages for Archive or Delete

Operators may override the automatic behavior to archive or delete messages by manually marking them **Ready for Archive** or **Ready for Delete**.

To mark messages to be archived:

1. ***Select the message or group of messages from a message list*** (on page 733).
2. Right-click, and select **Mark for Archive** from the pop-up menu.

The status *Ready for Archive* appears on the Message Properties window.



Message Id: 20090707141550003fh9
Input Message Id: 20090707141550003fh9
Original Message Id: 20090707141550003fh9
Kind: Input Size: 144 Priority: 3
Class ID: Content Type: text/plain
Location: DTOut
Adapter: MWDisk
Serviced by:
Retention Date: Ready for Archive
Sender: DTIn
Recipient: DTOut
Input Name: C:\DT\DTIn/Ir
Filename: InputFile2
Output Name: C:\DT\DTOut/
State: Complete
Processing Status:

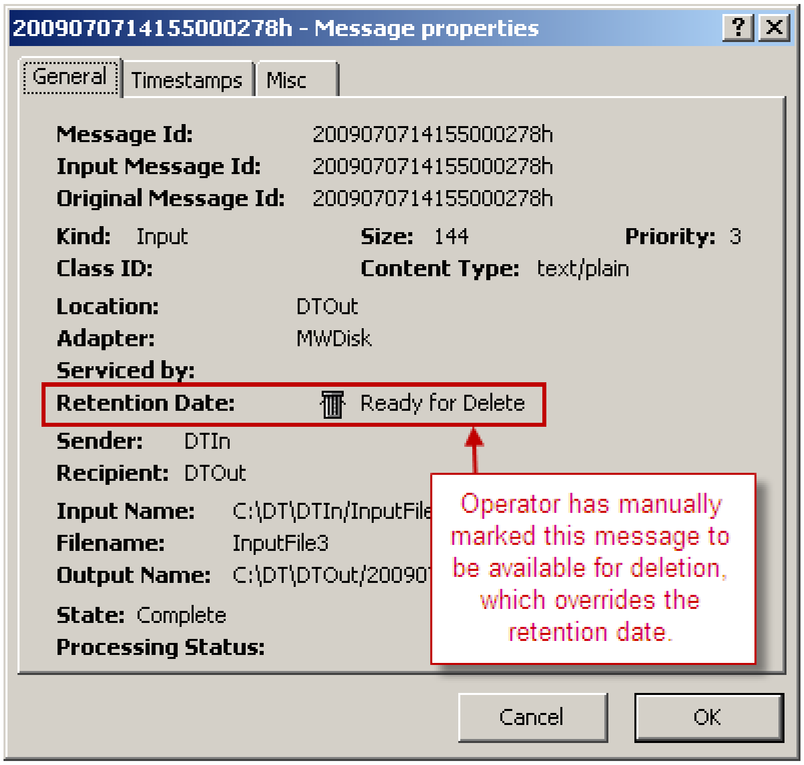
Operator has manually marked this message to be available for archiving, which overrides the retention date.

To mark messages to be deleted:

1 ***Select the message or group of messages from a message list*** (on page 733).

2 Right click, and select **Mark for Deletion** from the pop-up menu.

The status *Ready for Delete* appears on the Message Properties window.



Message Id: 2009070714155000278h
Input Message Id: 2009070714155000278h
Original Message Id: 2009070714155000278h
Kind: Input Size: 144 Priority: 3
Class ID: Content Type: text/plain
Location: DTOut
Adapter: MWDisk
Serviced by:
Retention Date: Ready for Delete
Sender: DTIn
Recipient: DTOut
Input Name: C:\DT\DTIn/InputFile
Filename: InputFile3
Output Name: C:\DT\DTOut/20090
State: Complete
Processing Status:

Operator has manually marked this message to be available for deletion, which overrides the retention date.

Archiving Locations and Folders to Different Files

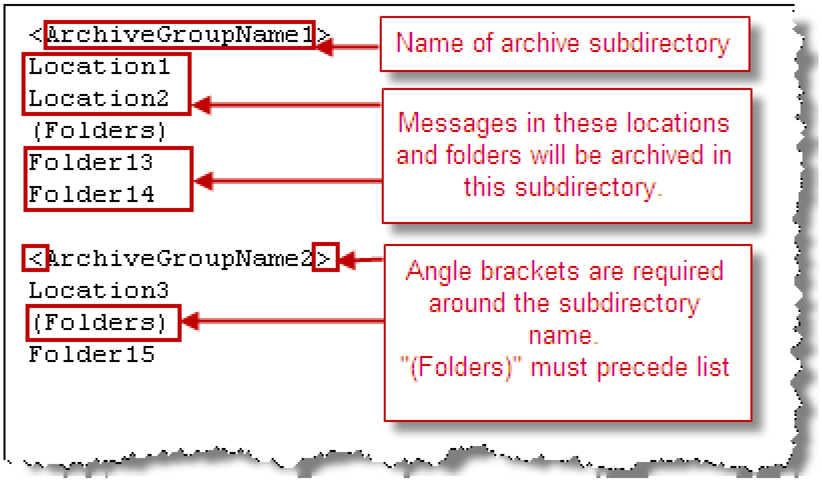
MessageWay provides an option for users to group archive information by original locations and folders and produce multiple output files during a single archiving session. To do this, modify the archive configuration file, whose name and location varies depending on the system where the MessageWay server runs. The default location is as follows:

System	Location of Configuration File
Windows	\MessageWay\archives\archive.config
UNIX/Linux	/var/opt/messageway/archives/archive.conf

A location name or folder name should not be included in more than one archive group. If a location or folder name is included in more than one group, then all references after the first will be ignored.

Group archives are created as subdirectories under the archives directory. The directory name will be created using the name of the archive group.

The syntax of the commands is explained in the comments of the archive configuration file. The following figure also explains the syntax.



```
<ArchiveGroupName1>
Location1
Location2
(Folders)
Folder13
Folder14

<ArchiveGroupName2>
Location3
(Folders)
Folder15
```

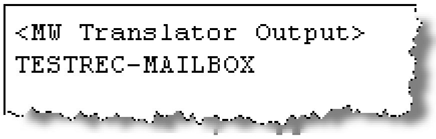
Name of archive subdirectory

Messages in these locations and folders will be archived in this subdirectory.

Angle brackets are required around the subdirectory name.
"(Folders)" must precede list

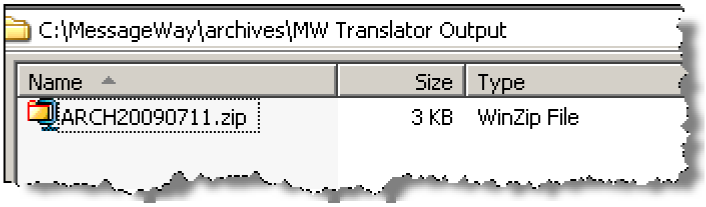
A message will only be archived once. When the message is not defined in any archive group, then the message will be archived in the archives directory.

In the following example, these commands are in the **archive.config** file:



```
<MW Translator Output>
TESTREC-MAILBOX
```

When a message is archived that is in the location TESTREC-MAILBOX, it will appear as a separate compressed file under the archives directory in the subdirectory, *MW Translator Output*.



C:\MessageWay\archives\MW Translator Output

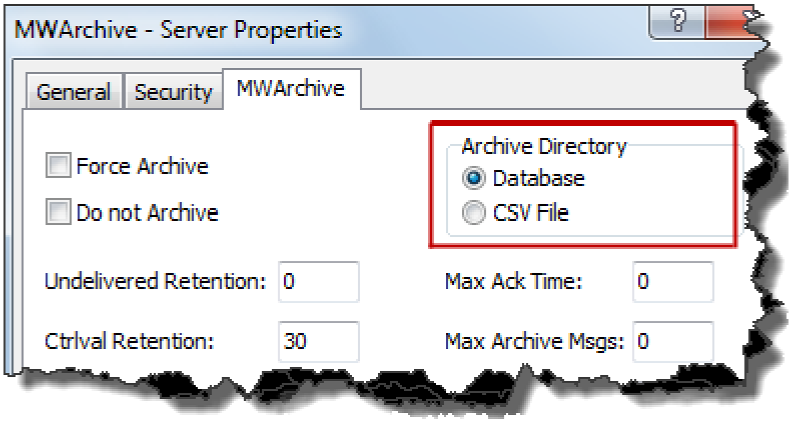
Name	Size	Type
ARCH20090711.zip	3 KB	WinZip File

More Options in the Archive Server Properties Window

Other options may be required for special cases in order to automatically archive or delete affected messages and to maintain the audit files. To handle special cases, users may specify options on the **MWArchive** ***page*** (on page 1320) of the Archive Server Properties window.

Options That Affect Message Archive Storage Location

On the **MWArchive** page of the Archive Server Properties window, you may choose whether to store the archive directory in the database, which is the default, or as a .csv file on disk.



□ Force Archive

□ Do not Archive

Archive Directory

● Database

○ CSV File

Undelivered Retention: 0

Max Ack Time: 0

Ctrlval Retention: 30

Max Archive Msgs: 0

Options To Archive Messages and Audit Files

This is a list of the options that affect archiving of messages and audit files. These options appear on the **MWArchive** ***page*** (on page 1320) of the Archive Server Properties window.

Option	**Description**
Force Archive	Archives all messages when they are eligible without checking the setting of the archive flag on the location's property window. The alternative is to manually mark every message *Ready for Archive*. When clear, the ***default archiving behavior*** (on page 786) occurs.
Do Not Archive	Deletes all messages when they are eligible without checking the setting of the archive flag on the location's property window. The alternative is to manually mark every message *Ready for Delete*. When clear, the ***default archiving behavior*** (on page 786) occurs.
Undelivered Retention	Normally, only messages with a status of *Complete* and that meet other criteria will be archived. This option affects messages with a status of *Error*, *Available* or *Canceled*. The *undelivered retention* option is the number of days after the date of the inbound timestamp when the qualifying message may be eligible for archive or delete. It will archive messages with one of these statuses when the later of two dates occurs (the later one takes precedence): the date it calculates or the retention date for the message, displayed on the Message Properties window. The value must be **1** or greater.
CtrlVal Retention	(MW Translator Enhanced Control Reference Processing) For enhanced control reference processing, delete records from the CTRLVAL file after a specified number of days. CTRLVAL is part of the optional Control Reference Processing in MW Translator that is used to validate control references in incoming data. The default value is 30 days. This setting does not affect deletion of messages.

Option	Description
Audit File Retention	This is the number of days to retain audit files in the /audit subdirectory or the database. The default is 20 days. Audit files, whose names begin with audit, record operator activity from the Manager. Service Interface audit files, whose names begin with siaudit, record activity from remote users.
Temp File Retention	The number of days to retain temporary files, which include any files in /messageway/server/temp or any files in the /temp or /tmp folders within a server's folder, such as /MWTranslator, or its sub-folders.
Archive File Mask	Use any combination of literals and MessageWay tokens to create the file names of the compressed and log files created by the archive program.
Archive File Retention	The number of days to retain archive zip files and all related archive messages. Archive zip files and related archive messages will be deleted when (Archive program run date > Archived Date - Archive File Retention). A value of 0 (zero) means that archive zip files and related archive messages will be retained indefinitely.
Retrieved Retention	The number of days to retain archive message retrieved content. Archive message retrieved content will be deleted when (Archive program run date > Retrieved Date - Retrieve Retention). A value of 0 (zero) means that retrieved content will be deleted along with the archive zip file (see Archive File Retention). Archive message retrieved content may also be manually deleted from the Manager program.
Max Ack Time	(MW Translator Reconciliation) When some part of the message is awaiting an acknowledgment, such as an interchange, functional group or document, by default, the message will not be archived until the required acknowledgment is received. This option ignores the requirement. The Max Ack Time specifies a number of days after the outbound timestamp when the message will be eligible for archive or delete.
Max Archive Messages	When a very large number of messages will be archived to one file, it is possible to run out of memory. To avoid memory problems, archive a specified number of messages to separate files, creating new files until all messages have been archived.
Max Archive Files	(Must use with Max Archive Msgs) Limit the number of files created, which may not archive all messages during the run, but remaining messages can be archived in subsequent runs.
Do Not Archive Audit Files	This option allows the archive program to delete audit files after they have passed the retention date. The default behavior is to archive audit files.
Do not Delete Archive Files	This option allows users to disable deletion of archive zip files. If checked, all archive related data stored in MessageWay will be deleted, but the archive zip file will be retained. This allows 3rd party offline archiving of the zip files where the 3rd party process which archives the zip files is also responsible for deleting them.

Running the Archive Program

The MessageWay Archive program may be run in several ways:

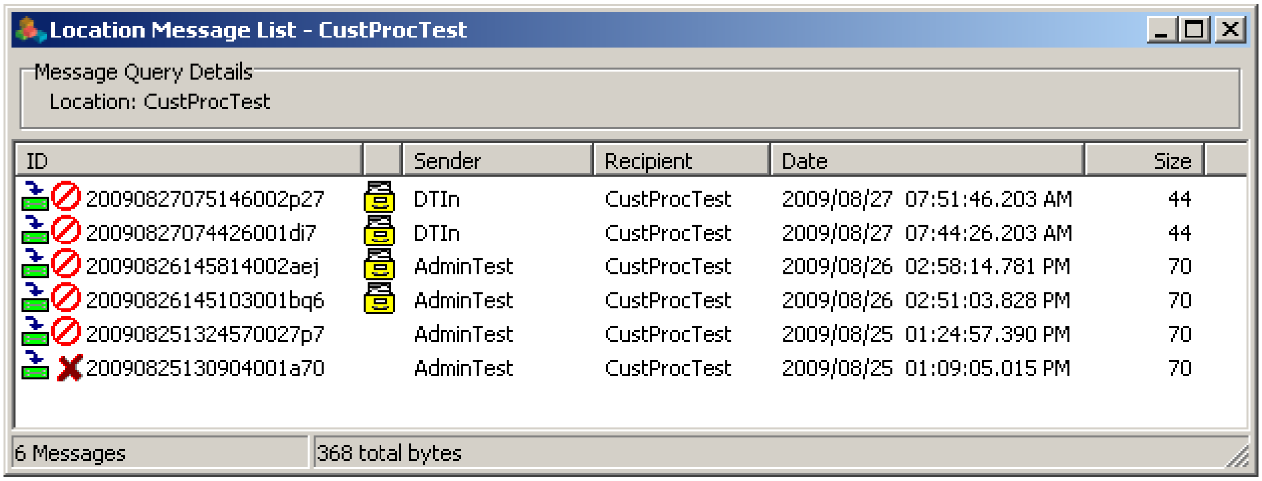
- From MessageWay, scheduled automatically using the system location, {Archive}
- From MessageWay, manually issuing an *Execute Now* command for the system location, {Archive}
- From the operating system, scheduled to run automatically
- From the operating system, manually

If a message is eligible for archive or deletion, then the program will first archive the message, including message processing information and content. It will then delete the message and all related records, such as those related to MWTranslator processing, which include interchange, functional group and document records. When no remaining linked messages remain, then the message content file will be deleted from the Message Store as well.

CAUTION: Operators should always use the MessageWay Archive program to maintain the Message Store and the Archive Retrieve Message Store. They should not manually delete files from disk.

The following windows show the contents of the CustProcTest location before and after the Archive program was run.

NOTE: Messages with a status of *Error*, *Available* or *Canceled* will *only* be archived or deleted if the *Undelivered Retention* value on the *Archive* tab of the MWArchive Server Properties window is 1 or greater, assuming other criteria have also been met, or if a user has ***manually marked a message for Archive or Delete*** (on page 795). Four of the canceled messages shown here were archived, because a user manually marked the message for archive.

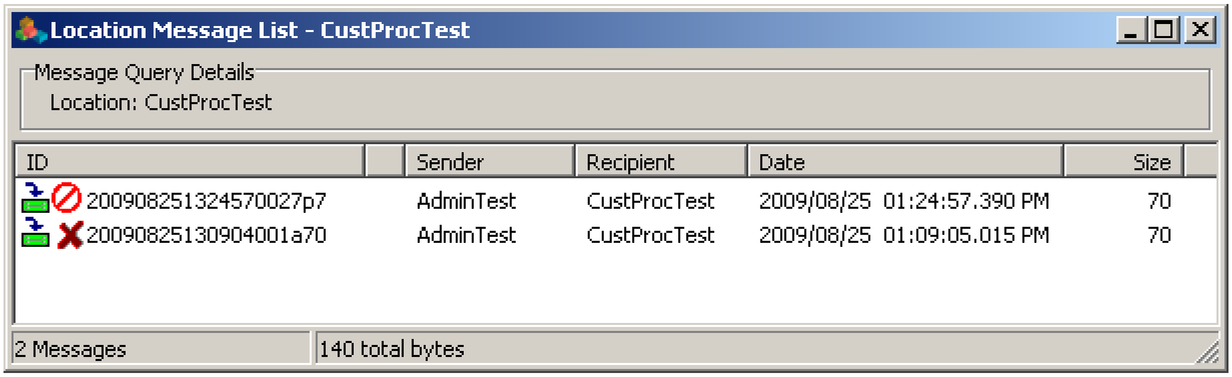


Message Query Details
Location: CustProcTest

ID		Sender	Recipient	Date	Size
⊘ 20090827075146002p27		DTIn	CustProcTest	2009/08/27 07:51:46.203 AM	44
⊘ 20090827074426001di7		DTIn	CustProcTest	2009/08/27 07:44:26.203 AM	44
⊘ 20090826145814002aej		AdminTest	CustProcTest	2009/08/26 02:58:14.781 PM	70
⊘ 20090826145103001bq6		AdminTest	CustProcTest	2009/08/26 02:51:03.828 PM	70
⊘ 20090825132457002 7p7		AdminTest	CustProcTest	2009/08/25 01:24:57.390 PM	70
✗ 20090825130904001a70		AdminTest	CustProcTest	2009/08/25 01:09:05.015 PM	70

6 Messages 368 total bytes

Message List before Running the Archive Program



Message Query Details
Location: CustProcTest

ID		Sender	Recipient	Date	Size
200908251324570027p7		AdminTest	CustProcTest	2009/08/25 01:24:57.390 PM	70
20090825130904001a70		AdminTest	CustProcTest	2009/08/25 01:09:05.015 PM	70

2 Messages | 140 total bytes

Message List after Running the Archive Program

How to Run Scheduled Archiving from MessageWay

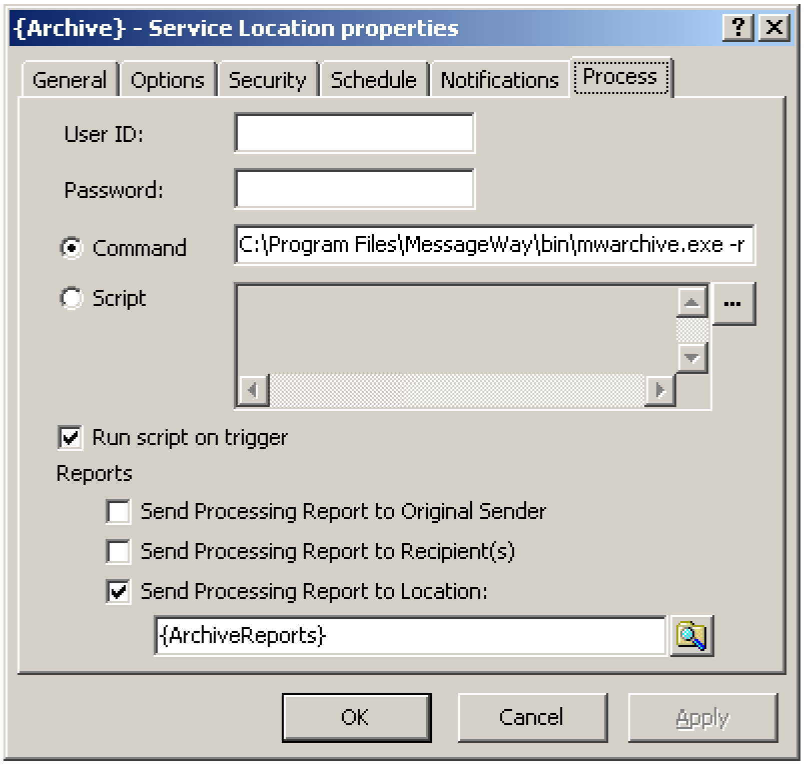
The system service location, {Archive}, uses the Custom Processing service to execute the archive program when it receives a scheduled trigger message. The archive program returns the processing report to the system pickup mailbox, {ArchiveReports}, which users can change.

CAUTION (UNIX/Linux): For MessageWay systems configured to encrypt data content in the database, if you run the archive process from a custom processing service location, as we do here, instead of the command line, you must have a passphrase file. To initiate the archive process, the encryption password must be saved as a file, because this process cannot be prompted for the password.

To modify the configuration, proceed as follows:

1 From the Locations folder, double-click **{Archive}**.

The Service Location properties window appears.



User ID:

Password:

● Command C:\Program Files\MessageWay\bin\mwarchive.exe -r

○ Script

☑ Run script on trigger

Reports

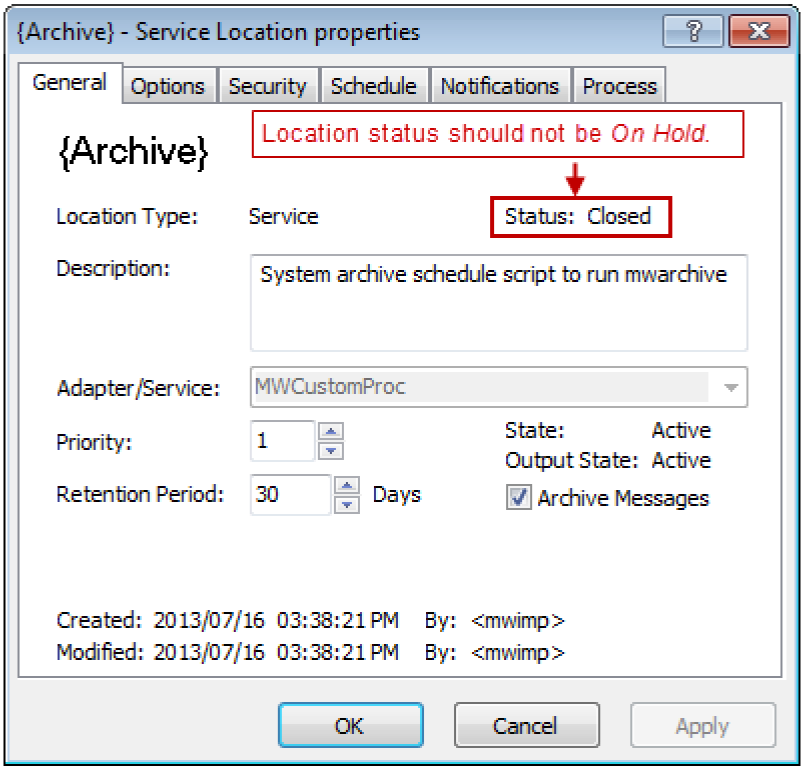
□ Send Processing Report to Original Sender

□ Send Processing Report to Recipient(s)

☑ Send Processing Report to Location:

{ArchiveReports}

CAUTION: Make sure the status of the location is not *On Hold*. If the location is *On Hold*, the trigger schedule will not send a trigger message to start the archive program. To remove a location from hold status, right-click the location, and then select **Release Messages** from the menu.



Location status should not be *On Hold*.

{Archive}

Location Type: Service

Status: Closed

Description: System archive schedule script to run mwarchive

Adapter/Service: MWCustomProc

Priority: 1

State: Active

Output State: Active

Retention Period: 30 Days

☑ Archive Messages

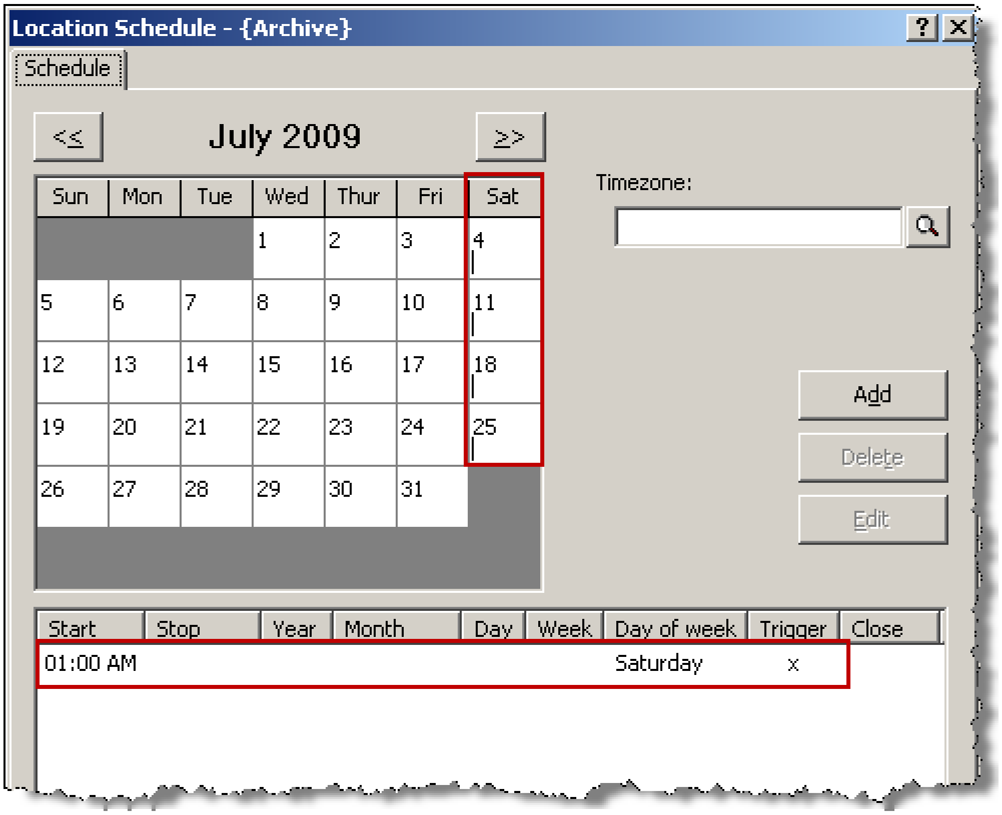
Created: 2013/07/16 03:38:21 PM By: <mwimp>

Modified: 2013/07/16 03:38:21 PM By: <mwimp>

2 To send processing reports to a location other than the default system location, {ArchiveReports}, select a different location.

3 Click the **Schedule** tab, and click the schedule button, 📅.

The Location Schedule window appears and shows the trigger message that is configured. This item sends an **Execute Now** command to the {Archive} location, which triggers the command to run the archive program. A default time is set, so you may need to reset it to meet your needs.



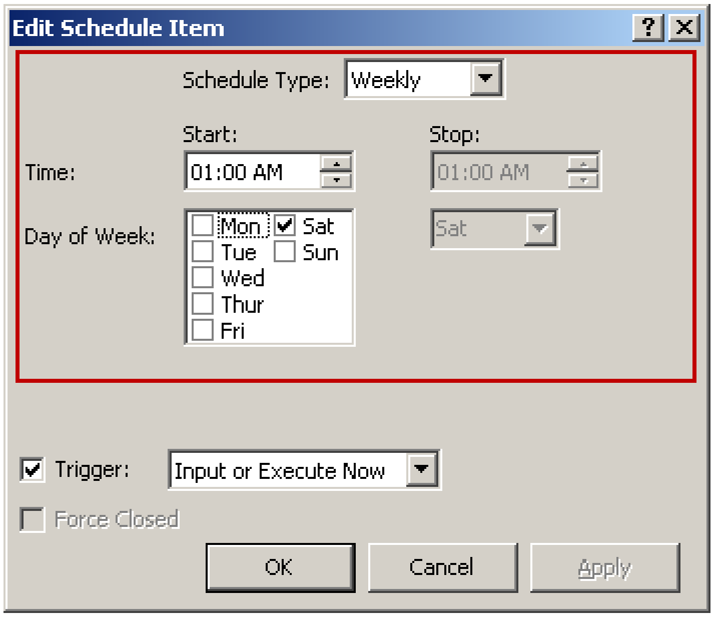
July 2009

Sun	Mon	Tue	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Start	Stop	Year	Month	Day	Week	Day of week	Trigger	Close
01:00 AM						Saturday	x	

4 To change when the trigger message is sent, select the item on the item list and click **Edit**.

The Edit Schedule Item window appears.



Schedule Type: Weekly

Time: Start: 01:00 AM Stop: 01:00 AM

Day of Week: □ Mon ☑ Sat □ Tue □ Sun □ Wed □ Thur □ Fri Sat

☑ Trigger: Input or Execute Now

□ Force Closed

5 Change the schedule as required.

IMPORTANT: Do not change the trigger option, or the trigger message will never be sent to start the archive program.

6 View the archive report.

How to Manually Run Archiving from MessageWay Manager

To start the archive program from MessageWay Manager with the installed default settings, proceed as follows:

1 Make sure the *Custom Processing* service (MWCustomProc) is started.

2 In the left pane of MessageWay Explorer, click **Locations**.

3 In the right pane, right-click the system location **{Archive}**.

4 From the pop-up menu, click **Execute now...**

A dialog box appears asking you to confirm the action.

5 Click **Yes**.

A trigger message is sent to the {Archive} custom processing location, which executes a command to run the Archive program.

6 View the archive report in the {ArchiveReports} mailbox.

NOTE: If the Archive program does not run, you will not receive a report. This may be because the MWCustomProc service is stopped. The *Execute Now* command will override locations on hold or closed schedules. However, if the service is not running, MessageWay discards the trigger message.

How to Manually Run the Archive Program from Windows

1 From the **Start** menu, depending on the operating system, select **All Programs** or **Programs**.

2 Select the **MessageWay Server** folder, and then **MessageWay Archive**.

The MessageWay Archive program runs in the background.

3 View the archive report.

How to Manually Run the Archive Program from UNIX or Linux

1 From */installation_directory/***bin**, type the following command:

./mwayarchive &

The MessageWay Archive program runs in the background.

2 View the archive report.

Running the Archive Maintenance Program

The MessageWay Archive Maintenance program may be run in several ways:

- From MessageWay, scheduled automatically using the system location, {ArchiveMaintenance}
- From MessageWay, manually issuing an *Execute Now* command for the system location, {ArchiveMainenance}

If an archive zip file is eligible for deletion, then the program will first delete all corresponding archive message table entries, then delete the archive zip file.

CAUTION: Operators should only use the MessageWay Archive Maintenance program to maintain the Archive.

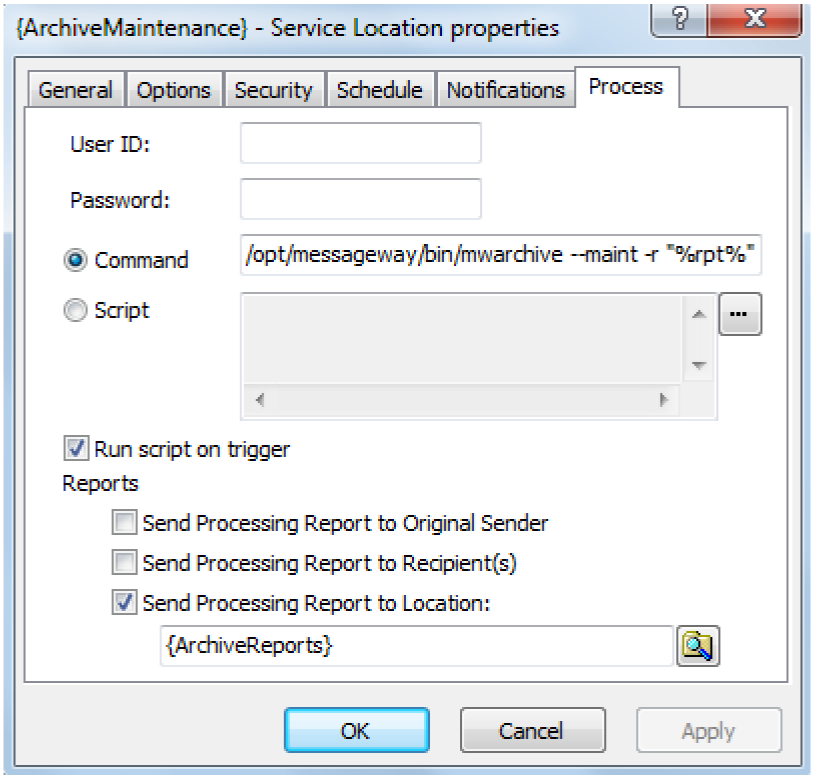
How to Run Scheduled Archive Maintenance from MessageWay

The system service location, {ArchiveMaintenance}, uses the Custom Processing service to execute the archive maintenance program when it receives a scheduled trigger message. The archive maintenance program returns the processing report to the system pickup mailbox, {ArchiveReports}, which users can change.

To modify the configuration, proceed as follows:

1 From the Locations folder, double-click **{ArchiveMaintenance}**.

The Service Location properties window appears.



{ArchiveMaintenance} - Service Location properties

User ID:

Password:

● Command /opt/messageway/bin/mwarchive --maint -r "%rpt%"

○ Script

☑ Run script on trigger

Reports

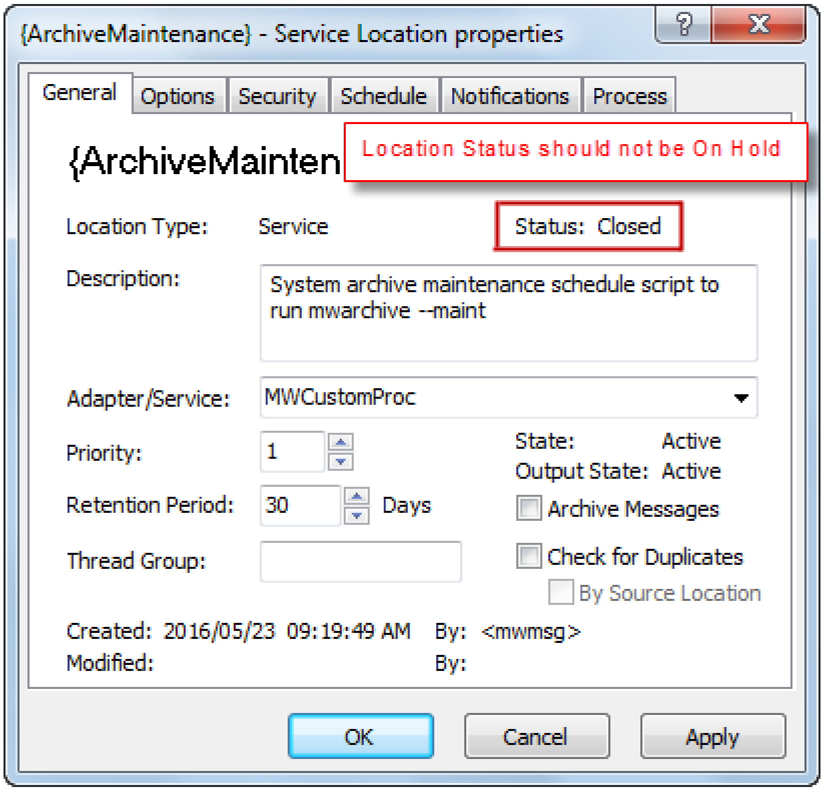
☐ Send Processing Report to Original Sender

☐ Send Processing Report to Recipient(s)

☑ Send Processing Report to Location:

{ArchiveReports}

CAUTION: Make sure the status of the location is not *On Hold*. If the location is *On Hold*, the trigger schedule will not send a trigger message to start the archive maintenance program. To remove a location from hold status, right-click the location, and then select **Release Messages** from the menu.



Location Status should not be On Hold

{ArchiveMainten

Location Type: Service

Status: Closed

Description: System archive maintenance schedule script to run mwarchive --maint

Adapter/Service: MWCustomProc

Priority: 1

State: Active

Output State: Active

Retention Period: 30 Days

□ Archive Messages

Thread Group:

□ Check for Duplicates

□ By Source Location

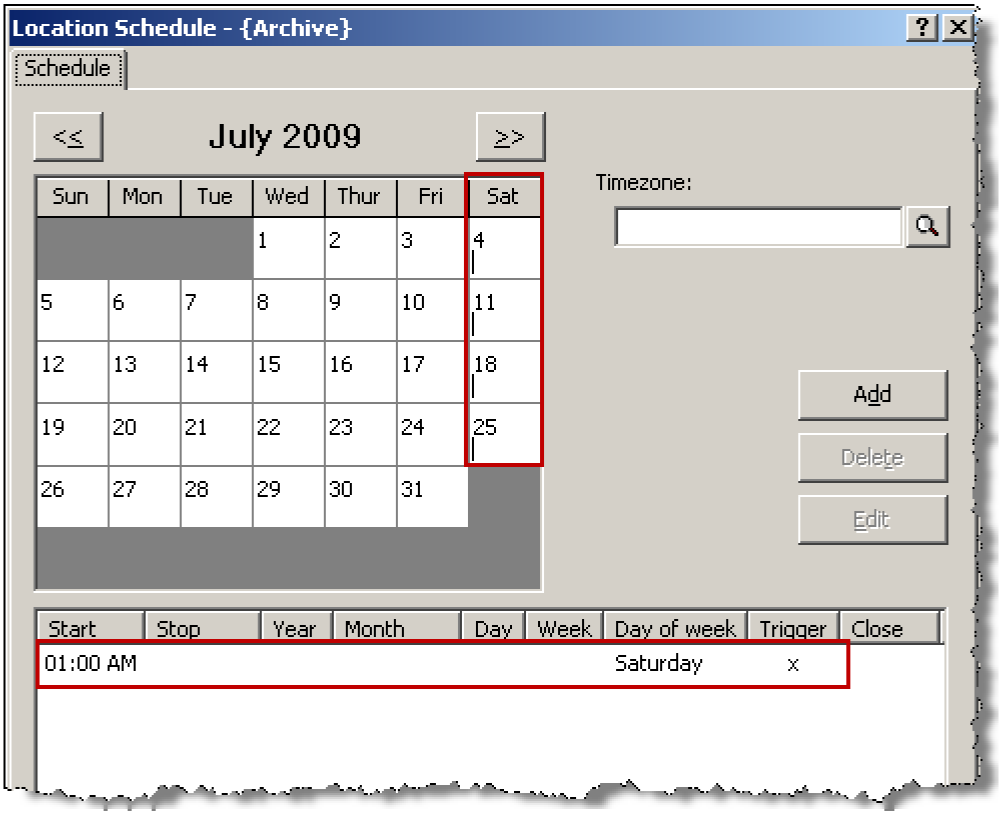
Created: 2016/05/23 09:19:49 AM By: <mwmsg>

Modified: By:

2 To send processing reports to a location other than the default system location, {ArchiveReports}, select a different location.

3 Click the **Schedule** tab, and click the schedule button, 📅.

The Location Schedule window appears and shows the trigger message that is configured. This item sends an **Execute Now** command to the {ArchiveMaintenance} location, which triggers the command to run the archive maintenance program. A default time is set, so you may need to reset it to meet your needs.

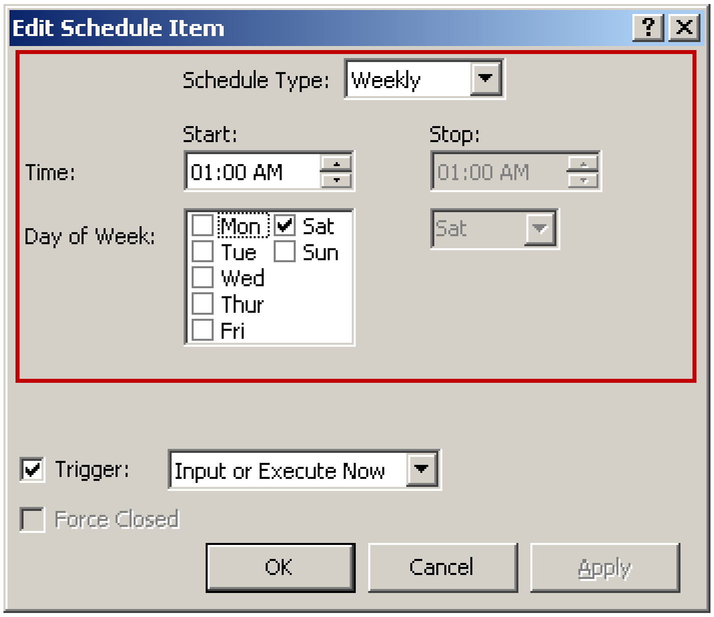


Sun	Mon	Tue	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Start	Stop	Year	Month	Day	Week	Day of week	Trigger	Close
01:00 AM						Saturday	x	

4 To change when the trigger message is sent, select the item on the item list and click **Edit**.

The Edit Schedule Item window appears.



Schedule Type: Weekly

Time: Start: 01:00 AM Stop: 01:00 AM

Day of Week: ☐ Mon ☑ Sat ☐ Tue ☐ Sun ☐ Wed ☐ Thur ☐ Fri Sat

☑ Trigger: Input or Execute Now

☐ Force Closed

5 Change the schedule as required.

IMPORTANT: Do not change the trigger option, or the trigger message will never be sent to start the archive maintenance program.

6 View the archive report.

How to Manually Run Archive Maintenance from MessageWay Manager

To start the archive maintenance program from MessageWay Manager with the installed default settings, proceed as follows:

1 Make sure the *Custom Processing* service (MWCustomProc) is started.

2 In the left pane of MessageWay Explorer, click **Locations**.

3 In the right pane, right-click the system location **{ArchiveMaintenance}**.

4 From the pop-up menu, click **Execute now...**

A dialog box appears asking you to confirm the action.

5 Click **Yes**.

A trigger message is sent to the {ArchiveMaintenance} custom processing location, which executes a command to run the Archive Maintenance program.

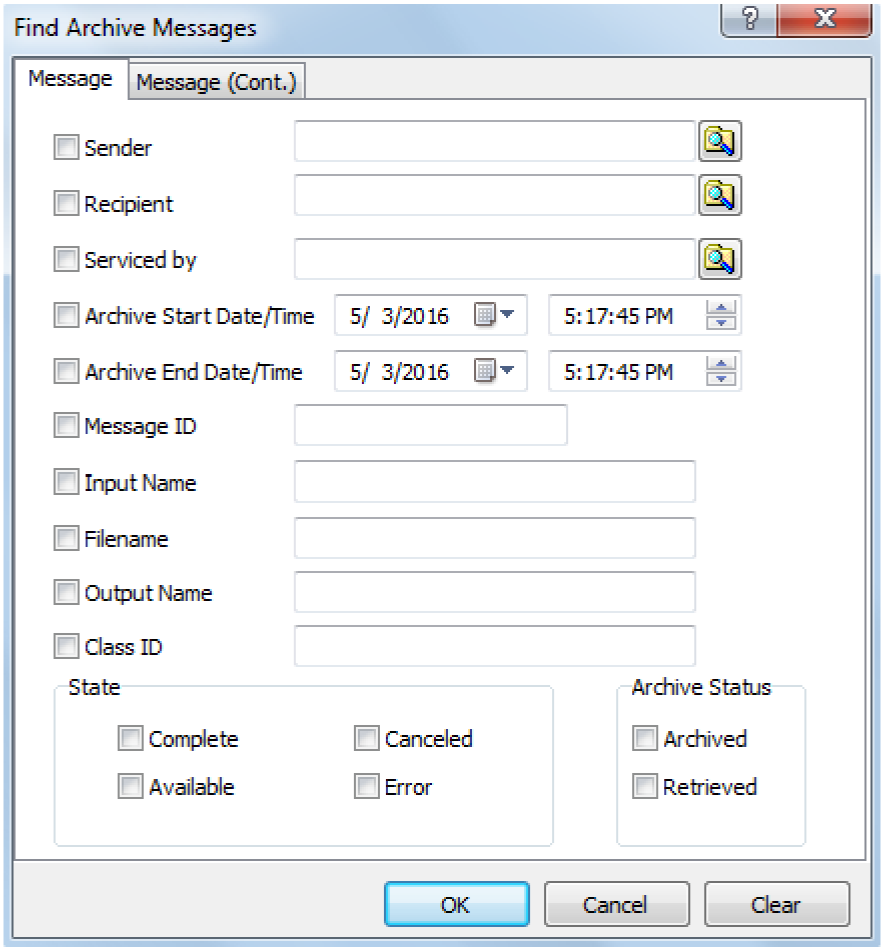
6 View the archive maintenance report in the {ArchiveReports} mailbox.

NOTE: If the Archive Maintenance program does not run, you will not receive a report. This may be because the MWCustomProc service is stopped. The *Execute Now* command will override locations on hold or closed schedules. However, if the service is not running, MessageWay discards the trigger message.

Finding Archive Messages

When users want to find messages that have been archived, they must use the **Find Archive Messages** window by selecting the **Search** menu or button on the toolbar.

Note that MessageWay does not support input filenames that contain backslashes, \. For operating systems, such as UNIX, that allow backslashes in filenames, the filename property will be whatever follows the final backslash.



□ Sender

□ Recipient

□ Serviced by

□ Archive Start Date/Time 5/ 3/2016 5:17:45 PM

□ Archive End Date/Time 5/ 3/2016 5:17:45 PM

□ Message ID

□ Input Name

□ Filename

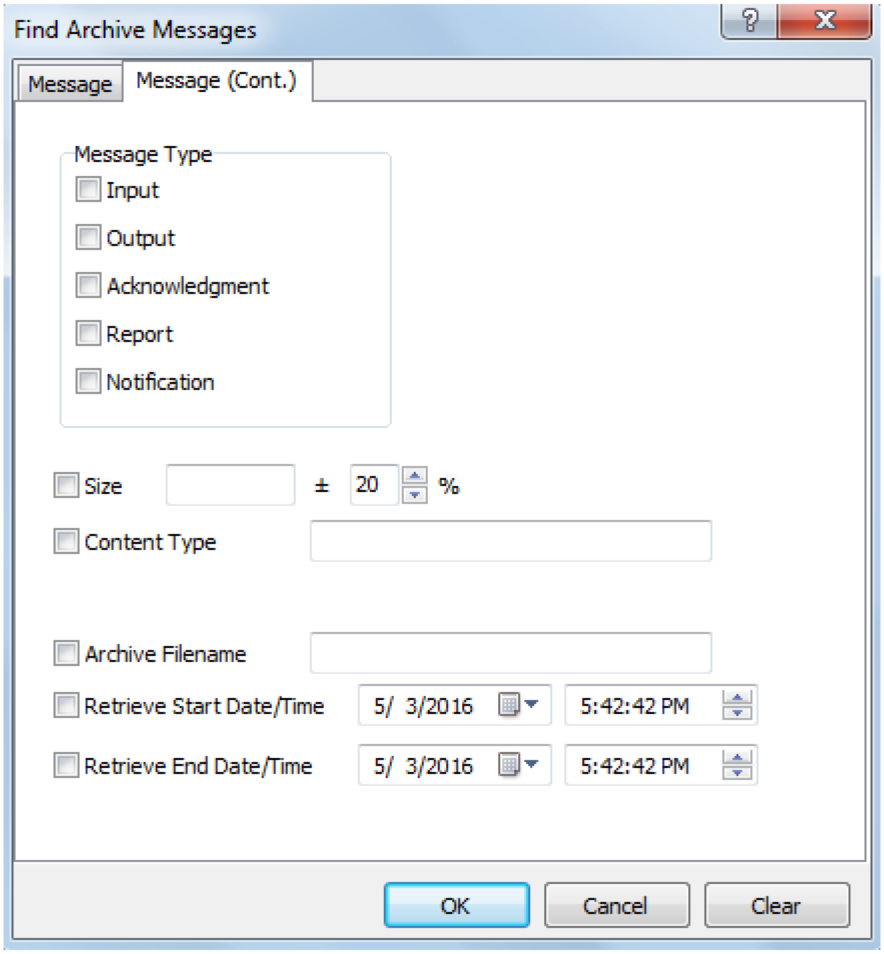
□ Output Name

□ Class ID

State: □ Complete □ Canceled □ Available □ Error

Archive Status: □ Archived □ Retrieved

Search Criteria on Find Archive Messages Window (Message page)



Find Archive Messages

Message | Message (Cont.)

Message Type

□ Input

□ Output

□ Acknowledgment

□ Report

□ Notification

□ Size ± 20 %

□ Content Type

□ Archive Filename

□ Retrieve Start Date/Time 5/ 3/2016 5:42:42 PM

□ Retrieve End Date/Time 5/ 3/2016 5:42:42 PM

Search Criteria on Find Archive Messages Window (Message (Cont.) page)

IMPORTANT: When you leave all values blank, the list shows all messages in the archive. Users should always select some criteria to limit the number of archive messages on the list. You can set system-wide limits for total messages returned and total displayed in a window on the **MWUser** tab of the ***Server Properties window*** (on page 1313).

Retrieving Messages from Archive

The Archive Retrieve program retrieves messages from archive. These retrieved archive messages are stored in the Archive Retrieve message store, separate from the message store. The Archive Retrieve message store has two storage options, just like the message store; on disk or in the database. Which storage option is used is based on the storage option of the message before it was archived, and cannot be changed. Messages retrieved into the Archive Retrieve message store do not yet exist as messages in any locations, but can still be viewed using the **Find Archive Messages** function. Messages retrieved from archive only exist as messages in locations after the **Resubmit to MessageWay...** function is performed.

NOTE: Archive zip files that have been moved or renamed in the archive directory cannot be retrieved from. Restoring archive zip files back to their original location or name will restore the ability to retrieve messages from them.

Regarding access rights, all actions performed against messages retrieved from archive are determined by the rights assigned to the location where the message was originally archived from. If the location no longer exists, then only 'Administrator' users can access the retrieved messages. The following access rights are required for the following actions:

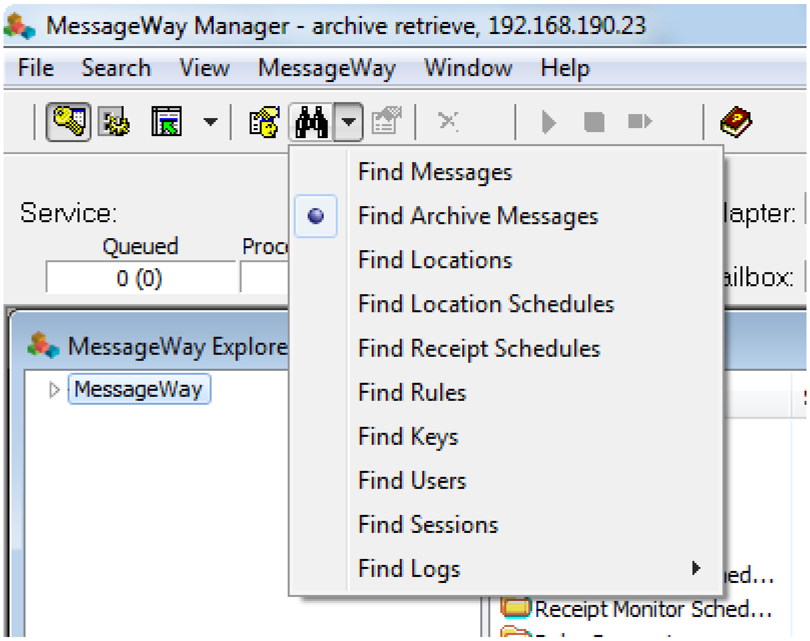
Action	Right
View Retrieved Message(s)	View Messages.
Retrieve from Archive	Retrieve Archive Messages.
Resubmit Retrieved Message(s)	Resubmit Archive Messages (on both the original location and system location {RetrievedMessages}).
Delete Retrieved Message(s)	Delete Archive Message Content.

There are two scenarios related to Archive Retrieve which require different steps to achieve:

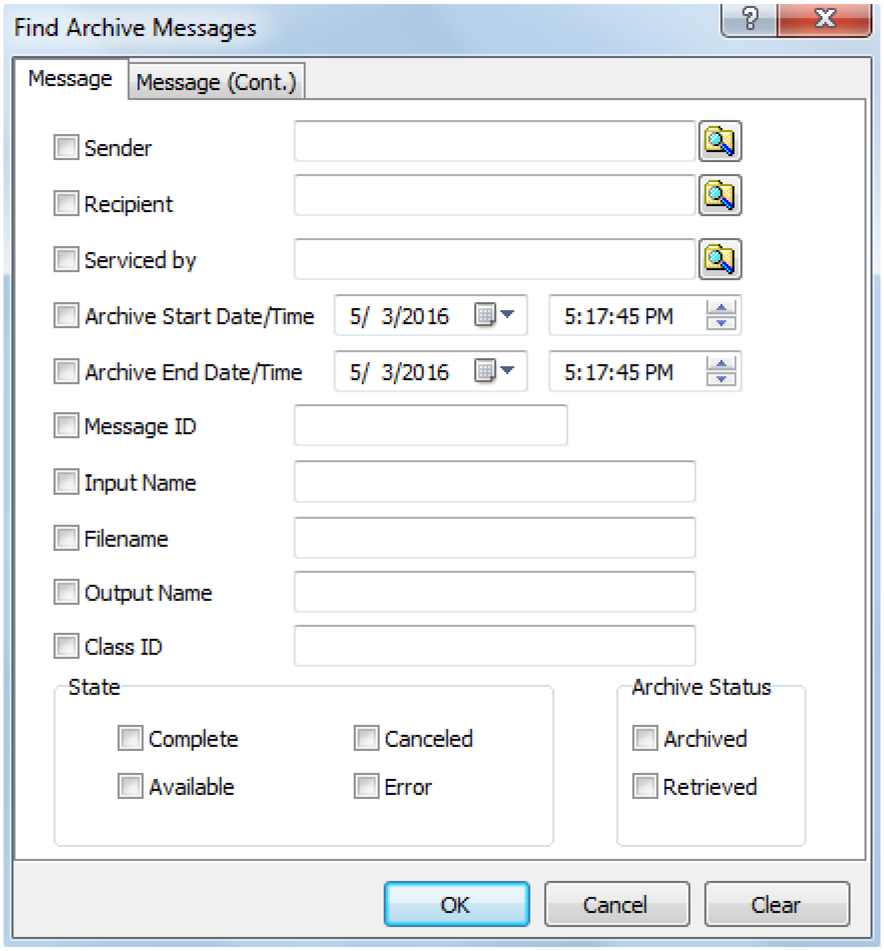
- Retrieve message(s) in order to view message content
- Retrieve message(s) in order to resend to either original recipient or a new recipient

Both scenarios start out the same way:

- Use **Find Archive Messages** to find archived messages that you want to retrieve:



and fill in the appropriate selection criteria:



Find Archive Messages

□ Sender

□ Recipient

□ Serviced by

□ Archive Start Date/Time 5/ 3/2016 5:17:45 PM

□ Archive End Date/Time 5/ 3/2016 5:17:45 PM

□ Message ID

□ Input Name

□ Filename

□ Output Name

□ Class ID

State

□ Complete □ Canceled

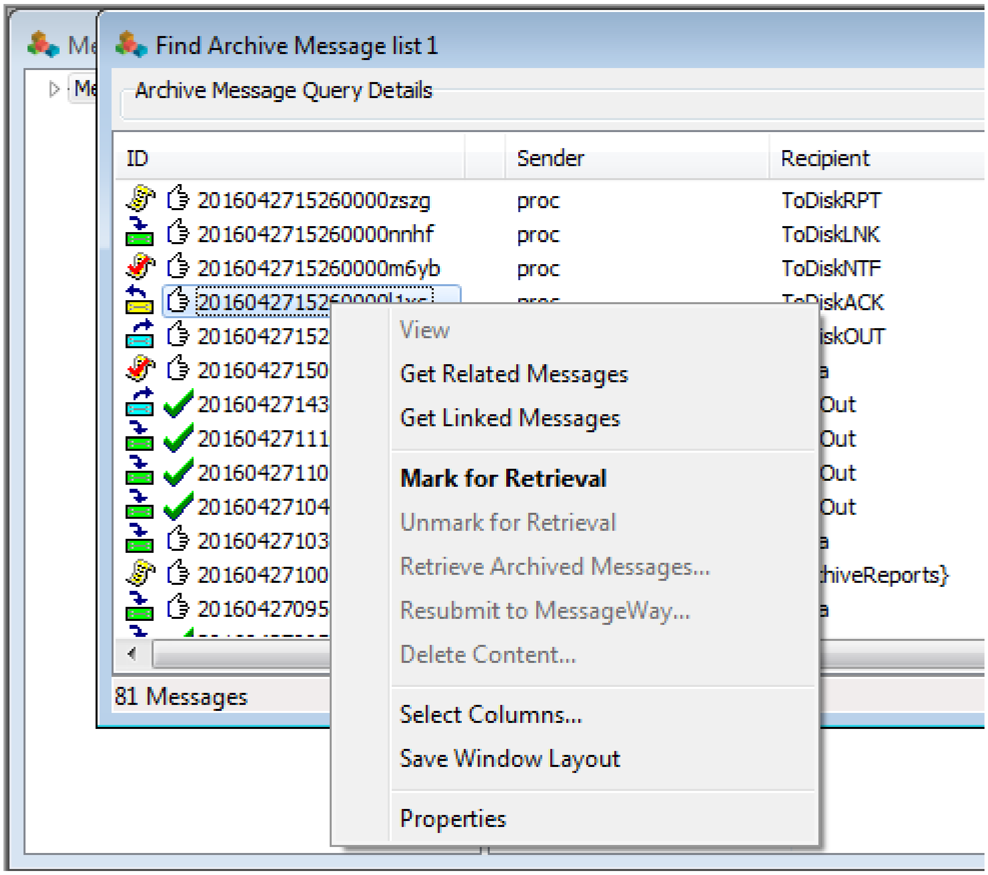
□ Available □ Error

Archive Status

□ Archived

□ Retrieved

- Next select one or more messages to **Mark for Retrieval**:



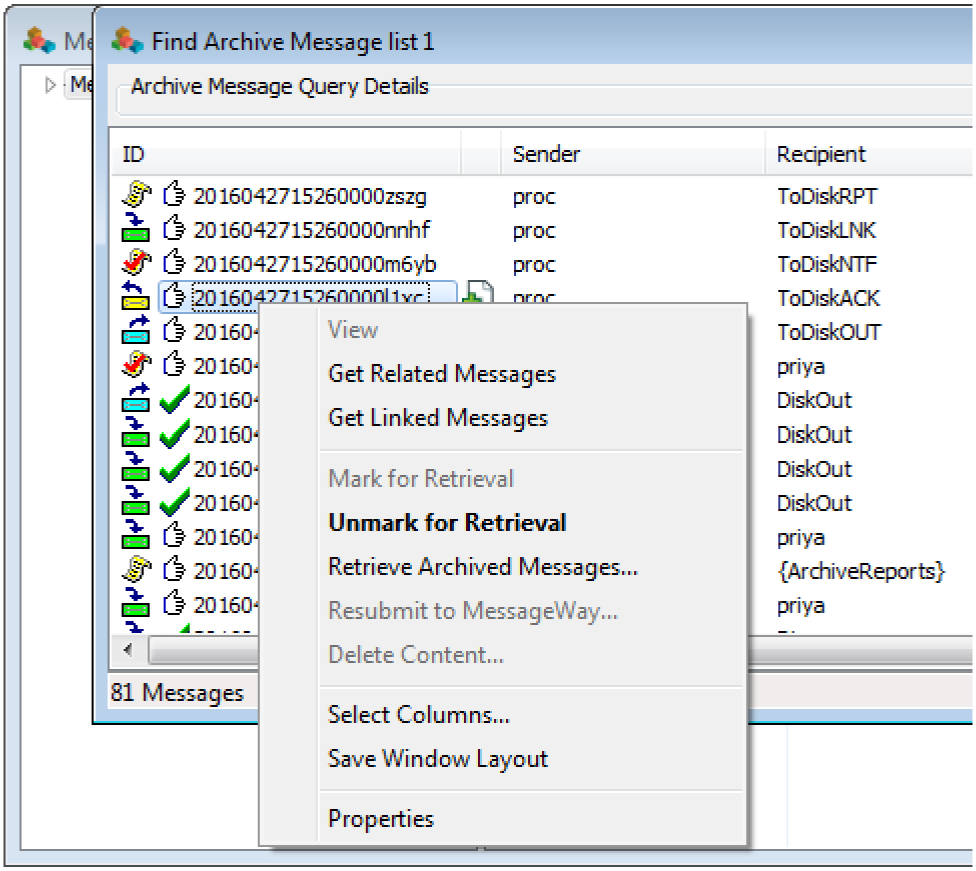
Find Archive Message list 1

Archive Message Query Details

ID	Sender	Recipient
2016042715260000zszg	proc	ToDiskRPT
2016042715260000nnhf	proc	ToDiskLNK
2016042715260000m6yb	proc	ToDiskNTF
20160427152600001xc	proc	ToDiskACK
20160427152		iskOUT
20160427150		a
20160427143		Out
20160427111		Out
20160427110		Out
20160427104		Out
20160427103		a
20160427100		hiveReports}
20160427095		a

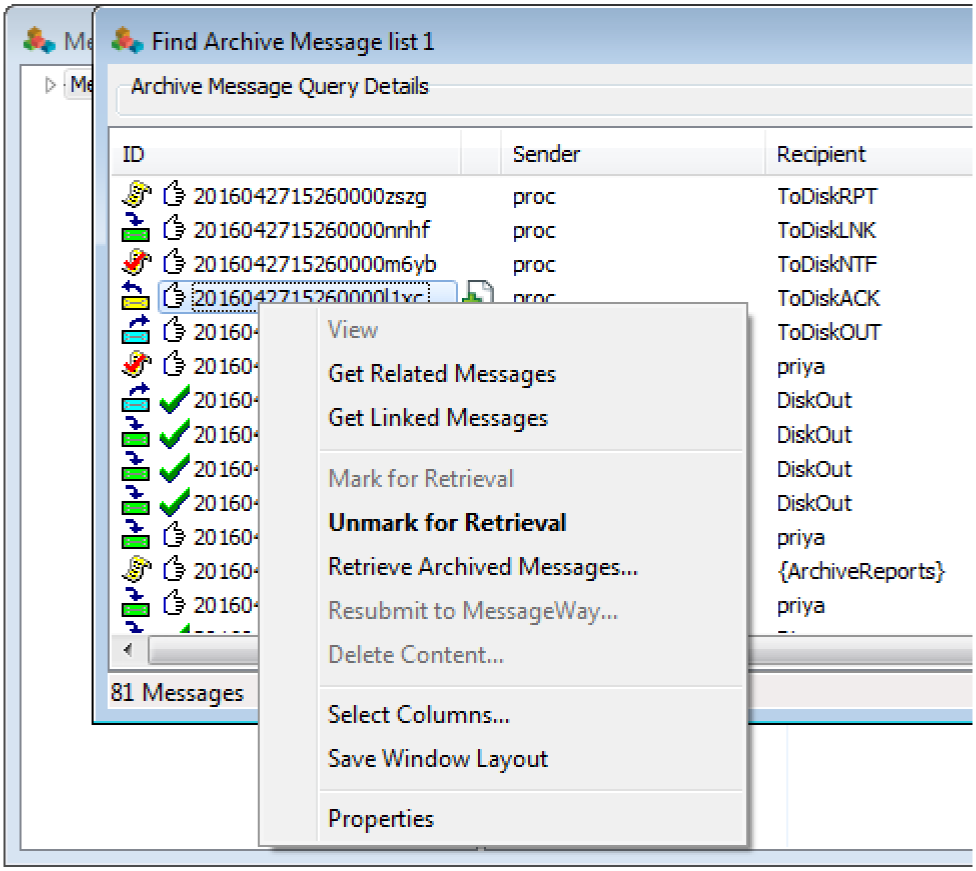
81 Messages

If you change your mind, you can select **Unmark for Retrieval**:



ID	Sender	Recipient
2016042715260000zszg	proc	ToDiskRPT
2016042715260000nnhf	proc	ToDiskLNK
2016042715260000m6yb	proc	ToDiskNTF
2016042715260000l1xc	proc	ToDiskACK
✓ 20160		ToDiskOUT
20160		priya
✓ 20160		DiskOut
✓ 20160		DiskOut
✓ 20160		DiskOut
✓ 20160		DiskOut
20160		priya
20160		{ArchiveReports}
20160		priya

- Next select **Retrieve Archived Messages...**:



ID	Sender	Recipient
2016042715260000zszg	proc	ToDiskRPT
2016042715260000nnhf	proc	ToDiskLNK
2016042715260000m6yb	proc	ToDiskNTF
2016042715260000l1xc	proc	ToDiskACK
20160		ToDiskOUT
20160		priya
20160		DiskOut
20160		DiskOut
20160		DiskOut
20160		DiskOut
20160		priya
20160		{ArchiveReports}
20160		priya

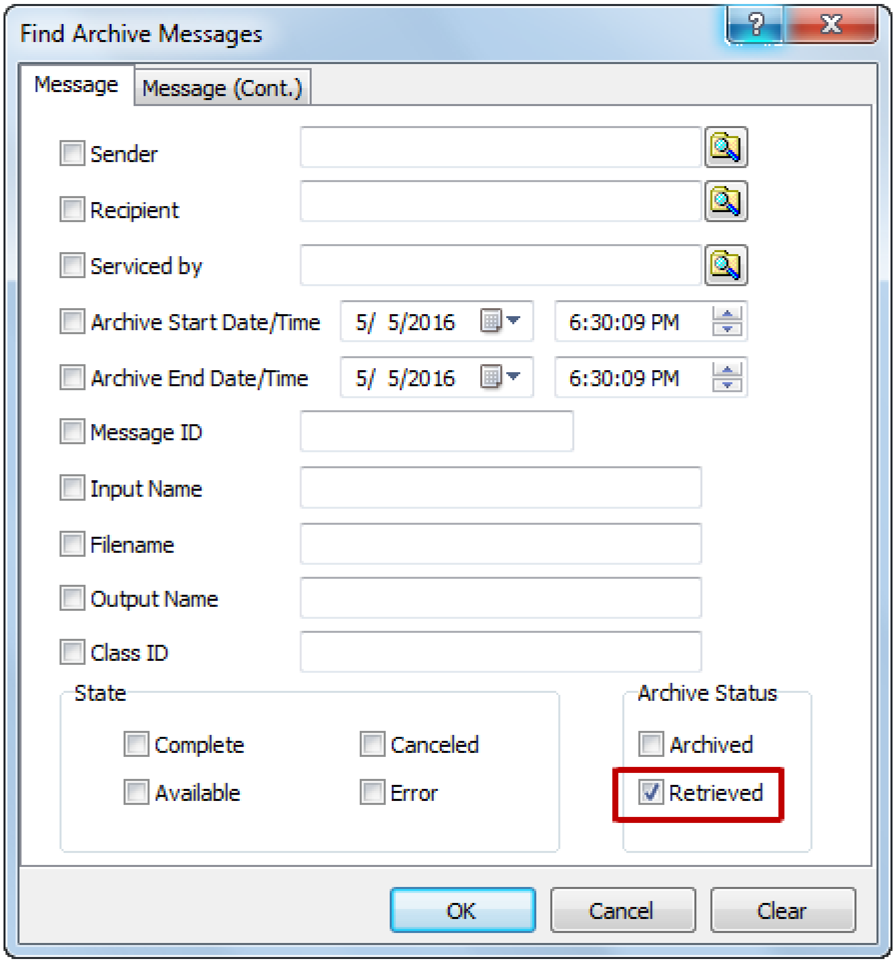
The user can monitor the retrieval process in the Manager, and when complete, view the resulting report file in system location {ArchiveReports}.

NOTE: The Manager will keep track of all messages marked for retrieval within each session even if they occur across multiple archived message lists. As long as the Manager is running, the marked messages will be remembered, even if the session times out. If you re-logon with the same Manager instance under the same system and user Id, then the last session marked messages will be retained. It will be possible to search for all messages that are marked for retrieval by the current session. Note that messages marked for retrieval by one Manager session cannot be retrieved by another Manager session except as described above.

Viewing Messages Retrieved from Archive

After completing the section '**Retrieving Messages from Archive**', you are now able to view the retrieved message(s) content.

- To view message content, use **Find Archive Messages** and select Retrieved:



Find Archive Messages

Message | Message (Cont.)

□ Sender

□ Recipient

□ Serviced by

□ Archive Start Date/Time 5/ 5/2016 6:30:09 PM

□ Archive End Date/Time 5/ 5/2016 6:30:09 PM

□ Message ID

□ Input Name

□ Filename

□ Output Name

□ Class ID

State

□ Complete □ Canceled

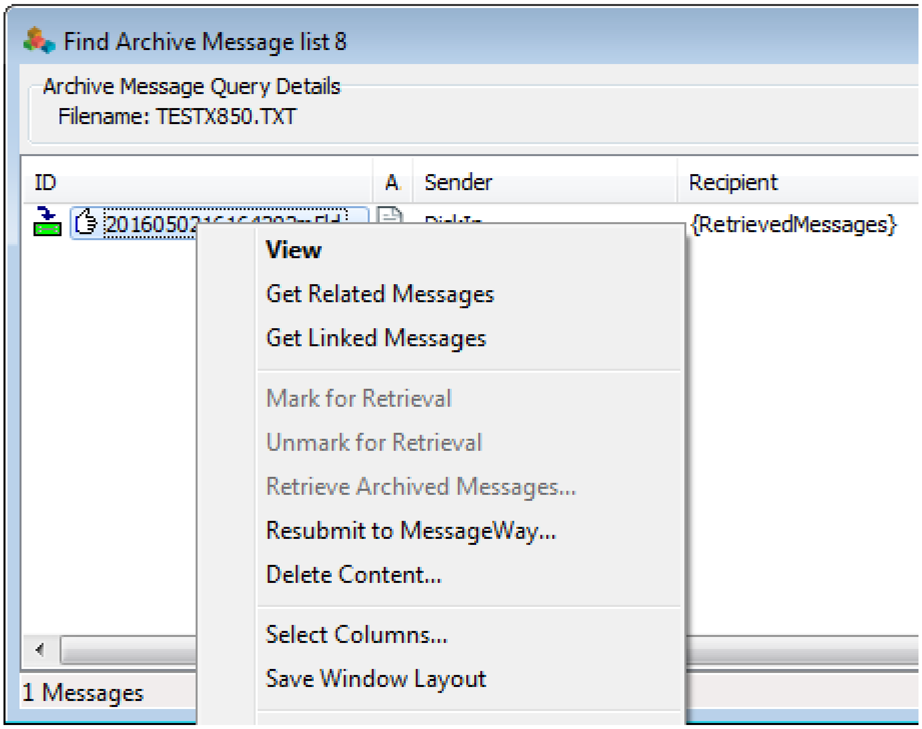
□ Available □ Error

Archive Status

□ Archived

☑ Retrieved

and select a message, right click on selected message and select **View**:

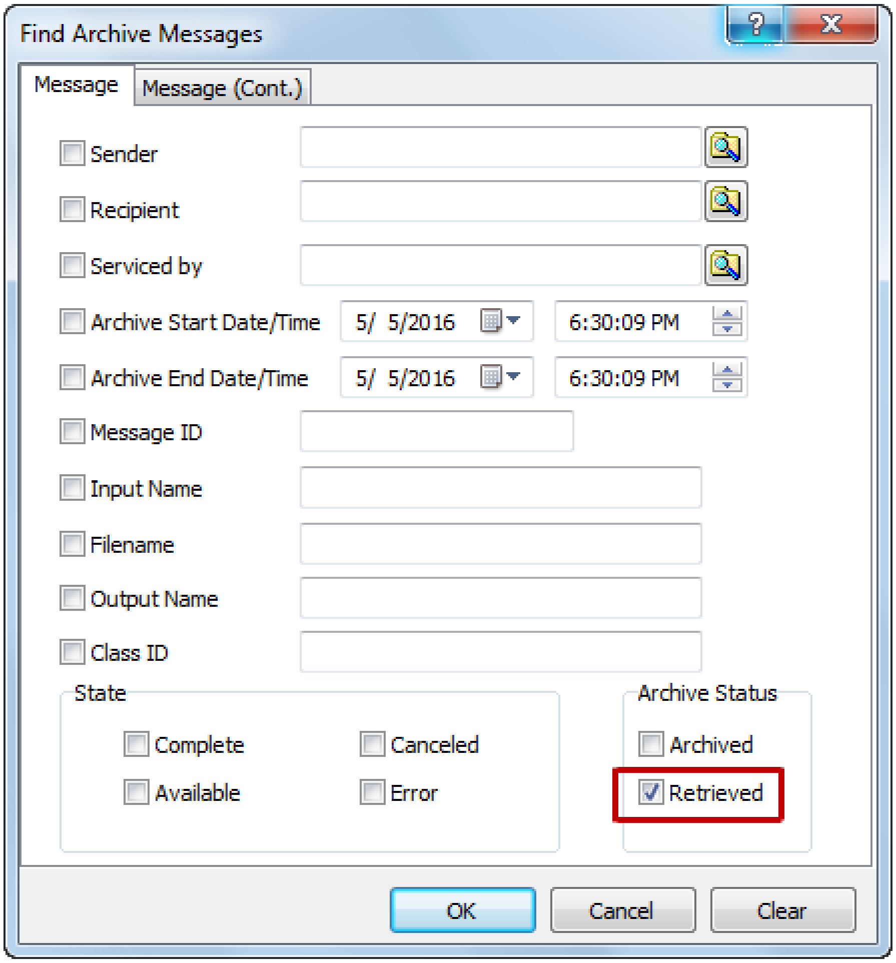


TIP: If the **Find Archive Messages** window is left open after initiating the **Retrieve Archived Messages...**, then once the retrieve has finished, simply double-click the retrieved message(s) to view its contents.

Resending Messages Retrieved from Archive

After completing the section '**Retrieving Messages from Archive**', you are now able to resend the retrieved message(s) back into the message store, thus allowing message(s) to be resent to trading partners.

- To resend a message retrieved from archive, use **Find Archive Messages** and select Retrieved:



Find Archive Messages

Message | Message (Cont.)

□ Sender

□ Recipient

□ Serviced by

□ Archive Start Date/Time 5/ 5/2016 6:30:09 PM

□ Archive End Date/Time 5/ 5/2016 6:30:09 PM

□ Message ID

□ Input Name

□ Filename

□ Output Name

□ Class ID

State

□ Complete □ Canceled

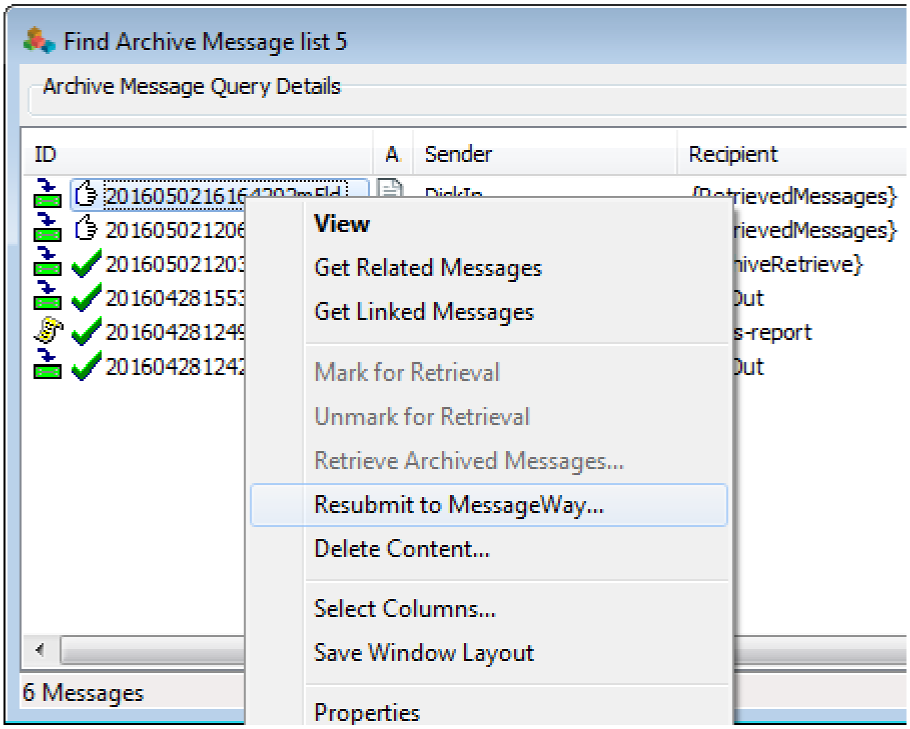
□ Available □ Error

Archive Status

□ Archived

☑ Retrieved

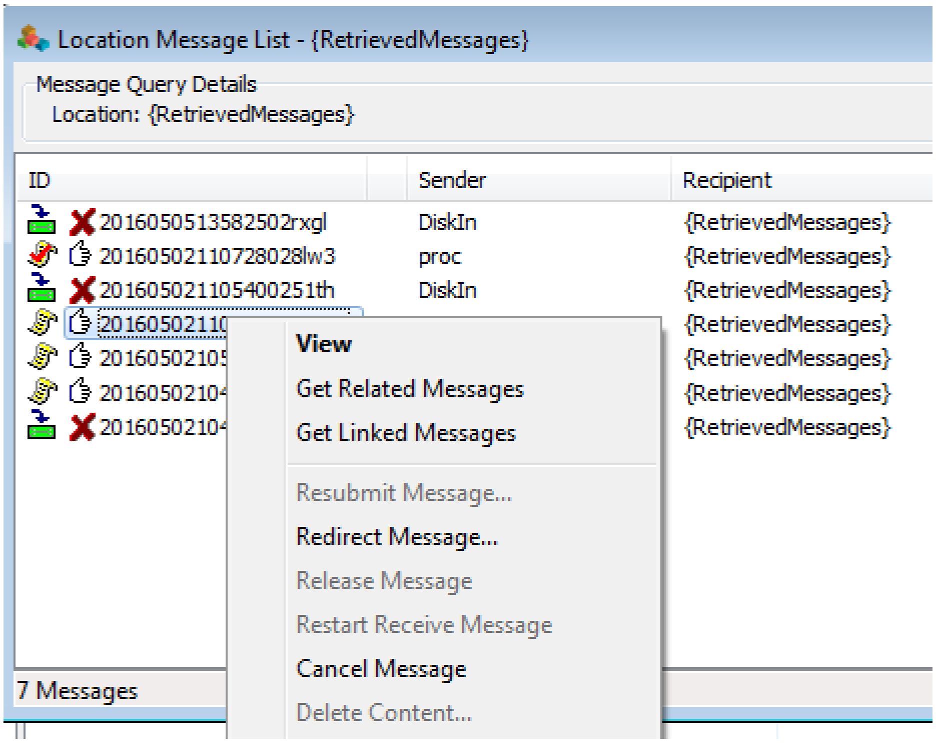
and select one or more messages, right click on selected message(s) and select **Resubmit to MessageWay…**:



This places the message retrieved from archive in a system location called {RetrievedMessages}.

NOTE: Messages placed in {RetrieveMessages} are created as new messages, so you must know the original recipient or new recipient before performing the next step. To help you determine the original recipient, the Input Name of any message placed in {RetrieveMessages} contains the message ID of the message retrieved from archive: **Input Name:** Archived message - 2015040915000900daa0 Use this message ID to determine the original recipient.

- From {RetrievedMessages} you can **Redirect Message...** to either the original recipient, or a new recipient:



Location Message List - {RetrievedMessages}

Message Query Details
Location: {RetrievedMessages}

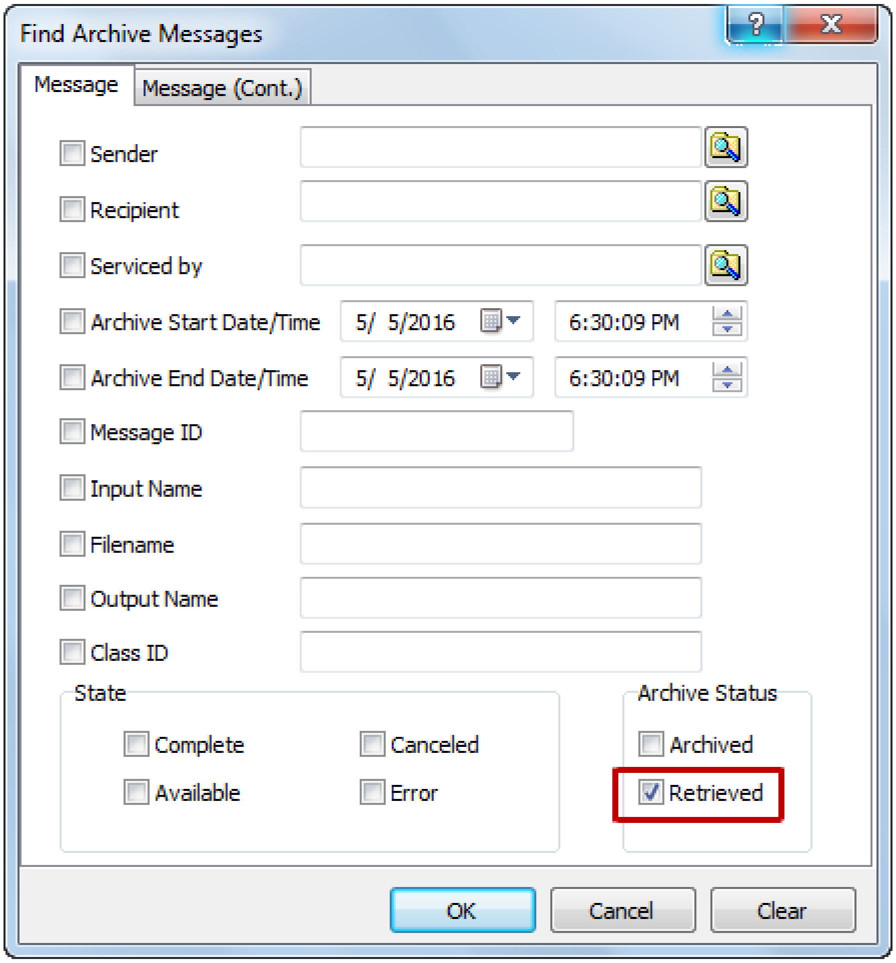
ID	Sender	Recipient
2016050513582502rxgl	DiskIn	{RetrievedMessages}
20160502110728028lw3	proc	{RetrievedMessages}
201605021105400251th	DiskIn	{RetrievedMessages}
2016050211(		{RetrievedMessages}
2016050210!		{RetrievedMessages}
2016050210·		{RetrievedMessages}
2016050210·		{RetrievedMessages}

7 Messages

Deleting Messages Retrieved from Archive

After completing the section '**Retrieving Messages from Archive**', and optionally '**Viewing Messages Retrieved from Archive**' and/or '**Resending Messages Retrieved from Archive**', you are now able to delete message(s) retrieved from archive.

- To delete a message retrieved from archive, use **Find Archive Messages** and select Retrieved:



Find Archive Messages

Message | Message (Cont.)

□ Sender

□ Recipient

□ Serviced by

□ Archive Start Date/Time 5/ 5/2016 6:30:09 PM

□ Archive End Date/Time 5/ 5/2016 6:30:09 PM

□ Message ID

□ Input Name

□ Filename

□ Output Name

□ Class ID

State

□ Complete □ Canceled

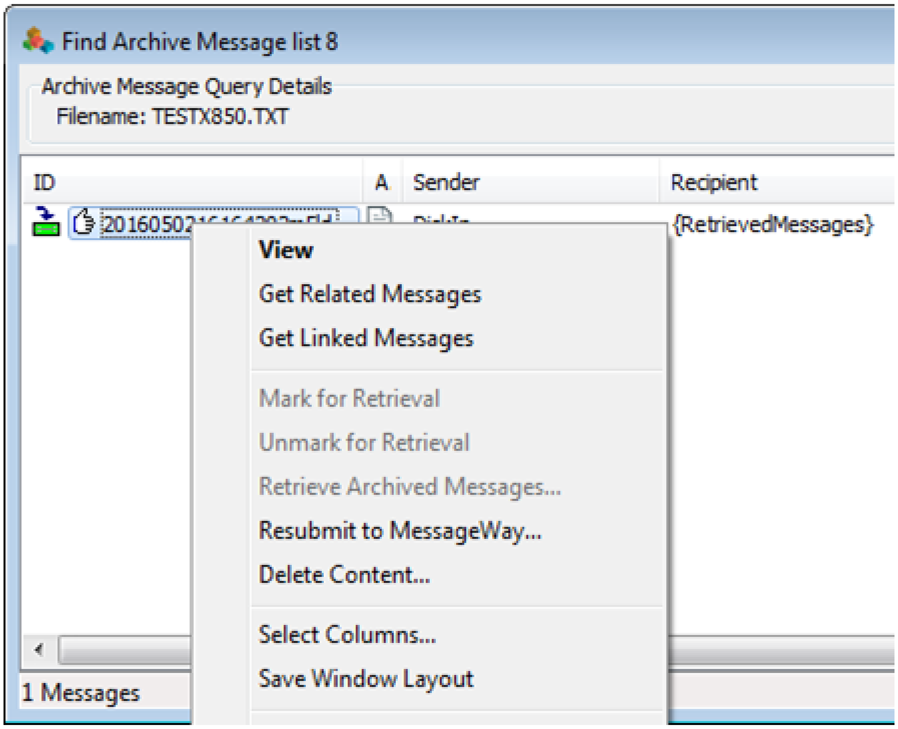
□ Available □ Error

Archive Status

□ Archived

☑ Retrieved

and select one or more messages, right click on selected message(s) and select **Delete Content…**:



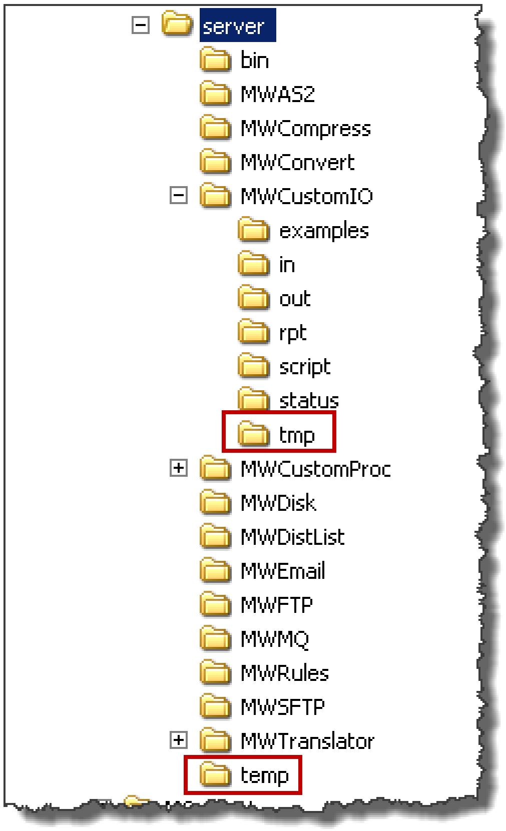
The result will be to delete the retrieved message content and to change the status of the message back to **Archived**. The delete action will take place immediately. Once the content has been deleted, the message may again be retrieved.

NOTE: Only messages retrieved from archive are deleted. Any messages resulting from **Resending Messages Retrieved from Archive** are not deleted by this action.

Maintaining the Server Directories

The Server directory contains several subdirectories, one each for the installed adapter and service. The type of information in each subdirectory depends on the type of adapter or service. Some, such as MWTranslator, have persistent information that users should not delete, such as the document and wrapper definitions it needs for processing. Many contain temporary subdirectories where the service stores information while it processes data. When errors occur during adapter or service processing, there may be temporary files that users should eventually delete.

Your directory structure should appear similar to the following:



Users should assess the following types of information in these subdirectories to determine whether they want to delete them:

- Files in temporary directories
- State logs that may be left from aborted processes are in service subdirectories

For example, temporary files are used by:

- MWTranslator for logging and reconciliation. Normally, these are automatically removed.
- MWCustomIO and MWCustomProc to place scripts for execution that are stored in MessageWay. These scripts are not started from a command line that resides in memory, but from this temporary disk location. In the event of a script failure, these may be left for debugging.

Maintaining the Audit Directory

For each session of the MessageWay Manager, MessageWay checks to see if an audit file exists, and if not, it creates one. The audit files log operator actions performed from the Manager. For more information, refer to the following topics:

- ***Viewing Audit Information*** (on page 699)
- ***Changing the Location of the MessageWay Directories*** (on page 785)

The MessageWay Archive program archives audit records after 20 days. To delete the logs without first archiving them, you must check the **Do Not Archive Audit Files** box in the MWArchive Server Properties window.

For more information about the entry, refer to the topic, ***More Options in the Configuration File*** (on page 799).

This page intentionally blank.

Using MessageWay Utilities

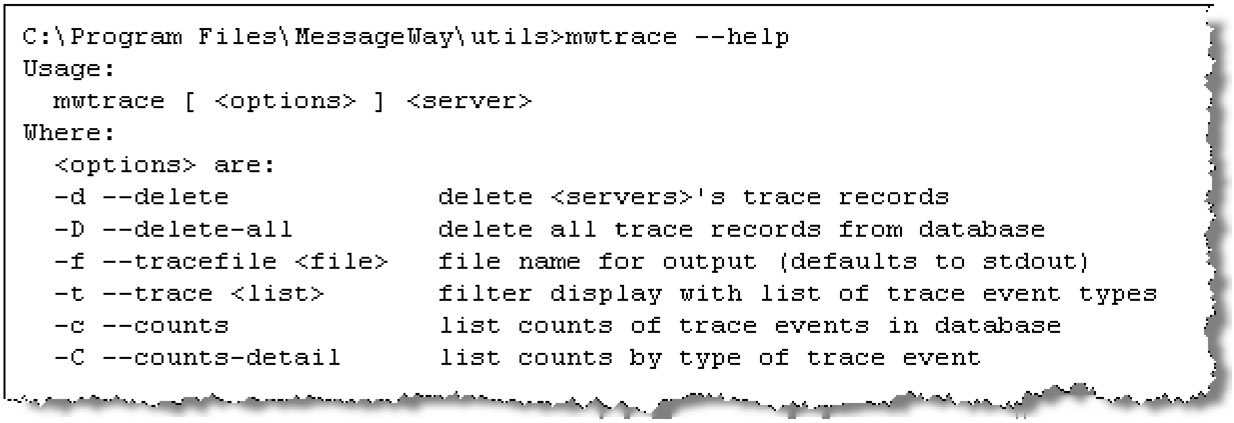
MessageWay includes several utilities to help with administration. You run these utilities from a command line. Information for each utility may appear in various locations, depending on their use. Click the utility name in the following table to access its information. The default location varies depending on the operating system, as follows:

System	Location of MessageWay Utilities
Windows (32-bit system)	\Program Files\MessageWay\utils
Windows (64-bit system)	\Program Files (x86)\MessageWay\utils
UNIX/Linux	/opt/messageway/utils

These utilities include the following:

Utility	Function
mwadmin (on page 830)	Allows administrator to change the database logon, add super users, change user passwords, re-sync message counts, and add, change, backup and restore MessageWay system keys, and add a passphrase file.
mwexp (on page 837)	Exports MessageWay configurations to an XML file.
mwimp (on page 839)	Imports MessageWay configurations from an XML file generated by the **mwexp** command.
mwkeygen (on page 281)	Generates shared key files to support connection security for the Remote Execution Server (RES), a MessageWay perimeter server option.
mwlogdump (on page 841)	Exports the contents of the log tables in the MessageWay database to a file.
mwrestart (on page 885)	Allows operator to obtain a count of restart records, write the records to a log file or display them at the terminal, delete a specific restart record, delete restart records for a specific adapter or service or delete all restart records in the database.
mwtrace (on page 877)	When users trace communications for an adapter, service or internal server, MessageWay writes the log records to the database. This utility allows users to review and filter the log records, output the information to disk and delete records from the database.

To access the command-line help, type the command followed by `--help,` as in the following example:



```
C:\Program Files\MessageWay\utils>mwtrace --help
Usage:
  mwtrace [ <options> ] <server>
Where:
  <options> are:
  -d --delete             delete <servers>'s trace records
  -D --delete-all         delete all trace records from database
  -f --tracefile <file>   file name for output (defaults to stdout)
  -t --trace <list>       filter display with list of trace event types
  -c --counts             list counts of trace events in database
  -C --counts-detail      list counts by type of trace event
```

Utility for Database, User, and Master Key Administration

The command-line utility, mwadmin, allows system administrators to do the following:

- Change the database logon, including the Data Source Name (DSN), the owner of the database and the owner's password
- Add super user
- Change user passwords
- Re-sync message counts
- Add a master key to encrypt message content that is stored in the database
- Change a master key
- Save the passphrase
- Back up system keys to an encrypted file
- Restore system keys from an encrypted file created by a backup

CAUTION: This utility should only be available to system administrators. You must understand the implications of changing a database logon and have the responsibility to add super users and control user logon and master keys to encrypt message content.

To view the options for mwadmin, at a command line type: **`mwadmin --help`**.

The syntax of the command is as follows:

`mwadmin` [*options*] *command* [*args*]

The *options* parameter must only be used with the **setdblogon** command for a non-standard messageway configuration file, where MessageWay was installed using a name other than the default for the ***MessageWay configuration file*** (on page 89) or in a different location:

- *Options* is: **`-f`** *FullPath*/*mwaycfgfile*

The following table describes the commands available and any arguments:

Command	Description
`setdblogon` *dsn* [*dbuser dbpassword*]	Changes the MessageWay database DSN, owner and password in the MessageWay configuration file, encrypting the password. Use the **-f** option when you have a non-standard MessageWay configuration file name or location.
`adduser` [*user* [*password*]]	Adds a MessageWay super user, and forces a password change on next logon. If you do not supply a user, the user defaults to **Administrator**. If you do not supply a password, the password defaults to the value, **12345**.
`changepswd` [*user* [*newpassword*]]	Changes an existing user's password. **CAUTION:** If you do not supply a user, the user defaults to **Administrator**. If you do not supply a password, the password defaults to the value, **12345** and forces the user to change the password at the next logon.
`msgcountsync`	Re-sync the MessageCounters table with the Messages table. Use this command when the message counts displayed in the Manager do not match the number of messages displayed in a list in the Manager.
`addmasterkey`	Adds an initial master key to encrypt the message content when stored in the database. **IMPORTANT:** You must use this command to add a master key before you can configure MessageWay to encrypt message content.
`changemasterkey`	Changes the master key by adding a new key to the list. Older keys are retained to support content that may have been encrypted previously with the keys.
`savepassphrase`	Saves the passphrase in an encrypted file. This allows UNIX/Linux users to use key commands in the mwadmin utility and start MessageWay without having to manually enter the master passphrase. The passphrase file is created automatically for Windows users, but this process can be used in case the passphrase file is ever deleted.
`backupkeys` *filename*	Backs up system keys to an encrypted file. **CAUTION:** Make sure you always back up keys after you add or change a master key. If you lose your passphrase file or the password, the only way to recover is to use the *restorekeys* command.

Command	Description
`restorekeys` *filename*	Restores system keys from an encrypted file created with *backupkeys* command. This command allows users to enter a new passphrase. **CAUTION:** If your backup key file is not current when you use this command, you will not be able to view message content that was encrypted with any keys not in the file.

Best Practice

Whenever you add an initial master key or change a master key, make sure you backup your key file. This ensures that all keys may be restored when required, for example when the passphrase is lost. The backup file contains a list of all keys, which allows users to decrypt and view all message content that has been encrypted. Without a complete list of keys, users will not be able to view content that was encrypted with the missing keys.

How to Change Database Logon Information

Use the **setdblogon** command for the mwadmin utility to do the following:

- Change the Data Source Name (DSN) of the MessageWay database
- Change the owner of the database, which is the logon ID used to access the database
- Change or encrypt the owner's password

These changes appear in the ***MessageWay configuration file*** (on page 89).

To change the MessageWay database logon information, you must type all the arguments, which include the DSN, the user ID and the password:

1. Stop MessageWay:
   - ***How to Stop MessageWay on UNIX or Linux*** (on page 30)
   - ***How to Stop MessageWay on Windows*** (on page 32)
2. At a command line, type the following, replacing DSN, User and Password with your values:
   - For a default install of the MessageWay configuration file, type:

     mwadmin setdblogon MessageWay_DSN mway *password*

     - or -
   - For a unique install of the MessageWay configuration file where you must include the option that specifies the unique file name or location, type:

     mwadmin -f */FullLocationPath/Filename* **setdblogon** *DSN User Password*

IMPORTANT: Do not leave any of the arguments blank, because they become null values in the configuration file.

How to Add a Super User

For backup security or in cases where the default super user, Administrator, is deleted from MessageWay, you may create another super user.

To add a super user:

1 At a command prompt, replacing the user and password with your own values, type:

mwadmin adduser [*user* [*password*]]

NOTE: If you do not supply a user, the user defaults to **Administrator**. If you do not supply a password, the password defaults to the value, **12345**.

A super user is added to MessageWay, but requires that you change the password at the next logon.

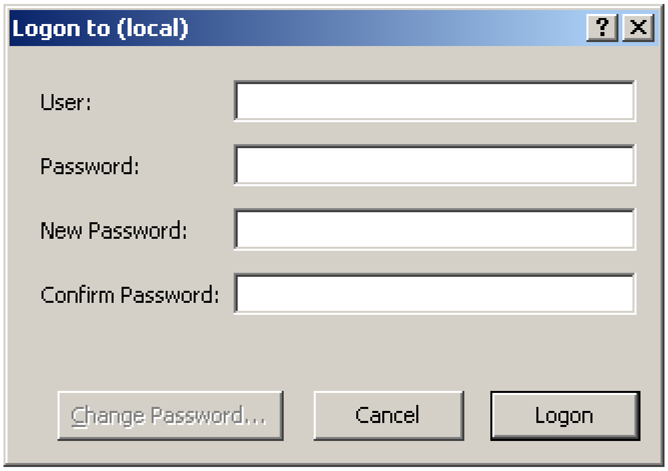
2 To test the user access, log on to MessageWay as the new user.

a) From the Manager, click the Logon button, 🔑.

The **Logon** dialog box appears.

b) Click **Change Password**.

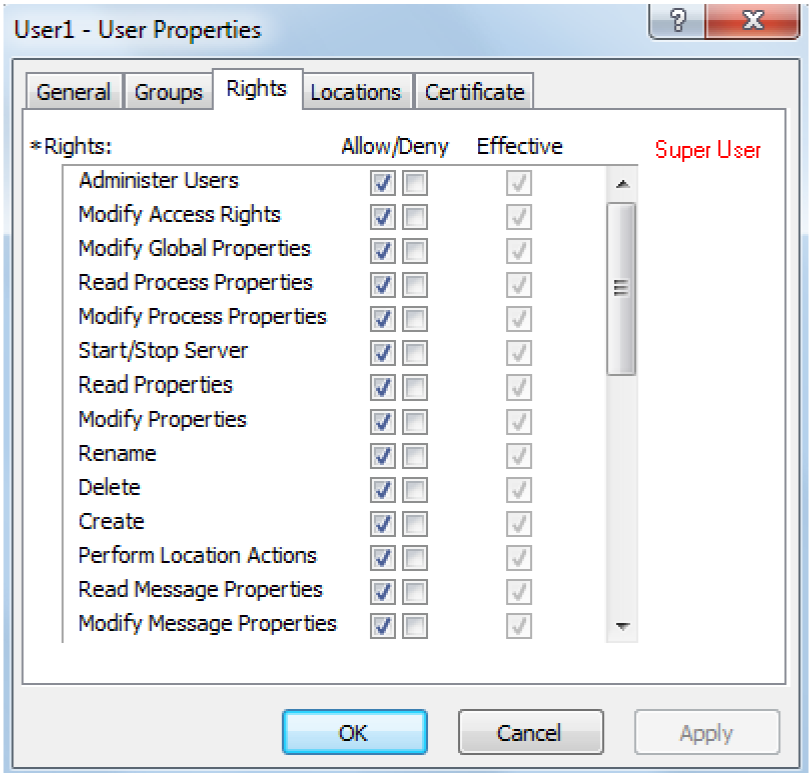
The full logon dialog box appears.



c) Type your user ID, the original password the new password and a password confirmation, and then click **Logon**.

d) View the **Rights** page of the User properties window for your new user.

Super User should appear in the upper right corner.



*Rights:	Allow/Deny		Effective
Administer Users	☑	□	✓
Modify Access Rights	☑	□	✓
Modify Global Properties	☑	□	✓
Read Process Properties	☑	□	✓
Modify Process Properties	☑	□	✓
Start/Stop Server	☑	□	✓
Read Properties	☑	□	✓
Modify Properties	☑	□	✓
Rename	☑	□	✓
Delete	☑	□	✓
Create	☑	□	✓
Perform Location Actions	☑	□	✓
Read Message Properties	☑	□	✓
Modify Message Properties	☑	□	✓

How to Change a User Password

To change a user's password outside of the Manager:

1 To change the password, at a command prompt, replacing the user and password with your own values, type:

mwadmin changepswd *user password*

The user's password is changed.

CAUTION: If you do not supply a user, the user defaults to **Administrator**. If you do not supply a password, the password defaults to the value **12345** and forces the user to change the password at the next logon.

2 To test the user access, log on to MessageWay as the new user.

How to Add a Master Key

To add the initial master key, MessageWay must be stopped:

1 Stop MessageWay:

- ***How to Stop MessageWay on UNIX or Linux*** (on page 30)
- ***How to Stop MessageWay on Windows*** (on page 32)

2 From a command line, ***use the mwadmin utility*** (on page 830) and type the following command:

mwadmin addmasterkey

3 At the prompt for a new master passphrase, type a password of up to 256 characters, and then re-enter it.

4 For Windows systems, mwadmin automatically saves the passphrase in a file.

- or -

For UNIX/Linux systems, at the prompt to save the passphrase, do one of the following:

a) Type **N**, which will not create a passphrase file, and will delete the passphrase file if one exists

- or -

b) Type **Y**, which creates a passphrase file

5 ***Backup your master keys to a file*** (on page 836).

How to Change a Master Key

For security, users may periodically change the master key.

TIP: Also, when the passphrase file has been deleted or if you do not know the passphrase, you need to create a new master key, which allows you to also create a new passphrase.

To change a master key:

1 Stop MessageWay:

- ***How to Stop MessageWay on UNIX or Linux*** (on page 30)
- ***How to Stop MessageWay on Windows*** (on page 32)

2 From a command line, type the following command:

mwadmin changemasterkey

3 At the prompt for a new master passphrase, type a password and then re-enter it.

4 For Windows systems, mwadmin automatically saves the passphrase file.

- or -

For UNIX/Linux systems, at the prompt to save the passphrase, do one of the following:

a) Type **N**, which will not create a passphrase file, and will delete the passphrase file if one exists

- or -

b) Type **Y**, which creates a passphrase file

5 ***Backup your master keys to a file*** (on page 836).

How to Save the Passphrase

CAUTION (Windows): To start the MessageWay server on Windows, when MessageWay or any location is configured to use encryption, you must have a passphrase file. When users add a master key and configure MessageWay or any location to use encryption, a passphrase file is created automatically. If Windows users delete their passphrase file, they will not be able to start MessageWay until they create a new file. To create a new passphrase file, users may change the master key or simply save the passphrase file without changing the master key.

When MessageWay is installed on UNIX/Linux, a passphrase file is not automatically created. Without a passphrase file, the user starting MessageWay must know the password of the passphrase file and respond at the command prompt. To start MessageWay using an unattended process, users must create a passphrase file.

Users are prompted to save the passphrase file when they ***add*** (on page 834) or ***change*** (on page 835) the master key. However, to save the current passphrase in a file without changing the master key:

1. At a command line, type:

   mwadmin savepassphrase

2. If you do not have a passphrase file, you must enter a password, which may be up to 256 characters.

How to Back Up Master Keys

MessageWay keeps a list of all master keys you have created for the database environment. This allows users to be able to view any message content that has been encrypted.

CAUTION: If you lose your passphrase file, or you forget the password, you will have to use the **restorekeys** command to be able to log on to MessageWay. If the backup file does not contain the latest keys, you will not be able to view message content that was encrypted with those missing keys.

Always back up your keys after you add or change master keys:

1. At a command prompt, replacing *filename* with the path and name of your backup file, type:

   mwadmin backupkeys *filename*

2. If you do not have a passphrase file, you must enter the password.

How to Restore Master Keys

CAUTION: If the backup file does not contain the latest keys, you will not be able to view message content that was encrypted with those missing keys. Always back up your keys after you add or change master keys:

To restore master keys:

1. At a command prompt, replacing *filename* with the path and name of your backup file, type:

   mwadmin restorekeys *filename*

2. If you do not have a passphrase file, you must enter the password.

Utility to Import and Export Configurations

The Import and Export Utilities allow users to copy configurations to and from XML files. This is useful to:

- Copy configurations from one MessageWay system to another
- Save backup copies of configurations

The utilities copy configurations from a MessageWay database to XML files (export) or from MessageWay XML files to a MessageWay database (import). You issue one of two commands from a command line to either export (mwexp) or import (mwimp) configurations.

System	Location of MessageWay Utilities
Windows (32-bit system)	\Program Files\MessageWay\utils
Windows (64-bit system)	\Program Files (x86)\MessageWay\utils
UNIX/Linux	/opt/messageway/utils

You can copy the following types of configurations:

- Folder (for locations in Locations folder, rules processing profiles or receipt schedules only)
- Locations (in Locations and File System folders)
- Schedules
- Rules processing profiles
- Users
- All configurations
- All location configurations (in both Locations and File System folders)

Exporting Configurations

To export configurations from the MessageWay database to an XML file, you type a command from a command line.

The syntax options of the command are as follows, depending on whether you are running from Windows or from UNIX/Linux:

- {**mwexp** | **./mwexp**} **-h**
- {**mwexp** | **./mwexp**} **-v**
- {**mwexp** | **./mwexp**} **-all** *filename*
- {**mwexp** | **./mwexp**} **--all-locs** *filename*
- {**mwexp** | **./mwexp**} {[**-f** *folders* [**-R**]] [**-l** *locations* [**-R**]] [**-s** *schedules*] [**-r** *rules*] [**-u** *users*] *filename*}

IMPORTANT: The file name must be last, but options that precede may occur in any order. When a command is successful but returns no configuration data, you will only see the header information in the file. You can use the asterisk, *, as a wildcard, but for UNIX/Linux, you must enclose any lists that use the wildcard within double quotation marks. In Windows, the quotation marks are optional. For example:

```
./mwexp -l "DCX*" dcxlocations
./mwexp -u "*" allusers
```

The following table describes the options available, which may have both a long form and a short form. You may have multiple arguments for each command that you separate with a space.

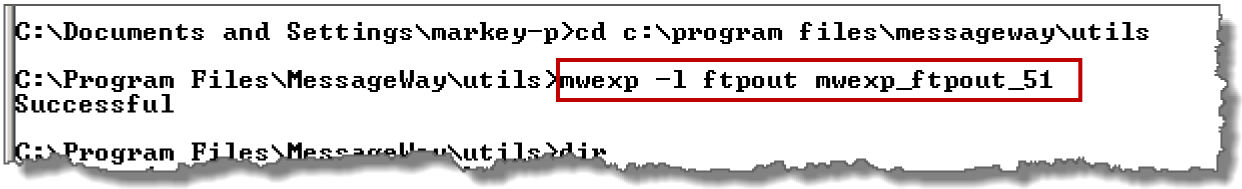
Option	Short Form	Description
N/A	N/A	The name of the output XML file. This is required with all options except **version**, and it must appear after all options. The output name is appended with a suffix, .mwd.
--all	-all	Exports all configurations in the MessageWay system, excluding the contents of the Keys folder.
--all-locs		Exports all configurations in both the Locations folder and the File System folder
--folder	-f	Exports the requested folder configurations and all of their contents from the Locations folder. When used with the wildcard, "*", it returns all folders, subfolders and their contents from the Locations folder. To obtain subfolders and their contents for specific folders, use this command with the **recursive** command. This is not a valid command for locations in the File System folder.
--help	-h	Displays the syntax of the command.
--location	-l	(Locations folder) Exports the requested location configurations. (File System folder) Exports contents of specific directories (locations). To obtain contents of subdirectories (sub-locations), use this command with the **recursive** command. For the location name, specify the full path name of the directory (location), using the forward slash / notation.
--recursive	-R	Exports subfolders and their contents from the Locations folder or locations and their sub-locations from the File System folder. For the Locations folder, use this only with the **folder** *folders* option. For the File System folder, you use this only with the **location** *locations* option.
--rule	-r	Exports the requested rules processing profiles.
--schedule	-s	Exports the requested schedules configurations associated with the Receipt Monitor option.
--user	-u	Exports the requested user configurations.
--version	-v	Displays the version of the program. Used alone.

When the output file already exists, you will have the option to overwrite it. You receive the following:

Export file - filename.mwd - already exist. Overwrite? (Y)es, (N)o:

Here are some examples.

IMPORTANT: When you export files, make sure you have access to write to the specified output location. For Windows, particularly for newer versions, the exported file may end up somewhere other that where you expect, such as C:\Users\MessageWay\AppData\Local\VirtualStore\Program Files\MessageWay\utils. The following examples will write by default to where the program runs, which is typically ..\Program Files\MessageWay\utils, as shown here:



```
C:\Documents and Settings\markey-p>cd c:\program files\messageway\utils

C:\Program Files\MessageWay\utils>mwexp -l ftpout mwexp_ftpout_51
Successful

C:\Program Files\MessageWay\utils>dir
```

This example exports all MessageWay configurations, excluding the contents of the Keys folder.

mwexp -all all_mway

This example exports all folders and locations from the Locations folder and all locations from the File System folder:

mwexp --all-locs all_folders_locations

This example exports all folders and their contents from the Locations folder:

mwexp -f "*" all_Locationfolders

This example specifies multiple configurations with different commands:

mwexp -l "A*" loc1 loc2 "copy*" -u tom brad "user*" -s schedule1 "holiday*" multiconfigs

This example exports the folder and all of its subfolders and their contents from the Locations folder:

mwexp -f folderA -R export1

This example exports all locations in the File System folder (the root location is always /):

./mwexp -l "/" -R allfslocations

This example exports the location and all of its sub-locations and their contents from the File System folder:

./mwexp -l "/fs_tests" -R exportFile

Importing Configurations

To import configurations from an XML .mwd file to the MessageWay database, you type a command from a command line. This command imports all definitions in the file and provides the option to overwrite existing definitions.

IMPORTANT: To access newly imported definitions, log off Manager and log back on.

The syntax options of the command are as follows, depending on the platform, Windows or UNIX/Linux:

- {**mwimp** | **./mwimp**} **-h**
- {**mwimp** | **./mwimp**} **-v**
- {**mwimp** | **./mwimp**} **-o** *filename*

The following table describes the options available, which have both a long form and a short form.

Option	Short Form	Description
N/A	N/A	The name of the XML file to import. This is required with all options except **version**, and it must occur last, after any options. You do not need to include the suffix, .mwd.
--help	-h	Displays the syntax of the command.
--version	-v	Displays the version of the program.
--override	-o	This potentially overrides the default state of imported locations, which is **On Hold**. Whenever the import program imports a new location or a location that exists but has changes, the import program automatically puts that location on hold, for all location types except pickup mailboxes. With this option, the location will be imported with the same state as the export. That also means, that if a location is **On Hold**, and the imported definition has a status of **Open**, the location status will be changed to **Open** after the import. **NOTE:** This setting does not affect pickup mailboxes. If the location type is a pickup mailbox, the location state is the same as what is in the imported file.

When you import definitions that exist in the database but have changed, you will be asked if you want to overwrite the existing definition(s):

```
<location-name> location exists.  Overwrite? (Y)es, Yes to (A)ll, (N)o,
No to A(L)L:
```

If definitions do not exist, or if there are no changes, you will simply see a response, **Successful**.

CAUTION: By default, when you import a location definition that is new or has changed, the location status is changed to **On Hold** for all location types except pickup mailboxes. To allow the locations to receive messages for delivery or pickup, you must manually issue a **Release Messages** command for the locations from the Manager. If you use the override option during import, and if the status of the location in the saved definition was **Open**, the location will be automatically reset to **Open**.

This example of the default syntax imports all definitions in the file and puts locations on hold:

```
mwimp dtout
```

This example imports all definitions in the file and uses the saved status of the location as the current status:

```
mwimp -o dtout
```

Utility to Export the Contents of Logs

The mwlogdump utility allows a user to export the contents of the Audit and Event log tables from the MessageWay database.

To view the options for mwlogdump, at a command line type:

- **`mwlogdump -help`** (Windows)
- **`./mwlogdump -help`** (Unix)

The syntax of the command is as follows:

- **`mwlogdump`** [*options*] (Windows)
- **`./mwlogdump`** [*options*] (Unix)

The following table describes the options available and any arguments:

Command	Description
-a or --auditlog	Export the audit logs. This is the default setting.
-c or --csv	Write the contents in a comma-separated value format.
-e or --eventlog	Dump the event logs.
-o (or --output) <*file*>	Write the contents to a file with the specified name. The default is to write the contents to stdout.
-s or --syslog	Write the contents in a Syslog format. This is the default format.

This example exports the contents of the audit log table to a Syslog format file:

```
mwlogdump -a -o auditlog111011.txt
```

This example exports the contents of the event log table to a CSV format file:

```
mwlogdump -e -c -o eventlog111011.txt
```

This page intentionally blank.

Troubleshooting

This section describes the messages that you might receive from MessageWay, how to trace communications activity, and how to review the various logs, including audit logs, system event logs and trace logs.

Overview of Troubleshooting

MessageWay troubleshooting techniques discussed here include the following:

- Reviewing and understanding event messages
- Tracking and reviewing communications events throughout MessageWay
- Restarting interrupted message processing
- Tuning a MessageWay system

MessageWay Events

MessageWay produces event messages that you can use to resolve problems. The troubleshooting information includes the following:

Category	Description
Text	Exact text of the message is in italics, usually followed by information specific to this event
Event Action	Important action that results from the event
Event Type	Type of event: ▪ Information ▪ Warning ▪ Error
Origin	Subsystem in MessageWay that generated the event, including: ▪ Adapters/services ▪ Locations ▪ Perimeter servers ▪ Internal servers or components of servers that are tightly integrated with Messaging Server
Description	Explanation of the event

These are the potential origins of messages, including product options:

Origin	Options
Services	▪ Compression ▪ Custom ▪ Distribution List ▪ Rules Processing ▪ Translator
Adapters	▪ Custom (option) ▪ Disk Transfer ▪ E-mail ▪ FTP
Locations	▪ Service locations ▪ Sites ▪ Mailboxes
Perimeter Servers	▪ FTP ▪ SSH ▪ AS2
Servers or components	▪ Messaging ▪ Archive/Delete ▪ Logging/Reconciliation ▪ Scheduling (includes Daylight Saving Time and RES Monitor) ▪ Service Interface (SI) ▪ User

These are the types of events:

Event Type	Description
Information	Typically describes processing milestones
Warning	Describes something important happened that may affect your processing, and where you could take some action to correct the problem
Error	Describes events that interrupt processing

The event number and message text will appear in the event log, which varies based on your operating system. The following table lists the default locations:

Windows	Application Event Viewer
UNIX	/var/adm/messages
Linux	/var/log/messages

When applicable, additional information may appear on an **Error** tab of the Message Properties window for a specific message.

1000 Server information

Text	*Server information*
Event Action	Varies
Event Type	Information
Origin	MessageWay adapters, services or servers
Description	This event may be critical and signal a malfunction.

1001 Server started

Text	*Server started*
Event Action	None
Event Type	Information
Origin	Messaging Server
Description	*component* or *server* has been started.

1002 Server stopped

Text	*Server stopped*
Event Action	None
Event Type	Information
Origin	Messaging Server
Description	*component* or *server* has been stopped.

1003 Winsock transfer

Text *Winsock transfer*, followed by information specific to this event

Event Action None

Event Type Information

Origin

Description

1004 Starting MessageWay, initializing message counts

Text *Starting MessageWay, initializing message counts. This may take several minutes*, followed by information specific to this event

Event Action None

Event Type Information

Origin Messaging Server

Description Message counts are being initialized for each location.

1005 Initializing message counts

Text *Initializing message counts*, followed by information specific to this event

Event Action None

Event Type Information

Origin Messaging Server

Description Message counts are being initialized.

1006 Server suspended

Text *Server suspended*

Event Action None

Event Type Information

Origin *component* or *server*

Description *component* or *server* has been suspended. May be effect of operator action.

1007 Server resumed

Text	*Server resumed*
Event Action	None
Event Type	Information
Origin	*component* or *server*
Description	*component* or *server* has resumed operation. May be effect of operator action.

2101 Queue read failed

Text	*Queue read failed*, accompanied by information specific to the error.
Error Action	
Error Type	Error
Origin	Translator Runtime Module (TRM)
Description	

2102 Queue erase entry failed

Text	*Queue erase entry failed*, followed by information specific to the error.
Event Action	
Event Type	Error
Origin	Translator Runtime Module (TRM)
Description	

2103 Queue initialization failed

Text	*Queue initialization failed*, followed by information specific to the error.
Event Action	
Event Type	Error
Origin	Translator Runtime Module (TRM)

2201 Generic database failure

Text *Generic database failure*, followed by information specific to the error.

Event Action

Event Type Error

Origin Translator Runtime Module (TRM)

Description

2202 Invalid transaction handle

Text *Invalid transaction handle*, followed by information specific to the error

Event Action

Event Type Error

Origin Translator Runtime Module (TRM)

Description

2203 Memory allocation failed

Text *Memory allocation failed*, followed by information specific to the error

Event Action

Event Type Error

Origin Translator Runtime Module (TRM)

Description

3000 Unable to move input file

Text *Unable to move input file to message store, file is in use. Will be delivered when next message arrives in this folder.* Followed by information specific to the event.

Event Action None

Event Type Warning

Origin Adapter (Disk Transfer, FTP)

Description

3001 Unable to copy input file

Text *Unable to copy input file to message store, file is in use. Will be delivered when next message arrives in this folder.* Followed by information specific to the event.

Event Action None

Event Type Warning

Origin Adapter (Disk Transfer, FTP)

Description

3002 File missing or access denied

Text *File missing or access denied,* followed by information specific to the event.

Event Action None

Event Type Warning

Origin Adapter (Disk Transfer, FTP)

Description To fix this problem, consider the following:

- Check permissions on the file to make sure the owner of the MessageWay database has access to the file.
- For FTP input transfers, some non-traditional FTP servers may provide a directory listing where the last extension on the file name does not actually exist. In order for MessageWay to retrieve the file, it must remove the extension before it issues a GET command. On the **FTP Input** tab of the FTP site properties window, check the box **Remove last file extension** to allow MessageWay to remove the invalid extension and retrieve the file.

3003 Ignore invalid command

Text *Ignore invalid command*, followed by information specific to the event.

Event Action None

Event Type Warning

Origin Adapter (Disk Transfer, FTP)

Description

3004 Agents file error

Text *Agents file error*, following by information specific to this event.

Event Action Remote user denied access to MessageWay.

Event Type Warning

Origin MessageWay server or interface that uses public key authentication to authenticate inbound requests (AS2 Interface, SSH Perimeter server)

Description A problem occurred with the agents file. Check to see that the file exists in the appropriate location. For more information, refer to the topics:

- For the AS2 Interface, ***How to Create an Agents File (AS2)*** (on page 150)
- For the SSH Perimeter server, ***How to Create the Agents File*** (on page 346)

3005 Agent authentication failure

Text *Agent authentication failure*, followed by information specific to the event.

Event Action Remote user denied access to MessageWay

Event Type Warning

Origin MessageWay server or interface that uses public key authentication to authenticate inbound requests (AS2 Interface, SSH Perimeter server)

Description The user is not configured in the agents file.

3007 Data Validation Incomplete

Text *Data validation incomplete*, followed by information specific to this event

Event Action None

Event Type Warning

Origin Content Validation (MessageWay Messaging Server)

Description Content Validation is a MessageWay option that integrates with third-party virus-checking software. It can check incoming files as well as files that are generated by MessageWay services. MessageWay might determine that message validation is incomplete, for example, when the anti-virus server is unavailable or some other error occurs during validation. If the configuration is set to continue processing, MessageWay delivers the message. The alternative option is to quarantine the message. This error appears in the system error log.

4001 Bad acknowledgment received

Text *Bad acknowledgment received*, followed by information specific to this event

Event Action Document reconciliation failed

Event Type Warning

Origin Translator (Operator Program Document Reconciliation)

Description An invalid acknowledgment was received. For more information, refer to the *MW Translator Operator Guide and Reference*.

4002 No matching records found

Text *No matching records found*, followed by information specific to this event

Event Action Document reconciliation failed

Event Type Warning

Origin Translator (Operator Program Document Reconciliation)

Description The subsystem that reconciles inbound acknowledgments with messages users have sent to their trading partners did not find a match between the information in the acknowledgment and the outbound documents previously sent. For more information, refer to the *MW Translator Operator Guide and Reference*.

4003 Multiple matching records found

Text *Multiple matching records found*, followed by information specific to this event

Event Action Document reconciliation failed

Event Type Warning

Origin Translator (Operator Program Document Reconciliation)

Description The subsystem that reconciles inbound acknowledgments with messages users have sent to their trading partners found more than one match. For more information, refer to the *MW Translator Operator Guide and Reference*.

4004 Reconciliation validation failure

Text *Reconciliation validation failure*, followed by information specific to this event

Event Action Document reconciliation failed

Event Type Warning

Origin Translator (Operator Program Document Reconciliation)

Description The validation process of document reconciliation associated with translation has failed. For more information, refer to the *MW Translator Operator Guide and Reference*.

4005 Field on ack does not match subject document ID

Text *Field on ack does not match subject document*, followed by information specific to this event

Event Action Document reconciliation failed

Event Type Warning

Origin Translator (Operator Program Document Reconciliation)

Description The subsystem that reconciles inbound acknowledgments with messages users have sent to their trading partners found that the document ID was not the same in the acknowledgment and document. For more information, refer to the *MW Translator Operator Guide and Reference*.

4006 Field on ack does not match generated detail count

Text *Field on ack does not match generated detail count*, followed by information specific to this event

Event Action Document reconciliation failed

Event Type Warning

Origin Translator (Operator Program Document Reconciliation)

Description The subsystem that reconciles inbound acknowledgments with messages the users have sent to their trading partners found that the detail count was not the same in the acknowledgment and document. For more information, refer to the *MW Translator Operator Guide and Reference*.

4007 Disabling Integrity Checking

Text *Warning: disabling integrity checking*, followed by information specific to this event

Event Action MessageWay has disabled integrity checking

Event Type Warning

Origin FTP adapter

Description Integrity checking uses algorithms and hash totals to verify the content of file transfers is valid. MessageWay issues this warning when:

- The remote FTP server that the adapter is communicating with does not support integrity
- Transfer mode is ASCII
- Append option is set

5000 Recipient location is not defined

Text *Recipient location is not defined; the message will be saved in {Unknown}. Location:* , followed by information specific to the event

Event Action Message goes to error status

Event Type Error

Origin Messaging Server

Description The location to which the message is destined does not exist. Such messages are saved in the system mailbox, {Unknown}. To correct the problem, create the location and then resubmit the message, forward the message to an existing location, or delete the message.

In cases of receive errors (status on **General** page of Message Properties window), where MessageWay has created a header, but the receipt of the message failed, there is no message content to be delivered or to be stored in {Unknown}. Correct the problem and resubmit the message.

5001 Adapter or service is undefined for recipient location

Text *Adapter or service is undefined for recipient location; the message will be saved in {Unknown}. Location:* , followed by information specific to this event

Event Action Message goes to error status

Event Type Error

Origin Messaging Server

Description The adapter or service associated with the location is not licensed. Although you can add copies of adapters or services from the MessageWay install program, they are not available until they are licensed. To request a license file, contact MessageWay Technical Support.

5002 Recipient location is not configured for output

Text *Recipient Location is not configured for output. Location:* , followed by information specific to the event

Event Action Message goes to error status

Event Type Error

Origin Messaging Server

Description The destination location is not configured to deliver outbound messages. Redirect message to a location configured for output.

5003 Message store failure

Text *Message store failure*, followed by information specific to this event.

Event Action Message goes to error status

Event Type Error

Origin Messaging Server

Description MessageWay has failed to store the message content either in the database or on disk.

5004 Outbound delivery failure

Text *Outbound delivery failure on attempt*, followed by information specific to the event

Event Action Execute retry strategy defined for the location

Event Type Warning

Origin Adapter or service

Description MessageWay executes the retry strategy defined for the location until it successfully delivers the message or exhausts the number of retries. One cause for Disk Transfer and FTP adapters may be that the file mask is blank. Make sure there is at least a default file mask defined for the adapter. You may override this default on the location configuration.

5005 Outbound delivery failure

Text *Outbound delivery failure on attempt* , followed by information specific to this event

Event Action Message goes to error status

Event Type Error

Origin Adapter

Description MessageWay has exhausted retry strategy attempts and failed to deliver the message:

- *Rename failure (invalid argument)* - on input sites, when using compound addresses in the delivery location, the syntax you are using may be wrong. Make sure colons follow service locations and commas follow sites (adapter locations), except at the end of the address
- *Destination directory must be fully qualified* - make sure the destination directory exists and the path is correct
- After MessageWay completes writing the file in the temporary location, it attempts to rename it to the final destination location on disk. When the file already exists, the rename fails. Remove the older file of the same name from the destination directory and resubmit the message for delivery.

5006 Inbound messages receipt failure

Text *Inbound messages receipt failure, attempting retry*, followed by information specific to this event

Event Action Message goes to error status while attempting to retry. For locations that have retries configured, the final retry will generate a 5007 error.

Event Type Warning

Origin Adapter or service configured for input

Description MessageWay has failed to retrieve a message for the reason stated in the event text. MessageWay will continue to retry the configured number of times. Check the following:

- The location where MessageWay is looking exists
- By default, MessageWay attempts to delete files from the input address after it receives them. MessageWay or users configured to log on to the external system must have the ability to delete the files.

5007 Inbound messages receipt failure on final retry

Text *Inbound messages receipt failure on final retry*, followed by information specific to this event

Event Action Message goes to error status

Event Type Error

Origin Adapter

Description MessageWay has failed to retrieve a message during retry for the reason stated in the event text:

Check the following:

- The location where MessageWay is looking may not exist, External applications, such as FTP servers, may be pointing to a different default location.
- By default, MessageWay attempts to delete files from the input address after it receives them. MessageWay or users configured to log on to the external system must have the ability to delete the files.
- There may be an open error on input file, because the file no longer exists in the location where the adapter or service expects to find it. Resend the original message.
- For disk storage, a file exists with that message ID in the destination location subdirectory within the message store, which is typically in /messageway/msgstore/data. This can happen when a retry process is interrupted. Delete the file and resend the original message. Check the file to make sure it is complete, and not a partial file. Delete the message from the message store disk location, right-click the message from the Manager, and select the **Restart Receive Message** command. If you receive a partial file, you must resend the original message.

5008 Processing failure on input message

Text *Processing failure on input message*, followed by information specific to this event

Event Action Message goes to error status

Event Type Error

Origin MessageWay service

Description A service, such as Rules Processing, Custom Processing or Translation, has failed to process the input message, for the reason stated:

- For Custom Processing, a file returned by the process outside of MessageWay may not exist
- For Rules Processing, there may be no match or error action rule to process the message, which will then be sent to the system mailbox, {Unknown}, because it could not be delivered

5009 Duplicate message received

Text *Duplicate message received*, followed by information specific to this event

Event Action Message goes to error status

Event Type Error

Origin Adapter or service

Description The destination location has **Check for duplicates** selected. Additional information about the error may appear on the **Error** tab of the Message Properties window. For more information about duplicate messages, refer to the topic, ***Identifying Duplicate Messages.*** (on page 470)

5010 Late or missing message(s) (Receipt Monitor)

Text *Late or missing message(s)*, followed by information specific to this event

Event Action Creates notifications

Event Type Error

Origin Receipt Monitor

Description Receipt monitor sends notifications when a monitored event occurs. This is configurable on the schedule item for a receipt schedule. For more information about the Receipt Monitor, refer to the topic, ***Receipt Monitor*** (on page 671).

5011 Unexpected message receipt

Text *Unexpected message receipt*, followed by information specific to this event

Event Action Creates notification

Event Type Error

Origin Receipt Monitor

Description Receipt monitor sends notifications when a monitored event occurs. This is configurable on the schedule item for a receipt schedule. For more information about the Receipt Monitor, refer to the topic, ***Receipt Monitor*** (on page 671).

5012 Connection attempt from invalid source IP address

Text *Connection attempt from invalid source IP address*, followed by information specific to this event

Event Action Connection rejected

Event Type Error

Origin Various (Service Interface, FTP Server, SFTP Server)

Description For connections to MessageWay from external locations, such as an FTP client, may be explicitly denied in the configuration file for the server that handles the connection, such as the MessageWay FTP Server. Check the configuration file to see if the IP address is denied access to MessageWay.

5017 Configured input location directory is invalid

Text *Configured input location directory is invalid*, followed by information specific to this event.

Event Action None

Event Type Error

Origin Adapter (Disk Transfer, FTP, Email)

Description This error occurs when adapters attemp to poll directories that do not exist. Input sites specify where the adapter should poll. Look for the invalid location directory on the input tab of the specified site.

5018 Error setting up directory change notification

Text *Error setting up directory change notification*, followed by information specific to this event

Event Action

Event Type Error

Origin Adapter (Disk Transfer, FTP)

Description

5019 Logon failure

Text *Logon failure*, followed by information specific to this event.

Event Action Access is not granted to MessageWay.

Event Type Error

Origin Adapter (AS2, Custom IO, Disk Transfer, E-mail, FTP, HTTP)

Description An attempt to logon to MessageWay through the adapter named in the event text has failed for the reason stated in the event text.

5020 Receipt Failure

Text *Receipt Failure* followed by information specific to this event.

Event Action Input message created, but content not stored.

Event Type Error (input)

Origin Adapter (AS2, Custom IO, Disk Transfer, E-mail, FTP, SFTP)

Description This happens when you have an error during input of a message.

- This error may occur during the retry or restart process. The process may leave a file in the temporary directory, /messageway/msgstore/data/StoreDisk. Resubmit the message. When this is the case, right-click the message from a message list and click, **Restart Receive Message** from the pop-up menu. The original error may have left a blank file, so you may need to resubmit the original message instead of issuing the restart command.

NOTE: When the disk adapter encounters files on disk that are busy, it will wait until another polling cycle when the file is no longer busy before it attempts to bring it into MessageWay. This avoids receipt errors that may be generated in version 5.0 or earlier.

5021 Processing Failure

Text *Processing Failure* followed by information specific to this event.

Event Action Input message created, but content not stored.

Event Type Error (input)

Origin Service

Description This happens when you have an error during processing of a message. The error may occur when the service is unable to access a file.

For example, if the MWCustomProc service expects a file, such as a report or a status file, to be returned from the process, and it is not, the service generates this error saying that it cannot open the file on disk where expected. If the service location is configured to retry, this error may be followed by 5008 errors, indicating similar failures.

5030 Connection Error During Proxy Session

Text *Connection error during proxy session*, followed by information specific to this event

Event Action MWProxy server will not connect to the external SFTP server

Event Type Error

Origin MWProxy server

Description When used by the MWSFTP adapter, the MWProxy server attempts to make the connection to an external SFTP server on behalf of the SFTP adapter.

5031 Error Loading MWProxy Config File

Text *Error Loading MWProxy Config File*, followed by information specific to this event

Event Action MWProxy server will not start

Event Type Error

Origin MWProxy server

Description MWProxy server uses a configuration file, mwproxy.conf. The error occurs when it cannot find or read the file. For more information, refer to the topic, ***Configuring the SFTP Proxy Server Components*** (on page 366).

5032 Listener Error

Text *Listener Error*, followed by information specific to this event

Event Action MWProxy server listener failed

Event Type Error

Origin MWProxy server

Description MWProxy server listens for connections from the MWSFTP adapter on the port specified in the configuration file, mwproxy.conf. If it cannot listen on the specified port, it issues this error. For example, if there is another SFTP proxy server listening on the same port, there will be contention. For more information about the MessageWay SFTP Proxy Server, refer to the topic, ***Configuring the SFTP Proxy Server*** (on page 364).

5033 Data Validation Failed

Text *Data validation failed*, followed by information specific to this event

Event Action Message is sent to the system mailbox, {Quarantine}

Event Type Error

Origin Content Validation

Description Content Validation is a MessageWay option that integrates with third-party virus-checking software. It can check incoming files as well as files that are generated by MessageWay services. When the software determines that a message contains a virus, MessageWay places the message in quarantine.

5034 Data Validation Incomplete Forcing Quarantine

Text *Data validation incomplete forcing quarantine*, followed by information specific to this event

Event Action Message is sent to the system mailbox, {Quarantine}

Event Type Error

Origin Content Validation

Description Content Validation is a MessageWay option that integrates with third-party virus-checking software. It can check incoming files as well as files that are generated by MessageWay services. MessageWay might determine that message validation is incomplete, for example, when the anti-virus server is unavailable or some other error occurs during validation. If the configuration is set to quarantine the message, MessageWay places the message in quarantine, retaining the content. The alternative option is to continue processing.

7001 DST Shift

Text *DST (Daylight Saving Time) Shift*, followed by information specific to this event

Event Action None

Event Type Information

Origin Schedule Server

Description A Schedule shift has occurred to transition to daylight saving time.

7002 Remote Execution Server is running

Text *Remote Execution Server is running*, followed by information specific to this event

Event Action None

Event Type Information

Origin ***Remote Execution Server (RES)*** (on page 270) Monitor

Description The Remote Execution monitor has determined during its periodic check that the Remote Execution Server is running.

7003 Remote Execution Server is stopped

Text *Remote Execution Server is stopped*, followed by information specific to this event

Event Action None

Event Type Warning

Origin Remote Execution Server (RES) Monitor

Description The Remote Execution monitor has determined that the optional Remote Execution Server has stopped. This is a warning, because the monitor does not know why the server stopped.

7004 Remote Execution Server primary is stopped

Text *Remote Execution Server primary is stopped; Secondary is running*, followed by information specific to this event

Event Action None

Event Type Warning

Origin Remote Execution Server (RES) Monitor

Description The Remote Execution monitor has determined that the primary Remote Execution Server is stopped, but the secondary is running. This is a warning, because the monitor does not know why the server stopped.

7005 Load Error RES config file

Text *Load error RES config file*, following by information specific to this event.

Event Action Stops the service/daemon

Event Type Error

Origin Remote Execution Server (RES) Monitor

Description At startup, the Remote Execution Server (RES) server component could not read and load the mwres.conf parameters into memory.

7006 Listener Error

Text *Listener error*, followed by information specific to the event

Event Action Service stops

Event Type Error

Origin Remote Execution Server (RES) Monitor

Description The listener, which is the thread that accepts a connection from remote server, encountered an error. All errors on the listener are considered critical and will cause the program to halt. An exception is the **Max connections exceeded** event, which is logged as a Warning event.

7007 Remote client connection failure

Text *Remote client connection failure*, followed by information specific to the event

Event Action Client not connected

Event Type Error

Origin Remote Execution Server (RES) Monitor

Description This event may occur for several reasons; some of them common ones are:

- Client configuration entry not found in mwres.conf
- Shared key file not found or could not be read (security;bad format;corrupt)
- Shared Key file mismatch

7008 User authentication failure

Text *User authentication failure*, followed by information specific to the event

Event Action None

Event Type Error

Origin Remote Execution Server (RES) Monitor

Description A valid **Command** request has been sent, but there is a user authentication failure: user not found, user unable to login at this time, invalid password, etc.

7009 Load error FTP configuration file

Text *Load error FTP configuration file*, followed by information specific to the event

Event Action

Event Type Error

Origin FTP server

Description

7010 Listener Error

Text *Listener error*, followed by information specific to this event

Event Action Connection not made

Event Type Error

Origin FTP server

Description More than one device may be using the socket (protocol/network address/port). Check the port on which MessageWay is listening and make sure that no other device is using that port.

7011 FTP client connection rejected

Text *FTP client connection rejected*, followed by information specific to this event

Event Action Client not connected

Event Type Error

Origin FTP server

Description An attempt to connect to the FTP server has been rejected because of a problem with the credentials sent from the client.

7012 Load error MWaySI config file

Text *Load error MWaySI config file*, followed by information specific to this event.

Event Action

Event Type Error

Origin Service Interface (SI) server

Description

7013 File missing or access denied

Text *Missing or access denied file*, followed by information specific to the event

Event Action Requested action fails

Event Type Warning

Origin Service Interface server (MWSI)

Description The file action request has failed, because the file is not present or access has been denied to the file.

7014 Ignore invalid command

Text *Ignore invalid command:*, followed by information specific to this event.

Event Action None

Event Type Warning

Origin Service Interface server (MWSI)

Description

8001 Database error trying to access adapter or service configuration record

Text *Database error trying to access adapter or service configuration record*, followed by information specific to this event

Event Action Requested action fails

Event Type Error

Origin

Description A database error has occurred while attempting to access an adapter or service record. See the text for a detailed description of the error.

8002 Adapter or service record not found or creation of record failed

Text *Adapter or service record not found and creation of record failed*, followed by information specific to this event

Event Action Requested action fails

Event Type Error

Origin Adapter or service

Description The requested action could not be completed, because of the following:

- The adapter or service record could not be found
- The creation of an adapter or service record failed in the database for the reason specified in the error text.

8003 Database error trying to access location definitions

Text *Database error trying to access location definitions*, followed by information specific to this event

Event Action Requested action fails

Event Type Error

Origin Messaging server or adapter

Description A database error has occurred while attempting to access a location record. See the text for a detailed description of the error.

This error also occurs on Windows when Multiple Active Result Sets (MARS) is not set for the ODBC DSN you created for MessageWay, such as MessageWay_DSN.

8004 Database error trying to access schedule definitions

Text *Database error trying to access schedule definitions*, followed by information specific to this event

Event Action Requested action fails

Event Type Error

Origin MWSched

Description A database error has occurred while attempting to access a schedule definition. See the text for a detailed description of the error.

8005 Database error trying to access message definition

Text *Database error trying to access message definition*, followed by information specific to this event

Event Action Requested action fails

Event Type Error

Origin

Description A database error has occurred while attempting to access a message definition. See the text for a detailed description of the error

8006 Database failure during update of Messages table

Text *Database failure during update of Messages table*, followed by information specific to this event

Event Action Requested action fails

Event Type Error

Origin

Description A database error has occurred while attempting to update the Messages table. See the text for a detailed description of the error.

8007 Database error during insert to Messages table

Text *Database error during insert to Messages table*, followed by information specific to this event

Event Action Requested action fails

Event Type Error

Origin

Description A database error has occurred while attempting to insert a record into the Messages table. See the text for a detailed description of the error.

8008 Database error trying to access routing definitions

Text *Database error trying to access routing definitions*, followed by information specific to this event

Event Action Requested action fails

Event Type Error

Origin

Description A database error has occurred while attempting to access a routing definition. See the text for a detailed description of the error.

8009 Database connect failure

Text *Database connect failure*, followed by information specific to this event

Event Action MessageWay does not start its servers and user cannot log on to MessageWay.

Event Type Error

Origin MessageWay server

Description A connection to the database has been lost or has failed for the reason stated in the text.

Check the MessageWay configuration file, messageway.conf, to make sure that it has the correct data source name for the database, which should look something like this:

DSN="MessageWay_DSN"

It should be between the open and close MessageWay tags. If the DSN parameter is missing, add it after the DataDir parameter.

8010 Database error trying to access timezone definition

Text *Database error trying to access timezone definition*, followed by information specific to this event

Event Action Requested action fails

Event Type Error

Origin

Description A database error has occurred while attempting to access a timezone definition. See the text for a detailed description of the error.

9001 Worker processing failed

Text *Worker processing failed*, followed by information specific to this event

Event Action Requested action failed

Event Type Error

Origin See event text

Description This refers to worker threads. Event text specifies failure and origin of failure

9002 Worker queue failed

Text *Worker queue failed*, followed by information specific to this event

Event Action

Event Type Error

Origin

Description

9003 Failure submitting request to admin queue or worker queue

Text *Failure submitting request to admin queue or worker queue*, followed by information specific to this event

Event Action

Event Type Error

Origin

Description

9004 Failure receiving request from named pipe or socket interface

Text *Failure receiving request from named pipe or socket interface*, followed by information specific to this event

Event Action

Event Type Error

Origin

Description

9005 Failure initializing named pipe or socket monitor interface

Text *Failure initializing named pipe or socket monitor interface*, followed by information specific to this event

Event Action

Event Type Error

Origin

Description

9006 Internal error, queues not defined

Text *Internal error, queues not defined*, followed by information specific to this event

Event Action

Event Type Error

Origin

Description

9007 Socket error

Text *Socket error*, followed by information specific to this event

Event Action Connection failure

Event Type Error

Origin Service Interface (MWSI)

Description An attempt to connect to MessageWay through the Service Interface has failed for the reason stated in the event text.

9008 Named pipe error

Text *Named pipe error*, followed by information specific to this event

Event Action Requested action fails

Event Type Error

Origin Messaging Server

Description The requested action has failed for the reason stated in the event text. Named pipes are typically used for remote connections.

9009 The license has expired for

Text *The license has expired for*, followed by information specific to the event

Event Action User cannot access MessageWay component

Event Type Error

Origin MessageWay server

Description The expiration date for the MessageWay license has passed. To request a license file, contact MessageWay Technical Support.

9010 Unable to find license for

Text *Unable to find license for*, followed by information specific to this event

Event Action Request ignored, MessageWay does not start

Event Type Error

Origin MessageWay server

Description This occurs when MessageWay attempts to start a system for which a user does not have the proper license. There are various causes:

- The license has not been renamed and placed in the proper location. See the *MessageWay Installation Guide* for more information.
- Users can add adapters, but when they try to start the adapter, this error occurs because they do not have a license for the adapter.
- The messageway configuration file cannot be read successfully.

To request a license file, contact MessageWay Technical Support.

9011 Invalid license

Text *The license for* <component> *is invalid*

Event Action User cannot access MessageWay component

Event Type Error

Origin Adapter, service or server

Description The MessageWay license is invalid. For analysis, contact MessageWay Technical Support.

9012 The licensed monthly volume limit has been exceeded

Text *The licensed monthly volume limit has been exceeded*, followed by information specific to this event

Event Action MessageWay will not process messages

Event Type Error

Origin MessageWay server

Description Contact MessageWay Technical Support

9013 Failure while attempting to move processing output file to message store

Text *Failure while attempting to move processing output file to message store*, followed by information specific to this event

Event Action Attempt to move file fails

Event Type Error

Origin Service

Description An attempt to move a processing output file to the message store has failed for the reason stated in the event text.

9014 System failure. Unable to obtain message ID for processing output

Text *System failure. Unable to obtain message ID for processing output*, followed by information specific to this event

Event Action The attempt to deliver the output message fails.

Event Type Error

Origin Service

Description

9015 Failure while attempting to move input file to message store

Text *Failure while attempting to move input file to message store*, followed by information specific to this event

Event Action Attempt to receive input fails

Event Type Error

Origin

Description For the reason stated in the event text the input file has failed an attempt to move it into the message store.

9016 Failure while attempting to copy input file to message store

Text *Failure while attempting to copy input file to message store*, followed by information specific to this event

Event Action Message not fully received in MessageWay

Event Type Error

Origin Adapter or service

Description For the reason stated in the event text the input file has failed an attempt to copy it into the message store:

- Open error on input file, because the file no longer exists in the location where the adapter or service expects to find it. Resend the original message.
- For disk storage, a file exists with that message ID in the destination location subdirectory within the message store, which is typically in /messageway/msgstore/data. This can happen when a retry process is interrupted. Delete the message from the message store disk location, and resend the message, right-click the message from the Manager, and select the Restart Receive Message command.

9017 Inbound monitor processing failed

Text *Inbound monitor processing failed*, followed by information specific to this event

Event Action Receipt Monitor processing fails

Event Type Error

Origin Receipt Monitor

Description The Receipt Monitor has failed for the reason stated in the event text.

9018 MW Translator API entry point is missing

Text *MW Translator API entry point is missing*, followed by information specific to this event

Event Action

Event Type Error

Origin Translator

Description

9019 TRM failure

Text *TRM failure*, followed by information specific to this event

Event Action Translation fails

Event Type Error

Origin Translator

Description Translation has failed because of an error in the Translator Runtime Module for the reason stated in the event text. Review the translation processing report for more information.

9020 Translator configuration does not exist

Text *Translator configuration does not exist*, followed by information specific to this event

Event Action Translation fails

Event Type Error

Origin Translator

Description The Translator Runtime Module (TRM) has failed to find the configuration files.

9021 Server directory does not exist

Text *Server directory does not exist*, followed by information specific to this event

Event Action Adapter or service fails to start

Event Type Error

Origin Adapter or service

Description Each installed MessageWay adapter or service must have a subdirectory in the /MessageWay/servers directory. Make sure the specified adapter or service directory has not been deleted. If it has, rerun the MessageWay installation program, and check to make sure it was created.

9022 Message store directory does not exist

Text *Message store directory does not exist*, followed by information specific to this event

Event Action Receipt and delivery of messages fails

Event Type Error

Origin Adapter or service

Description For message content that is stored on disk, the MessageWay adapter or service noted in the event has failed to deliver or receive a message because it cannot find the message store folder.

9024 Fatal queue error

Text *Fatal queue error*, followed by information specific to this event

Event Action Adapter or service has not received the input message

Event Type Error

Origin Adapter or service

Description Messages may be in the input queue when you stop an adapter or service. Use the **Suspend** command instead of **Stop** to allow MessageWay to clear the input queue before it stops the adapter or service. Messages may also be left in the queue during a failed retry or restart. For test systems, you can also clear the queue by stopping and starting MessageWay.

9025 Unable to write to audit directory

Text *Unable to write to audit directory*, followed by information specific to this event

Event Action User server fails to write to the audit file

Event Type Error

Origin User Server (MWUser)

Description The MWUser process is unable to write data to the audit file in the audit directory for the reason specified in the event text.

9026 The user policy record is missing

Text *The user policy record is missing*, followed by information specific to this event

Event Action User in unable to log on and perform any MessageWay actions

Event Type Error

Origin User server (MWUser)

Description The user noted in the event message is unable to perform any actions in MessageWay, because the user policy record is missing.

9027 SSL error

Text *SSL error*, followed by information specific to this event

Event Action Connection to the remote FTP server fails

Event Type Error

Origin MessageWay FTP server (MWFTP)

Description For the reason specified in the event message the FTP adapter was unable to make an SSL connection to the remote FTP server.

9028 LDAP Error

Text *LDAP error*, followed by information specific to this event

Event Action LDAP user authentication fails

Event Type Error

Origin Local LDAP layer or remote LDAP server

Description LDAP was unable to authenticate the user logging into MessageWay. Check to make sure that the user is both a valid LDAP user and a valid MessageWay user.

9029 The Archive/delete Server Configuration is Missing

Text *The archive/delete server configuration is missing*

Event Action Archive/delete program fails to run

Event Type Error

Origin MessageWay Archive Program

Description Configuration information for the Archive program is not in or unavailable in the MessageWay database. Users can configure this information from the Manager, in the Servers folder on the MWArchive Server Properties window.

9030 Logging Update Error Log

Text *Logging Update Error Log*, followed by information specific to this event

Event Action Update to error log fails

Event Type	Error
Origin	MessageWay Messaging Server
Description	For the reason specified in the event message, MessageWay was unable to update the error log.

9031 The MessageWay Configuration File is Missing

Text	*The MessageWay configuration file is missing*
Event Action	Connection to the MessageWay database fails
Event Type	Error
Origin	MessageWay Server
Description	The MessageWay configuration file, messageway.conf, contains information to log on to the database. MessageWay must be able to find this file, which is in the location you specified when you installed the MessageWay Server. For more information, refer to the *MessageWay Installation Guide*.

Tracing Communications Activity

To troubleshoot communications issues, users may run a trace to log activity to the database for adapters, services and MessageWay internal servers. Some perimeter servers also provide a log file parameter to write the log to disk.

Users may review and maintain the logged information using the trace utility, mwtrace.

Configuring Trace Parameters

To initiate a trace, users do one of the following:

- For MessageWay adapters, servers and internal servers, enter trace parameters in the **Trace** field on the **General** page of the properties window
- For MessageWay perimeter servers, such as MessageWay FTP Server, Remote Execution Server, and SFTP Server, enter trace parameters in the configuration file for the server

Configuring Trace Parameters for Adapters, Services and Internal Servers

You configure trace parameters for adapters, services or internal servers in the **Trace** field on the **General** page of the properties window. You have several options, some of which are more useful than others depending on the adapter, service or server. To turn the option on, enter parameters in the field. To turn it off, clear the field. For the MessageWay Messaging Server only, trace begins when you restart MessageWay.

CAUTION: The trace process may have a significant impact on performance, especially when you use the asterisk * to trace everything, and particularly for the MessageWay User Server, mwuser. Except for the MessageWay Messaging Server, tracing starts as soon as you enter your trace options and click **Apply** or **OK**. When you have finished debugging, clear the field of all text to turn off the trace. If there is an asterisk in a trace field of core or other active servers when MessageWay starts, you risk overwhelming your system with trace activity.

The syntax of the trace option is as follows:

trace-type-list [: [*location-list*] [: [*msgid-list*] [: [*user-list*] [: *ip-list*]]]]

Where the following rules apply:

- Trace-type is mandatory
- Each list must be separated from other lists by a colon (:)
- Each list may contain one or more items, separated by commas
- Trace-type-list only may use the asterisk (*) in place of a list of types (not recommended)

Trace Component	Description
trace-type	One of the predefined types in the following table, for example, ftp, queue, pipe, sched
location	Name of a MessageWay location
msgid	MessageWay message ID
user	Name of a MessageWay user
ip	Source IP address for an mwsi connection

The following table describes some examples. The value under Trace Option would be the value entered in the appropriate Trace field. The results vary depending on where the trace is defined.

Trace Option	Description
`*`	Logs all activity for the entity (not recommended)
`pipe:::AdminTest`	Logs all pipe activity for the entity associated with the user, AdminTest
`pipe:DTIN`	Logs all pipe activity for the location, DTIN

The following table shows which types are useful for MessageWay base adapters.

Trace Type	mwdisk	mwftp	mwemail	mwcustomio	mwsftp
dirlog		OK			
functions					OK
ftp		OK			
ftp-block		OK			
ftp-data		OK			
integrity		OK			
mailboxes		OK	OK	OK	
notification*	OK				
pipe	OK	OK	OK	OK	OK
pipe-buffer	OK	OK	OK	OK	OK
polling	OK	OK	OK	OK	OK
pop3			OK		
queue	OK	OK	OK	OK	OK
queue-input	OK		OK	OK	OK
rescan	OK	OK			OK
sftp					OK
sftpdata					OK
smtp			OK		
socks					OK
ssl		OK			
startup	OK				
tcp		OK	OK		OK
wip	OK	OK	OK	OK	OK
worker				OK	

The following table shows which types are useful for MessageWay optional adapters.

Trace Type	mwas2	mwmq	mwawss3
as2	OK		
awss3			OK
debug			OK
error			OK

Trace Type	mwas2	mwmq	mwawss3
fatal			OK
http	OK		
httpbody	OK		
info			OK
mailboxes		OK	
mq		OK	
pipe	OK	OK	
pipe-buffer	OK	OK	
polling		OK	
progress			OK
queue	OK	OK	
queue-input		OK	
tcp	OK		
trace			OK
warn			OK
wip		OK	

*Note that the notification type is only available for Windows systems that use event-driven polling. It is not available for UNIX/Linux systems.

The following table shows which types are useful for MessageWay base services.

Trace Type	mwcompress	mwcustomproc	mwdistlist	mwrules
pipe	OK	OK	OK	OK
pipe-buffer	OK	OK	OK	OK
queue	OK	OK	OK	OK
route				OK

The following table shows which types are useful for MessageWay optional services.

Trace Type	mwconvert	mwtranslator
pipe	OK	OK
pipe-buffer	OK	OK

Trace Type	mwconvert	mwtranslator
queue	OK	OK

The following table shows which types are useful for MessageWay internal system servers.

Trace Type	messageway	mwsched	mwuser	mwsi
auditlog	OK	OK	OK	OK
connects			OK	
counts	OK			
DST		OK		
enctcp			OK	
heartbeat			OK	
http				OK
httpbody				OK
http-chunk				OK
ldap			OK	OK
pipe	OK	OK	OK	OK
pipe-buffer	OK	OK	OK	OK
queue	OK	OK		
receipt		OK		
receipt-actual		OK		
receipt-detail		OK		
remote		OK		
remote-detail		OK		
resend	OK			
sched		OK		
sched-detail		OK		
sessions		OK		
si				OK
ssl		OK		OK
tcp			OK	OK

Note the following:

- messageway = MessageWay Messaging Server, MessageWay Server
- mwsched = MessageWay Scheduling Server
- mwuser = MessageWay User Server
- mwsi = MessageWay Service Interface

Configuring Trace Parameters for Perimeter Servers

Perimeter servers for MessageWay each have their own configuration file with their own trace parameter, which is where you control the trace activity for the server. Some are part of base MessageWay and some are options. For more information about the trace options for these servers, refer to their documentation, as follows:

- ***FTP Server configuration file (mwftpd)*** (on page 217)
- ***Remote Execution Server*** (on page 275)
    - ***Client configuration file (mwres)*** (on page 278)
    - ***Server configuration file (mwresd)*** (on page 275)
- ***SFTP Server configuration file (mwsftpd)*** (on page 323)
- ***SFTP Proxy Server configuration file (mwproxy)*** (on page 366)

This table shows which trace types are useful for MessageWay perimeter servers.

Trace Type	mwftpd	mwproxy	mwsftpd	mwres	mwresd
auth		OK			
ftp	OK				
ftp-data	OK				
ftp-mwa	OK				
http			OK		
httpbody			OK		
sess		OK			
tcp	OK	OK	OK	OK	OK

NOTE: ftp-mwa tags trace entries to be pulled into data repository for MW Analytics.

Reviewing and Maintaining Trace Information

To review the information in the disk files for perimeter servers that write to files, open the file with a text editor. The locations of the files are defined in the configuration file for the perimeter server.

NOTE: When you view output that contains Unicode characters from MessageWay, the characters should display correctly from within MessageWay Manager and any third party software that supports Unicode characters. Viewing the same output from a command-line terminal may not display the characters correctly, if it is not configured appropriately.

To review the information in the database:

- From MessageWay Manager, from the *Search* menu, select **Find Logs**>**Trace Logs**. For more information, refer to the topic ***Finding Trace Logs*** (on page 780).
- From a command line, use the mwtrace utility.

Mwtrace is a command line utility that is located in the install location of Messageway, in the subdirectory \utils.

To view the options for mwtrace, at a command line type: **`mwtrace --help`**.

The syntax of the command is as follows:

`mwtrace` [*options*] *server*

Where:

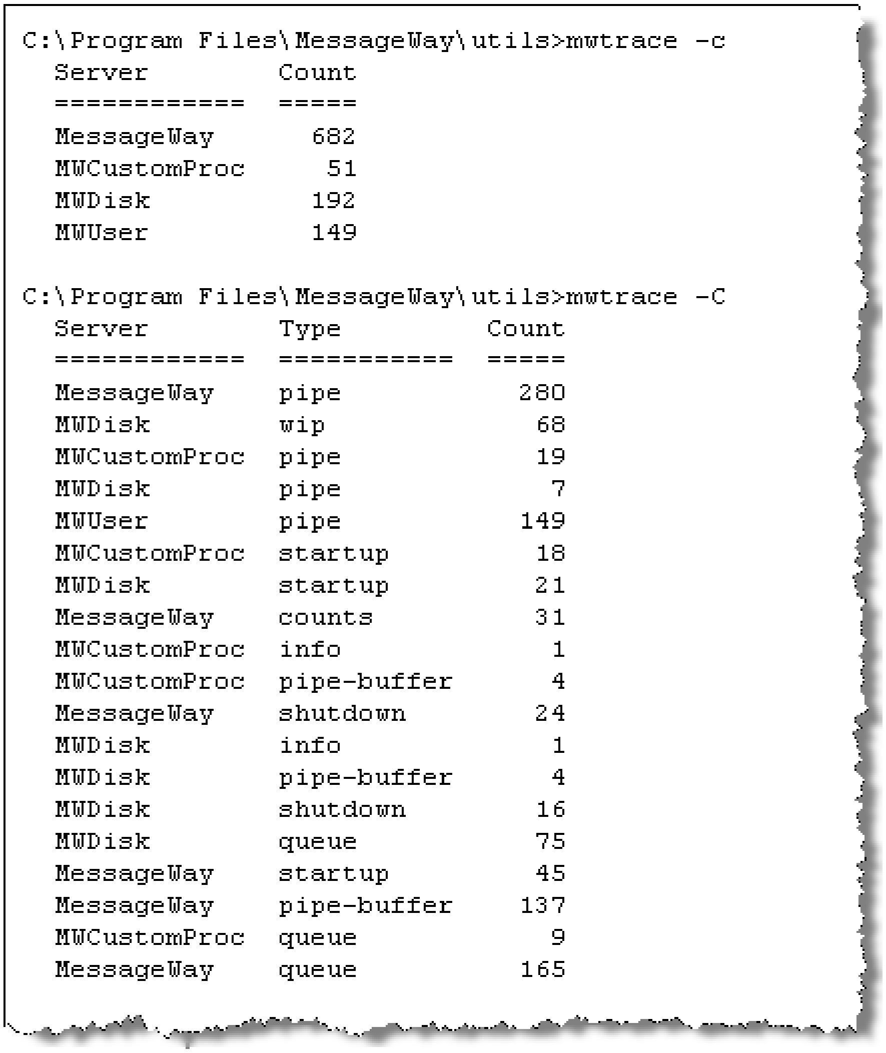
- Options are optional; when omitted, all trace types for the server are listed
- *Server* includes any of the following:
  - MessageWay
  - MWAS2
  - MWAWSS3
  - MWCustomIO
  - MWCustomProc
  - MWDisk
  - MWFTP
  - MWMQ
  - MWSFTP
  - MWUser
- Server is mandatory for the **`-f`** and **`-t`** commands, but may be used with other parameters to limit the scope

The following table describes the options available, with two forms for each option, short and long:

Short	Long	Description
`-d`	**`--delete`**	Deletes trace records for the specified server
`-D`	**`--delete-all`**	Deletes all trace records from the database
`-f`	**`--tracefile`** *file*	Writes trace file to an output file, when specified, or to stdout (the terminal) by default

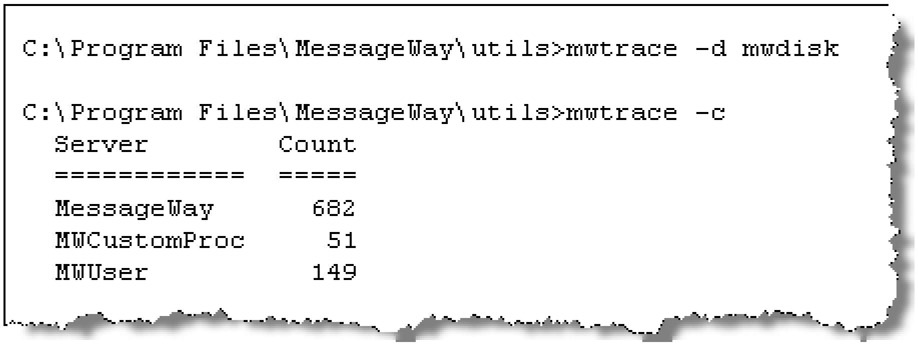
Short	Long	Description
-t	**--trace** *list*	Shows only those events of the types listed for the server. Use * to include all event types or create a list of specific types, separated by commas, without any spaces.
-c	**--counts**	Lists total number of events for each server in the database
-C	**--counts-detail**	Lists number of various types of trace events for each server in the database

The following examples show a list of servers with their event counts and a list of servers with the number of events for each event type:



```
C:\Program Files\MessageWay\utils>mwtrace -c
  Server         Count
  ============   =====
  MessageWay       682
  MWCustomProc      51
  MWDisk           192
  MWUser           149

C:\Program Files\MessageWay\utils>mwtrace -C
  Server         Type          Count
  ============   ===========   =====
  MessageWay     pipe            280
  MWDisk         wip              68
  MWCustomProc   pipe             19
  MWDisk         pipe              7
  MWUser         pipe            149
  MWCustomProc   startup          18
  MWDisk         startup          21
  MessageWay     counts           31
  MWCustomProc   info              1
  MWCustomProc   pipe-buffer       4
  MessageWay     shutdown         24
  MWDisk         info              1
  MWDisk         pipe-buffer       4
  MWDisk         shutdown         16
  MWDisk         queue            75
  MessageWay     startup          45
  MessageWay     pipe-buffer     137
  MWCustomProc   queue             9
  MessageWay     queue           165
```

The next example shows the effect of the delete command, after deleting the trace records associated with mwdisk:



```
C:\Program Files\MessageWay\utils>mwtrace -d mwdisk

C:\Program Files\MessageWay\utils>mwtrace -c
  Server        Count
  ============  =====
  MessageWay      682
  MWCustomProc     51
  MWUser          149
```

Restart Options for Interrupted Message Processing

When a MessageWay adapter or service starts a task, it generates state records in the database. The adapter or service then deletes the records upon successful completion of the task. When a task is interrupted that did not allow MessageWay to complete the task, MessageWay uses these records to restart the task.

In case MessageWay is not able to successfully restart the task, users may find that this prohibits other messages from being processed. To correct this problem, users may manually remove the restart records in the database using the mwrestart utility.

Utility to Display and Maintain Restart Records In the Database

This utility allows operators to display and remove restart records. Typically, it resides in the install directory within /utils subdirectory.

To view the options for mwrestart, at a command line type: **`mwrestart --help`**.

The syntax of the command is as follows:

`mwrestart` [*options*] *server* [*restart-key*]

Where:

- *Server* and *restart-key* are unique keys for the record
- *Server* is any service or adapter, identified by its service name, which is also visible with the **`-c`** command
- When *server* is used without an option, it sends restart records to stdout (the terminal)
- *Server* is mandatory for the **`-d`** command and when there is no option specified

The following table describes the options available, with two forms for each option, short and long:

Short	Long	Description
`-d`	`--delete`	Deletes all restart records for the specified adapter or service, or deletes a specific restart record when a restart key is provided
`-D`	`--delete-all`	Deletes all restart records from the database
`-f` *file*	`--restartlog` *file*	Writes restart logs to stdout, which is typically the terminal, or to an output file, when specified
`-c`	`--counts`	Lists total number of events for each server in the database

Recovering from Restart Failure

Typically, restart recovery is automatic. However, when users remove or change information that MessageWay needs to restart successfully, there may be restart records left in the database that will cause an adapter or service to not process other messages. In this case, users must manually remove the offending restart record.

To manually recover from a restart failure and allow MessageWay to remove restart records:

1. Determine the adapter or service that is failing:
   a) View the adapters/services monitor
   b) Look for values in the *Sending*, *Receiving* or *Processing* columns
2. Double-click the number in the *Sending*, *Receiving* or *Processing* column.

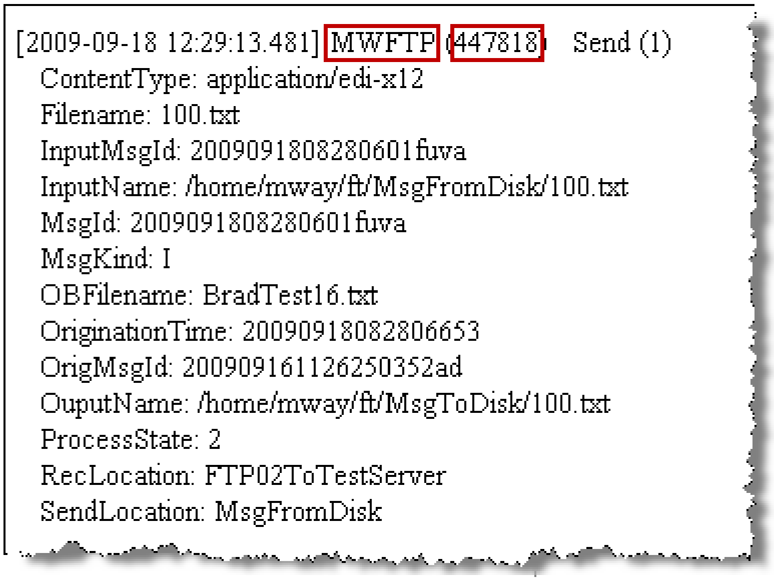
   A message list window appears.
3. Right-click the message, and select **Properties**.
4. Note the message ID or copy it to the clipboard, in case you need it for further reference.
5. Right-click the message again and click **Cancel**.

In the event that MessageWay does not remove restart records, users may do this manually:

1. If the adapter or service in question is still processing data, issue the **Suspend** command to allow it to finish, and then issue the **Stop** command.
2. From a command line, ***use the mwrestart utility*** (on page 885) to display the restart records for a specific adapter or service, for example:

   mwrestart mwftp

   The following example shows one restart record in the list, with the server and restart key highlighted:



```
[2009-09-18 12:29:13.481] MWFTP (447818)   Send (1)
   ContentType: application/edi-x12
   Filename: 100.txt
   InputMsgId: 2009091808280601fuva
   InputName: /home/mway/ft/MsgFromDisk/100.txt
   MsgId: 2009091808280601fuva
   MsgKind: I
   OBFilename: BradTest16.txt
   OriginationTime: 20090918082806653
   OrigMsgId: 200909161126250352ad
   OuputName: /home/mway/ft/MsgToDisk/100.txt
   ProcessState: 2
   RecLocation: FTP02ToTestServer
   SendLocation: MsgFromDisk
```

3 From the command line, use the mwrestart utility to delete the restart record(s):

- To delete a specific restart record, include the server and the restart key:

  mwrestart -d mwftp 447818

  - or -

- To delete all restart records for the server, type:

  mwrestart -d mwftp

  - or -

- To delete all restart records for all servers, type:

  mwrestart -D

CAUTION: Do not delete all restart records unless you know what you are doing.

This page intentionally blank.

Tuning a MessageWay System

Here are some suggestions to tune your MessageWay system.

Recommendations for High-volume Transfers Through Perimeter Servers on UNIX and Linux

We recommend the following changes to handle high volume transfers via perimeter servers on Linux and Solaris. These are the recommended minimums to handle 1000 parallel sessions for an extended period of time.

CAUTION: MySQL 5.5 does not support the earlier syntax in the my.cnf file that included *set-variable* = . If you upgrade MySQL to version 5.5 in preparation for an upgrade to MessageWay 6.1, you may need to edit my.cnf and remove all *set-variable* = values that precede the actual parameter setting. For example, if you have the parameter **set-variable = max_connections=1000**, you must change it to read **max_connections=1000**.

Recommendations for a Bash Profile for MySQL

These are recommended personal environment variables to set in the .bash_profile files for the root user and for the owner of MessageWay.

1 Log on as the root user.

2 From the home directory of the owner of MessageWay, typically *mway*, and then *root*, edit the **.bash_profile** files of each user to add the following lines:

The following sets the maximum number of open file descriptors:

ulimit -n 2048

The following sets the maximum number of processes available to a single user:

ulimit -u 4096

The following setting enables core file dumps, which may be required for troubleshooting:

ulimit –c unlimited

3 Save and close the files.

4 Log out and then log back in as the owner of MessageWay.

IMPORTANT: If you have already started MessageWay, you must restart it to make the change take effect.

Recommendations for Hard and Soft Limits on UNIX and Linux

We recommend that you set the HARD and SOFT limits for the owner of MessageWay.

For Linux systems, proceed as follows.

1 Open the file: /etc/security/limits.conf (linux)

2 Add the following lines to set the hard and soft limits for the owner of MessageWay, typically mway. If the owner is some user other than mway, replace mway in the following commands with your user:

```
mway soft nproc=4096
mway hard nproc=16384
mway soft nofile=2048
mway hard nofile=65536
```

For UNIX systems (solaris on global zone), proceed as follows:

1 Open the file /etc/system.

2 Add the following lines:

```
set max_nprocs=16384
set rlim_fd_max=65536
```

Recommendations for MessageWay Servers

We recommend the following settings for the MessageWay FTP Perimeter Server and the MessageWay Service Interface.

1 Add the following lines to the MessageWay FTP Perimeter Server configuration file /etc/messageway/mwftpd.conf in the Global section:

```
MaxConnections=1100
PortRange=20000 - 21500
```

2 Add the following line to the MessageWay Service Interface configuration file /etc/messageway/mwsi.conf in the Global section:

```
MaxConnections=2200
```

Recommendations for Oracle Databases

To improve performance, especially when starting adapters, you can execute the following commands:

```
dbms_stats.gather_schema_stats
(ownname=>'MWAY',
estimate_percent=>20,
degree=>1,
cascade=>TRUE);
```

```
dbms_stats.gather_table_stats
(ownname=>'MWAY',
TABNAME=>'MESSAGES',
ESTIMATE_PERCENT=>20,
CASCADE=>TRUE,
METHOD_OPT=>'FOR COLUMNS SIZE 10 status',
degree=>4 );
```

Recommendations for MySQL Databases

Here are some suggestions to improve performance with a MySQL database.

CAUTION: MySQL 5.5 does not support the earlier syntax in the my.cnf file that included *set-variable* = . If you upgrade MySQL to version 5.5 in preparation for an upgrade to MessageWay 6.1, you may need to edit my.cnf and remove all *set-variable* = values that precede the actual parameter setting. For example, if you have the parameter **set-variable = max_connections=1000**, you must change it to read **max_connections=1000**.

IMPORTANT: Perform the following as the user **root** from the installation directory, such as, /home/mway/mwayinstall/*name of install file*, which is created when you untar the install file as described in the topic, Using the Installation File.

The MySQL install for versions 5 or higher does not create the my.cnf configuration file. You should have already created this file, but if not, refer to the topic Creating the MessageWay Database in MySQL.

1. In /etc, open **my.cnf**.
2. In the section **[mysqld]**, add or change the following text in bold using the values specified.

   max_allowed_packet=64M (default was 1M)

   max_connections=5000 (default was 1000)

   lower_case_table_names=1

   interactive_timeout=2592000

   wait_timeout=2592000

   query_cache_size=20M

   thread_cache_size=40

   innodb_buffer_pool_size=128M

   innodb_log_buffer_size=8M

   innodb_log_file_size=64M

   innodb_flush_log_at_trx_commit = 0

   innodb_additional_mem_pool_size = 1M

This page intentionally blank.

Options

This section provides additional user and reference information for MessageWay options. For information about acquiring these options, contact MessageWay Technical Support.

Maker/Checker

The Maker/Checker option is a system-wide security setting that controls how users create or change MessageWay configurations for users or user groups from the MessageWay Manager. The two-step model sets updates made by a user, called a maker, as pending until the updates are committed by a separate user, the checker.

Licensing Requirements for Maker/Checker

The MessageWay security option, Maker/Checker, requires a license from Progress. For more information, contact MessageWay Technical Support.

Overview of Maker/Checker

When a MessageWay system uses the Maker/Checker security option, all user or user group configurations are controlled by the users who are defined as makers and the users who are defined as checkers. Only users who have the *Administer Users* right will be able to be a maker or checker. By default, any users that belong to the Administrators group inherit the *Administer Users* right, along with both *maker* and *checker* rights.

Administrators create and change configurations in a two-step process: one to make the changes, which are tagged as pending, and one to check and commit the changes. All actions are logged and viewable in the audit files.

The maker/checker process applies only to users and user groups. It does not apply to other configurations or MessageWay actions, such as, holding, releasing, resubmitting or redirecting messages or starting or stopping adapters or services.

IMPORTANT: Users may have both maker and checker rights. They may act as either a maker or a checker for modifications to a configuration, but not both. Only the super user for the MessageWay system has the right to be both maker and checker to make changes to a configuration.

Configuring Users as Makers and/or Checkers

Only users with the Administer Users right may configure users as makers or checkers. Users who belong to the Administrators group inherit the Administer Users right as well as the Maker and Checker rights, which are default settings of the group. Using the default settings, no changes are required for users who are administrators to be a maker or a checker.

IMPORTANT: The users who will be makers and checkers must have the necessary access to the objects they want to change or approve. For more information, refer to the topic, ***Configuring Access Lists for Objects*** (on page 391).

Adding a User with Maker/Checker

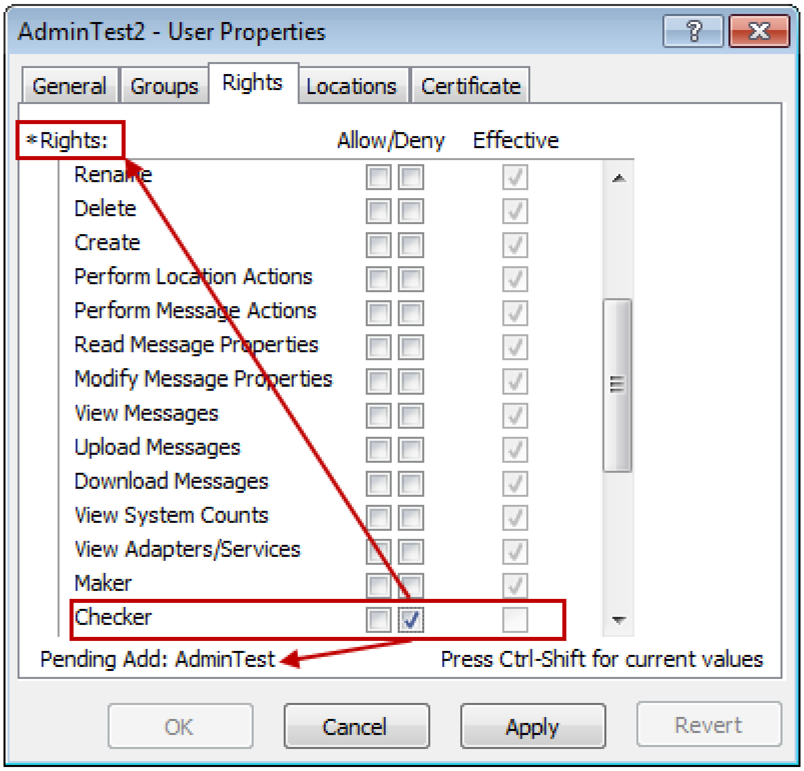
Assume that you want to add an administrator, and you want to restrict the rights to make changes but not approve them. In this case, as you add the administrator, you will remove the Checker right, which they would otherwise inherit from the group.

NOTE: Alternatively, if you do not want to give a user full administrative rights that come with belonging to the Administrators group, you can simply check the **Administer Users** and **Maker** rights for that user.

Log on to MessageWay as an administrator who has Maker rights, and proceed as follows:

1. ***Add and configure a user*** (on page 375) called AdminTest2, for example, and add this user to the Administrators group.
2. On the **Rights** tab, scroll to the bottom of the list of rights, and in the **Deny** column, check **Checker**.

This effectively allows the user to make changes but not commit any changes. An asterisk (*) appears next to the parameter that you changed, and a note at the bottom of all tabs states the type of operation pending, which is *Add*, followed by a colon and the name of the user who made the change, *AdminTest*.



AdminTest2 - User Properties

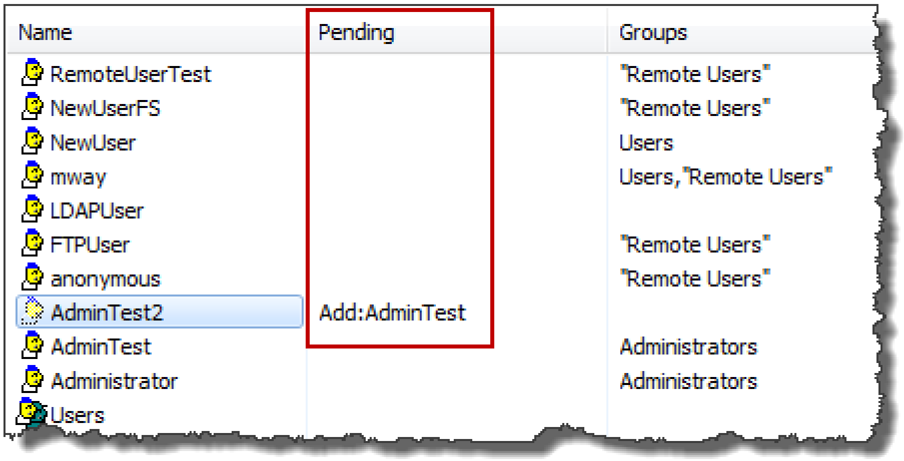
*Rights:	Allow/Deny		Effective
Rename	□	□	✓
Delete	□	□	✓
Create	□	□	✓
Perform Location Actions	□	□	✓
Perform Message Actions	□	□	✓
Read Message Properties	□	□	✓
Modify Message Properties	□	□	✓
View Messages	□	□	✓
Upload Messages	□	□	✓
Download Messages	□	□	✓
View System Counts	□	□	✓
View Adapters/Services	□	□	✓
Maker	□	□	✓
Checker	□	☑	□

Pending Add: AdminTest

Press Ctrl-Shift for current values

3 Click **Apply** or **OK**.

A note appears in the Pending column of MessageWay Explorer to indicate the user, AdminTest, has added a user, which has not been approved. The dimmed user icon indicates that this is not a live configuration.



Name	Pending	Groups
RemoteUserTest		"Remote Users"
NewUserFS		"Remote Users"
NewUser		Users
mway		Users,"Remote Users"
LDAPUser		
FTPUser		"Remote Users"
anonymous		"Remote Users"
AdminTest2	Add:AdminTest	
AdminTest		Administrators
Administrator		Administrators
Users		

4 (Optional) Before another administrator approves the change, you may back out or revert to the state of the configuration before the pending change.

NOTE: Only the user who has made the original change may continue to make changes to the configuration until it is committed.

To revert a change, open the appropriate user configuration, and click **Revert**.

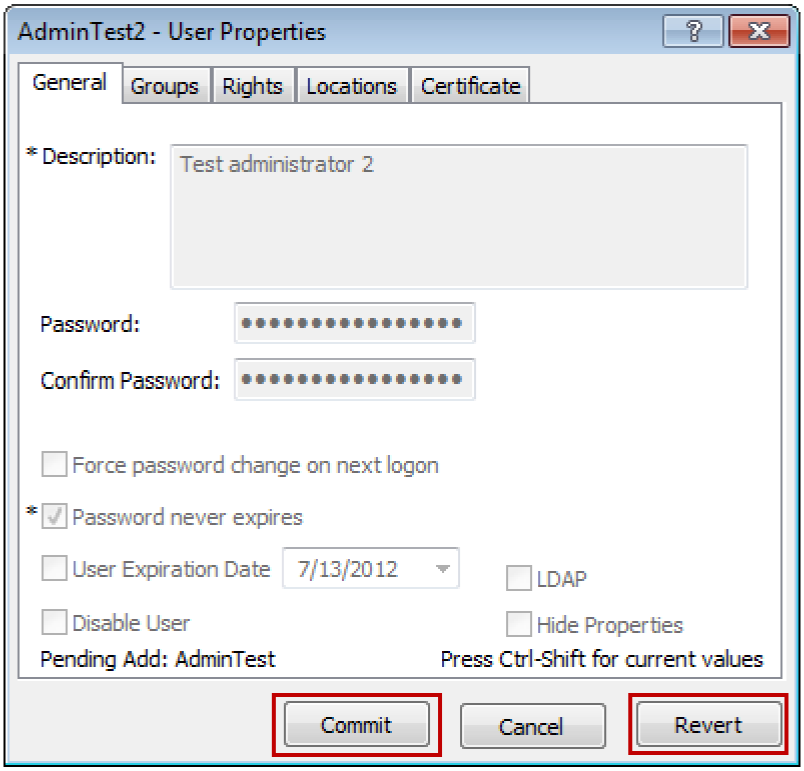
CAUTION: Clicking Revert will back out all changes that are currently pending for an object.

Approving A User with Maker/Checker

Have another administrator with **Checker** rights log on to the MessageWay Manager, and proceed as follows:

1 Open the User Properties window for the user that has pending changes.

All parameters are dimmed when you are not the user who made the pending changes.



AdminTest2 - User Properties

* Description: Test administrator 2

Password: ●●●●●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●●●●●

□ Force password change on next logon

* ☑ Password never expires

□ User Expiration Date 7/13/2012

□ LDAP

□ Disable User

□ Hide Properties

Pending Add: AdminTest

Press Ctrl-Shift for current values

2 (Optional) To view the changes that have been made:

a) An asterisk appears beside each item that has changed, so click each tab to find the changes.

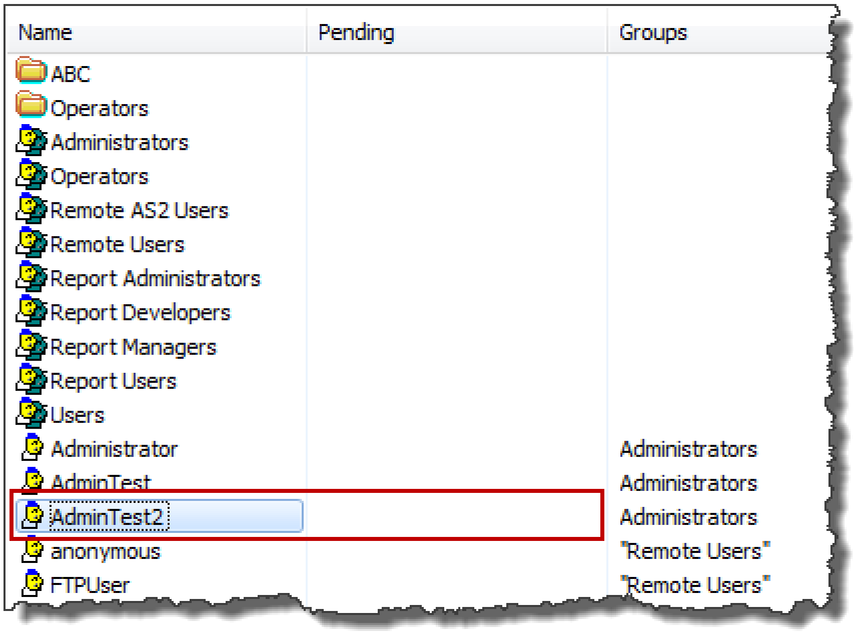
b) To view the settings before the pending changes were made, press and hold, CTRL+SHIFT.

3 To back out the changes without accepting them, click **Revert**.

- or -

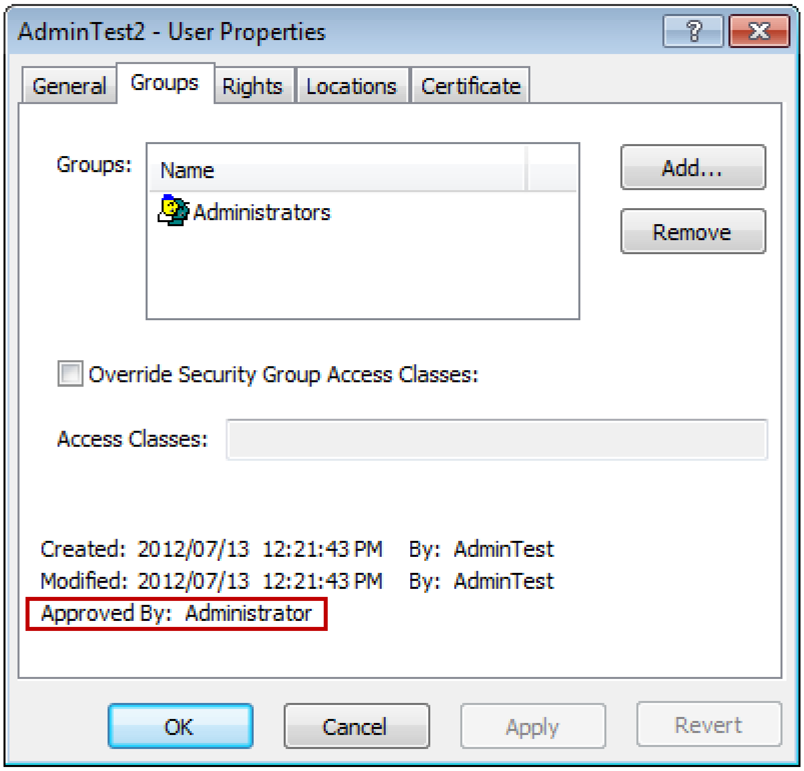
To accept the changes, click **Commit**.

After you commit the change to add the user, MessageWay Explorer shows the pending status has been removed.



Name	Pending	Groups
ABC		
Operators		
Administrators		
Operators		
Remote AS2 Users		
Remote Users		
Report Administrators		
Report Developers		
Report Managers		
Report Users		
Users		
Administrator		Administrators
AdminTest		Administrators
AdminTest2		Administrators
anonymous		"Remote Users"
FTPUser		"Remote Users"

4 Double-click **AdminTest2**, and view the **Groups** page. Note the date and time the user was created and modified and by whom appears at the bottom, followed by who approved the latest change.



AdminTest2 - User Properties

Groups:

Name
Administrators

□ Override Security Group Access Classes:

Access Classes:

Created: 2012/07/13 12:21:43 PM By: AdminTest
Modified: 2012/07/13 12:21:43 PM By: AdminTest
Approved By: Administrator

Changing User Group Configurations with Maker/Checker

Users who belong to groups inherit the combined rights of the groups.

You may wish to change the configurations of a user security group. For example, by default, the user group, Operators, does not have the right to view messages. Assume you want to change the user group, Operators, to allow all users within the group to view messages.

IMPORTANT: The users who will be makers and checkers must have the necessary access to the objects they want to change or approve. For more information, refer to the topic, ***Configuring Access Lists for Objects*** (on page 391).

Changing a User Group Configuration with Maker/Checker

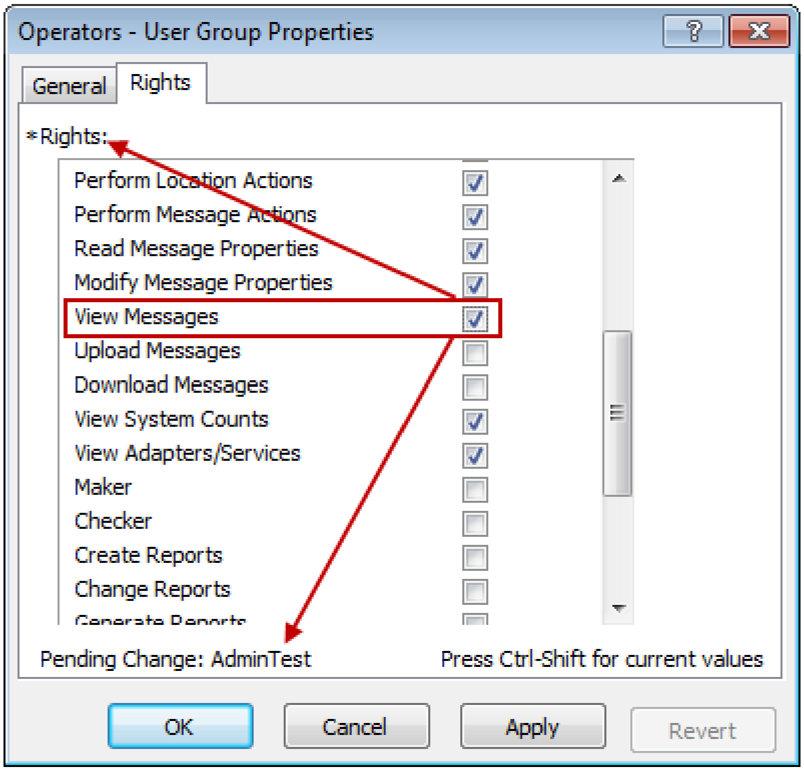
Log on to MessageWay as an administrator who has **Maker** rights, and proceed as follows:

1. From MessageWay Explorer, right click the user group, Operators, and select **Properties** from the menu.

   The Operators - User Group Properties window appears.

2. On the **Rights** tab, check **View Messages**.

   An asterisk (*) appears next to the parameter that you changed, and a note at the bottom of all tabs states the type of operation pending, which is *Change*, followed by a colon and the name of the user who made the change, AdminTest.



*Rights:

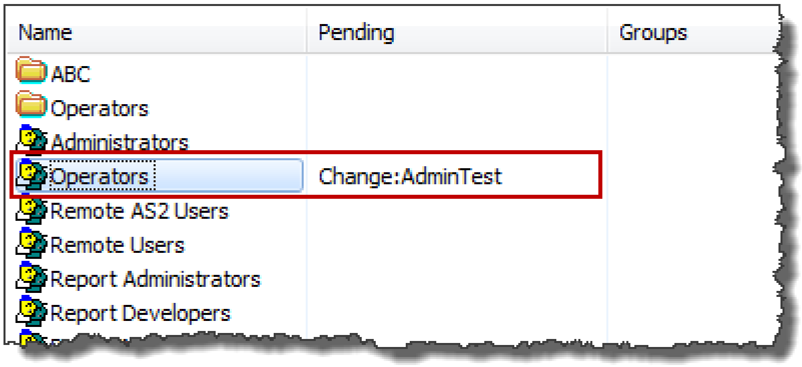
Perform Location Actions ☑
Perform Message Actions ☑
Read Message Properties ☑
Modify Message Properties ☑
View Messages ☑
Upload Messages □
Download Messages □
View System Counts ☑
View Adapters/Services ☑
Maker □
Checker □
Create Reports □
Change Reports □
Generate Reports □

Pending Change: AdminTest

Press Ctrl-Shift for current values

3. Click **Apply** or **OK**.

A note appears in the Pending column of MessageWay Explorer to indicate that there is a change made by the user, AdminTest, which has not been approved.



Name	Pending	Groups
ABC		
Operators		
Administrators		
Operators	Change:AdminTest	
Remote AS2 Users		
Remote Users		
Report Administrators		
Report Developers		

4 (Optional) Before another administrator approves the change, you may back out or revert to the state of the configuration before the pending change.

NOTE: Only the user who has made the original change may continue to make changes to the configuration until it is committed.

To revert a change, open the appropriate user configuration, and click **Revert**.

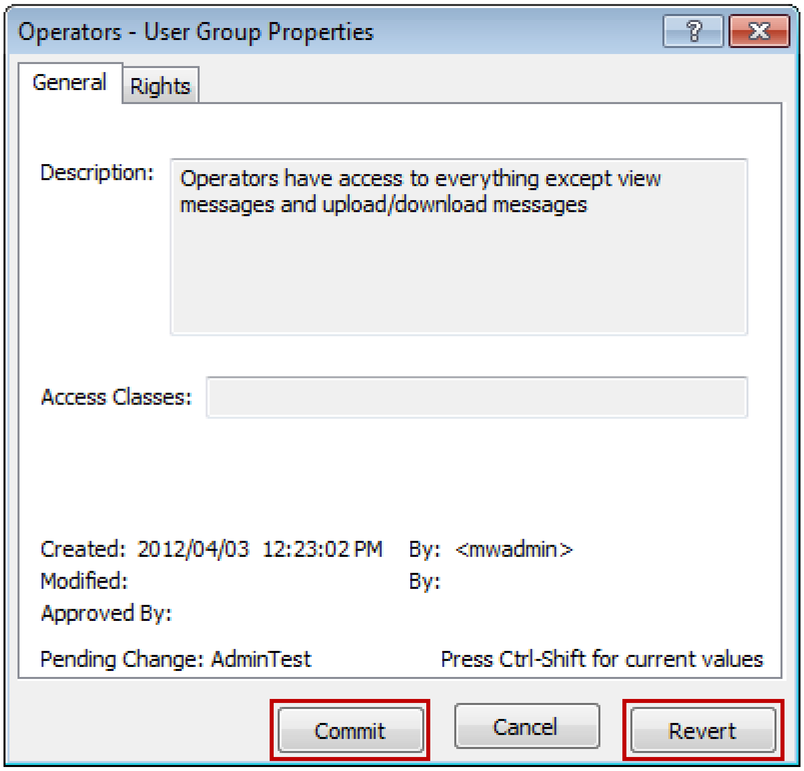
CAUTION: Clicking Revert will back out all changes that are currently pending for an object.

Approving a Change to a User Group Configuration with Maker/Checker

Have an administrator with **Checker** rights log on to the MessageWay Manager, and proceed as follows:

1 Open the Operators User Group Properties window.

All parameters are dimmed when you are not the user who made the pending changes. Note that at the bottom, the date and time the group was created and modified and by whom appear at the bottom, followed by the user who approved the latest change.



Description: Operators have access to everything except view messages and upload/download messages

Access Classes:

Created: 2012/04/03 12:23:02 PM By: <mwadmin>
Modified: By:
Approved By:
Pending Change: AdminTest Press Ctrl-Shift for current values

2 (Optional) To view the changes that have been made:

a) An asterisk appears beside each item that has changed, so click each tab to find the changes.

b) To view the settings before the pending changes were made, press and hold, CTRL+SHIFT.

3 To accept/approve the changes, click **Commit**.

- or -

To back out the changes without accepting them, click **Revert**.

4 Click **Apply** or **OK**.

Changing and Approving Configurations as Administrator

As the administrator super user, by default, Administrator, you may both make and approve changes to a configuration.

Assume you want to delete a user, UserTest2, and approve those changes.

Log on to the MessageWay Manager, and proceed as follows:

1 Right click the user, UserTest2, and from the menu click **Delete**.

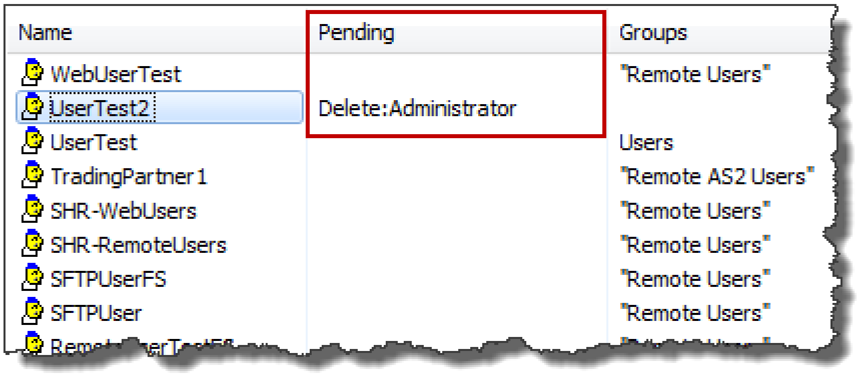
- or -

Select the user, UserTest2, and in the task bar, click the **Delete** button, ✕.

A confirmation dialog box appears.

2 Click **OK**.

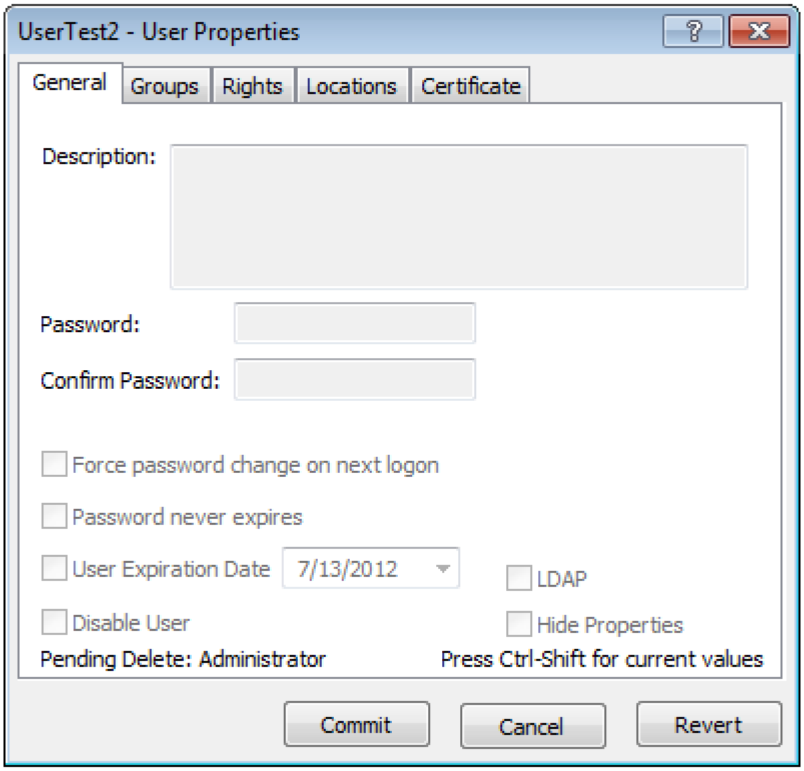
A note appears in the Pending column of MessageWay Explorer to indicate the user, Administrator, has deleted a user, which has not been approved.



Name	Pending	Groups
WebUserTest		"Remote Users"
UserTest2	Delete:Administrator	
UserTest		Users
TradingPartner1		"Remote AS2 Users"
SHR-WebUsers		"Remote Users"
SHR-RemoteUsers		"Remote Users"
SFTPUserFS		"Remote Users"
SFTPUser		"Remote Users"

3 From MessageWay Explorer, right-click and select **Confirm changes**.

This switches the Administrator to commit mode and opens the UserTest2 User Properties window.



UserTest2 - User Properties

Description:

Password:

Confirm Password:

□ Force password change on next logon

□ Password never expires

□ User Expiration Date 7/13/2012

□ LDAP

□ Disable User

□ Hide Properties

Pending Delete: Administrator

Press Ctrl-Shift for current values

4 To delete the user, click **Commit**.

- or -

To undo the delete action, click **Revert**.

5 Click **Apply** or **OK**.

Translation Service

The MessageWay Translation Service is a fully integrated business document format conversion process. It provides translation processing and partner-based routing. MessageWay Translation Service includes the following configurable entities:

- Logging server
- Reconciliation server
- MWTranslator service, created during installation
- MWTranslator service locations, configured by users

For more information about the product, MW Translator, refer to the *MW Translator Workbench User's Guide and Reference* and the *MW Translator Operator Guide and Reference.*

MW Translator uses the Xerces C++ XML validating parser version 2.7 to parse and validate incoming XML data with document type definitions (DTD) or schemas (XSD).

Licensing Requirements for the Translator Service

The MWTranslator service requires a license from Progress. You must have a license in order to start the service. Contact MessageWay Technical Support for more information.

Understanding the Messaging Process for MessageWay Translator

The following diagrams show the message flow of the example X12 850 through the adapters and service. The example uses the Disk Transfer adapter, because this is how the example is configured. Any of the I/O adapters could perform the same functions. Note that the functions shown here are related to specific tasks. Although an adapter may be performing only an input or output function at a given time, adapters are always capable of doing both. The color-coding is an aid to show the function of the components as follows:

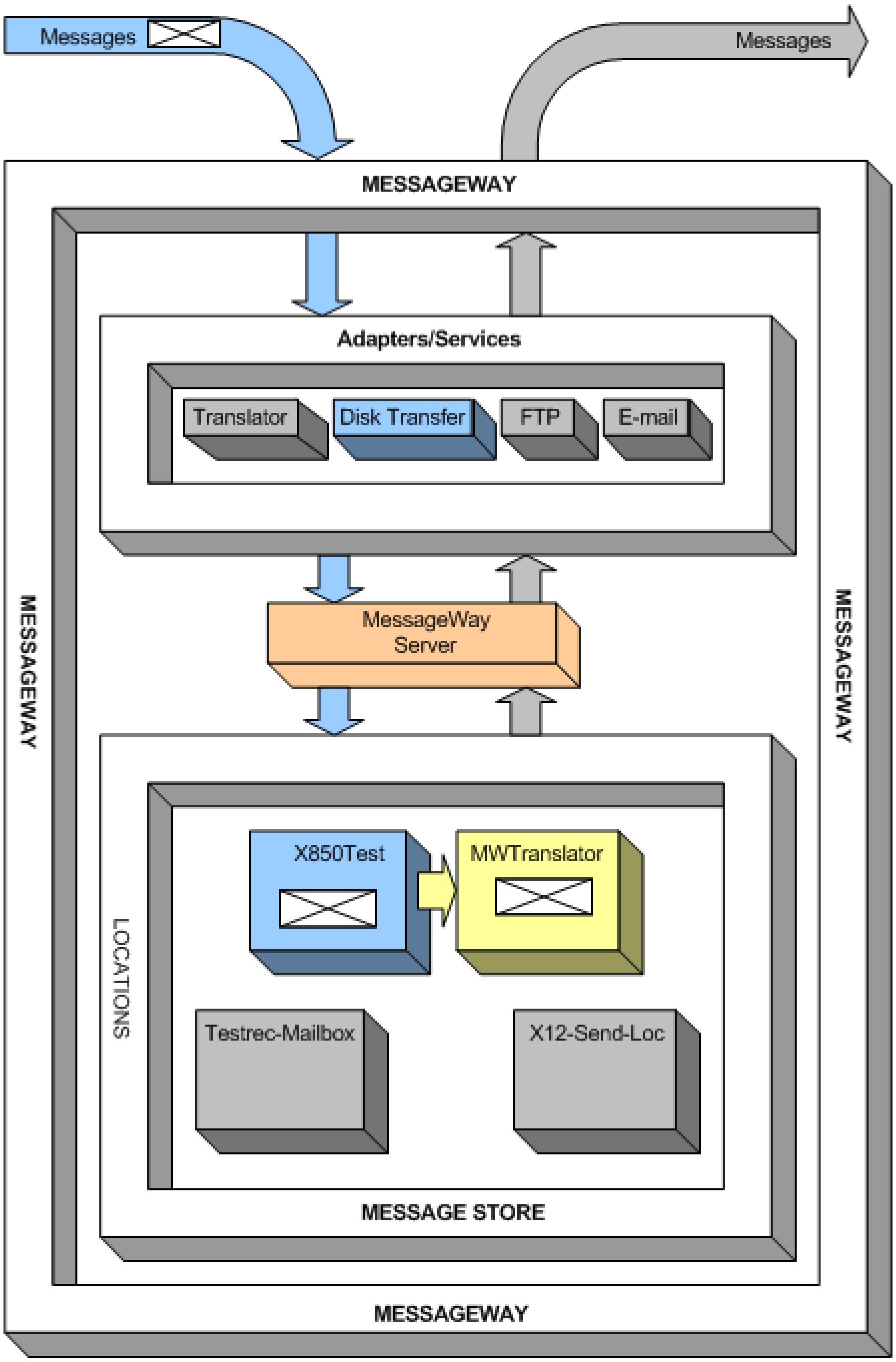
- Blue indicates input function
- Yellow indicates output function
- Green indicates both input and output functions
- Gray indicates the entity is not performing a function

The process is as follows:

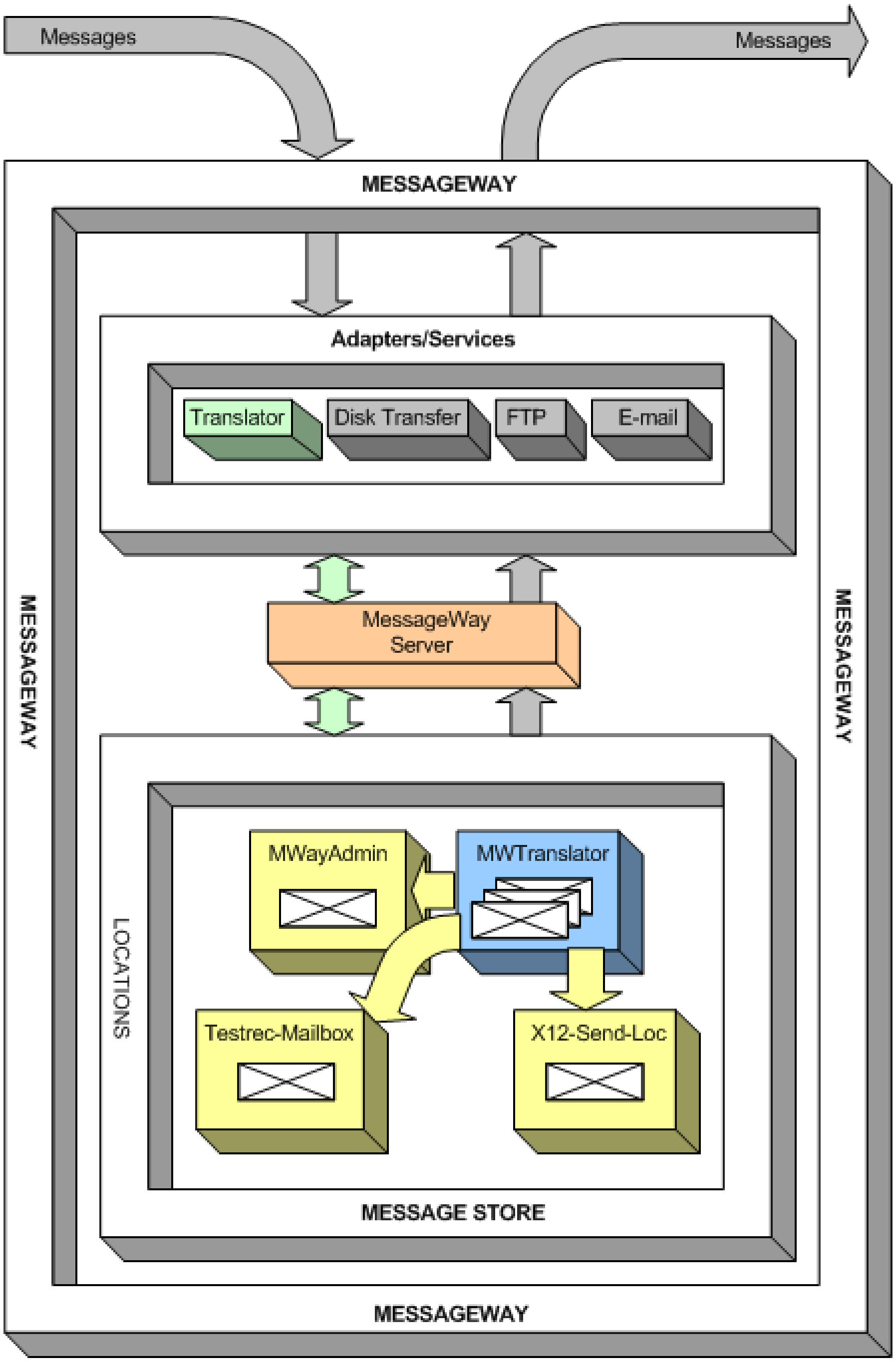
- Disk Transfer adapter moves X12 850 message from disk and delivers it to the MWTranslator service location.
- MWTranslator service location moves X12 850 message to Translator Runtime Module (TRM), TRM processes the X12 850 message producing 3 output messages, and the MWTranslator service location delivers the output messages as follows:
  - Proprietary documents to Testrec-Mailbox location

- X12 997 functional acknowledgment to X12-Send-Loc location
- Processing report to the MWayAdmin location

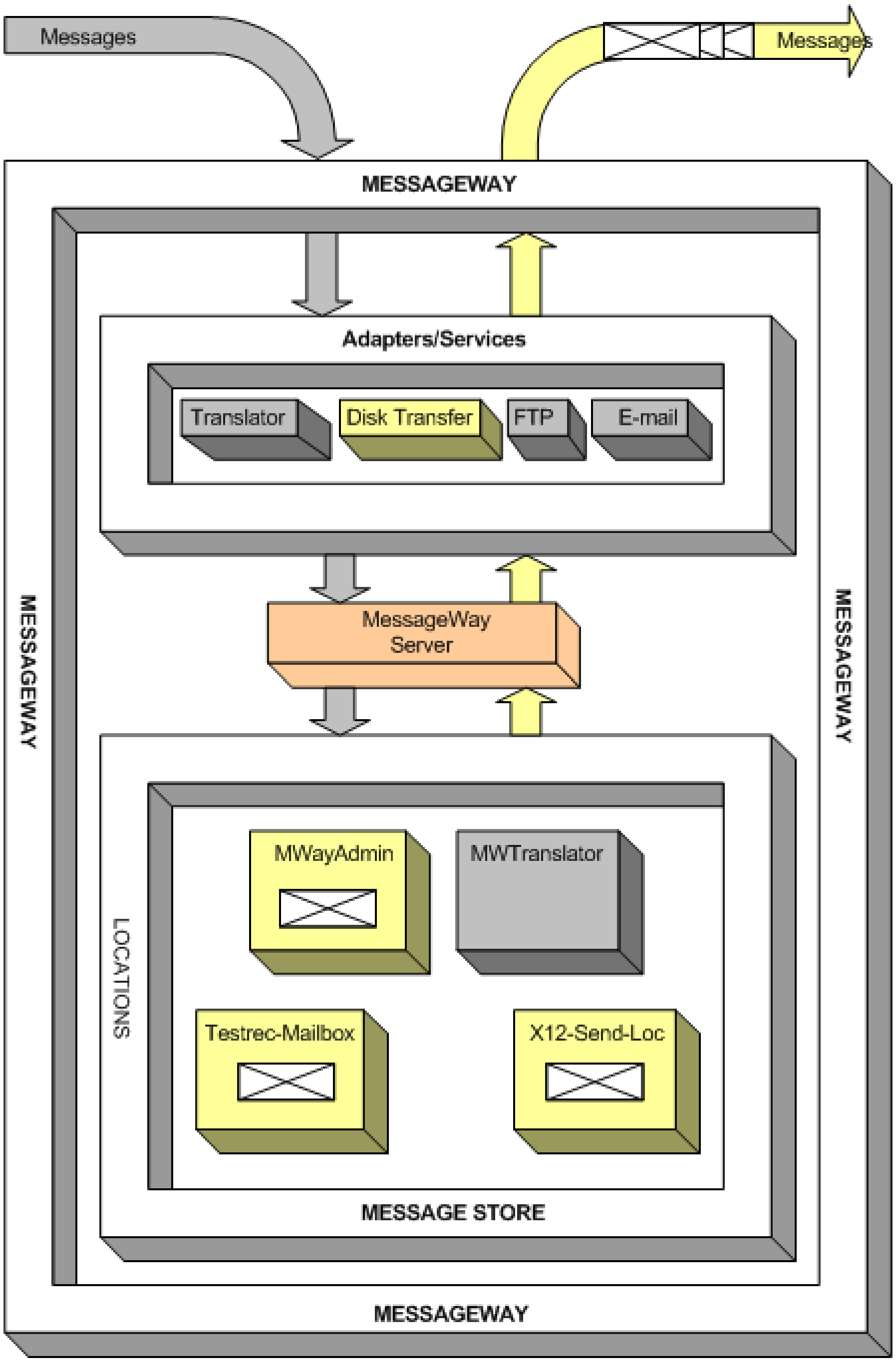
Disk Transfer adapter delivers the message to the MWTranslator service location.



Disk Transfer Adapter Delivers X12 850 Message to MWTranslator Service Location.

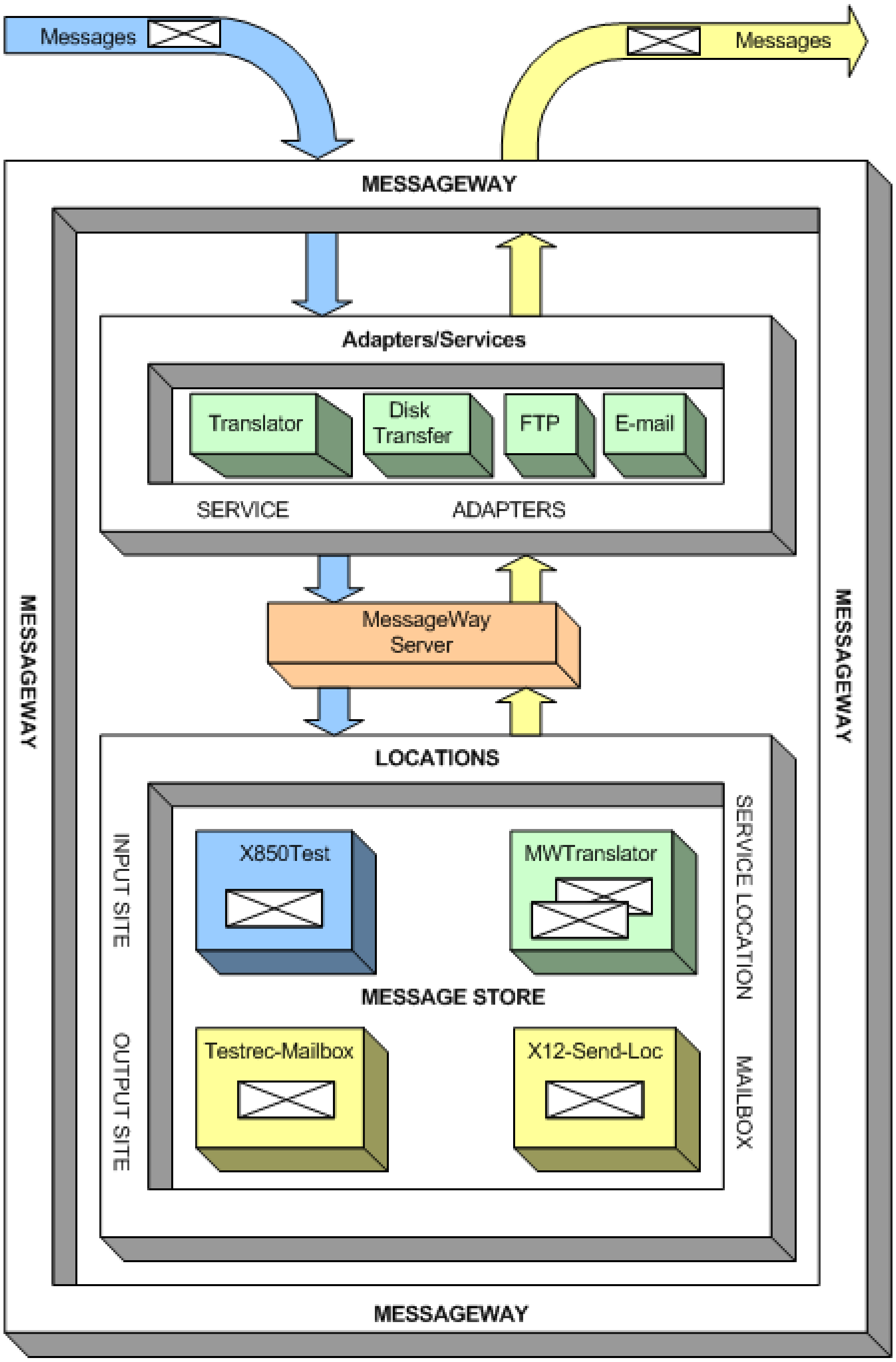


MWTranslator Service Moves X12 850 Message to Translator for Processing and Delivers Output Files to Output Locations in Message Store



Disk Transfer Adapter Moves Messages from the Message Store Locations to Disk

The following diagram gives an overview of the basic process for translation, featuring the locations used for the example installed with MWTranslator. The color schema key presents visually the flow of messaging traffic and the configurations that handle the traffic. Blue represents input data or configurations. Yellow represents output data or configurations. Green represents entities capable of both input and output.



Basic Messaging Process for MWTranslator

Processing Messages Using MWTranslator

MWTranslator processes incoming messages and routes them based on message content. Such messages may require routing only, routing and validation, or translation. MWTranslator also provides EDI processing. MWTranslator configurations determine the type of processing that is to be done and the destination of the message output.

When MessageWay sends messages to the translator, the translator must determine the source or input location in order to identify the standard of the input message so it can parse the message, as follows:

- If the source location that MessageWay specifies exists as a Standard ID location defined in MWTranslator, the translator searches the wrapper definitions in the location for a matching wrapper.
- When MessageWay does not specify a location, or if the location MessageWay specifies does not exist as a Standard ID location defined in MWTranslator, the translator searches the <Default> location for a matching wrapper.

The following table shows how MessageWay determines the source of the message, which varies depending on the adapter or service used to deliver the message.

Input Adapter or Server	Source	Notes
AS2 Server (option)	AS2 server AS2-From address on the AS2 message.	Default For messages that are signed, this value uniquely matches part of the sender's private key subject.
AWS S3 Adapter (option)	MessageWay (Name of AWS S3 input location)	Default
	MessageWay (Site Properties window **AWSS3 Input** tab **Sender** box)	Overrides default location
Custom IO Adapter	MessageWay (Name of Custom IO input site)	Default
	Text file (Script that contains status file with optional name of source location)	Overrides default location
Custom Processing Service	MessageWay (Name of original input location that sent message to custom processing service location)	Default
	Text file (Script that contains status file with name of source location)	Overrides default location

Input Adapter or Server	**Source**	**Notes**
Disk Transfer Adapter	MessageWay (Name of Disk Transfer input site)	Default
	MessageWay (Site Properties window **Disk Input** tab **Sender** box)	Overrides default location
Distribution List Adapter	MessageWay (Name of original input location that sent message to distribution list service location)	Default
	MessageWay (Service Location Properties window, Distribution List Recipients box, Sender (opt.) column)	Overrides default location
E-mail Adapter	E-mail server (Name of sender's e-mail account and e-mail address passed from the e-mail server)	Default
	MessageWay (Site Properties window **POP3** tab **Sender** box)	Overrides default location
FTP Adapter	MessageWay (Name of FTP input location)	Default
	MessageWay (Site Properties window **FTP Input** tab **Sender** box)	Overrides default location
FTP Server	MessageWay (User Properties window **Locations** tab, **Default Location** box)	Default
MQ Adapter (option)	MessageWay (Name of MQ input location)	Default
	MessageWay (Site Properties window **MQ Input** tab **Sender** box)	Overrides default location

Input Adapter or Server	Source	Notes
Rules Processing	MessageWay (Name of original input location that sent message to rules service location)	Default
	MessageWay (Process Rule window, **Action** tab, **Sender** box)	Overrides default location
SFTP Adapter	MessageWay (Name of SFTP input location)	Default
	MessageWay (Site Properties window **SFTP Input** tab **Sender** box)	Overrides default location
SFTP Server	MessageWay (User Properties window **Locations** tab, **Default Location** box)	Default
Translation Service (option)	MWTranslator (Sender's location, which is source location of output as determined by MWTranslator configurations)	Used when translation output is routed back to MWTranslator

Translation Logging and Reconciliation Information

The MessageWay Manager allows users to collect information about messages for logging and reconciliation. Logging provides information about outgoing messages generated by MWTranslator. Reconciliation provides the ability to reconcile responding acknowledgments with the outgoing messages. Users control this feature by running the Logging and Reconciliation servers, which they can start manually from the **Servers** folder in MessageWay Explorer.

When MWTranslator generates output files from a translation process, it logs information to the message database. EDI users who receive acknowledgments in response to messages they send to their trading partners have the option to track these responding acknowledgments. MWTranslator will reconcile the acknowledgments it receives from a trading partner with the original document sent to the trading partner. This information is also contained in the message database. The MW Translator Operator program interface allows users to query the message database by outbound document and to determine which documents have been reconciled. For more information about the MWTranslator logging and reconciliation process and the MW Translator Operator program capabilities, refer to the *MW Translator Operator Guide and Reference*.

Logging and Reconciliation of Acknowledgments

The Logging and Reconciliation servers provide optional services for translator processing. The Logging Server logs the output documents created by MWTranslator. The Reconciliation Server reconciles incoming acknowledgments from trading partners that respond to the logged output documents that you originally sent to those partners. This powerful feature provides automatic reconciliation for a process that can be unwieldy when done manually.

The configuration process for documents is explained in the *MW Translator Workbench User's Guide and Reference*. The configuration process to enable reconciliation is explained in the *MW Translator Operator Guide and Reference*.

To query the logged and reconciled information, you must use the Query function in the MW Translator Operator program. For more information refer to the online help for that program, or the *MW Translator Operator Guide and Reference*.

Requirements for Logging and Reconciliation

Auditing allows the Translator Runtime Module (TRM) to write information about outgoing documents to audit files, which will be logged to the MessageWay database. For MessageWay to collect and process audit information that may or may not be reconciled, the following must happen:

- In the MW Translator Operator Program, **Enable Logging** or **Enable Reconciliation** must be checked on the **Server Options** tab of the Options for MessageWay window (this sets parameters in the MessageWay configuration file)
- (Reconciliation only) In the MW Translator Workbench, the output documents must be configured to expect acknowledgments
- MWTranslator must translate data and produce output
- Supporting MessageWay processes must be running

The following MessageWay processes should be running:

Component	Windows Service	UNIX/Linux Startup Scripts
MessageWay Messaging Server	MessageWay	messageway
MessageWay Translation Service	MWTranslator	MWTranslator
MessageWay Logging Server	MWLogging	MWLogging
MessageWay Reconciliation Server	MWRecon	MWRecon

IMPORTANT: The MessageWay Reconciliation Server is only required if you are doing reconciliation. If you are only tracking output documents and not going to reconcile the responding inbound acknowledgments with the original output documents, you only need the MessageWay Logging Server, and not the MessageWay Reconciliation Server.

Understanding the Audit and Reconciliation Process in MessageWay

IMPORTANT: Both Logging and Reconciliation must be enabled for MW Translator and the servers must be running.

The data collection process is as follows:

1. For each translation, the TRM writes audit information in a temporary audit file with a name of *.AUD in the following location, depending on your platform:

Windows	C:\Messageway/server/MWTranslator/temp
UNIX/Linux	/var/opt/messageway/server/MWTranslator/temp

2. After writing the temporary audit file on disk, the TRM also writes a pointer to the file in the LogControl table of the MessageWay database.
3. The Logging Server reads the record from the LogControl table, processes information from the temporary audit file and writes the processed information to the Documents, FunctionalGroups and Interchanges and Messages tables in the MessageWay database.
4. Upon successful completion of task 3, the Logging Server deletes the associated records in the LogControl table and the *.AUD files on disk.

IMPORTANT: If the Logging Server is not running when translation occurs, the audit files will accumulate in the temporary subdirectory. When the server is restarted, it transfers the information to the MessageWay database and then cleans up the audit files.

To Start Translator Logging and Reconciliation Services

To start these MessageWay Translator services immediately, proceed as follows:

1. ***Start MessageWay on Windows*** (on page 32)

   - or -

   Start MessageWay on UNIX or Linux (on page 29).
2. From the MessageWay Manager, in the left pane of MessageWay Explorer, select the **Servers** folder.
3. In the right pane:
   a) To start the logging server, select **MWLogging**, and then click the **Start** button in the task bar.
   b) To start the reconciliation server, select **MWRecon**, and then click the **Start** button in the task bar.

To start these MessageWay Translator services automatically when MessageWay starts, proceed as follows:

1. ***Start MessageWay on Windows*** (on page 32)

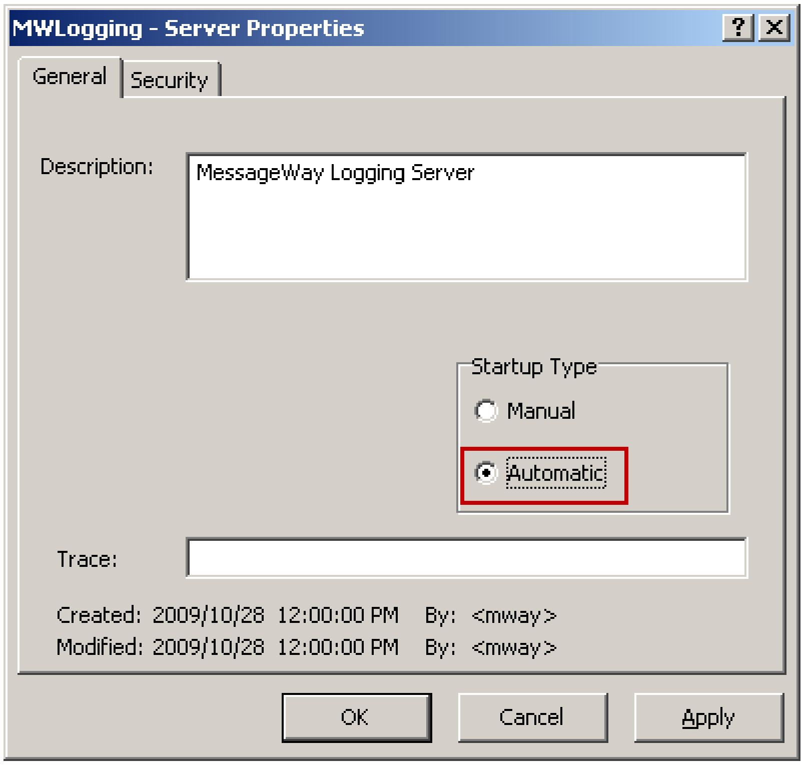
   - or -

   Start MessageWay on UNIX or Linux (on page 29).
2. From the MessageWay Manager, in the left pane of MessageWay Explorer, select the **Servers** folder.
3. To track outbound documents generated by MWTranslator, configure MWLogging as follows:

a) In the right pane, right-click **MWLogging** and then click **Properties** from the menu.

The Server Properties window appears.

b) From the **General** page, select **Automatic**, and then click **OK**.



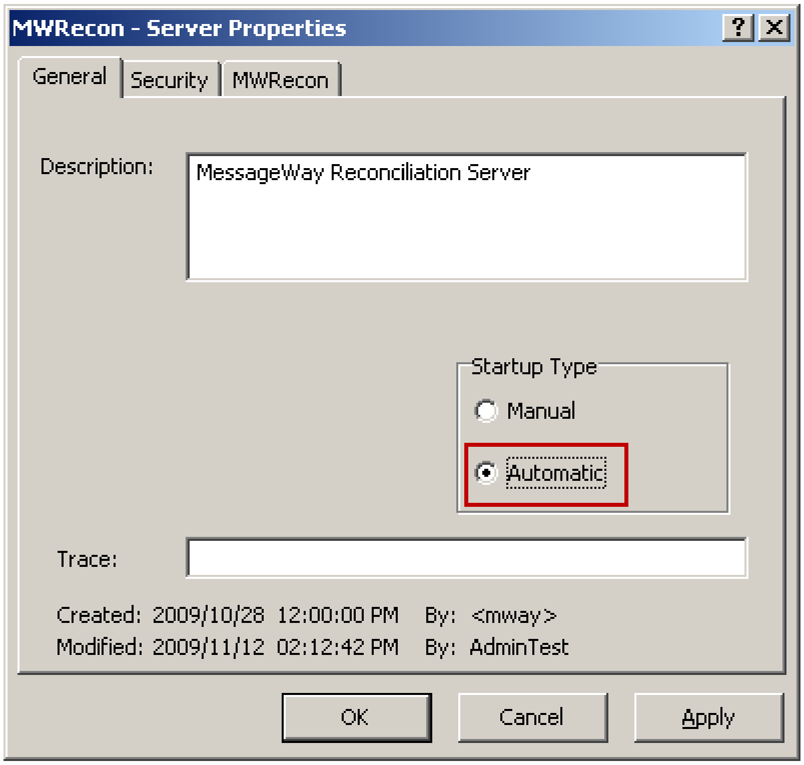
MWLogging - Server Properties
?
General
Security
Description:
MessageWay Logging Server
Startup Type
○ Manual
● Automatic
Trace:
Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/10/28 12:00:00 PM By: <mway>
OK
Cancel
Apply

4 To also reconcile incoming acknowledgments with documents generated by MWTranslator, configure MWRecon as follows:

a) In the right pane, right-click **MWRecon** and then click **Properties** from the menu.

The Server Properties window appears.

b) From the **General** page, select **Automatic**, and then click **OK**.



Description: MessageWay Reconciliation Server

Startup Type

○ Manual

● Automatic

Trace:

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/12 02:12:42 PM By: AdminTest

IMPORTANT: The logging server must be running and logging outbound messages tagged for reconciliation for the Reconciliation Server to be able to reconcile incoming acknowledgments. Thus, the Logging Server should always be started when the Reconciliation Server option is started. To track outbound documents only, do not start MWRecon.

The next time you start MessageWay, these services will be started.

Maintaining Logcontrol Table and Temporary Audit Files

The Logging Server maintains the Logcontrol table in the MessageWay SQL database, and after populating the Documents, FunctionalGroups and Interchanges tables, it removes the temporary audit files that are created by MWTranslator. These temporary audit files used by the Logging Server are created in different locations depending on the platform, as follows:

System	Location of Configuration File
Windows	**\MessageWay\server\***server name***\temp\**
UNIX/Linux	**/var/opt/messageway/server/***server name***/temp**

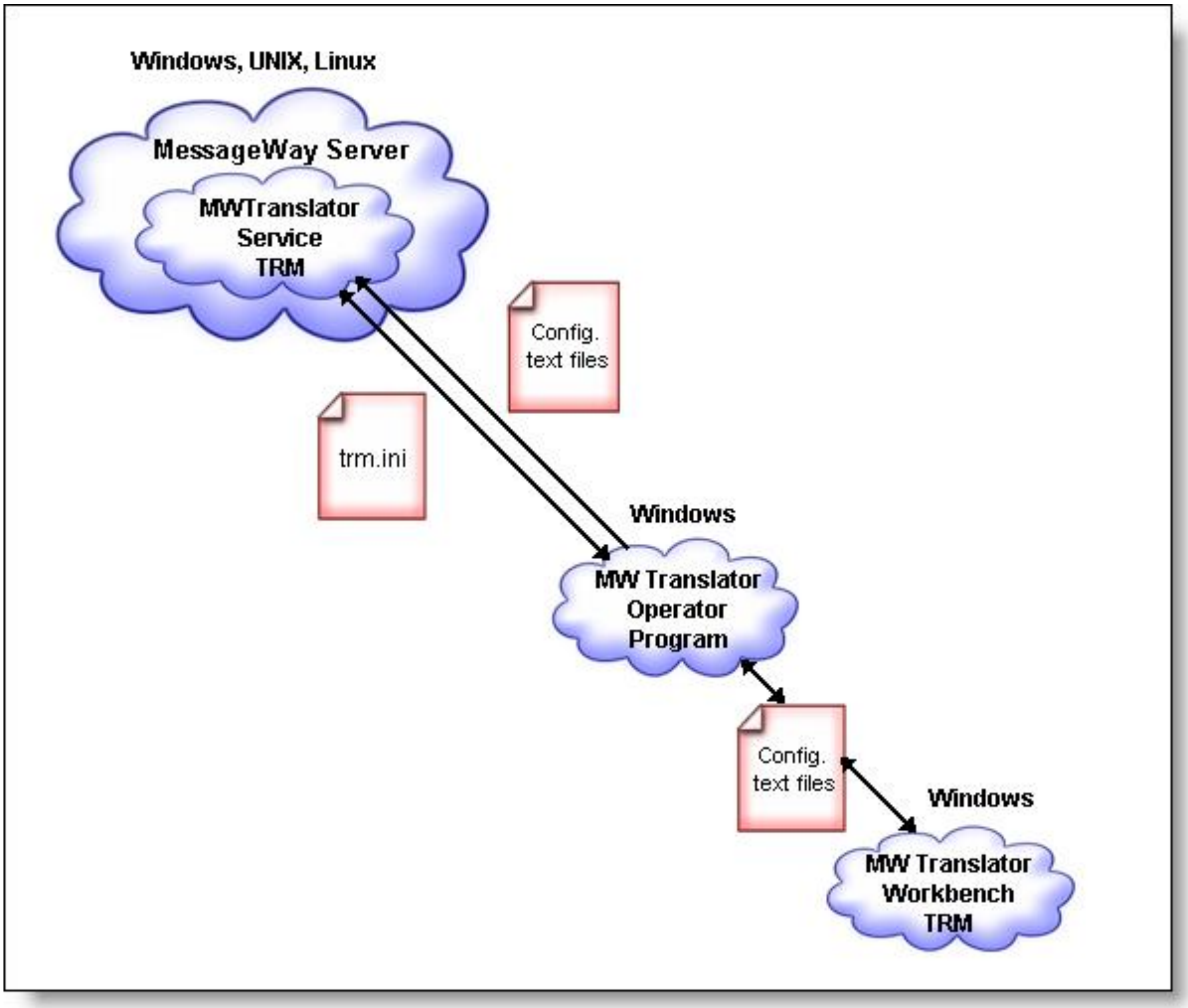
To maintain the Logcontrol table and remove the audit files, ***start the Logging Server*** (on page 911).

Transferring MWTranslator Configuration Information to MessageWay

Once you have fully tested your configurations on the MW Translator Workbench, you will transfer the configuration text files to MessageWay using the Operator Program. The text files are stored in ../MessageWay/server/MWTranslator/cfg.

For more information, refer to the MW Translator Operator Program online help or the *MW Translator Operator Program User's Guide and Reference*. The information transferred from the Operator Program to the Translator Runtime Module (TRM) running under MessageWay includes:

- Configuration text files created when you issue the **Generate** command in the Workbench or the Operator Program
- Changes to the TRM configuration file, trm.ini



MessageWay Manager Menus, Tools and Tasks

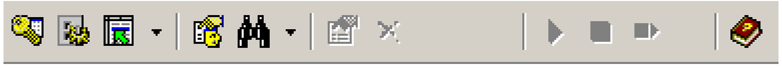
This section contains reference information about the general features of the MessageWay Manager interface, such as the tool bars, menus and task icons. Reference information about all windows are in the MessageWay Manager Reference section.

MessageWay Manager Toolbar

The task buttons available on the toolbar vary as users select different entities.

Basic Options on MessageWay Manager Toolbar

The following figure shows you the default toolbar task buttons.



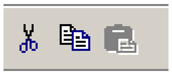
Basic Options on MessageWay Manager Toolbar

Icon	Description
	Logon allows you to log on to MessageWay. It first disconnects the current user, if any.
	Options allows you to specify the MessageWay server to which you want to connect.
	Select Environment allows you to select or create a new pointer to a different MessageWay database environment.
	Edit user policies allows you to modify policies that apply to all users.
	Find allows you to search for messages, locations, location schedules, receipt schedules, rules, keys, users or sessions.
	Properties allows you to view information about the currently selected object where appropriate.
	Delete allows you to delete the current object, where appropriate.

Icon	Description
▶	Start allows you to start the MessageWay Server on a Windows system, or an adapter or service.
■	Stop allows you to stop the MessageWay Server on a Windows system, or an adapter or service.
■▶	Restart allows you to restart an adapter or service.
📖	Help provides extensive user and reference information about MessageWay.

Edit Options on MessageWay Manager Toolbar

The following buttons appear when MessageWay definitions are selected that may be copied, such as locations.



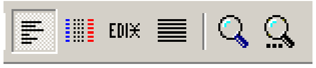
Edit Options on MessageWay Manager Toolbar

Icon	Description
✂	Cut allows you to remove objects that can be copied, such as locations, to the clipboard.
⎘	Copy allows you to copy objects, such as locations, to the clipboard. You can only copy selected locations, not entire folders or directories. Whether you copy locations in the Locations folder or in the File System folder, the copy acts only on the selected locations.
📋	Paste allows you to place what is on the clipboard in the current location

IMPORTANT: The affect on access rights is different depending on whether you do a copy and paste or a cut and paste/move. When you copy and paste an existing object (location, rules profile or key), MessageWay will remove all access rights that have been inherited from the object’s current parent folder and update all inherited access rights from the object’s new parent folder. When you cut and paste/move an existing object (folder, location, rules profile or key), MessageWay will retain all access rights that have been inherited from the object’s current parent folder. To update the inherited access rights to those of the object’s new parent folder, for each user and group on the list, you must first clear the Inherit new users/groups box and then recheck the box. After moving a folder, the access rights must be correctly updated for the folder itself and for all of its offspring (sub-folders, locations, rules profiles and keys).

Message Display Options on MessageWay Manager Toolbar

These buttons appear when the text of a message is displayed:



Message Display Options on MessageWay Manager Toolbar

Icon	Description
≡	*Text* displays data in normal text mode.
⋮	*Hex* displays data as both hexadecimal and ascii text
EDI	*EDI* displays text using segment terminators and release characters for line breaks.
☰	*Fixed* displays text using the column width.
🔍	*Find* allows you to find an occurrence of specified characters in the text.
🔍	*Search again* allows you to find another occurrence of the text specified in the **Find** dialog box.

Menus and Task Icons

The following tables describe the menu structure for the MessageWay Manager with an explanation of what the commands do and any associated icons for specific tasks that you might be able to select from the toolbar.

Adapters/Services Menu

The following commands appear on the **Adapters/Services** menu, which appears when the **Adapters/Services** folder or a specific adapter or service is selected from MessageWay Explorer.

Command	Shortcut	Icon	Description
Start		▶	Starts an adapter or service.
Stop		🟥	Stops an adapter or service.
Restart		🟥▶	Stops and then starts an adapter or service when it is running. This process rereads the adapter or service configuration files, so use this to make new configurations take effect.
Suspend		menu	When an adapter or service is running, suspends all new activity (sends, receives, polls), allowing current activity to complete processing.
Resume		menu	When an adapter or service is suspended, changes status to running and continues activity. This does not reread configuration files, so use this to continue processing as before.

Edit Menu

The following commands appear on the **Edit** menu, which appears when users select definitions that may be copied.

Command	Shortcut	Icon	Description
Cut	**Ctrl+X**	✂	Copy and then delete the selected definition to move it to a new location by using a subsequent **Paste** command.
Copy	**Ctrl+C**	📄	Copy the selected definition. You can only copy selected locations, not entire folders or directories. Whether you copy locations in the Locations folder or in the File System folder, the copy acts only on the selected locations.
Paste	**Ctrl+V**	📋	Paste a copied or cut definition. The definition may then be renamed.

IMPORTANT: The affect on access rights is different depending on whether you do a copy and paste or a cut and paste/move. When you copy and paste an existing object (location, rules profile or key), MessageWay will remove all access rights that have been inherited from the object's current parent folder and update all inherited access rights from the object's new parent folder. When you cut and paste/move an existing object (folder, location, rules profile or key), MessageWay will retain all access rights that have been inherited from the object’s current parent folder. To update the inherited access rights to those of the object’s new parent folder, for each user and group on the list, you must first clear the Inherit new users/groups box and then recheck the box. After moving a folder, the access rights must be correctly updated for the folder itself and for all of its offspring (sub-folders, locations, rules profiles and keys).

File Menu

The following commands appear on the **File** menu.

Command	Shortcut	Icon	Description
Logon			Displays the Logon to MessageWay window. When a user is already logged on, this command first logs that user off of all systems in the environment.
Logoff *user*| *system*			On a single-system environment, this logs the current user off MessageWay. On a multi-system environment, this logs the current user off all systems in the environment.
Select Environment			Select another MessageWay environment.
Options			Displays Connection Options window information required to make a connection to one or more MessageWay servers within an environment.
User Policies			Allows you to modify policies that apply to all users.
Properties			Displays properties page of selected entity.
Rename			Rename the current selection. This is shaded if the action is inappropriate.
Delete			Deletes entities selected in the MessageWay Explorer window.
Exit			Exits the MessageWay Manager.

Help Menu

The following commands appear on the **Help** menu.

Command	Shortcut	Icon	Description
Contents			Displays the help file.

Command	Shortcut	Icon	Description
About MessageWay Manager			Displays the copyright and version information for the MessageWay Manager.

Locations Menu

The following commands appear on the **Locations** menu, which appears when the **Locations** folder or a specific location is selected from MessageWay Explorer.

Command	Shortcut	Icon	Description
Show Messages			Displays all messages originally sent to this destination location in a message list window. It includes messages originally sent to this location but redirected to another location. The list shows all message contents stored as files on disk or in the database. Disk files are always located in the directory associated with the original destination, not any redirected destinations.
Show Dependent Messages			Provides a message list containing all messages that depend on the selected location. This is similar to **Show Messages** but also includes messages that were created in the location but were later redirected to a different location. Use this command to find all messages that must be deleted in order to delete the location.
Hold Messages			Places a location on hold, which prevents all messages queued to that location from being processed.
Release Messages			Releases a location from hold, which allows queued messages to be processed or delivered.
Hold Outputs			Places all output messages sent from a service location on hold, which prevents the messages from being delivered.
Release Outputs			Releases all output messages sent from a service location from hold, which allows the messages to be delivered.
Execute Now			Appears only for custom processing service locations. It generates a trigger message that is sent to the location, which initiates a script. This overrides closed schedules and locations on hold.
Input Now			Allows users to receive messages through an input location immediately, which overrides polling, closed schedules and locations on hold. This option is disabled when rescan time is used.
Add Folder			Allows users to add a folder to locations.

Command	Shortcut	Icon	Description
Add Location			Allows users to add a location, within a folder or not.
Add Distribution List			Allows users to add a distribution list in order to broadcast messages to multiple locations.
Create Receipt Schedule			For the Receipt Monitor option, this allows users to create a schedule to check the receipt of messages.

Messages Menu

The following commands appear on the **Messages** menu, which appears when a specific message is selected from a message list.

Command	Shortcut	Icon	Description
View			View the content of the message, assuming you have proper security.
Get Related Messages			Shows all messages associated by MWTranslator processing, notification or Rules Service processing. Related messages share the same Input Message ID (Message Properties window).
Get Linked Messages			Shows all messages associated by resubmitting or redirecting actions or by Rules Service processing. Linked messages share the same data content and the same Original Message ID (Message Properties window).
Resubmit Message			Resubmits to the original location a message that is in error, has been processed, or has been sent.
Redirect Message			Redirects to a different location a message that is queued, is in error, has been processed, or has been sent.
Release Message			Releases selected messages from hold.
Restart Receive Message			Attempts to receive a message again after the message failed the receipt process. Messages that fail receipt have a status of *Receive Error*.
Cancel Message			Cancels further processing including delivery of selected messages, including queued messages. Canceled messages have a status of *Error*.
Select Columns...			Select the information you want to display for messages. Message ID is mandatory, but you may select/deselect any other options.

Command	Shortcut	Icon	Description
Save Window Layout			Allows you to save the display setting for future message queries.
Modify Retention Date			Allows users to change the retention date of selected messages.
Change Priority			Allows users to change the priority of selected messages.
Mark for Archive			Sets the **Retention Time** to **Ready for Archive** action. These messages will be archived and then deleted. Use this to override the archive attributes set for the destination location.
Mark for Deletion			Sets the **Retention Time** to **Ready for Delete** action. These messages will be deleted and not archived. Use this to override the archive attributes set for the destination location.
Properties			Displays properties of selected message.

Search Menu

The following commands appear on the **Search** menu. The first two are active when the Messages window displays the content of a message, and the others are available to find object definitions.

NOTE: For a multi-system environment, when you use the *Find* options, MessageWay searches across all systems that are currently selected in the System Monitor.

Command	Shortcut	Icon	Description
Find		🔍	Displays Find dialog box to search the content of a displayed message.
Search Again	**F3**	🔍	Searches the content of the displayed message using previously entered criteria.
Find Archive Messages			Opens the Find Archive Messages window to search for messages that have been archived based on specified criteria. In a multi-system environment, searches across all systems that are currently selected in the system monitor.
Find Messages			Opens the Find Messages window to search for messages based on specified criteria. In a multi-system environment, searches across all systems that are currently selected in the system monitor.
Find Locations			Opens the Find Locations window to search for messages based on specified criteria.

Command	Shortcut	Icon	Description
Find Location Schedules			Opens the Find Location Schedules window to search for locations schedules based on specified criteria.
Find Receipt Schedules			Opens the Find Receipt Schedules window to search for receipt schedules based on specified criteria.
Find Rules			Opens the Find Rules window to search for rules based on specified criteria.
Find Keys			Opens the Find Keys window to search for client keys based on specified criteria.
Find Users			Opens the Find Users window to search for users based on specified criteria.
Find Sessions			Opens the Find Sessions window to search for current sessions by user name, IP address, or connection type. The drop-down list may not show all connection types. If you type a Connection Type rather than select one from the list, it must match the name recognized by MessageWay, for example **WEB**. The names are case-insensitive.
Find Logs			Opens the Find Audit Logs, Find Event Logs, or Find Trace Logs window to search for log entries based on date of entry or other properties.

View Menu

The following commands appear on the **View** menu. Except for System Monitor, which is visible all the time, the other monitor commands appear when your current environment includes more than one system, and the formatting options appear when the Messages window displays the content of a message. Only *System Monitor* appears for single-system environments, such as *Default*.

Command	Shortcut	Icon	Description
System Monitor			Displays statistical information about services and input and output adapters for the entire environment below the toolbar. When the environment is a multi-system environment, these numbers are combined values from all systems you are currently monitoring, which is determined by the choice you make from the group below and whether or not you are connected to the system. For example, *Monitor all Systems* for a 2-system environment shows the totals from both systems, but *Monitor tracks Explorer* depends on how many systems you currently have selected in the left pane of the MessageWay Explorer window.

Command	Shortcut	Icon	Description
Monitor all Systems			Shows combined statistics for all systems in your multi-system environment to which you are logged on. This also affects what is returned with a Find query.
Monitor tracks Explorer			Shows combined statistics for all systems in your multi-system environment to which you are logged on and that you currently have selected in the left pane of the MessageWay Explorer window. This also affects what is returned with a Find query.
Monitor *system*			Shows statistics for this system in your multi-system environment to which you are logged on. You will have one entry for each system. This also affects what is returned with a Find query.
Text		≡	Displays the content of a message in text mode using CR/LF characters for line breaks. Does not display non-printable characters.
Hex		⁞⁞⁞	Displays the content of a message in hexadecimal and ASCII characters.
EDI		EDI	Displays the content of a message using segment terminators and release characters for line breaks. Displays locations of non-printable characters.
Fixed		☰	Displays the content of a message in text mode using an 80-character column width.

Window Menu

The following commands appear on the **Window** menu.

Command	Shortcut	Icon	Description
Arrange All			Arranges all open windows in cascading format.
Close All			Closes all open configuration windows, not including the MessageWay Explorer window.
Minimize All			Minimizes all open windows, including the MessageWay Explorer window.
Current windows			Lists all open windows, with a check mark next to the current window.

MessageWay Manager Reference

This section provides reference information for all fields in all windows associated with the MessageWay Manager.

Adapter or Service Properties Window

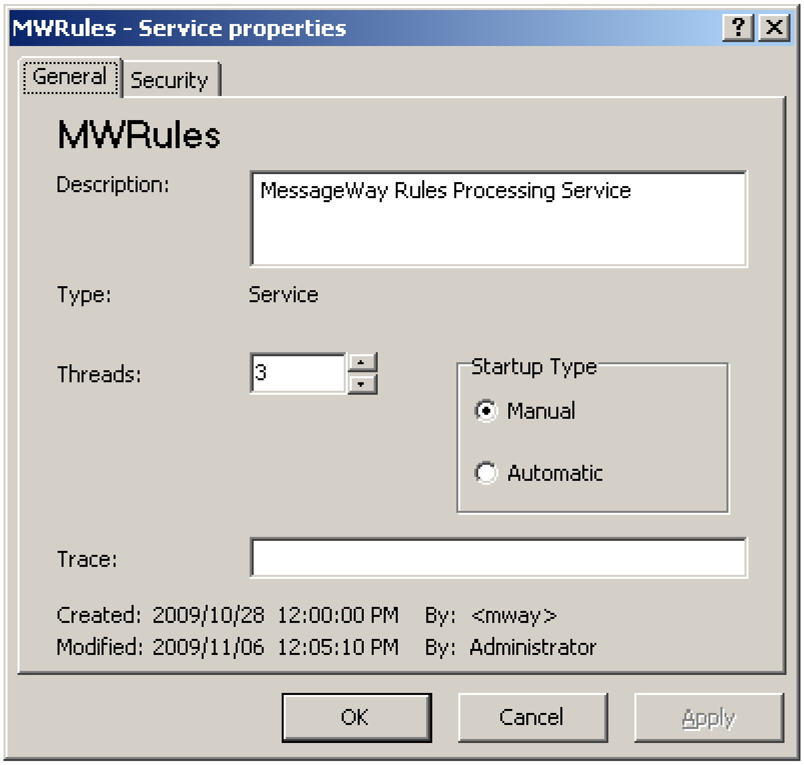
The Adapter or Service Properties window allows users to specify startup and processing parameters for an adapter or service.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

(Adapter or Service Properties) General Page

The **General** page of the Adapter or Service Properties window specifies a total number of threads to be used for simultaneous processing, expanding the processing capability. It is nearly the same for all adapters and services. There is a reserved thread for each one that processes only the highest priority messages, and it is not included in any of the thread counts. It also specifies the startup type and a trace option.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.



MWRules

Description: MessageWay Rules Processing Service

Type: Service

Threads: 3

Startup Type

● Manual

○ Automatic

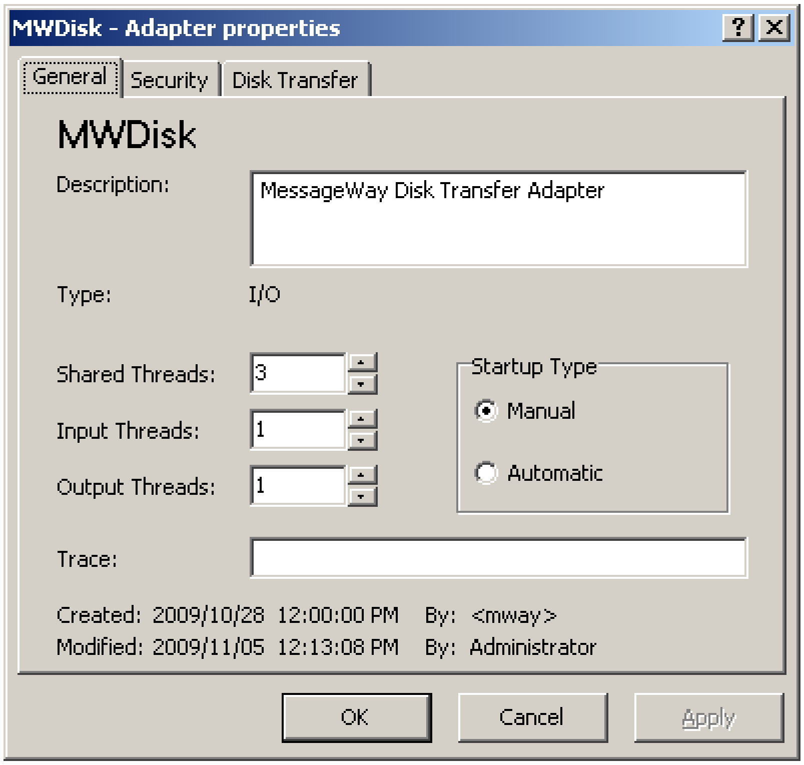
Trace:

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/06 12:05:10 PM By: Administrator

General Page, MWRules (Service Properties Window)

Additionally, the **General** page for adapters allows users to make distinctions between total shared threads, input threads, and output threads, allowing better control of the I/O resources.



MWDisk

Description: MessageWay Disk Transfer Adapter

Type: I/O

Shared Threads: 3

Input Threads: 1

Output Threads: 1

Startup Type
● Manual
○ Automatic

Trace:

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/05 12:13:08 PM By: Administrator

General Page, MWDisk (Adapter Properties Window)

Adapter or Service Name (information only)

The name of the adapter or service is assigned during installation.

Description

The description box allows users to enter text to provide information about the adapter or service. This description also appears when users place the mouse pointer over the adapter or service name on the MessageWay Explorer window.

Type (information only)

A service can process the data, changing it or not. An adapter controls the receipt and delivery of messages to and from MessageWay.

Threads

The threads are the number of threads available for parallel processing to a service. Change this value to test and determine the optimal number of threads for the operating environment. The amount of RAM, disk space, number of processors on the system and the workload all affect the assignment of threads. The reserved output thread that processes only the highest priority messages is not included in this count.

Shared Threads

The shared threads are the number of threads shared between input and output for an adapter. To ensure throughput of all priorities, at least one of the fields, Shared Threads, Input Threads, or Output Threads, should have a value of one or greater. The reserved thread that processes only the highest priority messages is not included in this count.

Input Threads

The input threads are the total number of threads for an adapter that must be used for input activity, which means either in use or in reserve. To ensure throughput of all priorities, at least one of the fields, Shared Threads, Input Threads, or Output Threads, should have a value of one or greater. The reserved thread that processes only the highest priority messages is not included in this count.

Output Threads

The output threads are the total number of threads for an adapter that must be used for output activity, which either means in use or held in reserve. To ensure throughput of all priorities, at least one of the fields, Shared Threads, Input Threads, or Output Threads, should have a value of one or greater. The reserved thread that processes only the highest priority messages is not included in this count.

Startup Type

The startup type can be either Manual or Automatic. Click **Automatic** to start the adapter or service when the MessageWay Server starts. Click **Manual** for the user to start the adapter or service.

Trace

CAUTION: The trace process may have a significant impact on performance, especially when you use the asterisk * to trace everything, and particularly for the MessageWay User Server, mwuser. Except for the MessageWay Messaging Server, tracing starts as soon as you enter your trace options and click **Apply** or **OK**. When you have finished debugging, clear the field of all text to turn off the trace. If there is an asterisk in a trace field of core or other active servers when MessageWay starts, you risk overwhelming your system with trace activity.

This option specifies the type of activity to log to the MessageWay database for the adapter or service. Then you can filter and view the information online or send it to a file using the trace utility. Enter a list of types, separated by commas, that you want to use to appear in the trace log. The types available vary by adapter or service. You may also type an asterisk (*) to trace all activity. You can limit the log information further by location, message ID, user and/or IP address.

The trace utility, mwtrace, allows you to view trace information, online or from a disk file, and to delete trace records from the database. For information about how to use the trace utility, in the Troubleshooting section, refer to the topic, ***Tracing Activity for an Adapter, Service or Server*** (on page 877).

The following table shows which types are useful for MessageWay base adapters.

Trace Type	mwdisk	mwftp	mwemail	mwcustomio	mwsftp
dirlog		OK			
functions					OK
ftp		OK			
ftp-block		OK			
ftp-data		OK			
integrity		OK			
mailboxes		OK	OK	OK	
notification*	OK				
pipe	OK	OK	OK	OK	OK
pipe-buffer	OK	OK	OK	OK	OK
polling	OK	OK	OK	OK	OK
pop3			OK		
queue	OK	OK	OK	OK	OK
queue-input	OK		OK	OK	OK
rescan	OK	OK			OK
sftp					OK
sftpdata					OK
smtp			OK		
socks					OK
ssl		OK			
startup	OK				
tcp		OK	OK		OK
wip	OK	OK	OK	OK	OK
worker				OK	

The following table shows which types are useful for MessageWay optional adapters.

Trace Type	mwas2	mwmq	mwawss3
as2	OK		
awss3			OK

Trace Type	mwas2	mwmq	mwawss3
debug			OK
error			OK
fatal			OK
http	OK		
httpbody	OK		
info			OK
mailboxes		OK	
mq		OK	
pipe	OK	OK	
pipe-buffer	OK	OK	
polling		OK	
progress			OK
queue	OK	OK	
queue-input		OK	
tcp	OK		
trace			OK
warn			OK
wip		OK	

*Note that the notification type is only available for Windows systems that use event-driven polling. It is not available for UNIX/Linux systems.

The following table shows which types are useful for MessageWay base services.

Trace Type	mwcompress	mwcustomproc	mwdistlist	mwrules
pipe	OK	OK	OK	OK
pipe-buffer	OK	OK	OK	OK
queue	OK	OK	OK	OK
route				OK

The following table shows which types are useful for MessageWay optional services.

Trace Type	mwconvert	mwtranslator
pipe	OK	OK

Trace Type	mwconvert	mwtranslator
pipe-buffer	OK	OK
queue	OK	OK

Best Practice

The trace option can impact performance. Only use it to debug a problem, such as when customer support asks for a trace. Use the minimum amount of tracing required. To turn off tracing, remove the tokens from the field. Use the utility, **mwtrace**, to delete the trace records from the database.

Created

Created is the date and time this adapter or service was created.

By (Created)

The system service itself creates this value, which appears in angle brackets, < >, to distinguish it from a MessageWay user.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

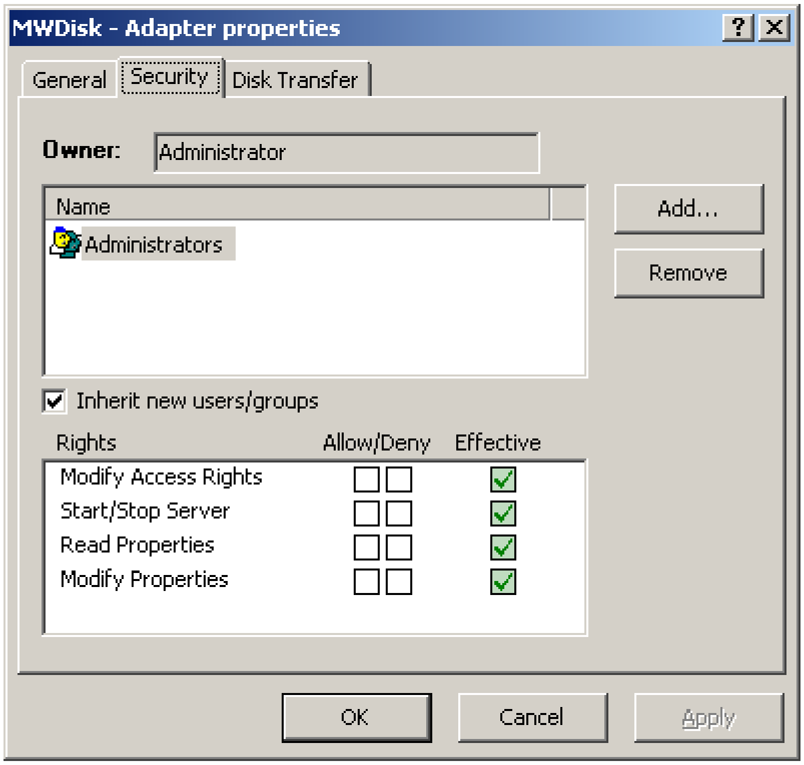
This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

(Adapter or Service Properties) Security Page

The **Security** page of the Adapter or Service Properties window shows the owner of the adapter or service, which users or user groups are allowed access to the adapter or service and what actions these users or user groups may perform.

Access to an adapter or service is controlled by an access list, which consists of a list of users or user groups and the rights that each one has. The adapter or service may inherit users and user groups and their rights from the **Adapters/Services** folder. These rights appear in the Effective rights column when you select the user or user group in the Name box.

IMPORTANT: To perform any functions for an adapter or service, users must also have appropriate rights set on their **Rights** page of the User Properties window.



Owner: Administrator

Name
Administrators

☑ Inherit new users/groups

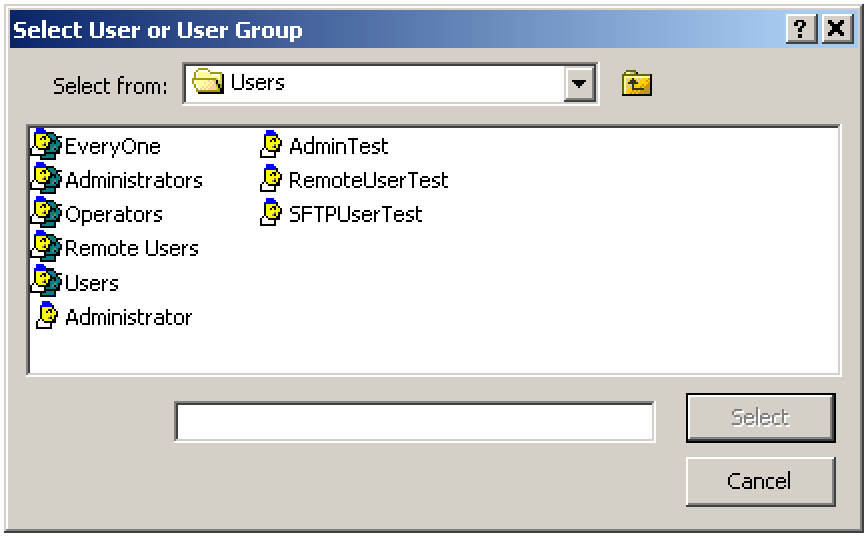
Rights	Allow/Deny		Effective
Modify Access Rights	□	□	☑
Start/Stop Server	□	□	☑
Read Properties	□	□	☑
Modify Properties	□	□	☑

Security Page (Adapter or Service Properties Window)

- To add the same users and groups and their rights as listed for the **Adapters/Services** folder, check the **Inherit new users/groups** box.
- To override inherited rights, check the appropriate boxes in the Allow/Deny columns.
- To give a user or user group access to this adapter or service:

1. Select the **Add** button.

The Select User or User Group window appears.



2. Select a group from the list or type the name of a group in the Select box, and click the **Select** button.

NOTE: The EveryOne group is on the selection list, but not on the list under the Users folder, unless someone has added it manually. This group is only available for access lists. Add this group to the list to grant access rights to all users. All users are implicitly members of the EveryOne user group. As a result, when EveryOne is added to an access list, the associated rights are granted to all users.

Owner

Initially, the owner is the user that created the adapter or service, which is always the original administrator. The owner may transfer ownership to another user. Owners have complete access rights to the adapter or service, regardless of other configurations. Owners always have the right to change the names on the access list and the right to read and change the properties of the adapter or service.

Browse Button

When you are the owner, you may select this button to give ownership to another user.

Name

The Name list contains users or user groups that are permitted to access this adapter or service. Use the **Add** and **Remove** buttons to maintain this list. The Name list and the Rights list comprise the access list used by MessageWay to determine who has what rights to this adapter or service.

Add Button

Select this button to add names of users or user groups to the Name list.

Remove Button

Select this button to delete names of users or user groups from the access list.

Inherit new users or groups

Check this box to add any users or user groups that are on the Name list of of the **Adapters/Services** folder to the Name list of this adapter or service. To remove users or user groups from the list that have been inherited from the **Adapters/Services** folder, you must clear this box first.

Rights

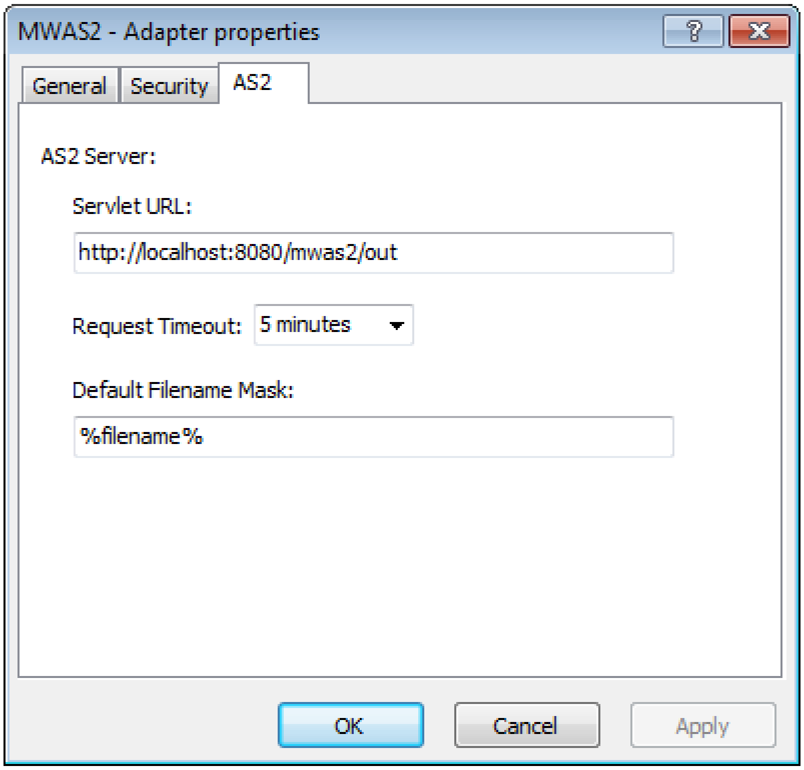
The Rights list contains the functions that the users or user groups in the Name list may perform. The Rights list and the Name list compose the access list to determine who has what rights to this adapter or service. Adapters or services may inherit rights from the **Adapters/Services** folder. These rights appear in the *Effective rights* column when you select the user or user group in the Name list. Check the Allow/Deny boxes to override these effective rights. To check or clear all rights at once, hold **SHIFT** while you click one of the boxes.

The rights for an individual adapter or service are as follows:

Right	Description
Modify Access Rights	Change values on **Security** page of the Adapter or Service Properties window. Also requires the right, **Read Properties**.
Start/Stop Adapter or Service	Start, stop, suspend or resume an adapter or service. Also requires the rights, **Read Properties**.
Read Properties	View the statuses of the adapters or services. Also requires the rights, **Read Properties**. When this is unchecked, users cannot access the Adapter or Service Properties window for that adapter or service.
Modify Properties	Change properties for the adapter or service, such as thread distribution, startup options and security. Also requires the rights, **Read Properties**. When this is unchecked, users may still be able to access the Adapter or Service Properties window, but the properties are dimmed.

(AS2 Adapter Properties) AS2 Page

The MessageWay AS2 adapter provides outbound AS2 client services to an AS2 server. The **AS2** page of the Adapter Properties window allows users to specify the address to connect to the AS2 client, which is the AS2 Outbound Servlet and a default timeout value that is applied to all new sites.



AS2 Server:

Servlet URL: http://localhost:8080/mwas2/out

Request Timeout: 5 minutes

Default Filename Mask: %filename%

NOTE: The MessageWay AS2 server and the AS2 adapter require a license from Progress. For more information, contact MessageWay Technical Support.

Servlet URL

This required field identifies the location of the outbound servlet. The values are case-sensitive. Type the Web address of the AS2 outbound servlet. For example, if the servlet is on the same system as the AS2 adapter, you might type, http://localhost:8080/mwas2/out. If the servlet is on a different machine than the AS2 adapter, you might type, http://192.168.0.4:8080/mwas2/out.

Request Timeout

Select or type the amount of time in seconds, minutes or hours to allow the AS2 outbound processing cycle to complete. This is a default value for AS2 sites, which users can override by selecting a Request Timeout value for a site.

The elapsed time of the AS2 outbound processing cycle starts when the AS2 Outbound Servlet posts the AS2 message to the recipient and ends when the AS2 Outbound Servlet receives the response indicating that the AS2 message has been received. When an MDN is not required, the response is a returned HTTP status code, where a success code would be in the 200 range. When an MDN is required, the response is the returned MDN.

Ensure enough time to receive a response. If a response is not returned within the timeout limit, the message will be placed in an error state. The error description will appear on the **Error** tab of the Message Properties window for the message.

To allow the AS2 Outbound Servlet to time out before the AS2 adapter times out, the adapter adds 15 seconds to the configured timeout value to use as its timeout limit when a response has not been received from the AS2 Outbound Servlet.

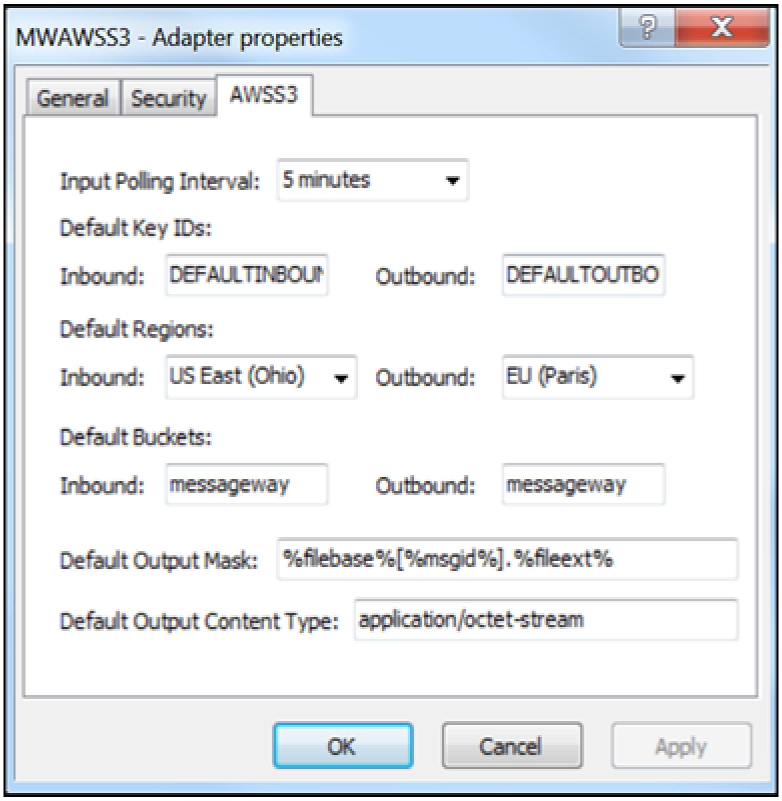
Default Filename Mask

This is a template to create a file name for the output file. For new installations, the default mask is **%filebase%[%msgid%].%fileext%**. This mask generates unique names using the MessageWay message ID, which is enclosed in square brackets, [ ]. This avoids sending files that might be rejected because the file name already exists at the remote location. To change this default mask, use any combination of constants and MessageWay tokens. You may override this default for a specific location. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name.

(MWAWSS3 Adapter Properties) AWSS3 Page

The **AWSS3** page of the Adapter Properties window contains the configuration information required for the inbound polling service of the adapter, the default key ids, regions and buckets for both inbound and outbound sites, as well as default output mask and default output content type. Location schedules determine whether the adapter polls for files for individual locations, and the schedule for a location must be open to allow polling.

NOTE: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.



Input Polling Interval: 5 minutes

Default Key IDs:

Inbound: DEFAULTINBOUN Outbound: DEFAULTOUTBO

Default Regions:

Inbound: US East (Ohio) Outbound: EU (Paris)

Default Buckets:

Inbound: messageway Outbound: messageway

Default Output Mask: %filebase%[%msgid%].%fileext%

Default Output Content Type: application/octet-stream

AWSS3 Page (Adapter Properties Window)

NOTE: The MessageWay AWSS3 adapter requires a license from Progress. For more information, contact MessageWay Technical Support.

Input Polling Interval

The input polling interval is used for the transfer of messages from an AWSS3 bucket into MessageWay. This is the amount of time that the AWSS3 client will wait before checking the bucket for files to transfer to the site. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

Select an interval from the list or type the number of hours, minutes or seconds between polling cycles. The option **Never** stops polling for this adapter. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

CAUTION: Polling causes a LIST request to be sent to AWS. Since there is a charge in AWS for a LIST request, setting a lower polling interval can cause excessive charges to be incurred. For example, if there are several hundred AWS S3 inbound locations all configured to poll at 5 second intervals, excessive charges may be incurred. When possible, set polling to hours or minutes, not seconds.

The **Schedule** option requires that the schedule type be *Trigger (Input or Execute Now)*, which polls at the time specified. You identify the schedule on the **Schedule** tab, and from there you can drill down to create or edit a schedule item.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds
30m	means 30 minutes
2 h	means 2 hours

(Default Key IDs) Inbound

Enter your AWS Identity and Access Management (IAM) access key id value for inbound transfers here. This key, along with your AWS IAM secret access key (not configurable on adapter, only location), allow you to control and secure your AWS S3 account. Key ID can be found on your AWS S3 IAM account by selecting **My Security Credentials**, then choosing **Get Started with IAM Users**, then clicking on User name followed by **Security Credentials**. This key is equivalent to user id in some applications.

(Default Key IDs) Outbound

Enter your AWS Identity and Access Management (IAM) access key id value for outbound transfers here. This key, along with your AWS IAM secret access key (not configurable on adapter, only location), allow you to control and secure your AWS S3 account. Key ID can be found on your AWS S3 IAM account by selecting **My Security Credentials**, then choosing **Get Started with IAM Users**, then clicking on User name followed by **Security Credentials**. This key is equivalent to user id in some applications.

(Default Regions) Inbound

Click the down arrow to the right of the **Inbound** field and select the appropriate AWS region name for inbound transfers. To reduce data latency in your applications, AWS offers multiple independent world-wide regional endpoints to make your upload requests from. Typically you would select a region closes to your physical location. A region is equivalent to a server in some applications.

(Default Regions) Outbound

Click the down arrow to the right of the **Outbound** field and select the appropriate AWS region name for outbound transfers. To reduce data latency in your applications, AWS offers multiple independent world-wide regional endpoints to make your download requests to. Typically you would select a region closes to your physical location. A region is equivalent to a server in some applications.

For your reference, following is a list of valid AWS regions:

Region Name	Region
US East (Ohio)	us-east-2
US East (N. Virginia)	us-east-1
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Tokyo)	ap-northeast-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Osaka-Local)	ap-northeast-3
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Canada (Central)	ca-central-1
China (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1
EU (Frankfurt)	eu-central-1
EU (Ireland)	eu-west-1
EU (London)	eu-west-2
EU (Paris)	eu-west-3
South America (São Paulo)	sa-east-1

(Default Buckets) Inbound

Enter your AWS bucket value for inbound transfers here. Bucket values are case-sensitive. Buckets in AWS are used to store objects, which consist of data and any metadata that describes the data. A bucket is equivalent to a disk drive in some applications.

(Default Buckets) Outbound

Enter your AWS bucket value for outbound transfers here. Bucket values are case-sensitive. Buckets in AWS are used to store objects, which consist of data and any metadata that describes the data. A bucket is equivalent to a disk drive in some applications.

Default Output Mask

CAUTION: Make sure you have a value in the **Default Output Mask** field. The install process provides a value, but if a user subsequently clears the field, messages may fail delivery attempts.

This is a template to create a file name or object name for outbound transfers. Use any combination of constants and MessageWay tokens. For new installations, the default mask is **%filebase%[%msgid%].%fileext%**. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name, for example, **MW%msgid%.txt**.

Use two percent (%) signs to enclose the tokens. MessageWay replaces the tokens with appropriate values. Add constants outside of these signs as required.

CAUTION: When a file of the same name already exists, it will be overlaid by default. Note that file names are case-sensitive.

The valid tokens are:

Token	Description
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: MyClassID@MyLocationName To assign a class ID to a mask for a file name, type: MyClassID%yyyymmdd%.txt
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.

Token	Description
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).
inputmsgid	Input Message Id of the message.
inputname	Input Name.
location	The MessageWay location where the message resides. Replaces mailbox.
msgid	The Message Id of the message. Replaces msg.
ms	Milliseconds (000-999). NOTE: The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.
yyyy	Four digit year.

Token	Description
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

MW%msgid%.txt

TR%yyyymmddhhnnss#%.txt

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml

TIP: On systems that allow file names longer than 8 characters, use the msgid token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the filename token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

Default Output Content Type

Enter the content type value that you want to associate with a file or object created in AWS S3 here. Although this value can be any characters that you choose, following is a list of typical content types that MessageWay supports:

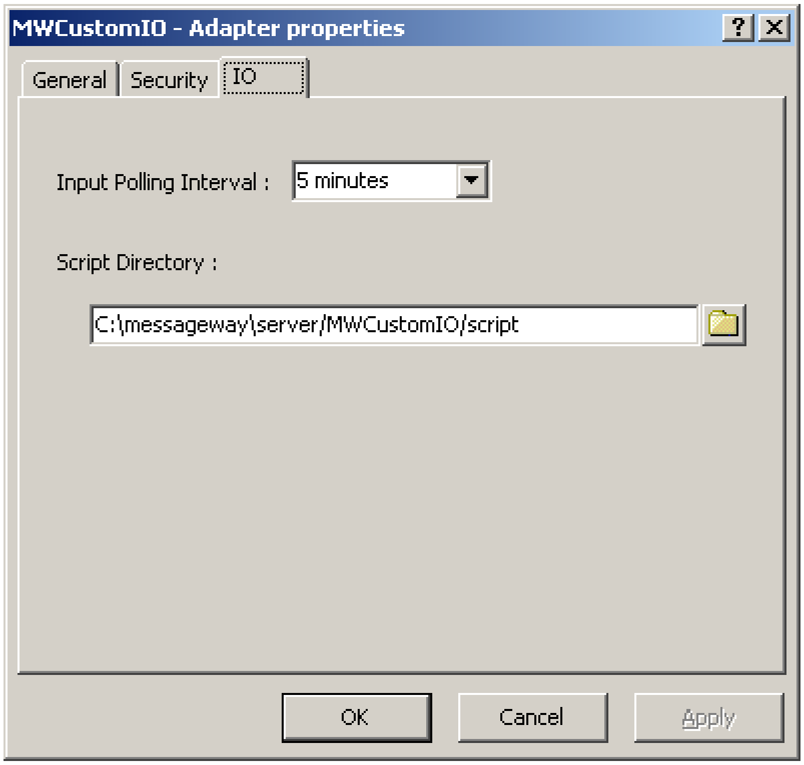
Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf

Type	Content Type	File Extension
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

(Custom IO Adapter Properties) IO Page

For the custom IO adapter, the **IO** tab of the Adapter Properties window contains a polling interval and the directory for the scripts to be run from the operating system outside of MessageWay.

IMPORTANT: To avoid complications with mapped drives, always use the full Universal Naming Convention (UNC) directory name. A Windows service should not directly access local or network resources through mapped drive letters. MessageWay servers, which includes MWTranslator, run as Windows services.

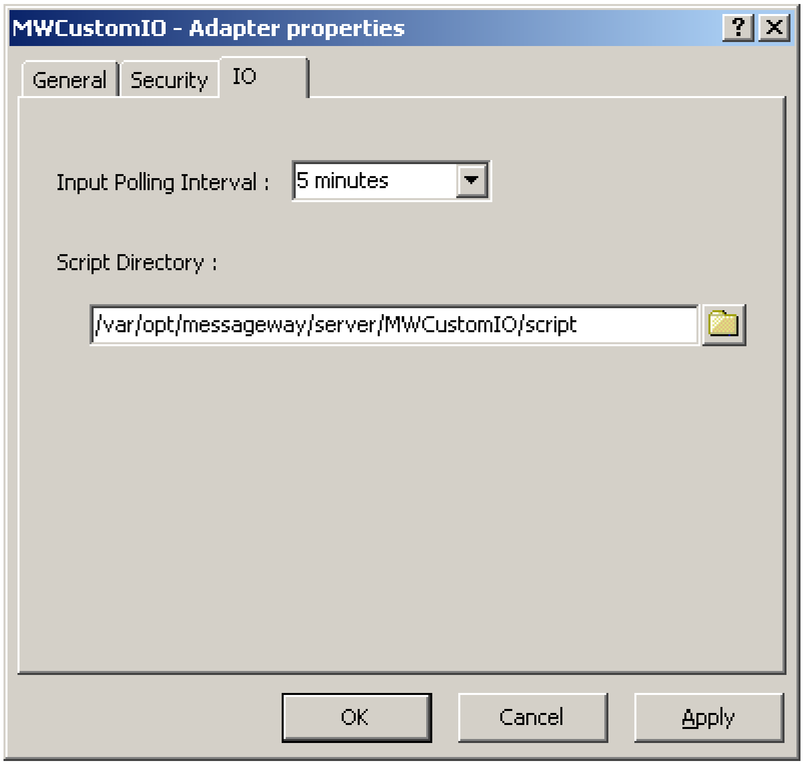


Input Polling Interval : 5 minutes

Script Directory :

C:\messageway\server/MWCustomIO/script

IO Page, Windows (Adapter Properties Window)



Input Polling Interval : 5 minutes

Script Directory : /var/opt/messageway/server/MWCustomIO/script

IO Page, UNIX/Linux (Adapter Properties Window)

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

Input Polling Interval

The polling interval is used to transfer messages into MessageWay. Enter the number of seconds, minutes, or hours that the adapter will wait before running commands or scripts specified on the **Input** tab of a Custom IO site.

Select an interval from the list. The option **Never** stops polling for this adapter. When the adapter starts, it polls all input locations whose schedules are open and it starts the poll interval timer.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds
30m	means 30 minutes
2 h	means 2 hours

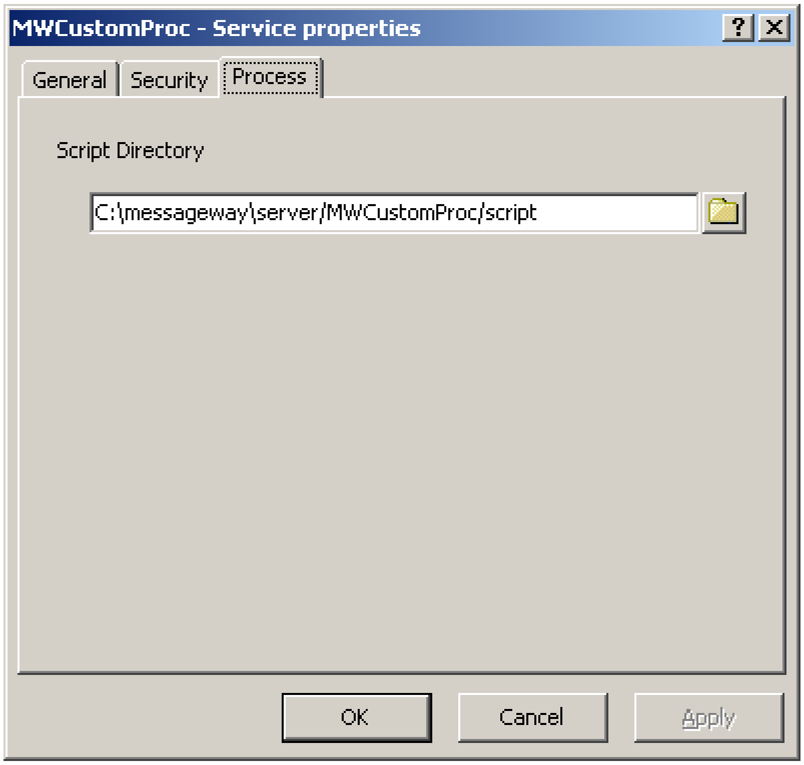
Script Directory

Select or type the default location for external scripts that are referenced from the Command field on the **Input** or **Output** page of the custom IO site. By default, scripts are stored in the /MessageWay/server/MWCustomIO/script (Windows) or /messageway/server/MWCustomIO/script (UNIX/Linux) directory of the installation directory. Do not use mapped drive letters to access network resources. Use full Universal Naming Convention (UNC) names instead.

(Custom Processing Service Properties) Process Page

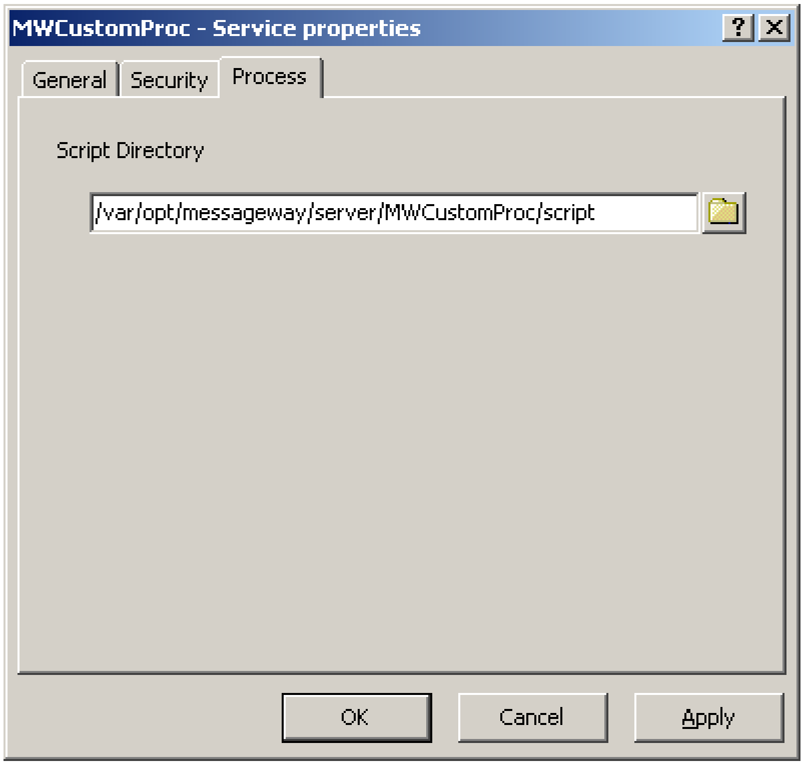
For the custom processing service, the **Process** tab of the Service Properties window defines the default directory for external scripts referenced in the **Command** field on the **Process** tab of the location properties window.

IMPORTANT: To avoid complications with mapped drives, always use the full Universal Naming Convention (UNC) directory name. A Windows service should not directly access local or network resources through mapped drive letters. MessageWay servers, which includes MWTranslator, run as Windows services.



Script Directory: C:\messageway\server/MWCustomProc/script

Process Page, Windows (Service Properties Window)



Script Directory

/var/opt/messageway/server/MWCustomProc/script

Process Page, UNIX/Linux (Service Properties Window)

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

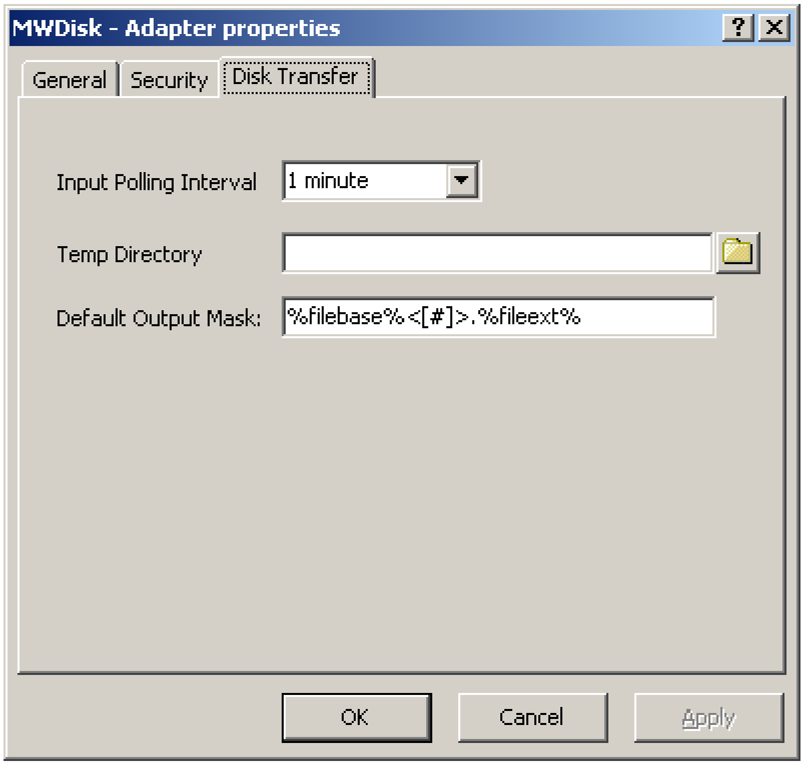
Script Directory

Select or type the default location for external scripts that are referenced from the Command field on the **Process** page of the service location. By default, scripts are stored in the /MessageWay/server/MWCustomProc/script (Windows) or /messageway/server/MWCustomProc/script (UNIX/Linux) directory of the installation directory. Do not use mapped drive letters to access network resources. Use full Universal Naming Convention (UNC) names instead.

(Disk Transfer Adapter Properties) Disk Transfer Page

For a disk transfer adapter, the **Disk Transfer** page of the Adapter Properties window allows users to specify whether input to MessageWay is event-driven using local file access (push) or achieved by polling (pull). The event-driven option is not available for remote systems, such as UNIX/Linux. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

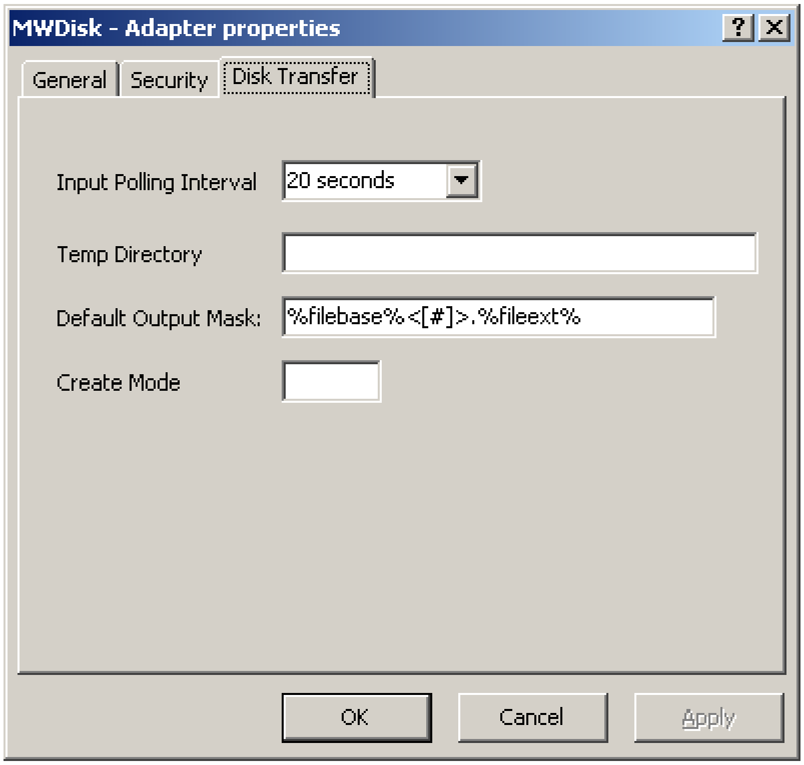


Input Polling Interval: 1 minute

Temp Directory:

Default Output Mask: %filebase%<[#]>.%fileext%

Disk Transfer Page, Windows (Adapter Properties Window)



Input Polling Interval: 20 seconds

Temp Directory:

Default Output Mask: %filebase%<[#]>.%fileext%

Create Mode:

Disk Transfer Page, UNIX/Linux (Adapter Properties Window)

Polling Interval

The polling interval is used for the transfer of messages from a local directory into MessageWay. Enter the number of seconds, minutes, or hours that the adapter will wait before checking the local directory for files to transfer. The directory to be polled and the location to which the inbound files will be transferred are on the page for the adapter of the Site Properties window. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

Select an interval from the list. The option **Event-Driven** ensures that messages are passed to MessageWay as soon as they appear in the subdirectory. Event-driven polling is not available on UNIX/Linux systems. The option **Never** stops all input for this adapter.

Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds

30m	means 30 minutes
2 h	means 2 hours

TIP: When you are using Disk Transfer to poll a location other than a LAN, make sure you allow enough time for the polling to occur without flooding the destination location with requests.

Temp Directory

To avoid files being retrieved before they are complete, MessageWay will write files to a temporary directory before it moves them to the final location. Type or select a default location where MessageWay will first write the files. Type a relative path to change the name. Type an absolute path to cause all disk locations to use the same directory.

When this is blank, MessageWay attempts to create a directory called *temp* beneath the directory location specified on the **Disk Output** page of a Disk Transfer site.

You can use this field, for example, if you want to deliver files to a directory that already has a sub-directory called temp, or if for some other reason the MessageWay user cannot create a temporary directory in the location specified in the URL for the site configuration.

CAUTION: If MessageWay finds a file already exists in this directory by the same name as the file it is attempting to rename\move from the \temp directory the rename\move of the file will fail.

Default Output Mask

This is a template to create a file name for the output file. For new installations, the default mask is **%filebase%<[#]>.%fileext%**. For upgrades from previous versions of MessageWay, the default mask remains **MW%yyyymmddhhnnss#%.dat**. To change this default mask, use any combination of constants and MessageWay tokens. You may override this default for a specific location. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name.

NOTE: The special <[#]> notation in the default file mask uses a pair of greater-than and less-than signs (< and >) to number each occurrence after the first with a numeric value beginning with 1 in square brackets, for example NewFile, NewFile[1]. Alternatively, if you were to use the normal notation [%#%] instead of <[#]>, all file names would have a number appended in square brackets, beginning with one, for example NewFile[1], NewFile[2].

The valid tokens are:

Token	Description
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: **MyClassID@MyLocationName** To assign a class ID to a mask for a file name, type: **MyClassID%yyyymmdd%.txt**
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).
inputmsgid	Input Message Id of the message.
inputname	Input Name.
location	The MessageWay location where the message resides. Replaces *mailbox*.

Token	Description
msgid	The Message Id of the message. Replaces *msg*.
ms	Milliseconds (000-999). **NOTE:** The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.
yyyy	Four digit year.
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

```
MW%msgid%.txt
```

```
TR%yyyymmddhhnnss#%.txt
```

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

```
%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml
```

TIP: On systems that allow file names longer than 8 characters, use the *msgid* token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the *filename* token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  `\ / : * ? " < > | ! & ` ' ;`

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

- Duplicate Filename values are allowed within the same location within the Locations folder.

Duplicate Filenames are *not* allowed within the same location within the File System folder, unless one has been canceled.When it generates a file, it uses the filename it received during input, where it exists. If there is no filename, it generates one. The rules vary depending on the adapter or service associated with the destination location. For more information, refer to the specific type of adapter or service location.

Create Mode

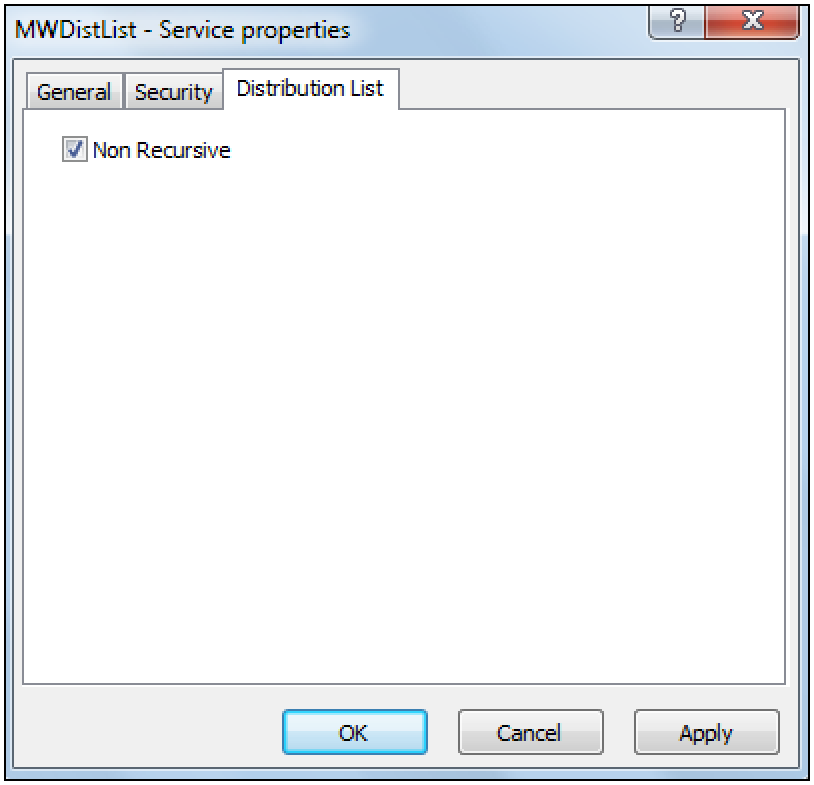
Type a 3-digit numeric value to set the default file permissions when MessageWay creates a file. You may override these settings in the properties for a disk transfer site.

Each digit may be from 0 to 7, representing permissions, from left to right, for owner/user, group, and all other users. To set the rights for each entity, add the total of the values assigned to each right, where, 4 = read (r), 2 = write (w), 1 = execute (x) and 0 = none (-). For example, 644 would give read and write (4+2=6) permissions to the owner/user, for example *mway*, and 4 would give read permissions to the group and others.

(Distribution List Service Properties) Distribution List Page

For a distribution list service, the **Distribution List** page of the Service Properties window allows users to specify whether they want to select Non Recursive or not.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select Suspend, and then after all traffic has cleared, select Stop.



Distribution List Page (Service Properties Window)

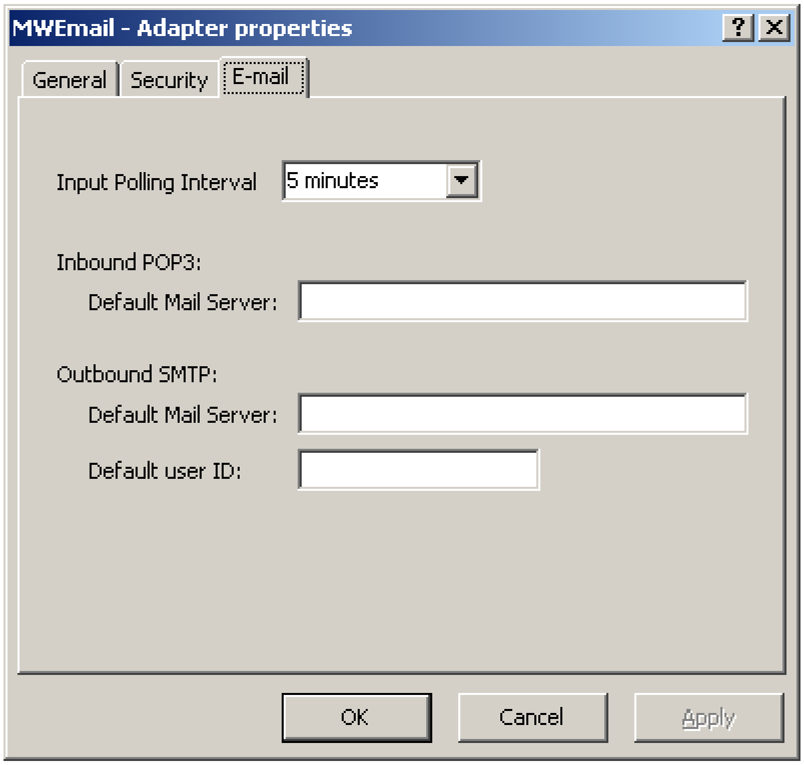
Non Recursive

This selection affects all Distribution List locations, and cannot be overridden on a location by location basis. When the **Non Recursive** box is checked, Distribution Lists will NOT evaluate recipients, but will instead create message aliases for all recipients, even those associated with another Distribution List. This will allow nested Distribution Lists to all be referenced in a 'Get Related' command, as well as any 'On Hold' or 'Closed' Distribution List status to be honored. Default is 'Recursive'.

(E-mail Adapter Properties) E-mail Page

For the e-mail adapter, the **e-mail** page of the Adapter Properties window contains the default configuration information to make inbound and outbound connections. This information may be overridden for a specific site in the Site Properties window.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.



MWEmail - Adapter properties

Input Polling Interval: 5 minutes

Inbound POP3:

Default Mail Server:

Outbound SMTP:

Default Mail Server:

Default user ID:

E-mail Page (Adapter Properties Window)

Polling Interval

The polling interval is used for the transfer of messages from a local directory into MessageWay. Enter the number of seconds, minutes, or hours that the adapter will wait before checking the local directory for files to transfer. The directory to be polled and the location to which the inbound files will be transferred are on the page for the adapter of the Site Properties window. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

Select an interval from the list. The option **Event-Driven** ensures that messages are passed to MessageWay as soon as they appear in the subdirectory. Event-driven polling is not available on UNIX/Linux systems. The option **Never** stops all input for this adapter.

Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds

30m	means 30 minutes
2 h	means 2 hours

TIP: When you are using an e-mail adapter to poll a location other than a LAN, make sure you allow enough time for the polling to occur without flooding the destination location with requests. The default of 5 minutes is probably a minimum amount of time for polling over the Internet, for example. Constant polling using any time less than five minutes might be viewed as an attack. One-second polling is only useful for testing on a local LAN.

Default Mail Server (Inbound POP3)

Enter the ID of the POP3 mail server from which to collect e-mail. This value is used as a default when users create new sites associated with this adapter.

CAUTION: When changes are made to this value, the values for all of the sites using this adapter are also changed. You can override this setting for specific sites on the **POP3** page of the Site Properties window.

Default Mail Server (Outbound SMTP)

Enter the name of the SMTP mail server from which you send e-mail. This value is used as a default when users create new sites associated with this adapter.

CAUTION: When changes are made to this value, the values for all of the sites using this adapter are also changed. You can override this setting for specific sites on the **SMTP** page of the Site Properties window.

Default User ID (Outbound SMTP)

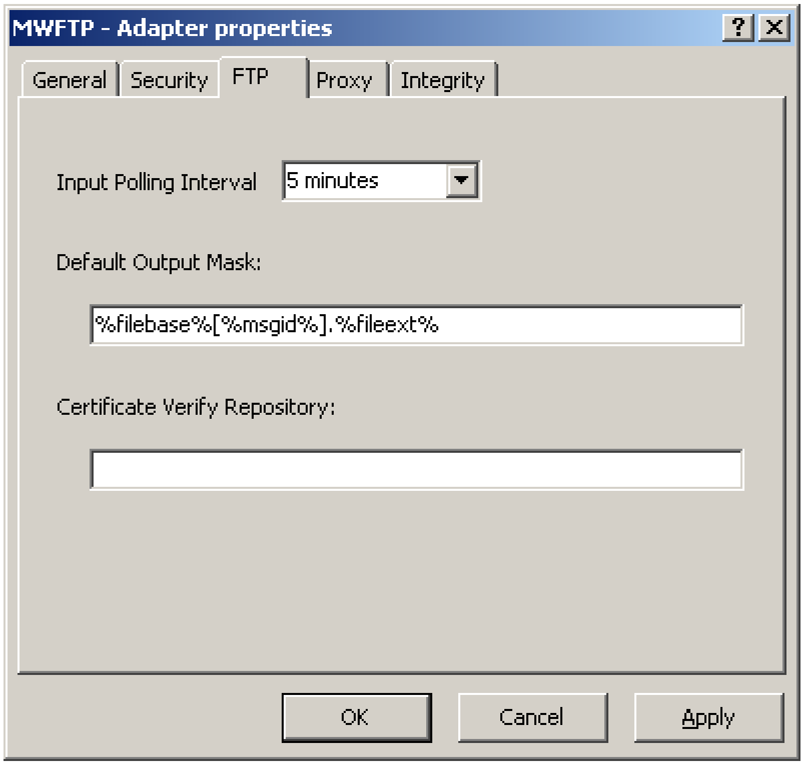
Enter the user ID required to log on to your SMTP server to send e-mail. This value may be optional depending on the server. The user ID does not include the domain name, for example **@mycompany.com**. This value is used as a default when users create new sites associated with this adapter. Adding a user ID may avoid messages being rejected because the value in the From Address is unknown to the mail server.

CAUTION: When changes are made to this value, the values for all of the sites using this adapter are also changed. You can override this setting for specific sites on the **SMTP** page of the Site Properties window.

(FTP Adapter Properties) FTP Page

The **FTP** page of the Adapter Properties window contains the configuration information required for the inbound polling service of the adapter and the default location for the SSL certificates.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.



Input Polling Interval: 5 minutes

Default Output Mask: %filebase%[%msgid%].%fileext%

Certificate Verify Repository:

Input Polling Interval

The polling interval is used for the transfer of messages from an FTP directory into MessageWay. This is the amount of time that the FTP client will wait before checking the directory for files to transfer to the site. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

The URL to be polled and the location to which the inbound files will be transferred are on the **FTP** page of the Site Properties window under **Input to MessageWay**.

Select an interval from the list or type the number of hours, minutes or seconds between polling cycles. The option **Never** stops polling for this adapter.   Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds
30m	means 30 minutes
2 h	means 2 hours

TIP: When you are using FTP to poll a location other than a LAN, make sure you allow enough time for the polling to occur without flooding the destination location with requests. The default of 5 minutes is probably a minimum amount of time for polling over the Internet, for example. Constant polling using any time less than five minutes might be viewed as an attack. One-second polling is only useful for testing on a local LAN.

Default Output Mask

This is a template to create a file name for the output file. For new installations, the default mask is **%filebase%[%msgid%].%fileext%**. This mask generates unique names, with the MessageWay message ID enclosed in square brackets, [ ]. It avoids sending files that might be rejected because the file name already exists at the remote location, unless you are resending a file with the same name as one you already sent. For upgrades from previous versions of MessageWay, the default mask remains **MW%yyyymmddhhnnss#%.dat**. For non-disk adapters, this is the same as **%filename%**. To change this default mask, use any combination of constants and MessageWay tokens. You may override this default for a specific location. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name.

The valid tokens are:

Token	Description
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: **MyClassID@MyLocationName** To assign a class ID to a mask for a file name, type: **MyClassID%yyyymmdd%.txt**
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).

Token	Description
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).
inputmsgid	Input Message Id of the message.
inputname	Input Name.
location	The MessageWay location where the message resides. Replaces *mailbox*.
msgid	The Message Id of the message. Replaces *msg*.
ms	Milliseconds (000-999). **NOTE:** The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.

Token	Description
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.
yyyy	Four digit year.
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

```
MW%msgid%.txt

TR%yyyymmddhhnnss#%.txt
```

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)

Token	Description
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

```
%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml
```

TIP: On systems that allow file names longer than 8 characters, use the *msgid* token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the *filename* token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  `\ / : * ? " < > | ! & ` ' ;`

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

- Duplicate Filename values are allowed within the same location within the Locations folder.

Duplicate Filenames are *not* allowed within the same location within the File System folder, unless one has been canceled.When it generates a file, it uses the filename it received during input, where it exists. If there is no filename, it generates one. The rules vary depending on the adapter or service associated destination location. For more information, refer to the specific type of adapter or service location, such as a disk transfer location.

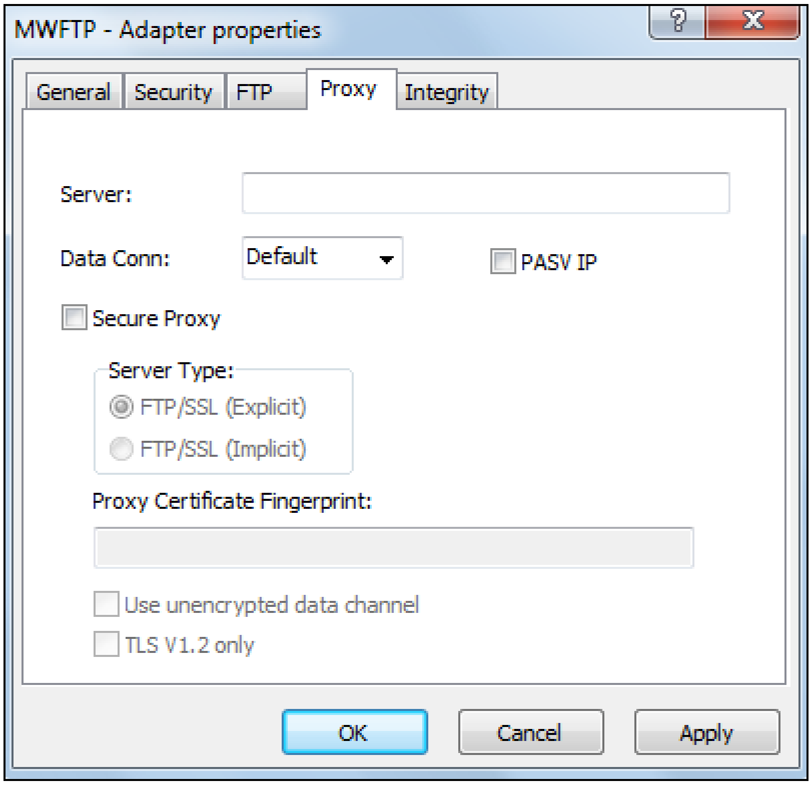
Certificate Verify Repository

Enter the full path name where the server certificates are stored. Typically, this is a certificate repository or certificate bundle. It contains the public key portion of the certificate authority (CA) certificates. This information is optional if the server certificate's fingerprint is specified on the **SSL** tab of the site configuration.

(FTP Adapter Properties) Proxy Page

By default, the FTP adapter communicates directly with an FTP server. To communicate with an FTP server through the MessageWay FTP Perimeter Server instead, you must provide information on the **Proxy** tab. The **Proxy** page allows you to specify the location of the perimeter server, the type of data connection between the adapter and the perimeter server and, if the connection is to be secure, additional security information. If you have more than one perimeter server, you can override these settings on the **Proxy** tab of the Site Properties window for an FTP site configuration.

IMPORTANT: Note that these parameters control the connection between the adapter and the FTP perimeter server. The type of connection from the perimeter server acting as a client to the external FTP server is controlled by the corresponding values on the **FTP Input** or **FTP Output** tab of the Site Properties window.



Server:

Data Conn: Default

□ PASV IP

□ Secure Proxy

Server Type:

● FTP/SSL (Explicit)

○ FTP/SSL (Implicit)

Proxy Certificate Fingerprint:

□ Use unencrypted data channel

□ TLS V1.2 only

Proxy Page (Adapter Properties Window)

Server

Type the URL of the FTP proxy server, and include the host and port. This URL will be the default for all sites using this adapter. If you have more than one proxy server, you can override this value for specific sites.

Data Connection

FTP clients determine the type of connection used with an FTP server. Since the FTP adapter is an FTP client, this is where you determine the type of default connection when the adapter connects to an FTP proxy server. Select one of the options, **Default**, **Active**, **Passive** or **Ext-Passive**, to determine how messages are sent from a site. You can override this value for specific sites.

IMPORTANT: Note that this parameter controls the connection between the adapter and the FTP proxy server. The type of connection from the proxy server acting as a client to the external FTP server is controlled by the Data Connection value on the **FTP Input** or **FTP Output** tab of the Site Properties window.

The options are as follows:

Data Connection	Description
Default	Attempt a passive connection first, and if it fails, try an active connection. This is the default behavior for MessageWay versions prior to 4.2.
Passive	Attempt a passive connection only.
Active	Attempt an active connection only.
Ext-Passive	Attempt an extended passive connection only, using IPv4 protocol. Communicates data connection endpoint information for network protocols through firewalls or network address translators (NATs). Use this extended passive command (*EPSV*) in place of the *PASV* command for FTP transfers where the control and data connection(s) are being established between the same two machines. Since the server only returns a port number, the client must assume the connection is to the same address to which it originally connected. This type of connection does not require the translation of the network address, so it also supports encrypted data.

PASV IP

Check this box to force use of the IP Address returned by a PASV response for the Proxy data channel connection.

IMPORTANT: Note that this parameter controls the data channel between the adapter and the FTP proxy server. The forcing of the IP Address returned by a PASV response of the data channel from the proxy server acting as a client to the external FTP server is controlled by the similar value on the FTP Input or FTP Output tabs of the Site Properties window.

Secure Proxy

Check this box to enable the fields that allow you to specify the parameters for a TLS/SSL session between the FTP Adapter and the FTP proxy server.This value will be the default for all sites using this adapter. If you have more than one proxy server, you can override this value for specific sites.

IMPORTANT: Note that this parameter controls the security between the adapter and the FTP proxy server. The security from the proxy server acting as a client to the external FTP server is controlled by the Secure Session check box on the **SSL** tab of the Site Properties window.

Server Type

This is the server type for the FTP adapter that connects to the FTP proxy server. This value will be the default for all sites using this adapter. If you have more than one proxy server, you can override this value for specific sites.

IMPORTANT: Note that this parameter controls the server type between the adapter and the FTP proxy server. The server type from the proxy server acting as a client to the external FTP server is controlled by the Server Type value on the **SSL** tab of the Site Properties window.

Check the Secure option that precedes, and then select the type of secure connection for the server. When the Secure option is clear, the default is non-secure FTP.

FTP/SSL (Explicit) The client connects to an unencrypted port on the server, typically 21. To connect to the MessageWay FTP perimeter server, we use 2190 to avoid conflict with other existing FTP servers. After starting a normal session, the client requests that SSL/TLS security be used, and when the appropriate handshake occurs, it sends the data.

FTP/SSL (Implicit) The client connects to an encrypted port, typically 990, and after an appropriate SSL handshake, it sends FTP commands.

Proxy Certificate Fingerprint

To use a fingerprint instead of a full certificate to authenticate the FTP proxy server, type that fingerprint here. Leave this blank if you want to authenticate the server with a full certificate. This value will be the default for all sites using this adapter. If you have more than one proxy server, you can override this value for specific sites.

IMPORTANT: Note that this parameter controls fingerprint authentication of the FTP proxy server. The fingerprint for an external FTP server is controlled by the corresponding value on the **SSL** tab of the Site Properties window.

NOTE: You specify the location of the Certificate Authority certificate bundles or repository on the **FTP** page of the FTP Site Properties window.

Use unencrypted data channel

For SSL communication, encryption can occur in the command channel (CC), the data channel (DC), or both. For SSL/implicit or SSL/explicit, users may check this box to not encrypt the data channel, that is, to use a clear data channel (CDC). This selection does not affect the command channel.

IMPORTANT: Note that this parameter controls encryption of the data channel between the adapter and the FTP proxy server. The encryption of the data channel from the proxy server acting as a client to the external FTP server is controlled by the similar value on the **SSL** tab of the Site Properties window.

TLS V1.2 only

Check this box to force use of the TLS V1.2 protocol for the connection to the Proxy.

IMPORTANT: Note that this parameter controls the connection between the adapter and the FTP proxy server. The forcing of TLS V1.2 protocol for the connection from the proxy server acting as a client to the external FTP server is controlled by the similar value on the SSL tab of the Site Properties window.

(FTP Adapter Properties) Integrity Page

A file integrity check is a component of guaranteed delivery where an FTP client and FTP server each performs a cryptographic hash of a transferred file. It allows MessageWay users to confirm that a file they uploaded to or downloaded from a third-party FTP server contains the same data on both source and destination, regardless of format. The FTP server must be able to support integrity checks.

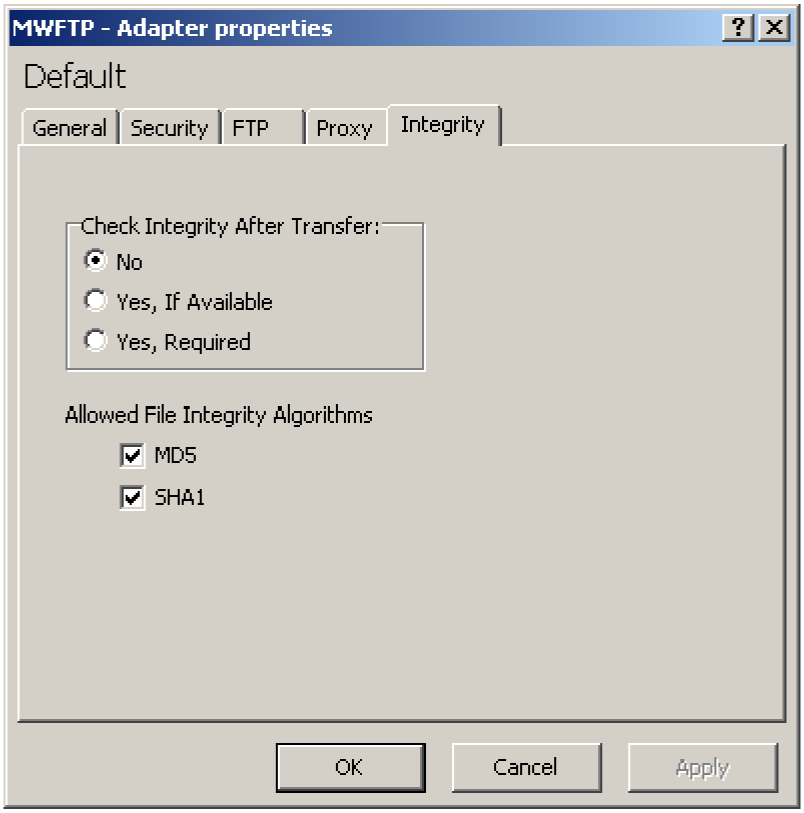
When used, the MessageWay FTP adapter calculates the hash value of a file and compares it with the value received from the server. When the values match, the hash algorithm used and the hash value appear on the **Misc** tab of the Message Properties window. When it fails, the message status is set to *Error*, and additional error information appears on the **Misc** tab.

These selections provide default values for all FTP sites, which you may override for a particular location.

The default options whether to select integrity checking after a transfer are as follows:

- No
- Yes, If Available
- Yes, Required

The algorithms that the MessageWay FTP adapter supports appear under *Allowed File Integrity Algorithms* heading. It issues a FEAT command to determine whether the server supports an algorithm and uses the strongest one that the server also supports.


MWFTP - Adapter properties

Default

Check Integrity After Transfer:
● No
○ Yes, If Available
○ Yes, Required

Allowed File Integrity Algorithms
☑ MD5
☑ SHA1

No

Select **No** to *not* check the integrity of the message. You may override this default for a specific FTP site.

Yes, If Available

Select **Yes, If Available** to check the integrity of the message when possible. MessageWay uses the strongest algorithm selected that the FTP server also supports. When the comparison of hash values succeeds, the algorithm and hash value used appear on the **Misc** tab of the Message Properties window. When the comparison of hash values fails, MessageWay marks the message with a status of *Error*, and displays the error information on the **Error** tab of the Message Properties window. When the FTP server does not support integrity checks or does not support any of the algorithms selected, the adapter does not perform an integrity check.

Yes, Required

Select **Yes, Required** to check the integrity of the message. MessageWay uses the strongest algorithm selected that the FTP server also supports. When the comparison of hash values succeeds, the algorithm and hash value used appear on the **Misc** tab of the Message Properties window. When the FTP server does not support integrity checks or does not support any of the algorithms selected, or the comparison of hash values fails, MessageWay marks the message with a status of *Error*, and displays the error information on the **Error** tab of the Message Properties window.

MD5

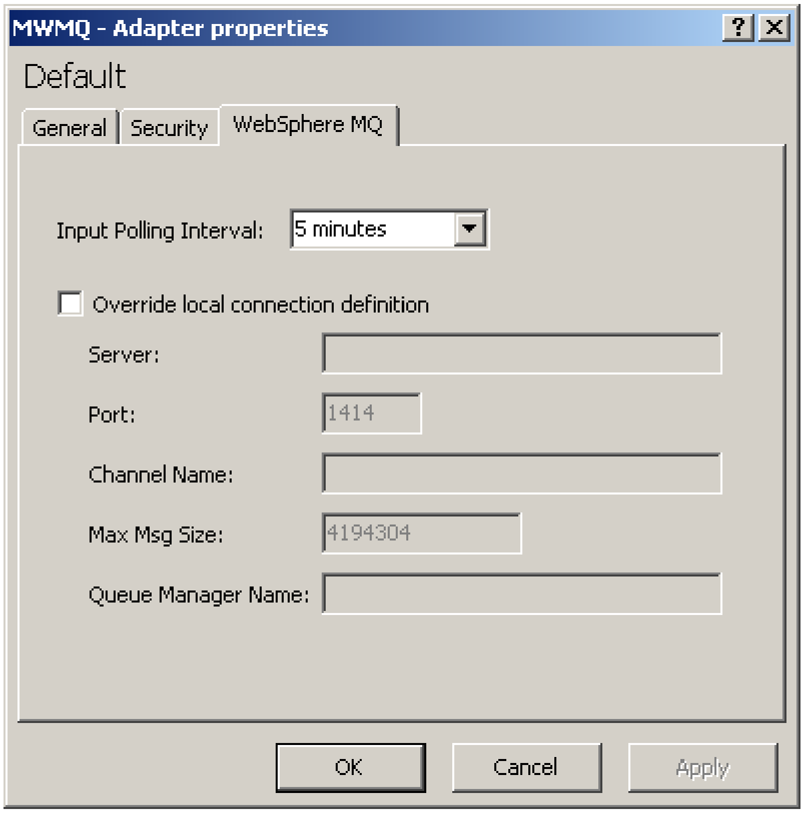
Check this box to potentially use the MD5 (Message-Digest algorithm 5) to determine the integrity of the message. This is a default for all input and output FTP locations. You may override this option for a specific location on the **Integrity** tab of the Location Properties window.

SHA1

Check this box to potentially use the SHA-1 (Secure Hash Algorithm 1) to determine the integrity of the message. This is a default for all input and output FTP locations. You may override this option for a specific location on the **Integrity** tab of the Location Properties window.

(MQ Adapter Properties) WebSphere MQ Page

The **WebSphere MQ** page of the Adapter Properties window contains the configuration information required for the inbound polling service of the adapter and other values to connect this WebSphere MQ Client to a WebSphere MQ Manager.


MWMQ - Adapter properties

Default

Input Polling Interval: 5 minutes

□ Override local connection definition

Server:

Port: 1414

Channel Name:

Max Msg Size: 4194304

Queue Manager Name:

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

NOTE: The MessageWay MQ Adapter requires a license from Progress. You must have a license in order to start the adapter. For more information, contact MessageWay Technical Support.

Input Polling Interval

The polling interval is used to transfer messages from a WebSphere MQ queue manager into MessageWay. Enter the number of seconds, minutes, or hours that the adapter will wait before checking a queue for files to transfer. The queue to be polled and the location to which the inbound files will be transferred are on the MWMQ Input page of the Site Properties window. A location configuration may override the default polling set for the adapter. Location schedules determine when the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

Select an interval from the list. The option **Never** stops all input for this adapter. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds
30m	means 30 minutes
2 h	means 2 hours

Override local connection definition

Check this box to override the default definitions for the MQ adapter. The default values in the **Port** and **Max Msg Size** fields are part of the adapter definition that was created during installation.

Server

Type the IP address or the host name where the MQ server resides.

Port

Type TCP/IP port for the MQ server.

Channel Name

Type the name of the MQI channel required to connect from the MQ adapter through the MQ client to the MQ server. The channel name must be the same for both the MQ client and the MQ server. The channel is a two-way link that processes calls and responses to send and receive messages.

Max Msg Size

If necessary, type the maximum message size in bytes allowed for the MQ adapter. The default value for the adapter is 4 MB (4194304 bytes). The actual maximum message size that is allowed will be the lower of the configured queue manager value, the configured queue value, the configured server connection value and this adapter value.

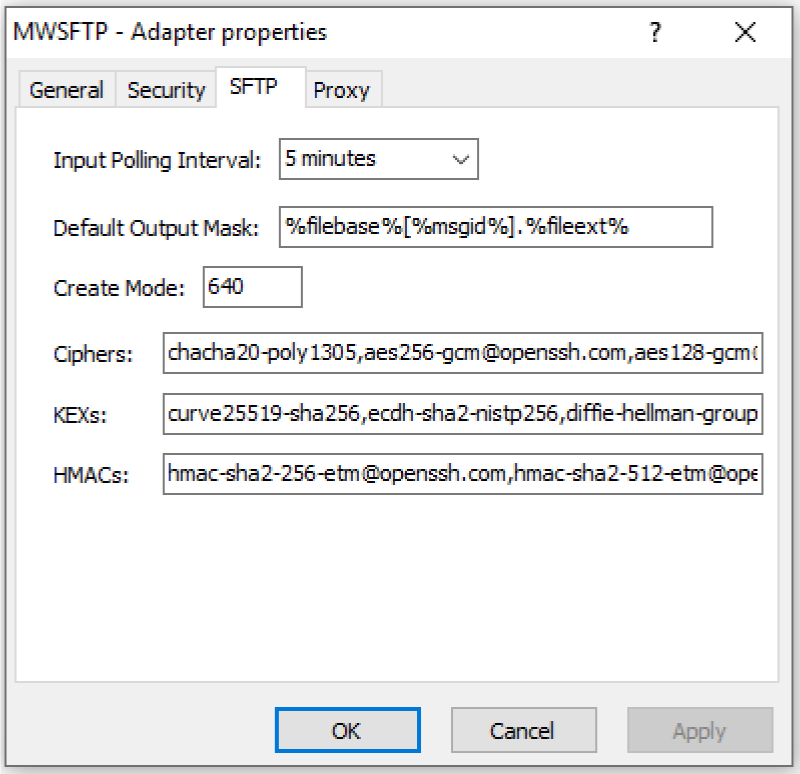
Queue Manager Name

MQ servers may have multiple MQ queue managers. Type the name of the queue manager to which you want to connect. You can leave this blank if there is only one queue manager.

(SFTP Adapter Properties) SFTP Page

The **SFTP** page of the Adapter Properties window contains the configuration information required for the inbound polling service of the adapter, the default mask to create output file names and the rights to create the file.

NOTE: MessageWay uses a default value of **640** for Create Mode rights when no value is provided in either the SFTP adapter configuration or the SFTP site configuration.



Input Polling Interval: 5 minutes

Default Output Mask: %filebase%[%msgid%].%fileext%

Create Mode: 640

Ciphers: chacha20-poly1305,aes256-gcm@openssh.com,aes128-gcm(

KEXs: curve25519-sha256,ecdh-sha2-nistp256,diffie-hellman-group

HMACs: hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@ope

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.

NOTE: The MessageWay SFTP Adapter is included as part of the license for the SFTP Proxy Server and the SFTP perimeter server, although you install and configure them separately. For more information, contact MessageWay Technical Support.

Input Polling Interval

The polling interval is used to transfer of messages from an SFTP directory into MessageWay. This is the amount of time that the SFTP client will wait before checking the directory for files to transfer to the site. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

The URL to be polled and the location to which the inbound files will be transferred are on the **SFTP Input** page of the Site Properties window under **Input to MessageWay**.

Select an interval from the list or enter the number of hours, minutes or seconds between polling cycles. The option **Never** stops polling for this adapter. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds
30m	means 30 minutes
2 h	means 2 hours

Default Output Mask

This is a template to create a file name for the output file. For new installations, the default mask is **%filebase%[%msgid%].%fileext%**. This mask generates unique names using the MessageWay message ID, which is enclosed in square brackets, [ ]. This avoids sending files that might be rejected because the file name already exists at the remote location. To change this default mask, use any combination of constants and MessageWay tokens. You may override this default for a specific location. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name.

Create Mode

Type a 3-digit numeric value to set the default file permissions when MessageWay creates a file. The default value is **640**. You may override these settings in the properties for an SFTP site.

Each digit may be from 0 to 7, representing permissions, from left to right, for owner/user, group, and all other users. To set the rights for each entity, add the total of the values assigned to each right, where, 4 = read (r), 2 = write (w), 1 = execute (x) and 0 = none (-). For example, 644 would give read and write (4+2=6) permissions to the owner/user, for example *mway*, and 4 would give read permissions to the group and others.

CAUTION: You may not be able to set the permissions for files on remote systems from the MessageWay SFTP adapter, based on the remote server/system settings for umask. The setting is controlled differently depending on whether you use SFTP or SCP to transfer the files. You should contact the administrator for the remote SFTP server for further information and help.

Ciphers

When FIPS is not enabled, overrides the default list of ciphers that the Adapter will use to negotiate an SSH session with the remote SFTP server. In the SSH protocol, asymmetric ciphers are used to handle encrypt and decrypt functions. Each individual value is separated with a comma, the values are negotiated from left to right in order to determine a match and any invalid or misspelled values are ignored. You may override this default for a specific location.

KEXs

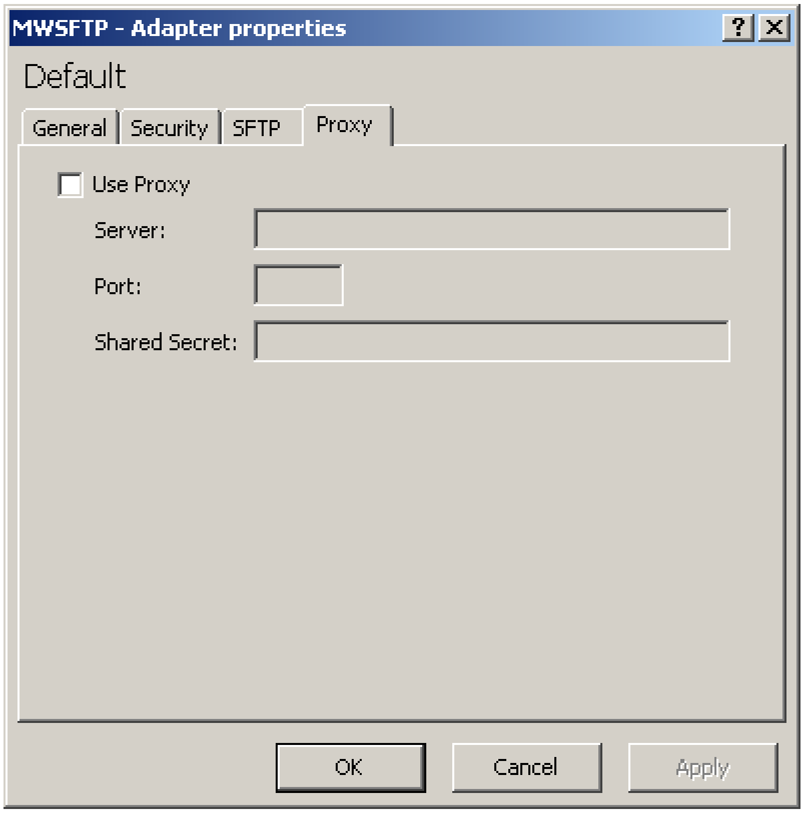
Overrides the default list of Key Exchange algorithms that the Adapter will use to negotiate an SSH session with the remote SFTP server. KEX algorithms are used to exchange the keys (public and private) that will be used to encrypt and decrypt. Each individual value is separated with a comma, the values are negotiated from left to right in order to determine a match and any invalid or misspelled values are ignored. You may override this default for a specific location.

HMACs

When FIPS is not enabled, overrides the default list of Hashed MAC functions that the Adapter will use to negotiate an SSH session with the remote SFTP server. HMACs are used to calculate the Message Authentication Code involving a function in combination with a secret key. In the SSH protocol, it is used to verify the integrity and authenticity of a message. Each individual value is separated with a comma, the values are negotiated from left to right in order to determine a match and any invalid or misspelled values are ignored. You may override this default for a specific location.

(SFTP Adapter Properties) Proxy Page

By default, the SFTP adapter communicates directly with an SFTP server. To communicate with an SFTP server through the MessageWay SFTP Proxy Server instead, you must provide information on the **Proxy** tab. The **Proxy** page allows you to specify the location of the proxy server and a shared secret key that the adapter uses to authenticate the proxy server. You can override these settings on the **Proxy** tab of the Site Properties window for an SFTP site configuration.



□ Use Proxy

Server:

Port:

Shared Secret:

NOTE: The MessageWay SFTP Adapter is included as part of the license for the SFTP Proxy Server and the SFTP perimeter server, although you install and configure them separately. For more information, contact MessageWay Technical Support.

Use Proxy

Check this box to send messages from this adapter through the MessageWay SFTP Proxy Server rather than directly to an external SFTP server. Users may override this default setting for a given SFTP site configuration.

Server

Type the URL of the MessageWay SFTP Proxy Server. This URL will be the default for all sites using this adapter. If you have more than one proxy server, you can override this value for specific sites.

Port

Type the port number on which the MessageWay SFTP Proxy Server listens for connection requests from the SFTP adapter. This port will be the default for all sites using this adapter. If you have more than one proxy server, you can override this value for specific sites.

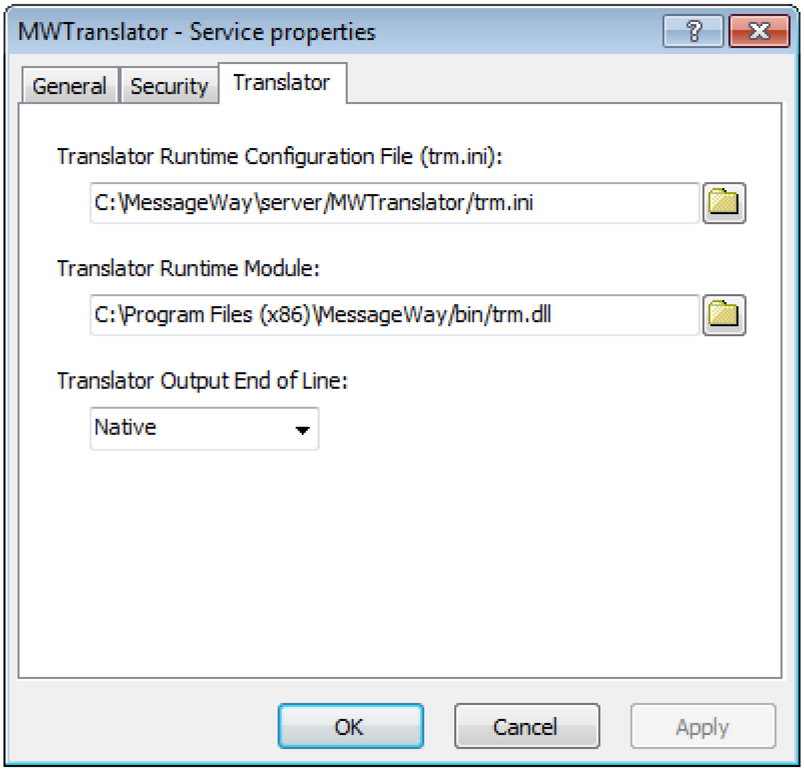
Shared Secret

Type a random ASCII string to be used for mutual authentication between the adapter and proxy server. This value must also be stored in the proxy configuration file, mwproxy.conf. Since the value is masked, you can copy the value and paste it into the field to avoid data entry errors.

(Translator Service Properties) Translator Page

The **Translator** page of the Service Properties window allows users to specify the configuration information required for the service. This information is determined during the installation process and displays here. These values should not be changed for production environments. They are available to advanced users for testing purposes.

IMPORTANT: To make changes in adapter or service configurations take effect, you must stop and restart the adapter or service. To assure that all message traffic has been sent before the adapter or service is stopped, you should first select **Suspend**, and then after all traffic has cleared, select **Stop**.



Translator Runtime Configuration File (trm.ini):
C:\MessageWay\server/MWTranslator/trm.ini

Translator Runtime Module:
C:\Program Files (x86)\MessageWay/bin/trm.dll

Translator Output End of Line:
Native

Translator Runtime Configuration File (trm.ini)

This is the location of the trm.ini file. The trm.ini file contains the startup parameters required for MWTranslator processing. This location is entered during the installation process. Advanced users may change the path for testing. Whenever you make changes to the trm.ini file, you must restart the MWTranslator service.

Translator Runtime Module

This is the location of the Translator Runtime Module (TRM) that provides translation services. This information is entered during the installation process. Advanced users may change the path for testing.

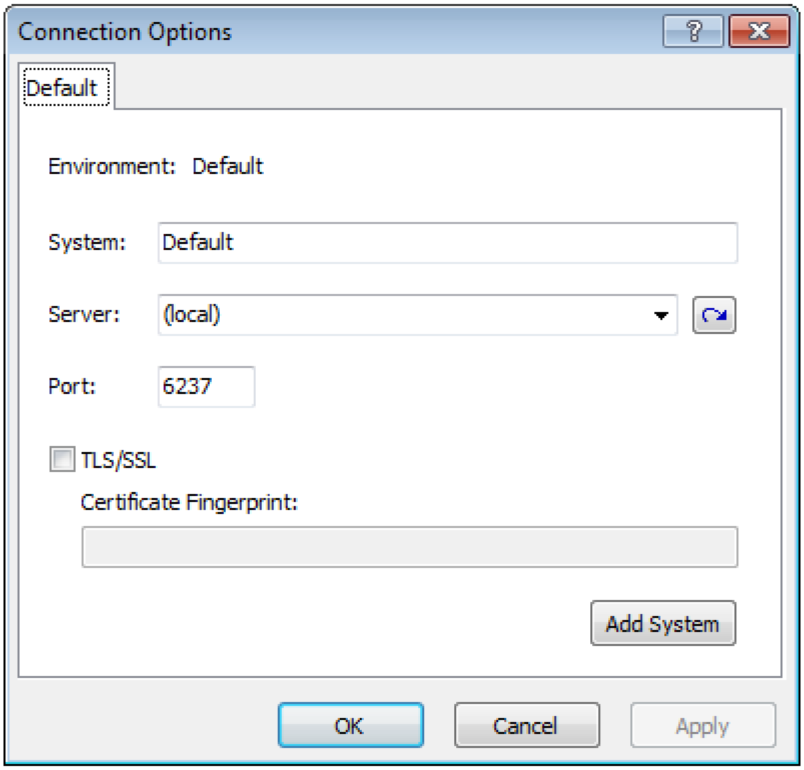
Translator Output End of Line

In MessageWay version 5.0, the line endings for text mode translator output on Windows were changed from CRLF to NL to be consistent across platforms. This has been fixed in 5.5 to depend on a translator service configuration field, **Translator Output End of Line**. It defaults to *Native*, but may be set to *CRLF*, *NL* or *Unchanged*. *Native* matches 4.2 behavior and *Unchanged* matches 5.0 behavior.

Connection Options Window

The Connection Options window allows users to connect to and monitor one or more MessageWay systems from the MessageWay Manager. You define and select the environment in the MessageWay Environment window.

The initial environment is called *Default*, which is created during installation. In this example, it points to a MessageWay server that is on the same Windows system as the Manager.



Environment: Default

System: Default

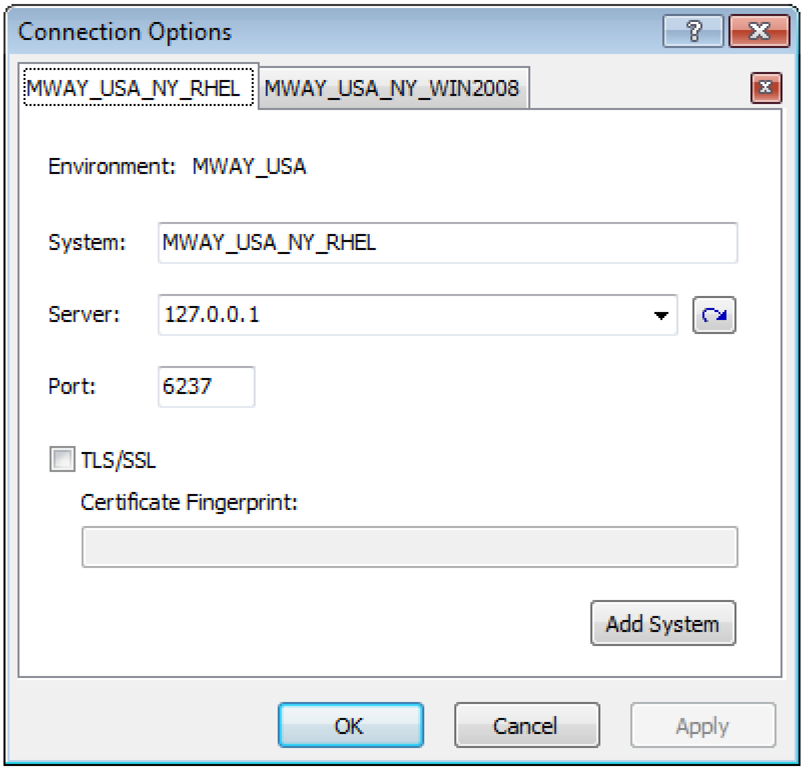
Server: (local)

Port: 6237

□ TLS/SSL

Certificate Fingerprint:

The following example shows an environment that accesses multiple systems, each identified on a separate tab.



Environment: MWAY_USA

System: MWAY_USA_NY_RHEL

Server: 127.0.0.1

Port: 6237

□ TLS/SSL

Certificate Fingerprint:

Delete Button

When you have more than one system in your environment, a delete button appears to the right of the tabs. To remove a system from an environment, select the system's tab and click the delete button.

System

Type a name up to 64 characters that you want to call the MessageWay server system. When multiple systems are assigned to an environment, users can then log on and monitor the systems from a single instance of the MessageWay Manager.

Server

This indicates to which server the selected system will connect. The default value **(local)** will connect to the MessageWay system installed on the same machine as the MessageWay Manager. Any value other than *(local)* is considered a remote server. For a remote server, enter a valid IP address or select a server name. When you are connected to the default environment, the title bar appears as follows:

MessageWay Manager - Default, (local)

Refresh List Button

Select this button to refresh the list of servers on your LAN or WAN visible to MessageWay.

Port

The Port is the TCP address used by MessageWay to contact the MessageWay User server (MWUser), or it may be a UDP broadcast from the MessageWay Manager to various MWUser servers. The default value is 6237. When you check the TLS/SSL box, this port changes to 6239 by default. If this port is already in use on the server, you may change it to another port.

TLS/SSL

By default, the MessageWay User server (MWUser) authenticates users who log on to MessageWay from the MessageWay Manager. Alternatively, users whose properties have the LDAP box checked, will be authenticated using the Light Directory Access Protocol (LDAP). The LDAP server may or may not require a TLS/SSL connection from the MessageWay Manager through the MWUser server to the LDAP server. Note that the LDAP server means any server application that supports LDAP, such as Active Directory.

Check this box to allow the MessageWay Manager to access the MWUser server using TLS/SSL. If you are using LDAP authentication through a secure TLS/SSL port, you must check this box. The MWUser configuration, mwuser.conf, determines the type of connection between the MWUser server and LDAP. Leave this unchecked when the LDAP server to which you connect does not require TLS/SSL or when you do not need TLS/SSL encryption between the MessageWay Manager and the MWUser server.

NOTE: the default connection between the MessageWay Manager and the MWUser server, without TLS/SSL, uses proprietary encryption.

Certificate Fingerprint

Type or paste the fingerprint of the certificate that the MessageWay Manager uses to authenticate the MWUser server. This fingerprint must match the finger print calculated from the certificate defined in the Listener Configurations section of the mwuser.conf file in the ClientCertFile parameter. The default certificate delivered with MessageWay is testcert.pem, which is for use during testing only. The fingerprint is:

59:57:1B:C2:D6:FA:B1:55:35:DC:DA:2B:BF:FE:25:36:1A:EB:DC:D6

CAUTION: The use of this fingerprint is not secure, because at least every MessageWay customer has access to the private key for this certificate and can therefore impersonate any server using this certificate.

Add System

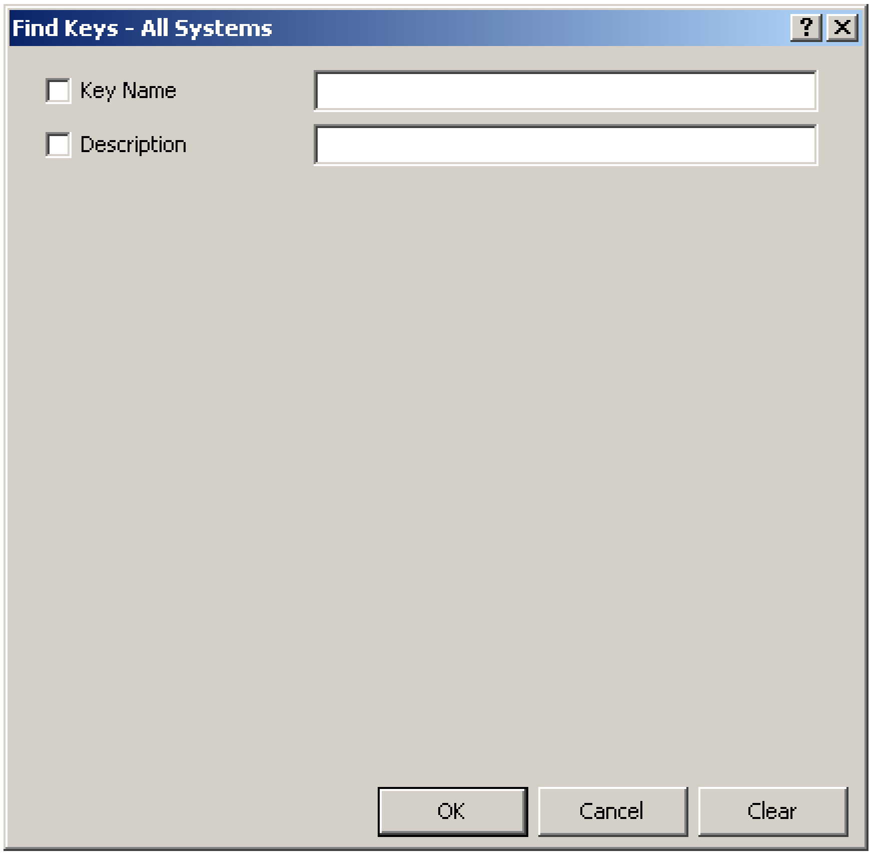
Click the **Add System** button to add a system to the environment that the Manager will monitor. A new tab appears. You can add up to 4 systems to an environment.

Find Keys Window

The Find Keys window provides search parameters to find key configurations. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

To access the Find Keys window, click the down arrow on the **Find** button from the toolbar, and select **Find Keys**, or from the **Search** menu, select the **Find Keys** command. When the Keys List window appears with the results of the search, the selection criteria appear in the header of the Keys Query Details window.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



Key Name

Type the name of the key to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Description

Type all or part of a description to use as a search criterion to find keys. Use the asterisk, *, as a wildcard to broaden your search.

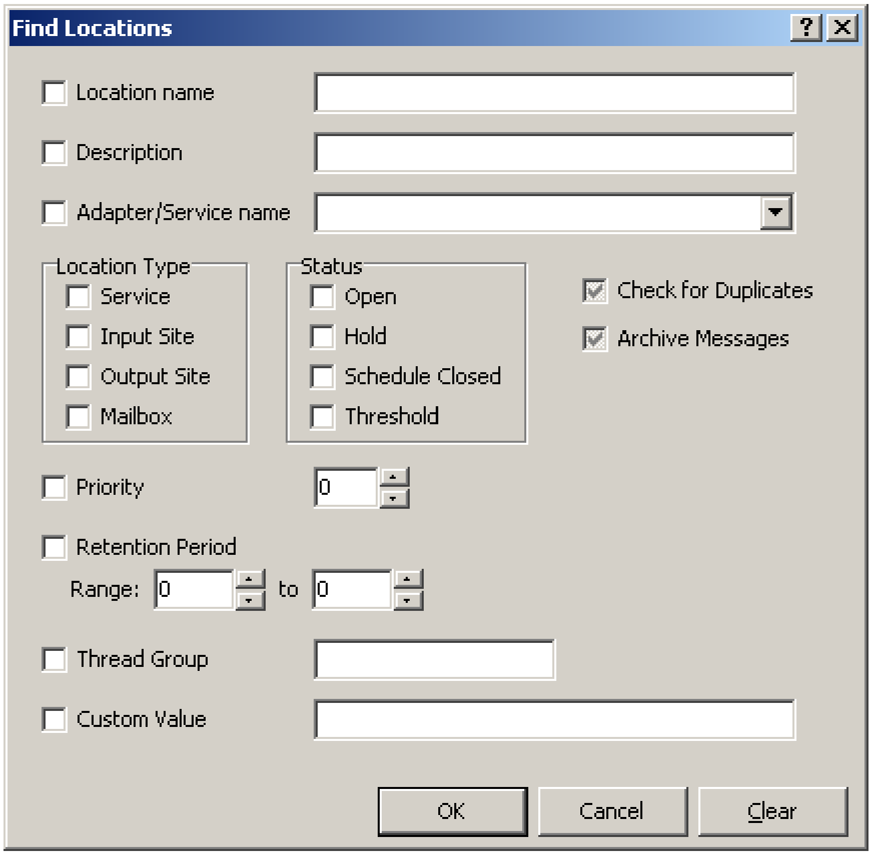
Find Locations Window

The Find Locations window provides search parameters to find location configurations. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

To access the Find Locations window, click the down arrow on the **Find** button 🔍 from the toolbar, and select **Find Locations**, or from the **Search** menu, select the **Find Locations** command. When the

Location List window appears with the results of the search, the selection criteria appear in the header of the Location Query Details window.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.


Find Locations

□ Location name
□ Description
□ Adapter/Service name

Location Type
□ Service
□ Input Site
□ Output Site
□ Mailbox

Status
□ Open
□ Hold
□ Schedule Closed
□ Threshold

☑ Check for Duplicates
☑ Archive Messages

□ Priority 0
□ Retention Period
Range: 0 to 0
□ Thread Group
□ Custom Value

Find Locations Window

Location Name

Type the name of the location to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search. Note that the naming convention is different for locations under the Locations folder versus locations under the File System folder. To limit your search to locations under the File System folder, you must include a forward slash as part of the location name, for example, */*tests*. Otherwise, **tests* would return all locations that end with *tests* that are in both the Locations and the File System folders. To find a specific location in the File System folder, you must type the full pathname, for example, */home/FS_Tests*.

Description

Type all or part of a description to use as a search criterion to find locations. Use the asterisk, *, as a wildcard to broaden your search.

Adapter/Service Name

Type the name of the adapter or service that is associated with the locations for which you are searching, or select the adapter or service from the list. Use the asterisk, *, as a wildcard to broaden your search.

Location Type

Check any of these boxes to search for locations by location type: service, input site, output site or mailbox.

The following table describes the choices:

Location Type	Description
Service	Location for a service, such as, MWTranslator, MWCompress and MWRules
Input Site	Site configured for input
Output Site	Site configured for output
Mailbox	Location where users may pick up messages or system location, such as {Unknown}, {Dist} or {Archive}

Status

Check any of these boxes to search for locations by the status of the location: *Open*, *On Hold*, *Closed* or *Threshold*.

Check for Duplicates

You can select one of three options here: checked only, clear only, checked and dimmed or colored only (depending on the Windows version). Check this box to search for locations that currently have the **Check for Duplicates** option selected. Clear the box to find locations that do not have the box checked. Click this box until it is both checked and dimmed or just colored to find all locations with the option either checked or unchecked.

Archive Messages

You can select one of three options here: checked only, clear only, checked and dimmed or colored only (depending on the Windows version). Check this box to search for locations that currently have the **Archive Messages** option selected. Clear the box to find locations that do not have the box checked. Click this box until it is both checked and dimmed or just colored to find all locations with the option either checked or unchecked.

Priority

Type or select a priority from 1 (low) to 5 (high) to search for locations by priority.

Retention Period Range (Start)

Type or select the least number of days that messages sent to the location will be retained within MessageWay, and not archived or deleted.

Retention Period Range (End)

Type or select the greatest number of days that messages sent to the location will be retained within MessageWay, and not archived or deleted.

Thread Group

Type the name of a thread group assigned to locations to use as a search criterion. Multiple locations may use the same thread group. Use the asterisk, *, as a wildcard to broaden your search.

Custom Value

Type the value of a custom property to use as a search criterion. Custom properties are those properties that reside on tabs specific to a service or adapter for a location. This is very useful for things such as checking for a specific inbound disk (or ftp) location. The longer and more specific the text, the more likely this will be helpful. Use the asterisk, *, as a wildcard to broaden your search.

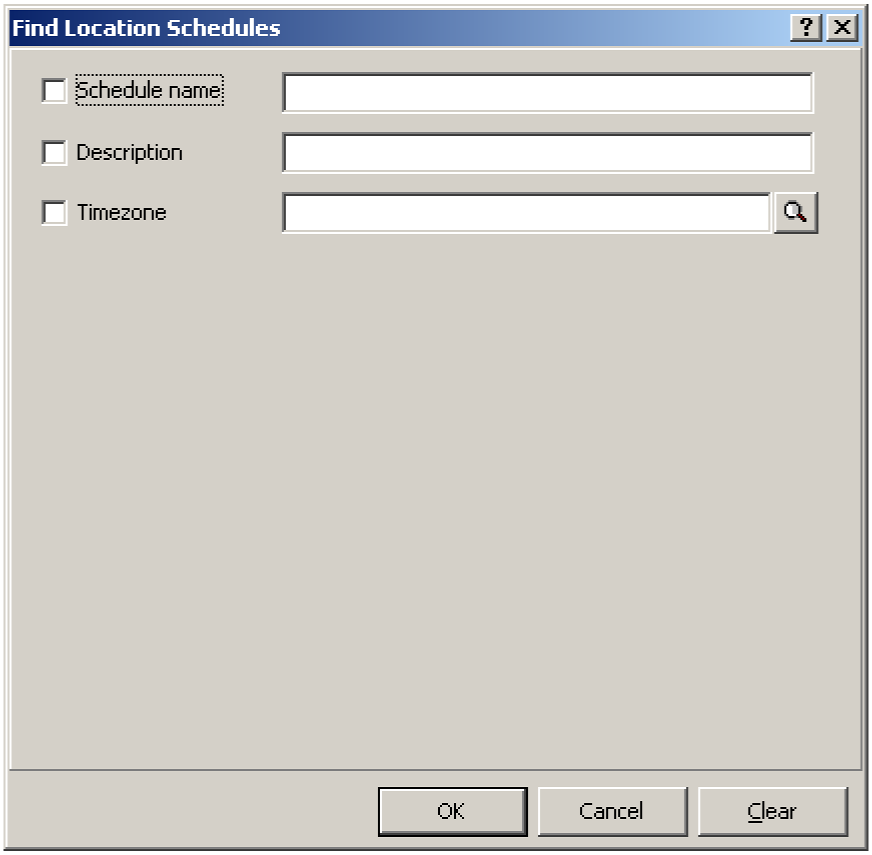
Find Location Schedules Window

The Find Location Schedules window allows uses to search for master and local location schedules based on schedule name, schedule description or timezone.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.

The location schedules list that appears when the search completes uses different icons for master location schedules and local location schedules, as follows:

Icon	Schedule Type
📅	Master location schedule
📆	Local location schedule



Find Location Schedule Window

Schedule Name

Type the name of a schedule for locations to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Description

Type the description you want to use to search for schedules for locations. Use the asterisk, *, as a wildcard to broaden your search.

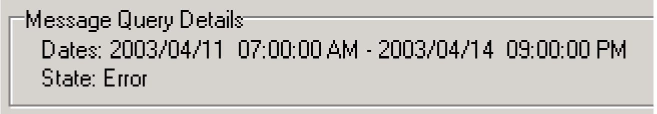
Timezone

Click the **Select Schedule Timezone** button, , and select the timezone you want to use to search for master schedules for locations.

Find Messages Window

The Find Messages window provides search parameters to locate specific messages using four types of criteria: message, interchange, functional group, and document. The last three, interchange, functional group, and document criteria only apply to data that have been processed by the MWTranslator service. To search for messages processed by MWTranslator, you must start the Logging Server, which adds translation audit records, from *.aud files that reside in the /MessageWay/server/MWTranslator/temp directory, to the database tables that MessageWay searches. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

To access the Find Messages window, click the down arrow on the **Find** button from the toolbar and select **Find Messages**, or from the **Search** menu, select the **Find Messages** command. When the Message List window appears with the results of the search, the selection criteria appear in the header of the Message Query Details window.



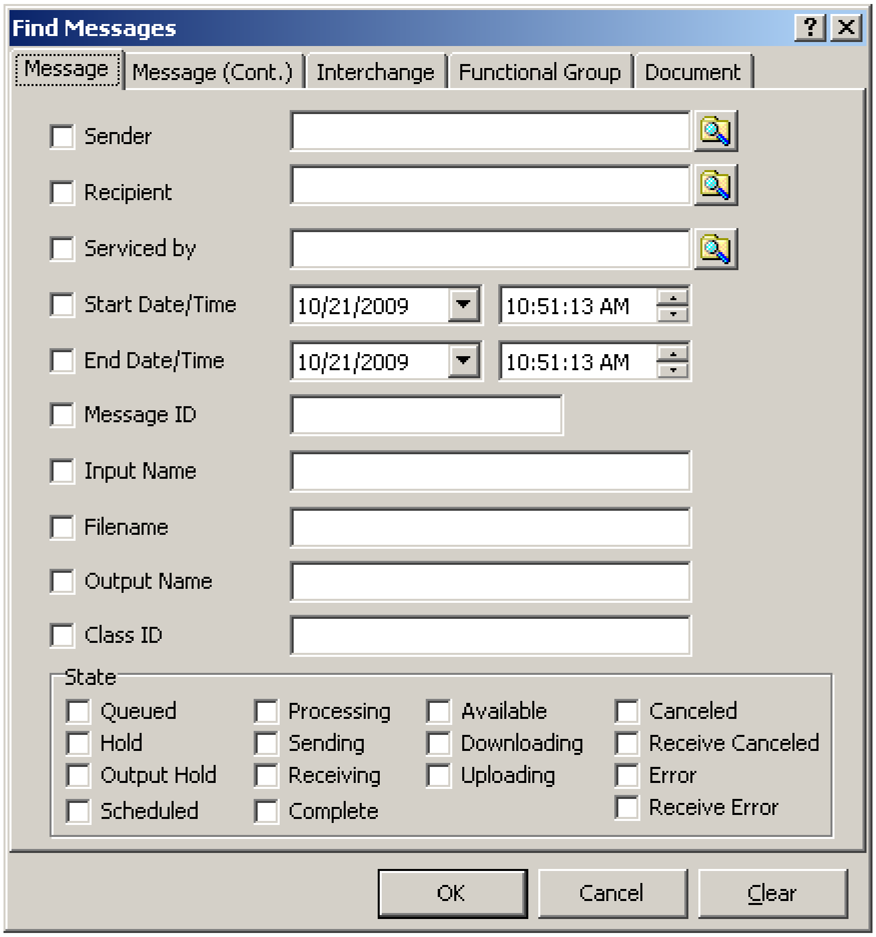
Message Query Details
Dates: 2003/04/11 07:00:00 AM - 2003/04/14 09:00:00 PM
State: Error

IMPORTANT: Clicking **OK** without selecting any criteria will return the maximum number of messages allowed, as defined in the Server Properties window of MWUser Server. Beware that such a list may be very long.

(Find Messages) Message Page

The **Message** page of the Find Messages window contains information applicable to the entire message, such as sender, recipient and service locations, date and time parameters, message ID, input name, filename, output name, class ID and state parameters.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



□ Sender

□ Recipient

□ Serviced by

□ Start Date/Time 10/21/2009 10:51:13 AM

□ End Date/Time 10/21/2009 10:51:13 AM

□ Message ID

□ Input Name

□ Filename

□ Output Name

□ Class ID

State

□ Queued
□ Hold
□ Output Hold
□ Scheduled
□ Processing
□ Sending
□ Receiving
□ Complete
□ Available
□ Downloading
□ Uploading
□ Canceled
□ Receive Canceled
□ Error
□ Receive Error

Message Page (Find Messages Window)

Sender

Type or select an existing location that represents the sender of the message. Select from a list of valid locations using the **Select** button 🔍. Since most methods of finding messages require that you know the recipient, this option allows you to find messages when you want to search by sender. Use the asterisk, *, as a wildcard to broaden your search.

Recipient

Type or select an existing location that represents the intended recipient of the message. Select from a list of valid location using the select button 🔍. When the recipient location does not exist, the messages are stored in the system mailbox {Unknown} until users correct the error and resubmit the message for delivery. Use the asterisk, *, as a wildcard to broaden your search.

Serviced by

Type or select an existing service location that identifies the processing performed for this message. Select from a list of valid service locations using the select button 🔍. Use the asterisk, *, as a wildcard to broaden your search.

Start Date

Type or select the date with which you want to begin your query. Click the arrow to select a date from the pop-up calendar. When the adjacent box is not checked, the query starts with the earliest entry in the file.

Start Time

Type or select the time with which you want to begin your query. You modify the hours, minutes, seconds and AM/PM separately. Use the arrows to adjust the hours, minutes, seconds and AM/PM as required.

End Date

Type or select the date with which you want to terminate your query. Click the arrow to select a date from a calendar. When this box is not checked, the query ends with the latest entry in the file.

End Time

Type or select the time with which you want to terminate your query. You modify the hours, minutes, seconds and AM/PM separately. Use the arrows to adjust the hours, minutes, seconds and AM/PM as required.

Message ID

Type a valid message ID. Message IDs are assigned by MessageWay. Use the asterisk, *, as a wildcard to broaden your search.

Input Name

Type a valid name for the input message, assuming one is known. This name varies depending on the adapter or service for the location that passes the name to MessageWay. For Disk Transfer or the FTP adapter sites, this would be a file name without the directory. For an E-mail adapter site, the name might represent the name of an attached file. For a service location, it might represent the name of a file processed on a target system using a mask that would reformat the input file name. Since the Message ID is only useful within MessageWay, this name may be used in lieu of the Message ID to relate a message to an external system. Use the asterisk, *, as a wildcard to broaden your search.

Filename

Type a valid file name. Filename is a persistent name from either the name of the input file or, when no input file name exists, from rules that determine one based on other message properties in MessageWay. Its purpose is to provide a name that does not depend on the requirements of adapter or service that receives the message, as does input name, nor on the requirements of the adapter or service that delivers the message, as does output name.

Output Name

Type a valid name for the output message, assuming one is known. This name differs depending on the type of adapter or service for the location that generates the name. For Disk Transfer or the FTP sites, this would be a file name generated by a mask. For an E-mail adapter site, the name might represent the name of an attached file. For a service location, it might represent the name of a file generated on a target system using a mask that would reformat the output file name. Since the Message ID is only useful within MessageWay, this name may be used in lieu of the Message ID to relate a message to an external system. Use the asterisk, *, as a wildcard to broaden your search.

Class ID

Type a valid class ID for the output message to use as a search criterion. This value is also useful for rules processing. A class ID may be assigned to a message in MessageWay using the syntax *classid@* or *classid@recipient* in the various destination options, such as the **Deliver to** field in input locations, the **Recipient** field on the Process Rule window or MWTranslator destination fields. Use the asterisk, *, as a wildcard to broaden your search.

State check boxes

Check any of these boxes to refine your query by message state.

Descriptions of the states are listed in the following table:

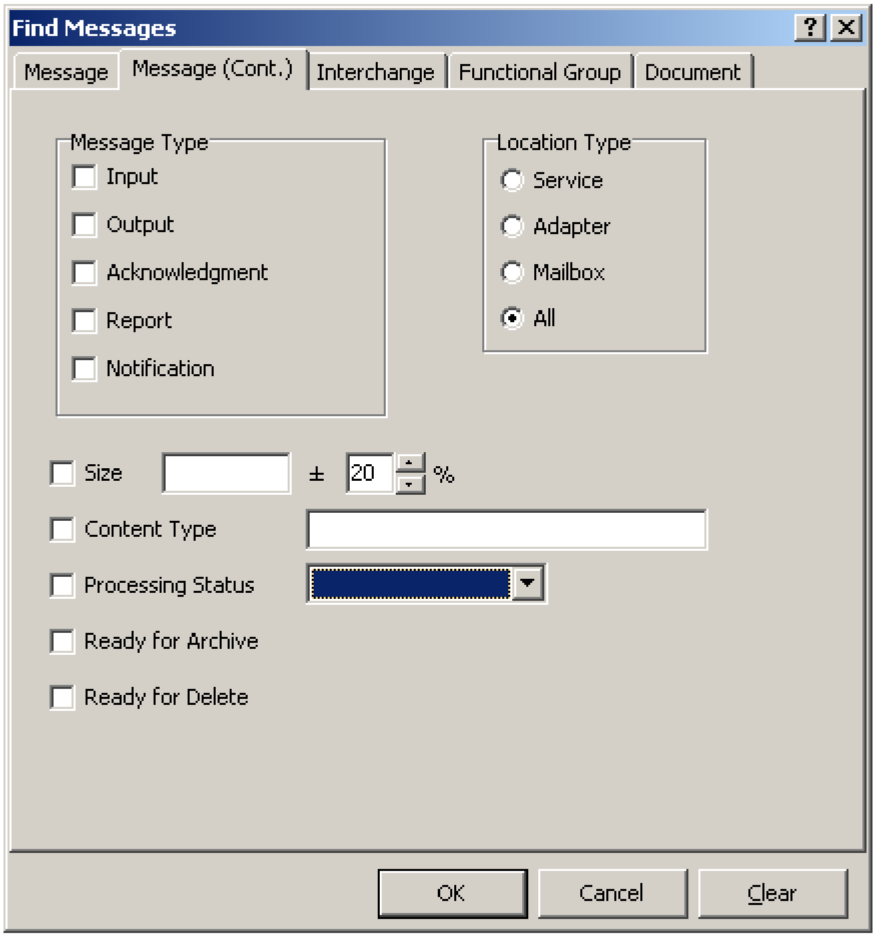
State	Description
Queued	The message is currently queued for service or delivery action.
Hold	The message is on hold awaiting further action by an operator.
Output Hold	The message is output from a service location and is on hold at its destination location awaiting further action by an operator.
Scheduled	The schedule is currently closed and the message is on hold.
Processing	The message has been received by a service location and is currently being processed.
Sending	The message is in a send and perhaps retry cycle.

State	Description
Receiving	The message is being received into MessageWay.
Complete	The message has been delivered or picked up.
Available	The message is ready to be picked up by a user.
Downloading	The message is being sent from MessageWay to a remote user.
Uploading	The message is being sent into MessageWay from a remote user.
Canceled	The message has been canceled.
Receive Canceled	The message was being received, but may not have completed receipt. Users may cancel such messages.
Error	The message has an error that occurred during processing or delivery or it failed duplicate checking.
Receive Error	Message receipt has failed, potentially leaving a partial file in MessageWay. Retry strategies will overlay any partial files.

(Find Messages) Message (Cont.) Page

The **Message (Cont.)** page of the Find Messages window contains more information applicable to the entire message, such as message type, location type, size, content type, processing status and archive state.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



Message Type
□ Input
□ Output
□ Acknowledgment
□ Report
□ Notification

Location Type
○ Service
○ Adapter
○ Mailbox
● All

□ Size ± 20 %

□ Content Type

□ Processing Status

□ Ready for Archive

□ Ready for Delete

Message (Cont.) Page (Find Messages Window)

Message Type

Check any of these boxes to refine your query by message type.

Descriptions of the message types are listed in the following table:

Message Type	Icon	Description
Input		An input message is any message sent into MessageWay for processing, automatic delivery or pickup. Input messages may also be cloned from other messages by services such as Distribution List or Rules Processing, or by resubmitting or redirecting a message that has a status of *Canceled* or *Complete*.
Output		An output message is one possible type of output from a service.

Message Type	Icon	Description
Acknowledgment	↩	An acknowledgment is a message returned to the sender acknowledging some aspect of the input message. Whether a service returns an acknowledgment depends on the service application.
Report	📜	A report is a processing report generated by a service, such as MWTranslator.
Notification Report	✓	A notification report is a brief message describing an event regarding a message transfer or message processing. It may be created by a service or auto-generated by MessageWay, based on configurations for a location. Trigger messages, a type of notification, may be auto-generated by MessageWay or by operator action.

Location Type

Select one of these options to specify messages transferred to a service location, an adapter location or a mailbox, such as a pickup type mailbox or the system mailbox, {Unknown}. The option **All** is the default.

Size

Type the size of the file in bytes, which you can modify with the adjacent field by selecting a percent variance to select any files within this percentage, plus or minus. To use an exact file size, the **%** field should be zero.

Percent (%)

Type or select a plus or minus percent within which the file size can vary using the arrows. To use an exact file size, this value should be zero.

Content Type

Type the content type, using the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay may try to determine the type from the data. A blank content type is assumed to be **application/octet-stream**. Content types can be used with FTP input or output to dynamically determine the transfer mode, when the mode is set to **AUTO**. Use the asterisk, *, as a wildcard to broaden your search.

The following table shows the content types that MessageWay supports:

Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

Processing Status

Select the status for your query from the list: **Accept**, **Accept with Errors**, **Partially Accepted**, **Reject**, **Security Reject**.

Ready for Archive

Check the Ready for Archive box to find messages that are ready to be archived and then deleted.

Ready for Delete

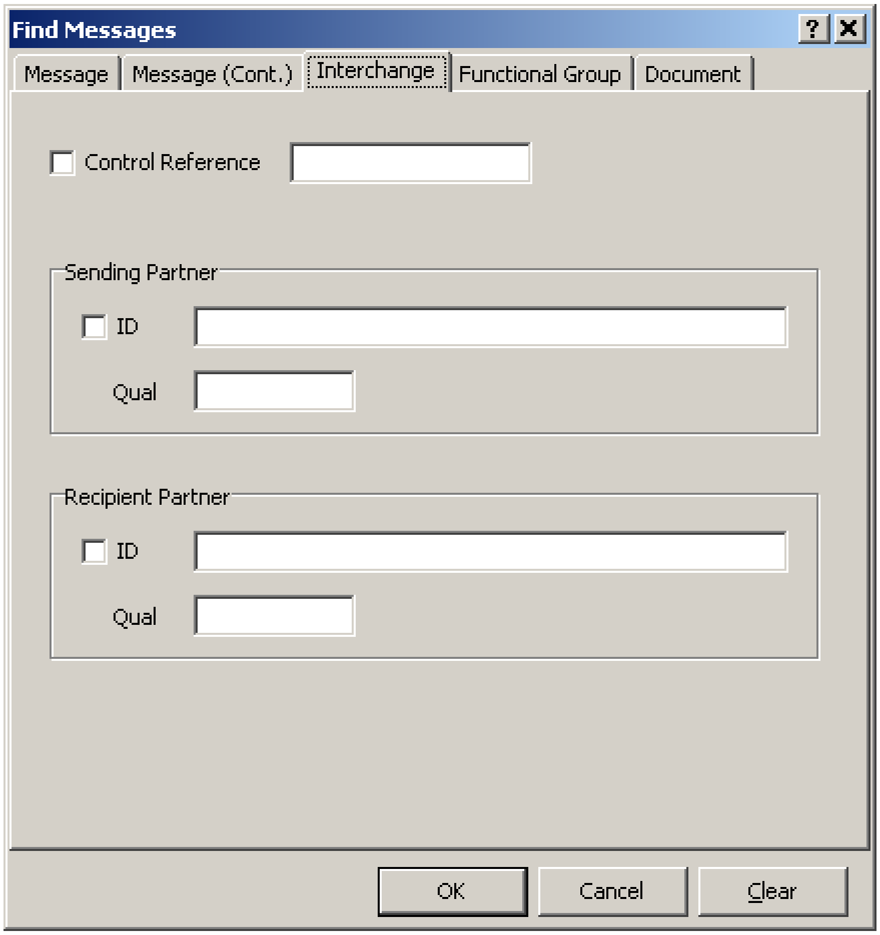
Check the Ready for Delete box to find messages that are ready to be deleted.

(Find Messages) Interchange Page

The **Interchange** page allows you to enter detailed interchange-level criteria for your search, such as control reference and sending and recipient partners.

NOTE: These criteria are only valid for data that have been processed by MWTranslator. To search for messages processed by MWTranslator, you must first start the Logging Server. The MWTranslator service creates audit records, *.aud files, that accumulate in the /MessageWay/server/MWTranslator/temp directory until the Logging Server adds them to the database where they are available for searches.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



Interchange Page (Find Messages Window)

Control Reference (Interchange)

Type a control reference value that you want to find in this box.

Sending Partner ID (Interchange)

Type a sending partner ID that you want to find in this box. This ID is paired with the value in the qualifier during the search. Use the asterisk, *, as a wildcard to broaden your search.

Sending Partner Qual (Interchange)

Type a sending partner qualifier that you want to find in this box. This qualifier is paired with the value in the ID during the search, so you must also have a value in the ID field.

Recipient Partner ID (Interchange)

Type a recipient partner ID that you want to find in this box. This ID is paired with the value in the qualifier during the search. Use the asterisk, *, as a wildcard to broaden your search.

Recipient Partner Qual (Interchange)

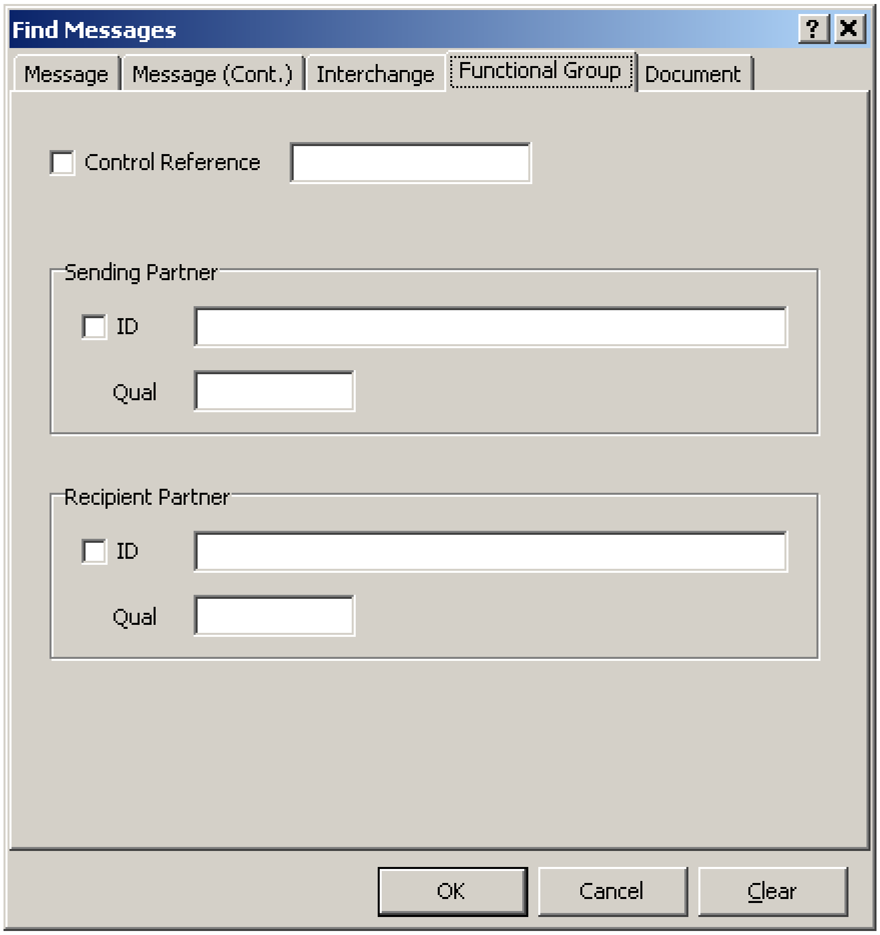
Type a recipient partner qualifier that you want to find in this box. This qualifier is paired with the value in the ID during the search, so you must also have a value in the ID field.

(Find Messages) Functional Group Page

The **Functional Group** page allows you to enter detailed functional group-level criteria for your search, such as control reference and sending and recipient partners.

NOTE: These criteria are only valid for data that have been processed by MWTranslator. To search for messages processed by MWTranslator, you must first start the Logging Server. The MWTranslator service creates audit records, *.aud files, that accumulate in the /MessageWay/server/MWTranslator/temp directory until the Logging Server adds them to the database where they are available for searches.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



Functional Group Page (Find Messages Window)

Control Reference (Functional Group)

Type a control reference value that you want to find in this box.

Sending Partner ID (Functional Group)

Type a sending partner ID that you want to find in this box. This ID is paired with the value in the qualifier during the search. Use the asterisk, *, as a wildcard to broaden your search.

Sending Partner Qual (Functional Group)

Type a sending partner qualifier that you want to find in this box. This qualifier is paired with the value in the ID during the search, so you must also have a value in the ID field.

Recipient Partner ID (Functional Group)

Type a recipient partner ID that you want to find in this box. This ID is paired with the value in the qualifier during the search. Use the asterisk, *, as a wildcard to broaden your search.

Recipient Partner Qual (Functional Group)

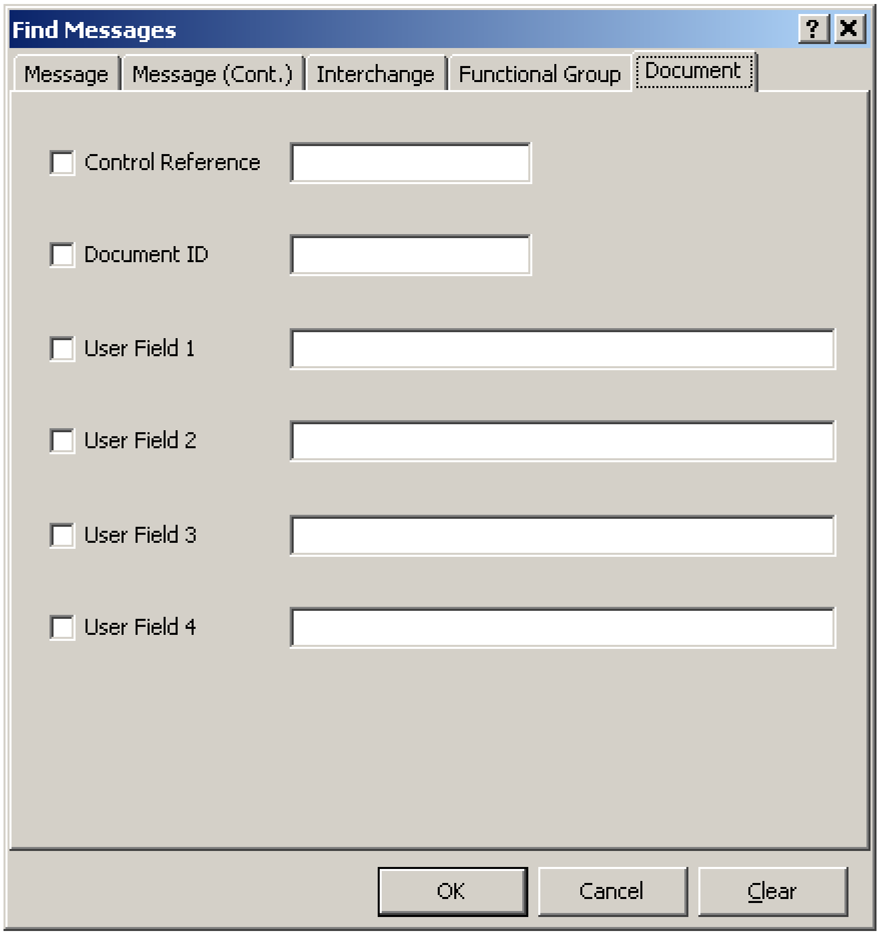
Type a recipient partner qualifier that you want to find in this box. This qualifier is paired with the value in the ID during the search, so you must also have a value in the ID field.

(Find Messages) Document Page

The **Document** page allows you to enter detailed document-level criteria for your search, such as control reference, document ID and user fields.

NOTE: These criteria are only valid for data that have been processed by MWTranslator. To search for messages processed by MWTranslator, you must first start the Logging Server. The MWTranslator service creates audit records, *.aud files, that accumulate in the /MessageWay/server/MWTranslator/temp directory until the Logging Server adds them to the database where they are available for searches.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



Document Page (Find Messages Window)

Control Reference (Document)

Type a control reference value that you want to find in this box.

Document ID (Document)

Type a document ID value that you want to find in this box. Use the asterisk, *, as a wildcard to broaden your search.

User Field 1 (Document)

Type a value that you want to find in this box. User fields must have been configured as part of the outbound document definition in order for you to be able to search for a value. For a discussion about configuring user fields, refer to the topic "Using Audit and Reconciliation" in the M*W Translator* Operator Guide and Reference. Use the asterisk, *, as a wildcard to broaden your search.

User Field 2 (Document)

Type a value that you want to find in this box. User fields must have been configured as part of the outbound document definition in order for you to be able to search for a value. For a discussion about configuring user fields, refer to the topic "Using Audit and Reconciliation" in the M*W Translator* Operator Guide and Reference. Use the asterisk, *, as a wildcard to broaden your search.

User Field 3 (Document)

Type a value that you want to find in this box. User fields must have been configured as part of the outbound document definition in order for you to be able to search for a value. For a discussion about configuring user fields, refer to the topic "Using Audit and Reconciliation" in the M*W Translator* Operator Guide and Reference. Use the asterisk, *, as a wildcard to broaden your search.

User Field 4 (Document)

Type a value that you want to find in this box. User fields must have been configured as part of the outbound document definition in order for you to be able to search for a value. For a discussion about configuring user fields, refer to the topic "Using Audit and Reconciliation" in the M*W Translator* Operator Guide and Reference. Use the asterisk, *, as a wildcard to broaden your search.

Find Archive Messages Window

The Find Archive Messages window provides search parameters to locate specific messages that have been archived. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

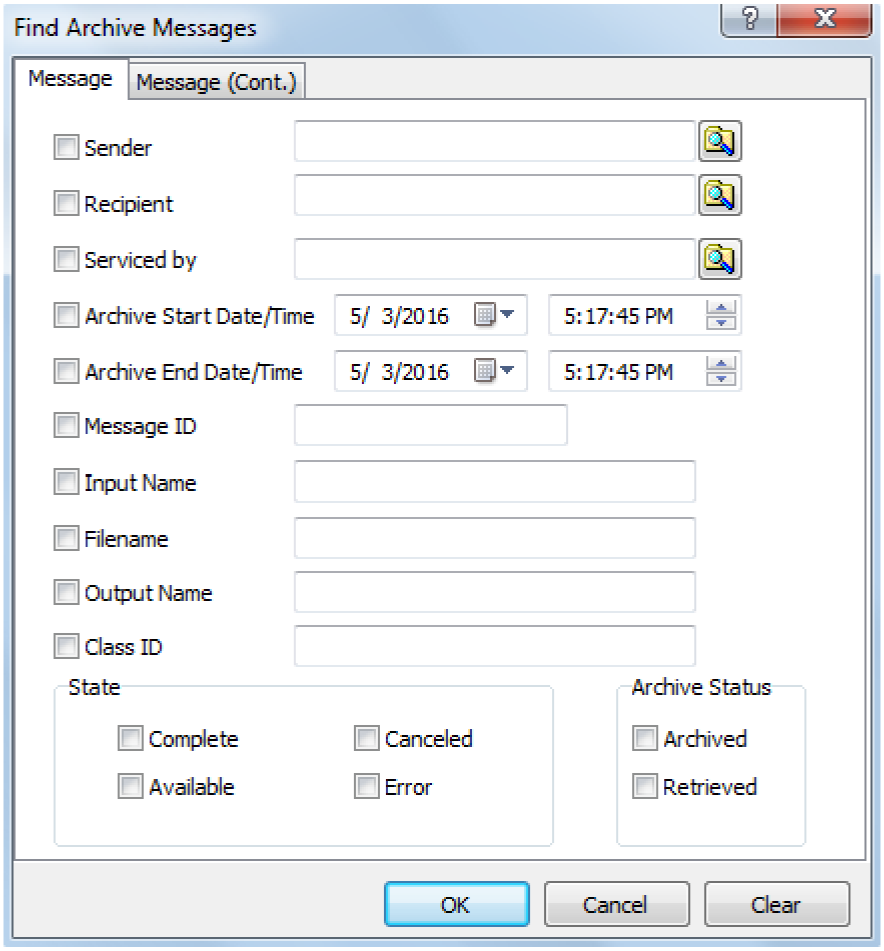
To access the Find Archive Messages window, click the down arrow on the **Find** button from the toolbar and select **Find Archive Messages**, or from the **Search** menu, select the **Find Archive Messages** command. When the Archive Message List window appears with the results of the search, the selection criteria appear in the header of the Archive Message Query Details window.

IMPORTANT: Clicking **OK** without selecting any criteria will return the maximum number of messages allowed, as defined in the Server Properties window of MWUser Server. Beware that such a list may be very long.

(Find Archive Messages) Message Page

The **Message** page of the Find Archive Messages window contains information applicable to the entire message, such as sender, recipient and service locations, archive date and time parameters, message ID, input name, filename, output name, class ID, state parameters and archive status parameters.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



Find Archive Messages

Message | Message (Cont.)

□ Sender

□ Recipient

□ Serviced by

□ Archive Start Date/Time 5/ 3/2016 5:17:45 PM

□ Archive End Date/Time 5/ 3/2016 5:17:45 PM

□ Message ID

□ Input Name

□ Filename

□ Output Name

□ Class ID

State

□ Complete □ Canceled

□ Available □ Error

Archive Status

□ Archived

□ Retrieved

Message Page (Find Archive Messages Window)

Sender

Type or select an existing location that represents the sender of the message. Select from a list of valid locations using the **Select** button. Since most methods of finding messages require that you know the recipient, this option allows you to find messages when you want to search by sender. Use the asterisk, *, as a wildcard to broaden your search.

Recipient

Type or select an existing location that represents the intended recipient of the message. Select from a list of valid location using the select button. Use the asterisk, *, as a wildcard to broaden your search.

Serviced by

Type or select an existing service location that identifies the processing performed for this message. Select from a list of valid service locations using the select button 🔍. Use the asterisk, *, as a wildcard to broaden your search.

Archive Start Date

Type or select the date with which you want to begin your query. Click the arrow to select a date from the pop-up calendar. When the adjacent box is not checked, the query starts with the earliest entry in the file.

Archive Start Time

Type or select the time with which you want to begin your query. You modify the hours, minutes, seconds and AM/PM separately. Use the arrows to adjust the hours, minutes, seconds and AM/PM as required.

Archive End Date

Type or select the date with which you want to terminate your query. Click the arrow to select a date from a calendar. When this box is not checked, the query ends with the latest entry in the file.

Archive End Time

Type or select the time with which you want to terminate your query. You modify the hours, minutes, seconds and AM/PM separately. Use the arrows to adjust the hours, minutes, seconds and AM/PM as required.

Message ID

Type a valid message ID. Message IDs are assigned by MessageWay. Use the asterisk, *, as a wildcard to broaden your search.

Input Name

Type a valid name for the input message, assuming one is known. This name varies depending on the adapter or service for the location that passes the name to MessageWay. For Disk Transfer or the FTP adapter sites, this would be a file name without the directory. For an E-mail adapter site, the name might represent the name of an attached file. For a service location, it might represent the name of a file processed on a target system using a mask that would reformat the input file name. Since the Message ID is only useful within MessageWay, this name may be used in lieu of the Message ID to relate a message to an external system. Use the asterisk, *, as a wildcard to broaden your search.

Filename

Type a valid file name. Filename is a persistent name from either the name of the input file or, when no input file name exists, from rules that determine one based on other message properties in MessageWay. Its purpose is to provide a name that does not depend on the requirements of adapter or service that receives the message, as does input name, nor on the requirements of the adapter or service that delivers the message, as does output name.

Output Name

Type a valid name for the output message, assuming one is known. This name differs depending on the type of adapter or service for the location that generates the name. For Disk Transfer or the FTP sites, this would be a file name generated by a mask. For an E-mail adapter site, the name might represent the name of an attached file. For a service location, it might represent the name of a file generated on a target system using a mask that would reformat the output file name. Since the Message ID is only useful within MessageWay, this name may be used in lieu of the Message ID to relate a message to an external system. Use the asterisk, *, as a wildcard to broaden your search.

Class ID

Type a valid class ID for the output message to use as a search criterion. This value is also useful for rules processing. A class ID may be assigned to a message in MessageWay using the syntax *classid***@** or *classid***@***recipient* in the various destination options, such as the **Deliver to** field in input locations, the **Recipient** field on the Process Rule window or MWTranslator destination fields. Use the asterisk, *, as a wildcard to broaden your search.

State check boxes

Check any of these boxes to refine your query by message state.

Descriptions of the states are listed in the following table:

State	**Description**
Complete	The message has been delivered or picked up.
Available	The message is ready to be picked up by a user.
Canceled	The message has been canceled.
Error	The message has an error that occurred during processing or delivery or it failed duplicate checking.

Archived Status check box

Check this box to use status of **Archived** as a search criterion.

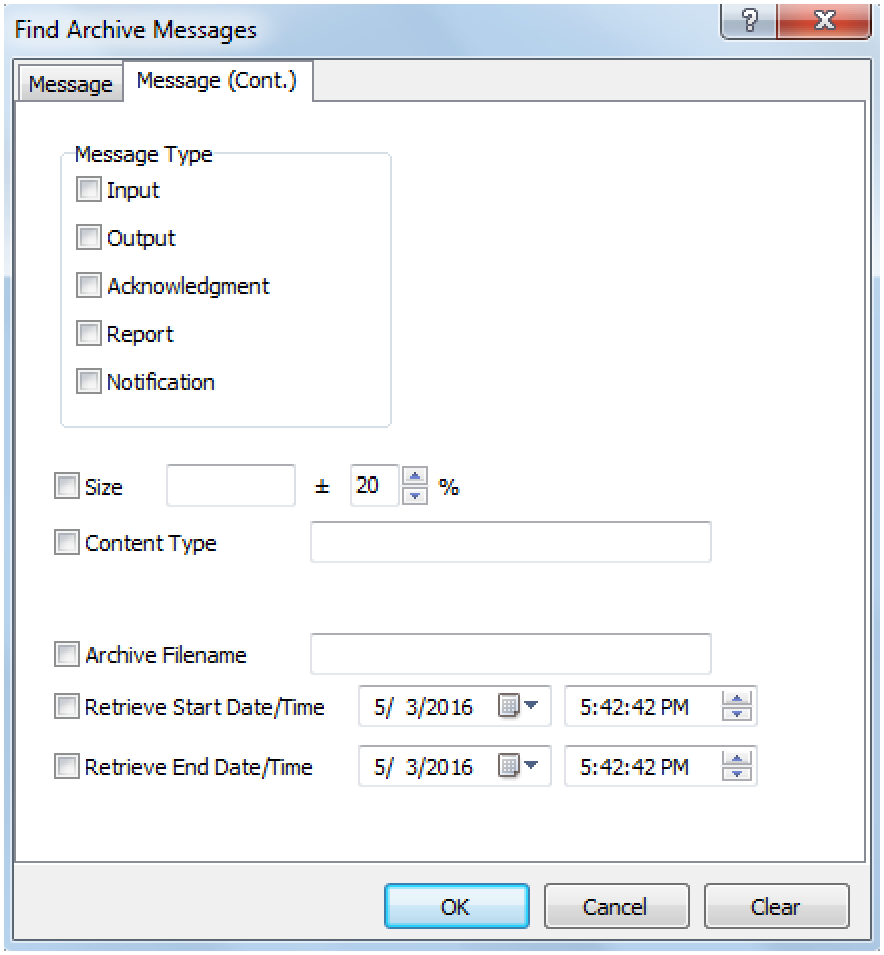
Retrieved Status check box

Check this box to use status of **Retrieved** as a search criterion.

(Find Archive Messages) Message (Cont.) Page

The **Message (Cont.)** page of the Find Archive Messages window contains more information applicable to the entire message, such as message type, size, content type, archive filename and retrieve date and time parameters.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



Message (Cont.) Page (Find Archive Messages Window)

Message Type

Check any of these boxes to refine your query by message type.

Descriptions of the message types are listed in the following table:

Message Type	Icon	Description
Input	⤵	An input message is any message sent into MessageWay for processing, automatic delivery or pickup. Input messages may also be cloned from other messages by services such as Distribution List or Rules Processing, or by resubmitting or redirecting a message that has a status of *Canceled* or *Complete*.
Output	⤴	An output message is one possible type of output from a service.
Acknowledgment	↩	An acknowledgment is a message returned to the sender acknowledging some aspect of the input message. Whether a service returns an acknowledgment depends on the service application.
Report	📜	A report is a processing report generated by a service, such as MWTranslator.
Notification Report	✓	A notification report is a brief message describing an event regarding a message transfer or message processing. It may be created by a service or auto-generated by MessageWay, based on configurations for a location. Trigger messages, a type of notification, may be auto-generated by MessageWay or by operator action.

Size

Type the size of the file in bytes, which you can modify with the adjacent field by selecting a percent variance to select any files within this percentage, plus or minus. To use an exact file size, the **%** field should be zero.

Percent (%)

Type or select a plus or minus percent within which the file size can vary using the arrows. To use an exact file size, this value should be zero.

Content Type

Type the content type, using the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay may try to determine the type from the data. A blank content type is assumed to be **application/octet-stream**. Content types can be used with FTP input or output to dynamically determine the transfer mode, when the mode is set to **AUTO**. Use the asterisk, *, as a wildcard to broaden your search.

The following table shows the content types that MessageWay supports:

Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi

Type	Content Type	File Extension
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

Archive Filename

Type a valid archive filename. Archive filenames are determined by the ‘Archive File Mask:’ field on the MWArchive - Server Properties MWArchive tab, typically ARCH%yyyymmdd%, but any combination of constants and MessageWay tokens may have been used.

Retrieve Start Date

Type or select the date with which you want to begin your query. Click the arrow to select a date from the pop-up calendar.

Retrieve Start Time

Type or select the time with which you want to begin your query. You modify the hours, minutes, seconds and AM/PM separately. Use the arrows to adjust the hours, minutes, seconds and AM/PM as required.

Retrieve End Date

Type or select the date with which you want to terminate your query. Click the arrow to select a date from a calendar.

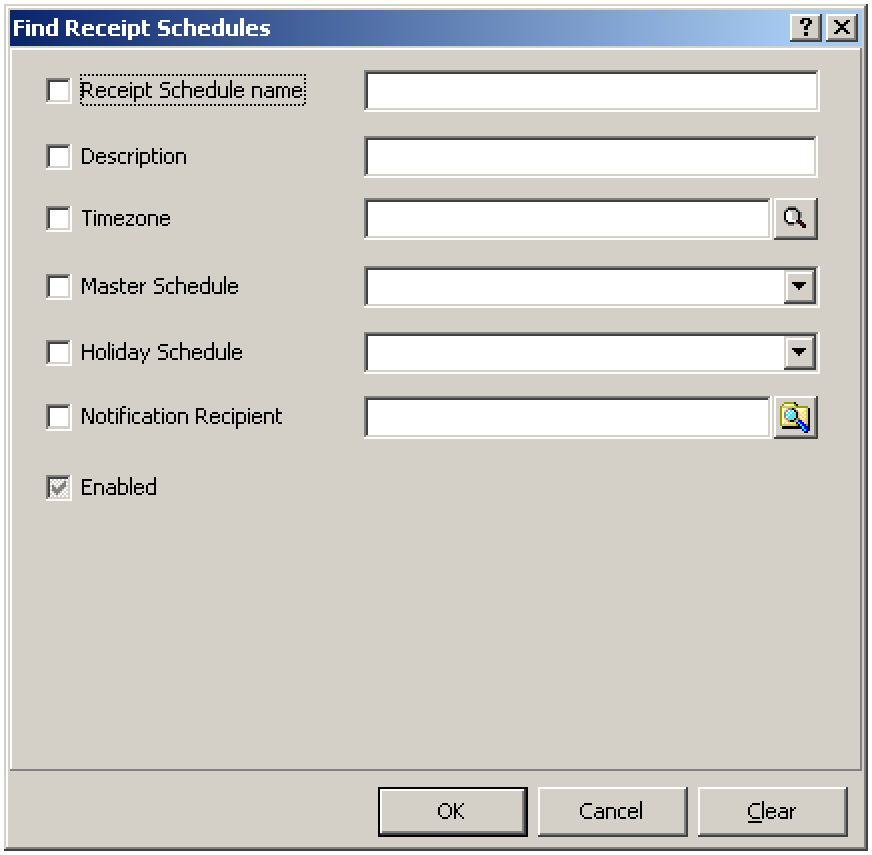
Retrieve End Time

Type or select the time with which you want to terminate your query. You modify the hours, minutes, seconds and AM/PM separately. Use the arrows to adjust the hours, minutes, seconds and AM/PM as required.

Find Receipt Schedules Window

The Find Receipt Schedules window allows users to find schedules for the Receipt Monitor by schedule name, description, timezone, master schedule, holiday schedule, notification recipient or the enabled property. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



Find Receipt Schedules Window

Receipt Schedule Name

Type the name of a receipt schedule to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Description

Type the description of a receipt schedule to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Timezone

Click the **Select Schedule Timezone** button, 🔍, and select the timezone you want to use to search for receipt schedules.

Master Schedule

Type or select a master schedule to find receipt schedules that use this master schedule. Use the asterisk, *, as a wildcard to broaden your search. Note that the **Enabled** box has no affect on the selection of master schedules.

Holiday Schedule

Type or select a holiday schedule to find receipt schedules that use this holiday schedule. Use the asterisk, *, as a wildcard to broaden your search.

Notification Report

Type or select a location for this notification recipient that you want to use a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

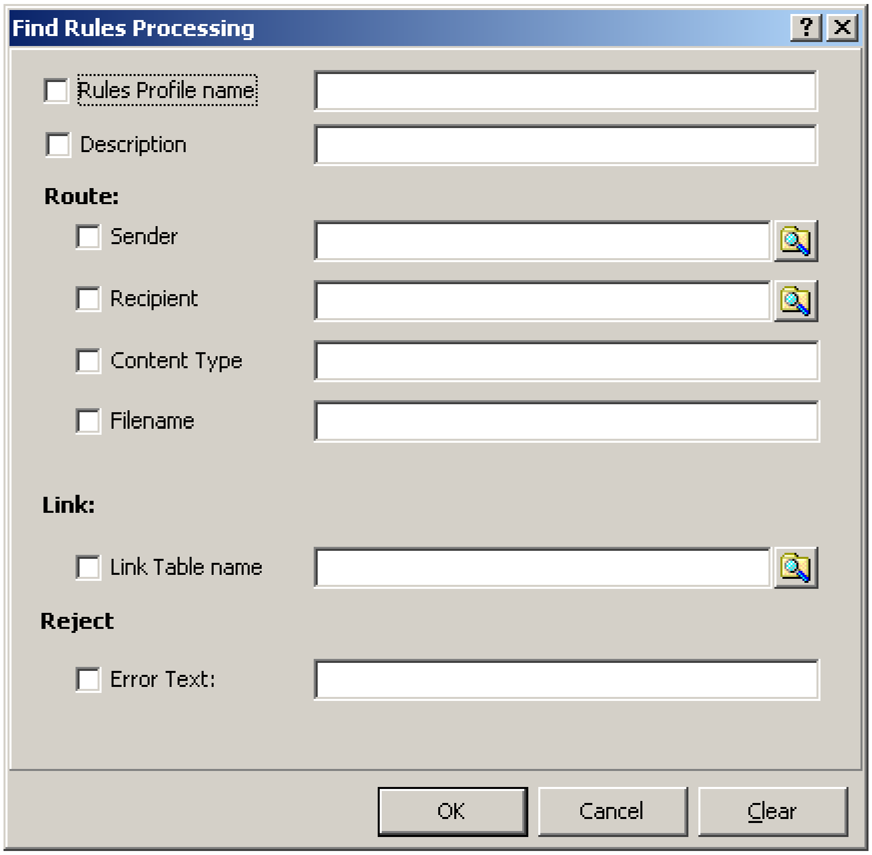
Enabled Check Box

You can select one of three options here: checked only, clear only, checked and dimmed or colored only (depending on the Windows version). Check this box to search for receipt schedules that are currently enabled. Clear this box to search for receipt schedules that are disabled. When the box is checked and dimmed or just colored, MessageWay searches for both enabled and disabled receipt schedules. Master schedules are always enabled. They will display with the list of enabled receipt schedules, unless they are excluded by other search criteria.

Find Rules Processing Window

The Find Rules Processing window allow you to search for a profile configured for the Rules service. The Rules service uses profiles that contain one or more rules based on message characteristics or content to filter and route messages. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



Find Rules Processing Window

Rules Profile Name

Type the name of the rules profile that you want to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Description

Type a description for a rules profile to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Sender

For a processing rule that specifies a route action, type or select the location of the sender to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Recipient

For a processing rule that specifies a route action, type or select the location of the receiver to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Content Type

For a processing rule that specifies a route action, type the content type to use as a search criterion. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream. Use the asterisk, *, as a wildcard to broaden your search.

The following table shows the content types that MessageWay supports:

Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv

Type	Content Type	File Extension
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

Filename

For a processing rule that specifies a route action, type the filename to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Link Table Name

For a processing rule that specifies a link action, type the name of the link table to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

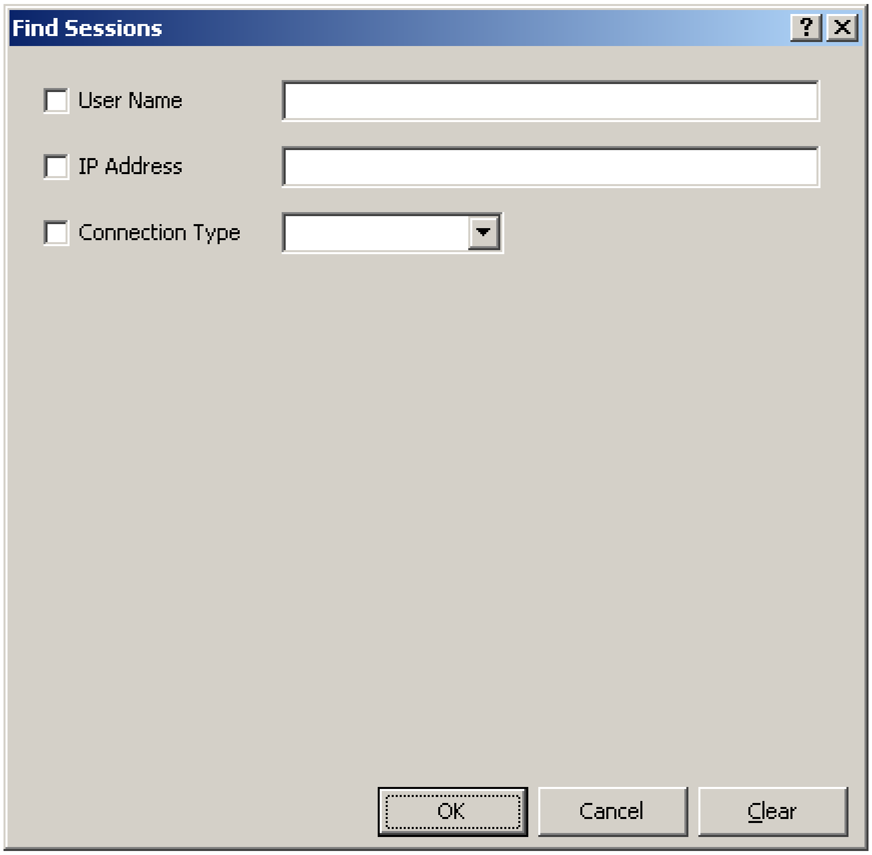
Error Text

For a processing rule that specifies a reject action, type the error message of the rule to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Find Sessions Window

The Find Sessions window allows operators to see which users are currently connected to the MessageWay system. Operators can search by user name, IP address or connection type: *AS2*, *Manager*, *FTP*, *SFTP* or *WEB*. Note that WEB identifies the Web Client. A session remains active until the user logs off or the session times out, which is determined by the configurations for the entity that makes the connection. For example, if you are logged on through the MessageWay Manager, the *Logon Idle Lifetime* setting on the **General** tab of the User Policies window determines when a user's session times out. The Scheduling Server cleans out invalid sessions based on its Receipt Monitor Interval setting. If this is blank, it will not clean out invalid sessions. If you change the monitor interval, you must restart the Scheduling Server for the changes to take effect. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



User Name

Type the name of a MessageWay user to use as a search criterion to find sessions.

IP Address

Type an IP address to use as a search criterion to find a session.

Connection Type

Select a connection type or type the name of a known type to use as a search criterion to find a current session. The drop-down list may not show all connection types. If you type a Connection Type rather than select one from the list, it must match the name recognized by MessageWay, for example **WEB**. The names are case-insensitive. Current options are *AS2*, *Manager*, *FTP*, *SFTP*, *WEB and MWIR.*

NOTE: The drop-down list may not show all connection types. If you type a Connection Type rather than select one from the list, it must match the name recognized by MessageWay, for example **WEB**. The names are case-insensitive.

Here are descriptions of client connections that access MessageWay through one of these connection types:

Connection Type	Description
AS2	AS2 Interface
FTP	MessageWay FTP Perimeter Server
SFTP	MessageWay SFTP Perimeter Server
Manager	MessageWay Manager (Graphical User Interface)
WEB	Web Client (client connects via Web browser eventually through MWSI)
MWIR	Reporting (client connects via Web browser eventually through MWSI)

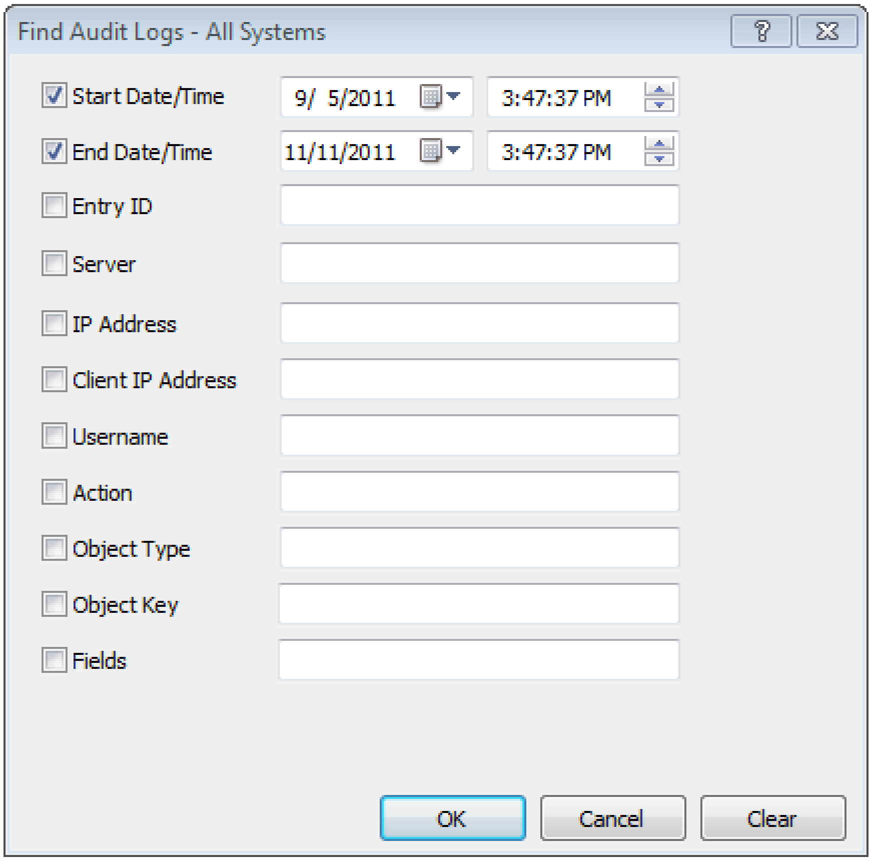
Find Logs

The Find Logs group allows users to find audit logs, system event logs and trace logs.

Find Audit Logs Window

The Find Audit Log Window lets you search the database for Audit log entries that match the selected criteria. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.


Find Audit Logs - All Systems

☑ Start Date/Time 9/ 5/2011 3:47:37 PM

☑ End Date/Time 11/11/2011 3:47:37 PM

□ Entry ID

□ Server

□ IP Address

□ Client IP Address

□ Username

□ Action

□ Object Type

□ Object Key

□ Fields

Start Date/Time (Find Audit Logs)

Check the Start Date/Time box to begin your query with the date and time listed in the date and time selection boxes. When this box is not checked, the query starts with the earliest entry in the file.

End Date/Time (Find Audit Logs)

Check the End Date/Time box to terminate your query with the date and time listed in the date and time selection boxes. When this box is not checked, the query ends with the latest entry in the file.

Entry ID (Find Audit Logs)

Enter the ID value for the log entry.

Server (Find Audit Logs)

Enter the name of the server that logged the entry.

IP Address (Find Audit Logs)

Enter the IP address of the MessageWay Manager client system (for MWUser), or the IP address of the perimeter server (for MWSI) that performed the action.

Client IP Address (Find Audit Logs)

Enter the IP address of the client that started the transaction. Currently used only by audit records from MWSI.

Username (Find Audit Logs)

Enter the Username of the user associated with the log entry.

Action (Find Audit Logs)

Enter the action logged, for example: logon, disconnected, add, modify.

Object Type (Find Audit Logs)

Enter the type of MessageWay object associated with the entry, for example: location, adapter/service, user. You can use the asterisk, *, as a wild card. For example, ***Schedule** will return audit records for the following objects: Schedule (Receipt Monitor, receipt schedule), Holiday Schedule (Receipt Monitor, holiday schedule), Master Schedule (Receipt Monitor, master receipt schedule) and Location Schedule (schedules for specific locations and master location schedules).

The following table describes all objects for which you can currently obtain audit information.

Object Type	Description of Object Type
Adapter/Service	Adapters or services
Location	Sites, service locations, pickup mailboxes, system locations
Folder	Folders that contain locations or other location folders
Location schedules	Master location schedules, to be shared by multiple locations, or schedules for individual locations
Schedule	Receipt Monitor, receipt schedules
Master Schedule	Receipt Monitor, master receipt schedules
Holiday Schedule	Receipt Monitor, holiday schedules
Server	Internal servers such as mwsi, mwuser
User	Users
User security groups	User groups

Object Type	Description of Object Type
User folder	Folders that contain users or user groups
User policy	System security policies for users
Rules	Rules Processing, profiles
Key	SSH security keys, in Keys folder
Message	MessageWay messages

Object Key (Find Audit Logs)

Enter the user-defined name of the object, such as a location name.

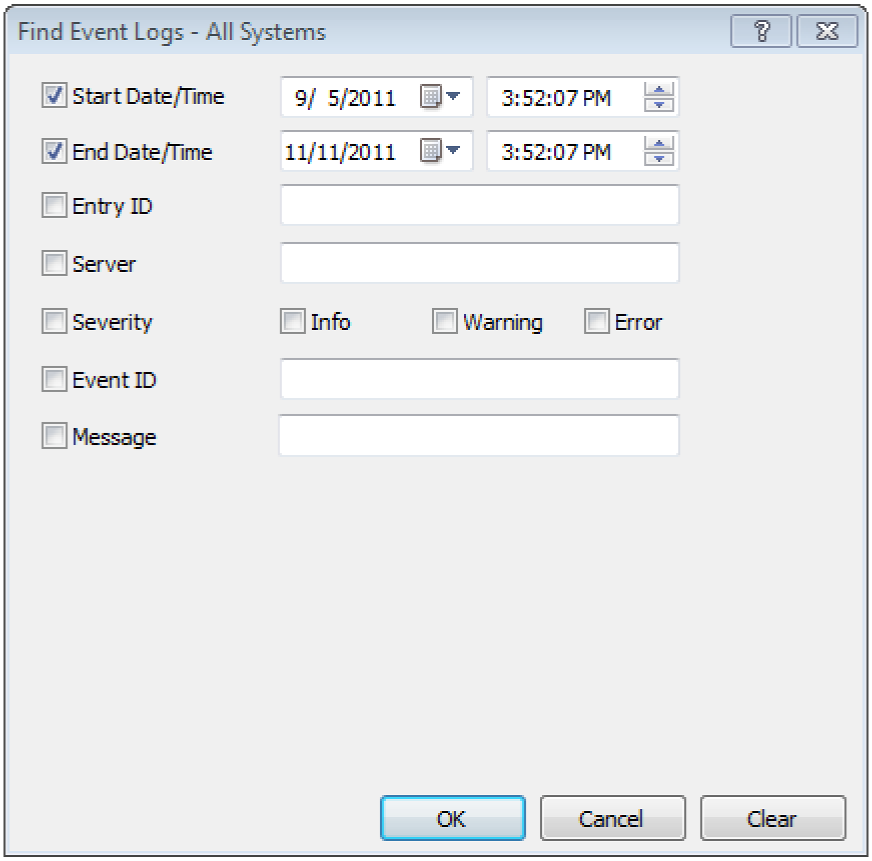
Fields (Find Audit Logs)

Enter any of the settings associated with the object in the log entry. For example, for an FTP location this could be a configuration setting, such as associated adapter, input or output, security, schedule, notifications. This is a text-based search, so you can enter partial search text.

Find Event Logs Window

The Find Event Logs Window lets you search the database for Event log entries that match the selected criteria. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.



Find Event Logs - All Systems

☑ Start Date/Time 9/ 5/2011 3:52:07 PM

☑ End Date/Time 11/11/2011 3:52:07 PM

□ Entry ID

□ Server

□ Severity □ Info □ Warning □ Error

□ Event ID

□ Message

Start Date/Time (Find Event Logs)

Check the Start Date/Time box to begin your query with the date and time listed in the date and time selection boxes. When this box is not checked, the query starts with the earliest entry in the file.

End Date/Time (Find Event Logs)

Check the End Date/Time box to terminate your query with the date and time listed in the date and time selection boxes. When this box is not checked, the query ends with the latest entry in the file.

Entry ID (Find Event Logs)

Enter the ID value for the log entry.

Server (Find Event Logs)

Enter the name of the server that logged the entry.

Severity (Find Event Logs)

Select one or all of the types of event, which indicate severity: Info, Warning, Error.

Event ID (Find Event Logs)

Enter the Event identification code. For Windows, this is the Windows Event ID; for UNIX systems, this is the syslog message ID.

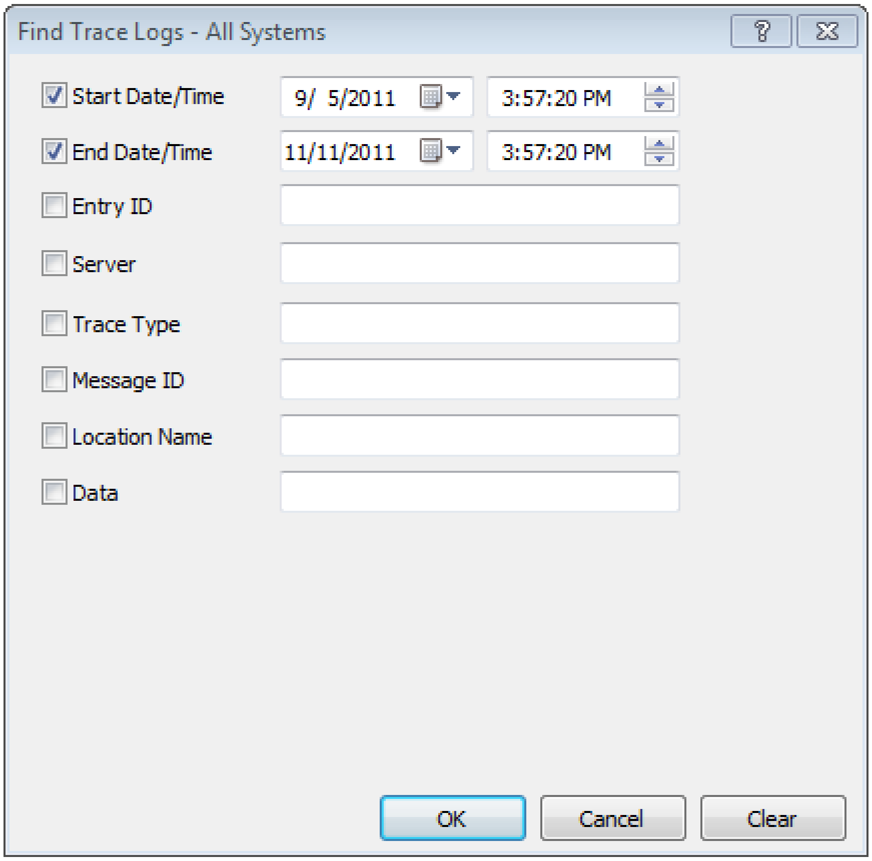
Message (Find Event Logs)

Enter the message associated with an event that occurred. Examples: an Error such as "Unable to find [product] license"; an Info message, such as "Server started." This is a text-based search, so you can enter a partial message.

Find Trace Logs Window

The Trace Logs window lets you search the database for Trace log entries that match the selected criteria. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.


Find Trace Logs - All Systems

☑ Start Date/Time 9/ 5/2011 3:57:20 PM

☑ End Date/Time 11/11/2011 3:57:20 PM

□ Entry ID

□ Server

□ Trace Type

□ Message ID

□ Location Name

□ Data

Start Date/Time (Find Trace Logs)

Check the Start Date/Time box to begin your query with the date and time listed in the date and time selection boxes. When this box is not checked, the query starts with the earliest entry in the file.

End Date/Time (Find Trace Logs)

Check the End Date/Time box to terminate your query with the date and time listed in the date and time selection boxes. When this box is not checked, the query ends with the latest entry in the file.

Entry ID (Find Trace Logs)

Enter the ID value for the log entry.

Server (Find Trace Logs)

Enter the name of the server that logged the entry.

Trace Type (Find Trace Logs)

Enter one of the predefined Trace types, for example, http, queue, pipe, sched. The types available vary by server. See the Server Properties, General page help for a list of the types.

Message ID (Find Trace Logs)

Enter a MessageWay message ID.

Location Name (Find Trace Logs)

Enter the name of a MessageWay location.

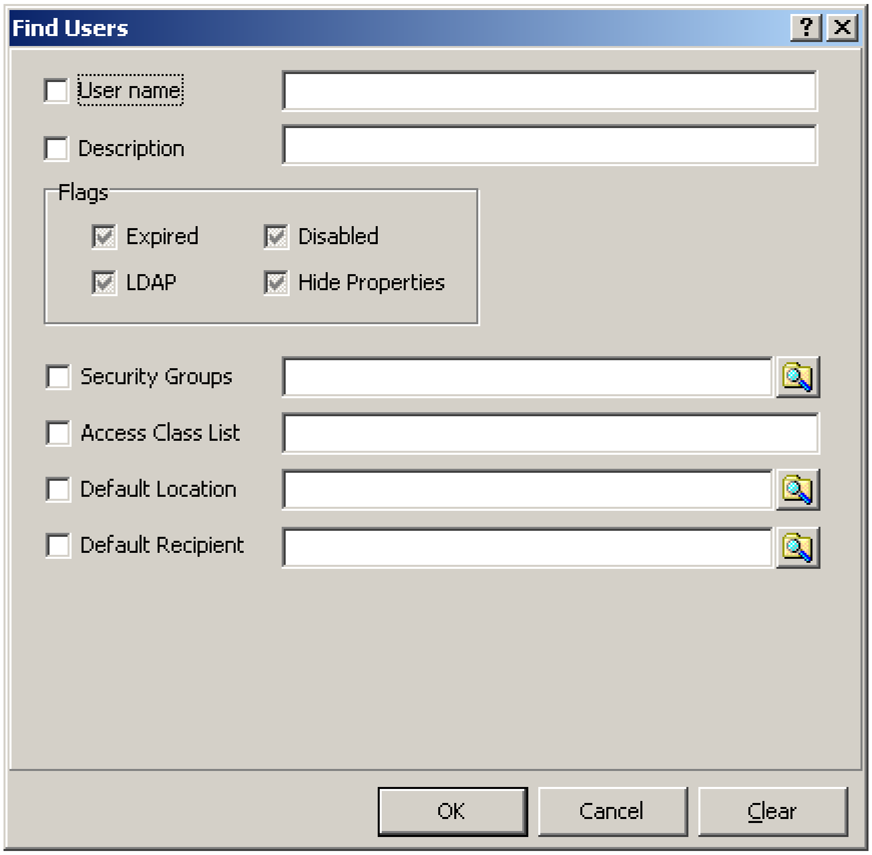
Data (Find Trace Logs)

Enter any data associated with this trace log entry, for example, for a tcp-send, this could be IP address, port number of the sender, or file size.

Find Users Window

The Find Users window allows you to search for users based on user properties. If you are currently monitoring a multi-system environment, the search will include all systems in the environment.

TIP: You do not need to first check a box that has a related field, because they are checked when you type information in the adjacent box. Clear a box to not use the information as a search criterion, but to retain it for a future search.


Find Users

□ User name

□ Description

Flags

☑ Expired ☑ Disabled

☑ LDAP ☑ Hide Properties

□ Security Groups

□ Access Class List

□ Default Location

□ Default Recipient

User Name

Type the name of a user you want to find. Use the asterisk, *, as a wildcard to broaden your search.

Description

Type all or part of a description to use as a search criterion to find a user. Use the asterisk, *, as a wildcard to broaden your search.

Flags

You can select one of three options here for each of the user properties: checked only, clear only, checked and dimmed or colored only (depending on the Windows version). Check these boxes to search for users that currently have the **Expired**, **Disabled**, **LDAP**, or **Hide** option boxes selected. Clear the boxes to find users that do not have the boxes checked. Click the boxes until it is both checked and dimmed or just colored to find all users with the option either checked or unchecked.

Security Groups

Type or select a security group to which a user belongs to use as a search criterion. Use the asterisk, *, as a wildcard to broaden your search.

Access Class List

Type one or more access classes, separated by commas, to use as a search criterion to find users. Use the asterisk, *, as a wildcard to broaden your search.

Default Location

Type or select a default location to use as a search criterion to find users. Use the asterisk, *, as a wildcard to broaden your search.

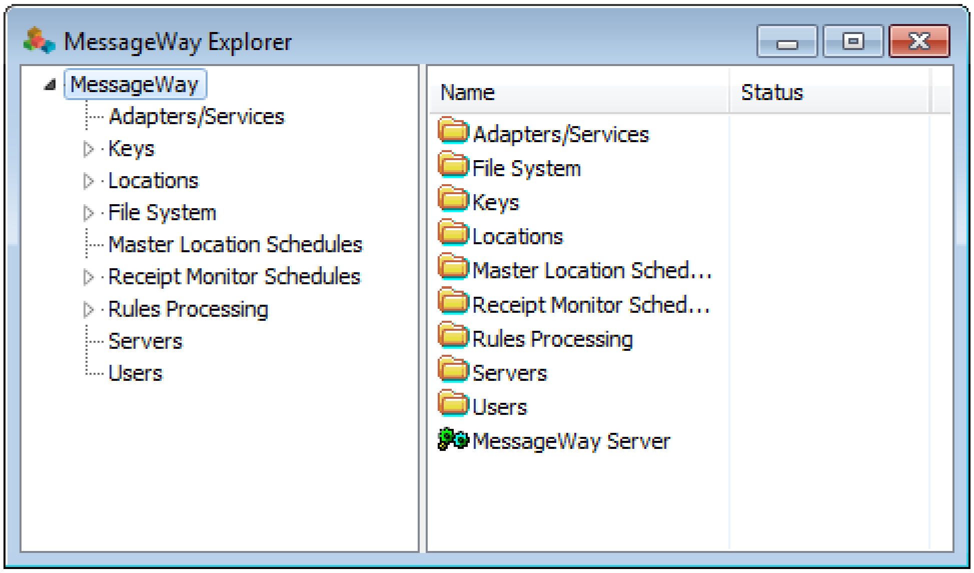
Default Recipient

Type or select a default recipient to use as a search criterion to find users. Use the asterisk, *, as a wildcard to broaden your search.

Folder Properties Window

The Folder Properties window allows you to configure security for operations associated with an object, such as an adapter or service, keys, location, master location schedule, receipt monitor schedule, rule, server or user. Each folder has an access list that identifies which users or user groups may access that folder, and what they may do. Users and user groups also have their own access rights. When users attempt to access a folder or an object within a folder, their effective access rights are compared with the effective access rights on the object, and the requested action is permitted when the common rights allow the action.

Folders are identified by the folder icon 📂. Each folder has its set of properties, as does every other object, such as a location, an adapter or service or a user. Folders may be embedded within folders. Users may create sub-folders to organize their definitions. The highest set of folders are those installed with MessageWay. The number of folders will vary depending on which options you have and how many sub-folders you have created, but they all have properties. Lower-level folders can inherit security settings from higher-level folders. To access Folder Properties windows, refer to the topic, ***How to View Properties*** (on page 1214).

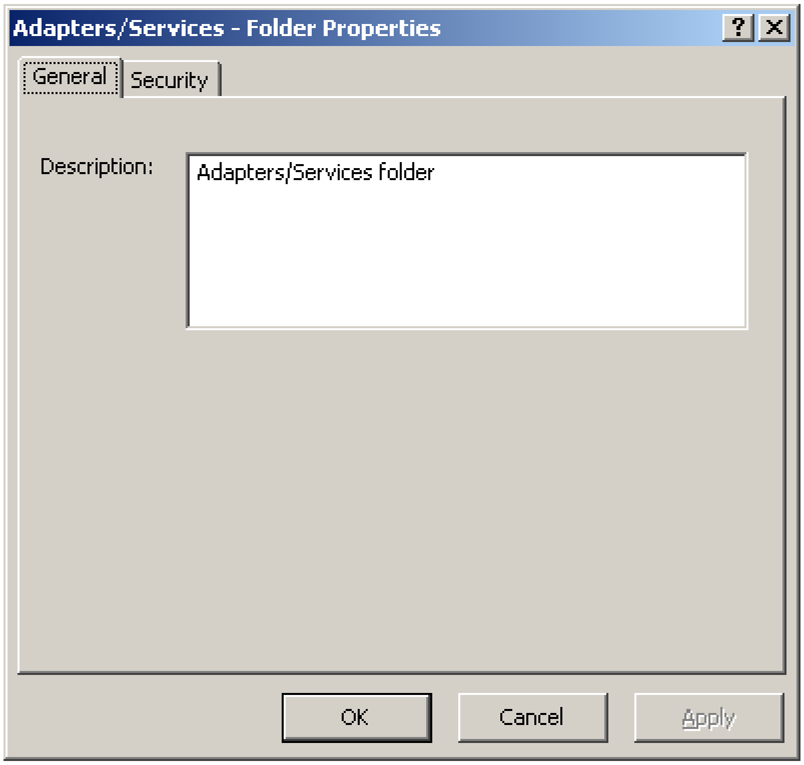


(Folder Properties) General Page

The **General** page of the Folder Properties window contains an area to enter a description of the folder.

IMPORTANT: To perform any functions for a folder, users must have appropriate security, as listed on their **Rights** page of the User Properties window.

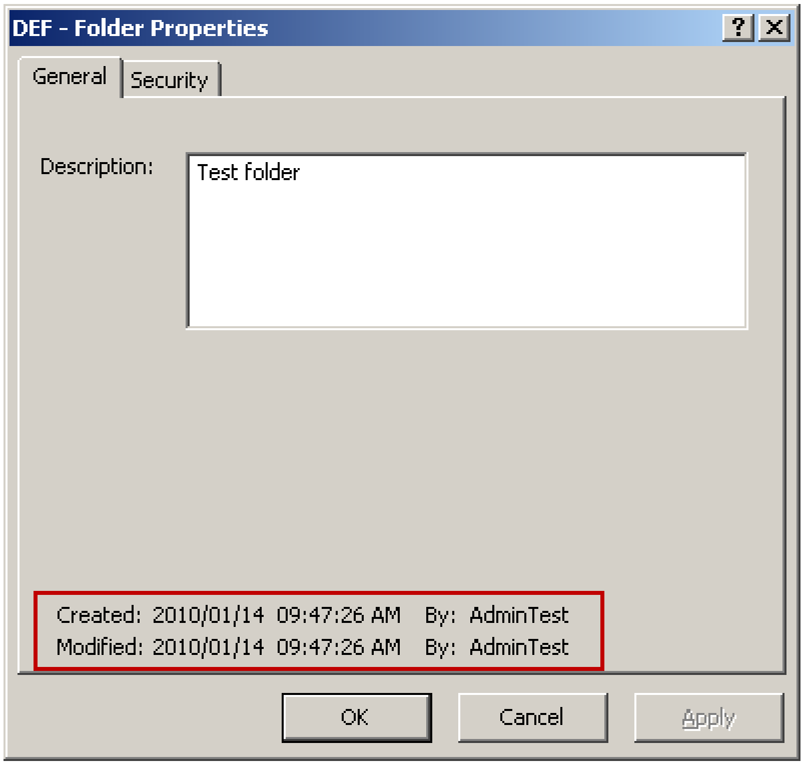
Only folders that users create will display information about its creation. System folders created during the install process do not have this information. For example, there is no information about creation of the Adapters/Services folder, because it is a system folder.



Description: Adapters/Services folder

General Page, System Folder (Folder Properties Window)

A user, AdminTest, created the following folder, so it does show the creation information.



Description: Test folder

Created: 2010/01/14 09:47:26 AM By: AdminTest
Modified: 2010/01/14 09:47:26 AM By: AdminTest

General Page, Folder Created by User (Folder Properties Window)

Description

The Description box allows users to enter text about the folder.

Created

Created is the date and time this folder was created.

By (Created)

This value is the MessageWay user that created the folder. When a system service creates an entity, this value identifies the service, which appears in angle brackets, < >, to distinguish it from a MessageWay user. For example, imported definitions will use <mwimp>.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

(Folder Properties) Security Page

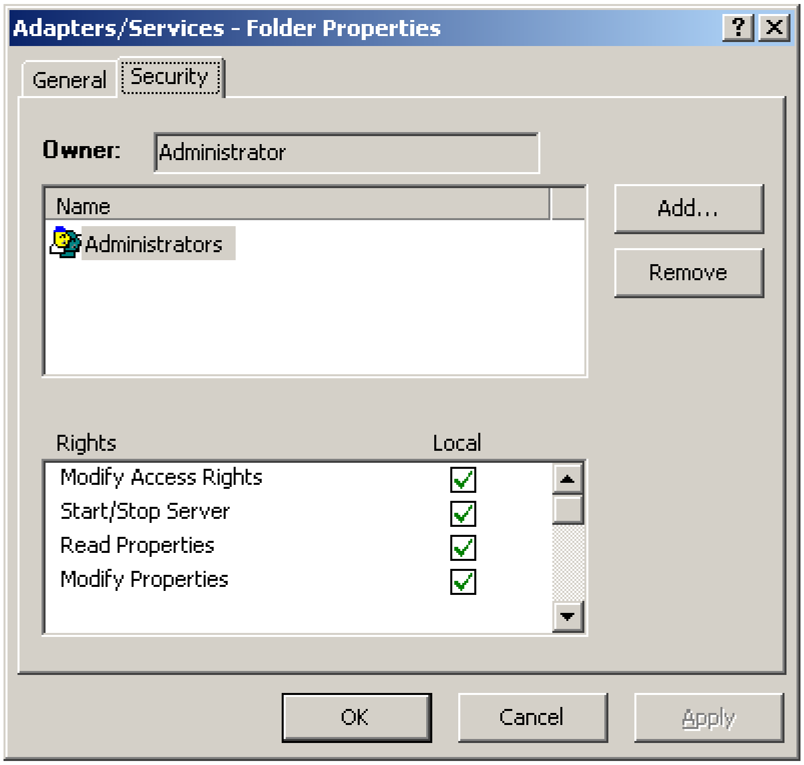
The **Security** page of the Folder Properties window shows the owner of the folder, which users or user groups are allowed access to the folder and its contents and what actions these users or user groups may perform. Access to this folder is controlled by an access list, which consists of a list of users or user groups and the rights that each one has. The access list may be inherited by objects directly beneath the folder.

IMPORTANT: When you copy or move this object, the affect on access rights varies. When you copy and paste an existing object (location, rules profile or key), MessageWay will remove all access rights that have been inherited from the object's current parent folder and update all inherited access rights from the object's new parent folder. When you cut and paste/move an existing object (folder, location, rules profile or key), MessageWay will retain all access rights that have been inherited from the object's current parent folder. To update the inherited access rights to those of the object's new parent folder, for each user and group on the list, you must first clear the Inherit new users/groups box and then recheck the box. After moving a folder, the access rights must be correctly updated for the folder itself and for all of its offspring (sub-folders, locations, rules profiles and keys).

Different folders have different rights. For more information about the rights for a specific folder, refer to the topic, ***Rights (Folder Properties)*** (on page 1029).

IMPORTANT: To perform any functions for a folder, users must have appropriate security, as listed on their **Rights** page of the User Properties window.

Owners of folders may give ownership to another user. System folders are originally owned by the user *Administrator*.



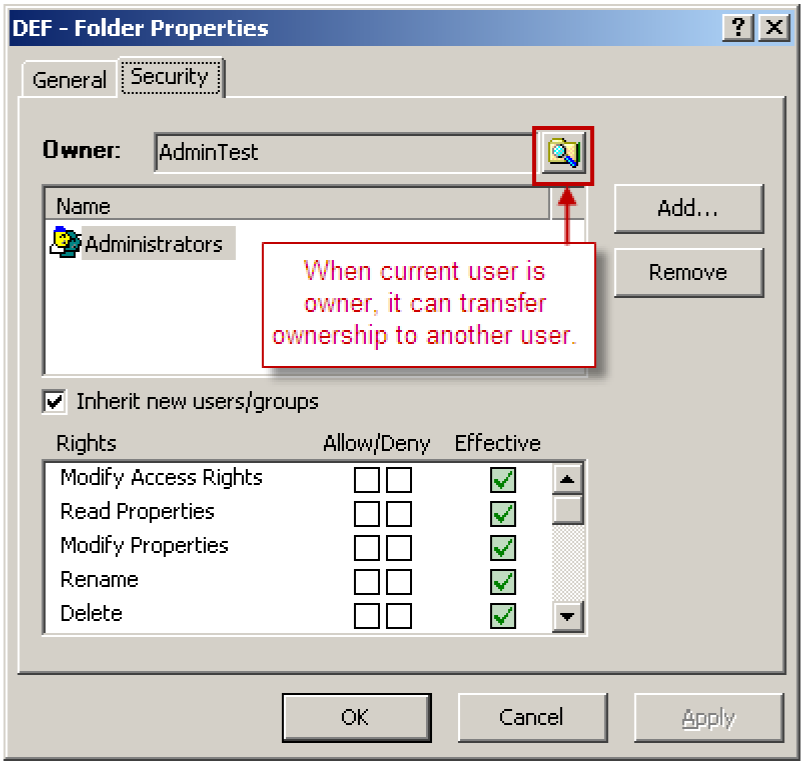
Owner: Administrator

Name
Administrators

Rights	Local
Modify Access Rights	☑
Start/Stop Server	☑
Read Properties	☑
Modify Properties	☑

Security Page for Adapters/Services Folder, Current User Not Owner (Folder Properties Window)

Folders created by users are owned by the user that created the folder.



Owner: AdminTest

Name: Administrators

When current user is owner, it can transfer ownership to another user.

☑ Inherit new users/groups

Rights	Allow/Deny	Effective
Modify Access Rights	□ □	☑
Read Properties	□ □	☑
Modify Properties	□ □	☑
Rename	□ □	☑
Delete	□ □	☑

Security Page for User Folder, Current User Is Owner (Folder Properties Window)

Owner

Initially, the owner is the user that created the folder, which is the original administrator. The owner may transfer ownership to another user. Owners have complete access rights to the folder, regardless of other configurations. They have the right to change the names on the access list and the right to read and change the properties of the folder.

Browse Button

When you are the owner, you may select this button to give ownership to another user.

Name

The Name list contains users or user groups that are permitted to access this folder. Use the **Add** and **Remove** buttons to maintain this list. The Name list and the Rights list compose the access list used by MessageWay to determine who has what rights to this folder.

Add Button

Select this button to add names of users or user groups to the Name list.

Select from

From the Select User or User Group window, click the down arrow. Select a folder from the list that contains the user or user group you want to show in the list box. Typically, this is the Users folder.

Group Listbox

Choose from among the users and user groups on the list to which you want to give access. To show a list of users and user groups, you must select a folder from the Select From list where the users and groups are defined. The rights for a user on this list are the combined rights for all groups to which the user belongs. You may add a user to the list who also belongs to a group on the list. In such a case, it only makes sense to add capabilities for the individual, because denying capabilities has no effect.

Select

To add this user or user group to the Name list, either choose a group from the list box and it will display in the box beneath it or type a group name in the box. Click the **Select** button to complete the process.

Remove Button

Select this button to delete names of users or user groups from the access list.

Inherit new users or groups

This check box appears for subfolders. Each folder has an access list, which comprises users or user groups and their rights. When this box is selected, the entire access list of a higher level folder will be added to the access list of this folder. To remove users or groups from the list, clear this box first.

Rights

The Rights list contains the functions that the users or user groups in the Name list may perform. The Rights list and the Name list compose the access list to determine who has what rights to this folder. Select the user or user group in the Name list to see their rights, which will be selected. Click a box to select or clear the right. To select or clear all rights at once, hold **SHIFT** while you select one of the boxes.

Subfolders may inherit rights from their parent folders. These inherited rights are their effective rights, and are display-only. The rights for a user on this list are the combined rights for all groups to which the user belongs. You may add a user to the list who also belongs to a group on the list. In such a case, it only makes sense to add capabilities for the individual, because denying capabilities has no effect. You may add rights for a user by selecting the Allow boxes.

Different folders will have different rights. The following tables describe the rights for the predefined system folders.

The rights for the **Adapters/Services** folder are as follows:

Right	Description
Modify Access Rights	Change values on **Security** page of Adapters/Services Folder Properties window. Also requires the right, **Read Properties**.
Start/Stop Server	Start, stop, suspend or resume adapters or services. Also requires the rights, **Read Properties**.
Read Properties	View the statuses of the adapters and services. When this is unchecked, users cannot access the Adapters/Services Properties window.
Modify Properties	Change properties for the adapters or services, such as thread distribution, startup options and security. Also requires the rights, **Read Properties**. When this is unchecked, users may still be able to access the Adapters/Services Properties window, but the properties are dimmed.

The rights for the **File System**, **Locations**, **Keys**, **Receipt Schedules** and **Rules Processing** folders are as follows:

CAUTION: Except for the *File System* folder, changes to any one of these folders, affects all of them.

Right	Description
Modify Access Rights	Change values on **Security** page of the **Locations**, **Receipt Schedules**, and the **Rules Processing Folder Properties** window. Also requires the right, **Read Properties**.
Read Properties	View properties of the **Locations**, **Rules Processing** and the **Receipt Schedules** folder.
Modify Properties	Change properties of the **Locations**, **Rules Processing** and the **Receipt Schedules** folder. Also requires the right, **Read Properties**.
Rename	Change the name of user-defined folders. Also requires the right, **Read Properties**.
Delete	Delete user-defined folders. Also requires the right, **Read Properties**.
Create	Create folders and locations. Also requires the right, **Read Properties**.
Perform Location Actions	Controls user ability to hold messages, release messages, hold outputs or release outputs for a location. Also requires the right, **Read Properties**.
Resubmit Messages	Controls user ability to resubmit messages. Also requires the right, **Read Properties** and **Modify Message Properties**.
Redirect Messages	Controls user ability to redirect messages. Also requires the right, **Read Properties** and **Modify Message Properties**.
Release Messages	Controls user ability to release messages. Also requires the right, **Read Properties** and **Modify Message Properties**.

Right	Description
Restart Receive	Controls user ability to restart transfer of messages only partially received. Also requires the right, **Read Properties** and **Modify Message Properties**.
Cancel Messages	Controls user ability to cancel messages. Also requires the right, **Read Properties** and **Modify Message Properties**.
Retrieve Archive Messages	Controls user ability to retrieve messages from archive. Also requires the right, **Read Properties** and **Modify Message Properties**.
Resubmit Archive Messages	Controls user ability to resubmit messages retrieved from archive. Also requires the right, **Read Properties** and **Modify Message Properties**.
Delete Archive Message Content	Controls user ability to delete messages retrieved from archive. Also requires the right, **Read Properties** and **Modify Message Properties**.
Read Message Properties	View the properties of messages. Also requires the right, **Read Properties**.
Modify Message Properties	Controls user ability to: modify retention date and change priority; mark for archive and mark for deletion. Also requires the rights, **Read Properties** and **Read Message Properties**.
View Messages	Read message content. Also requires the rights, **Read Properties** and **Read Message Properties**.
Upload Messages	Send messages to MessageWay. Required for the user or user group on the access list when this is the destination location. Also requires the rights, **Read Properties** and **Read Message Properties**.
Download Messages	Retrieve messages from MessageWay. Required for the user or user group on the access list when this is the sending location or the destination location. Also requires the rights, **Read Properties** and **Read Message Properties**.

The rights for the **Servers** folder are as follows:

Right	Description
Modify Access Rights	Change values on **Security** page of **Servers** Folder Properties window. Also requires the right, **Read Properties**.
Start/Stop Server	Start, stop, suspend or resume servers. Also requires the rights, **Read Properties**.
Read Properties	View the statuses of the **Servers**. When this is unchecked, users cannot access the Servers Properties window.
Modify Properties	Change properties for the servers, such as startup type, trace or security. Also requires the rights, **Read Properties**. When this is unchecked, users may still be able to access the Servers Properties window, but the properties are dimmed.

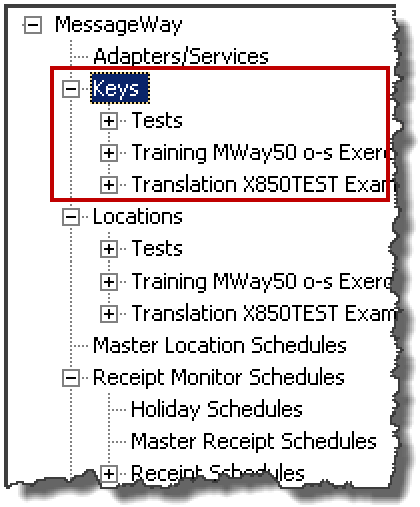
The rights for the **Users** folder are as follows:

Right	Description
Modify Access Rights	Change values on **Security** page of **Users** folder. Also requires the right, **Read Properties.**
Read Properties	View properties of **Users** folder.
Modify Properties	Change properties of **Users** folder. Also requires the right, **Read Properties.**
Delete	Delete user-defined folders. Also requires the right, **Read Properties.**
Create	Create folders and users. Also requires the right, **Read Properties.**

Key Properties Window

The Key Properties window allows you to configure properties for an existing key used by MessageWay. The Key Properties window is created when a key is generated or imported.

Keys are accessible from the **Keys** folder in MessageWay Explorer. You can store them in one of the existing locations folders, all of which display beneath the **Keys** folder, or you can create additional folders.

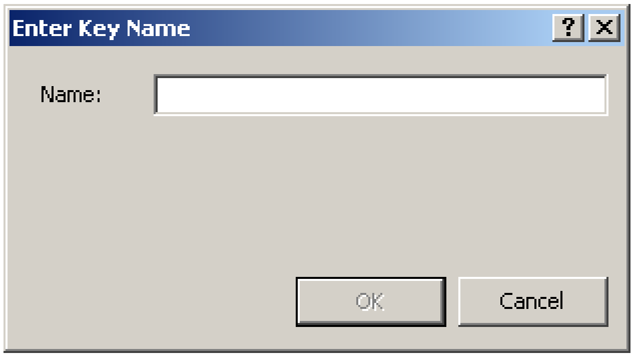


IMPORTANT: To better organize configurations, locations folders also appear beneath other folders whose configurations are related to location configurations, such as the **Keys** folder, **Receipt Schedules** folder, and the **Rules Processing** folder. Any changes to the folder structure in these folders affects all folders that use it, including the **Locations** folder. When you add a new folder, it also appears in the other folders. You cannot delete a folder that contains configurations, but if you delete an empty folder, it is also removed from the other folders.

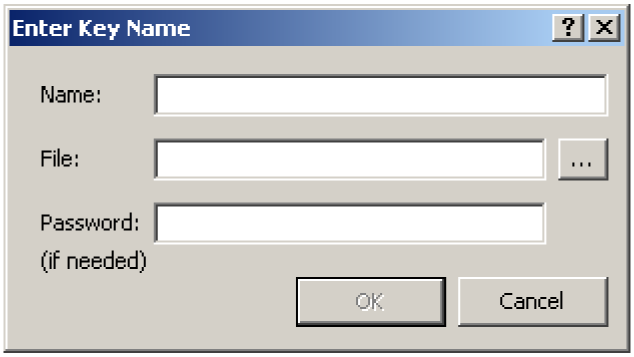
Enter Key Name Dialog Box

The **Enter Key Name** dialog box appears when you generate a key and when you import a key. The import version has additional fields.

The following dialog box appears when you generate a key.



This dialog box appears when you import a key.



Name

Type the name of a key up to 64 displayable characters.

File

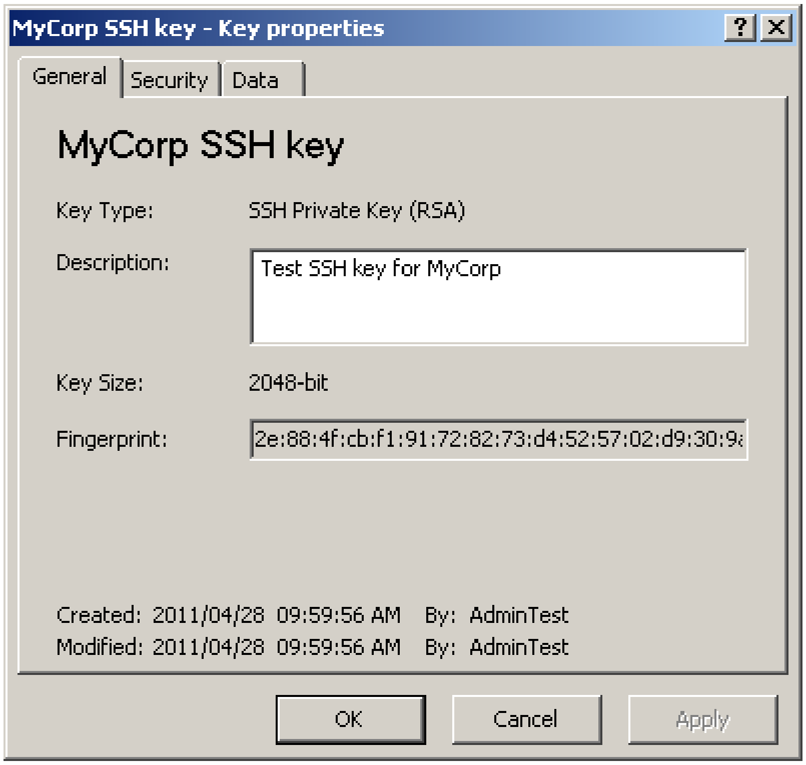
Enter the path and file name of the key file to import.

Password

If there is a password protecting the private key, type the password associated with the key to be imported.

(Key Properties) General Page

The **General** page of the Key Properties window displays the name of the key, the key type, a description, the key size, the fingerprint of the key, and creation and modification information of any properties displayed in the window.



MyCorp SSH key

Key Type: SSH Private Key (RSA)

Description: Test SSH key for MyCorp

Key Size: 2048-bit

Fingerprint: 2e:88:4f:cb:f1:91:72:82:73:d4:52:57:02:d9:30:9a

Created: 2011/04/28 09:59:56 AM By: AdminTest
Modified: 2011/04/28 09:59:56 AM By: AdminTest

Key Name (display only)

This is the name of the key assigned by the user.

Key Type (display only)

This is the type of the key. For SSH keys, this algorithm used to create the key will be DSA or RSA.

Description

Type a description to provide useful information about this key.

Key Size (display only)

This is the number of bits used by the cyper algorithm. Various algorithms use various key lengths to encrypt the data.

Key Fingerprint

This is the fingerprint of the public part of your client key. You cannot change this value, but you can copy it to the clipboard.

Created

Created is the date and time this key was created or imported.

By (Created)

This value is the MessageWay user that created or imported the key.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

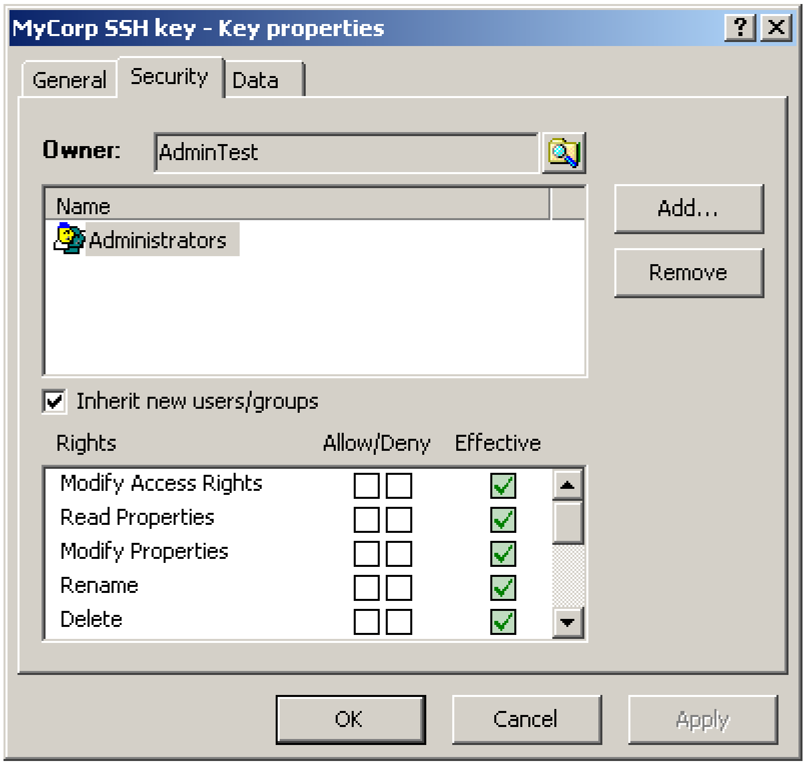
(Key Properties) Security Page

The Security page of the Key Properties window shows the owner of the key, which users or user groups are allowed access to the key and what actions these users or user groups may perform.

After moving a folder, the access rights must be correctly updated for the folder itself and for all of its offspring (sub-folders, locations, rules profiles and keys).

The access list controls access to a key. It consists of a list of users or user groups and the rights that each one has. The key may inherit users and user groups and their rights from the Keys folder or one of its subfolders. These rights appear in the Effective column when you select the user or user group in the Name box.

IMPORTANT: To perform any functions for a key, users must also have appropriate rights set on their Rights page of the User Properties window.



Owner: AdminTest

Name: Administrators

☑ Inherit new users/groups

Rights	Allow/Deny	Effective
Modify Access Rights	□ □	☑
Read Properties	□ □	☑
Modify Properties	□ □	☑
Rename	□ □	☑
Delete	□ □	☑

IMPORTANT: When you copy or move this object, the affect on access rights varies. When you copy and paste an existing object (location, rules profile or key), MessageWay will remove all access rights that have been inherited from the object's current parent folder and update all inherited access rights from the object's new parent folder. When you cut and paste/move an existing object (folder, location, rules profile or key), MessageWay will retain all access rights that have been inherited from the object's current parent folder. To update the inherited access rights to those of the object's new parent folder, for each user and group on the list, you must first clear the Inherit new users/groups box and then recheck the box. After moving a folder, the access rights must be correctly updated for the folder itself and for all of its offspring (sub-folders, locations, rules profiles and keys).

For more information about users and user security, refer to the topic, ***Configuring User Security*** (on page 375).

Owner

Initially, the owner is the user that created the object. The owner may transfer ownership to another user. Owners have complete access rights to the object, regardless of other configurations. Owners always have the right to change the names on the access list and the right to read and change the properties of the object.

Browse Button

When you are the owner, click this button to give ownership to another user.

Name

The Name list contains users or user groups that are permitted to access this object. Use the **Add** and **Remove** buttons to maintain this list. The Name list and the Rights list compose the access list used by MessageWay to determine who has what rights to this object.

Add Button

Select this button to add names of users or user groups to the Name list.

Remove Button

Select this button to delete names of users or user groups from the access list.

Inherit new users or groups

This box refers to different entities depending on whether the location is in the *Locations* folder or the *File System* folder. When this box is checked, any users or user groups that are added to the Name list of the parent folder under the Locations folder or to the Name list of the containing location/directory under the File Systems folder will also be added to the Name list of this object. To remove users or user groups from the list, you must clear this box first.

Rights

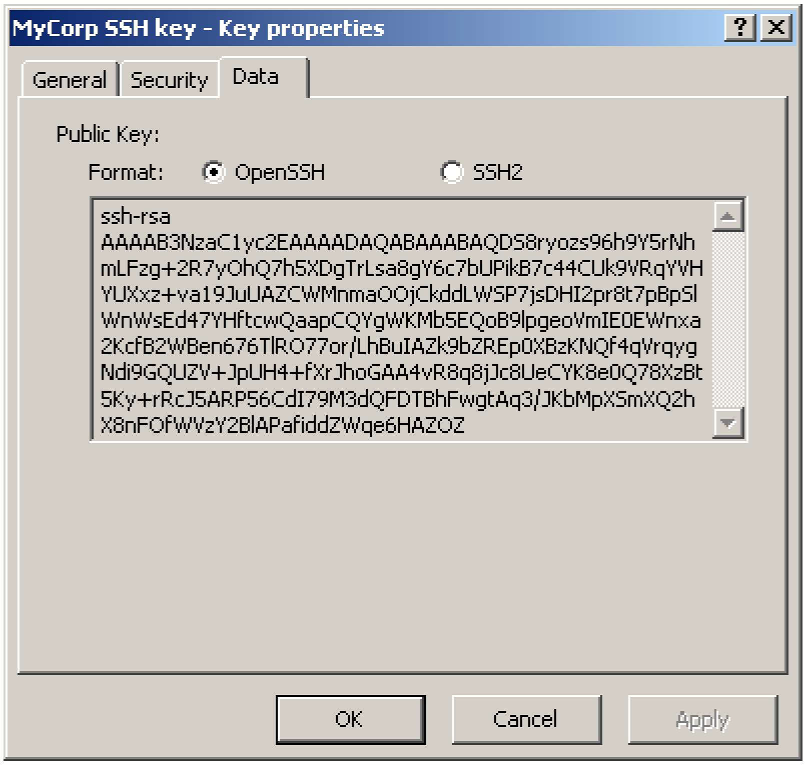
The Rights list contains the functions that the users or user groups in the Name list may perform. The Rights list and the Name list compose the access list to determine who has what rights to this object. Objects may inherit rights from their parent folder. These rights appear in the Effective Rights column when you select the user or user group in the Name list.You may override these effective rights by checking the Allow/Deny boxes. To check or clear all rights at once, hold **SHIFT** while you click one of the boxes.

The rights for an individual key are as follows:

Right	Description
Modify Access Rights	Change values on **Security** page of the Key Properties window. Also requires the right, **Read Properties**.
Read Properties	View properties of the key.
Modify Properties	Change properties of the key. Also requires the right, **Read Properties**.
Rename	Change the name of the key. Also requires the right, **Read Properties**.
Delete	Delete the key. Also requires the right, **Read Properties**.

(Key Properties) Data Page

The **Data** page of the Key Properties window shows the public key in OpenSSH or SSH2 format.



Public Key:

Format: ● OpenSSH ○ SSH2

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDS8ryozs96h9Y5rNh
mLFzg+2R7yOhQ7h5XDgTrLsa8gY6c7bUPikB7c44CUk9VRqYVH
YUXxz+va19JuUAZCWMnmaOOjCkddLWSP7jsDHI2pr8t7pBpSl
WnWsEd47YHftcwQaapCQYgWKMb5EQoB9lpgeoVmIE0EWnxa
2KcfB2WBen676TlRO77or/LhBuIAZk9bZREp0XBzKNQf4qVrqyg
Ndi9GQUZV+JpUH4+fXrJhoGAA4vR8q8jJc8UeCYK8e0Q78XzBt
5Ky+rRcJ5ARP56CdI79M3dQFDTBhFwgtAq3/JKbMpXSmXQ2h
X8nFOfWVzY2BlAPafiddZWqe6HAZOZ
```

Format

Select either the OpenSSH or the SSH2 format to view the public key.

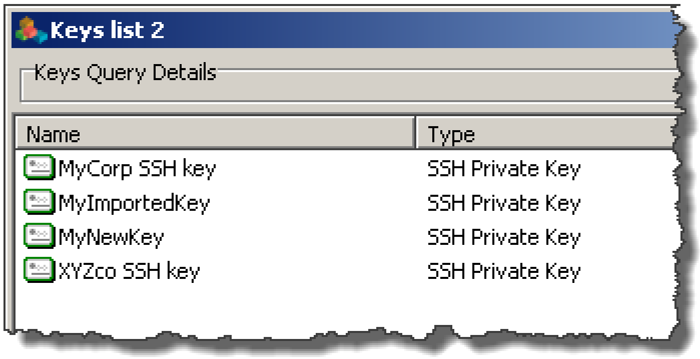
Public Key Data

This is the public part of your client key. You cannot change it, but you can copy it to the clipboard. You must provide this information to the server with which you will communicate. The server uses this to authenticate you as a client.

Keys List Window

The Keys List window appears when you use the **Find Keys** command to search for client keys. When you search through multi-system environments, a System Name column also appears.

To sort by column content, click the column heading.

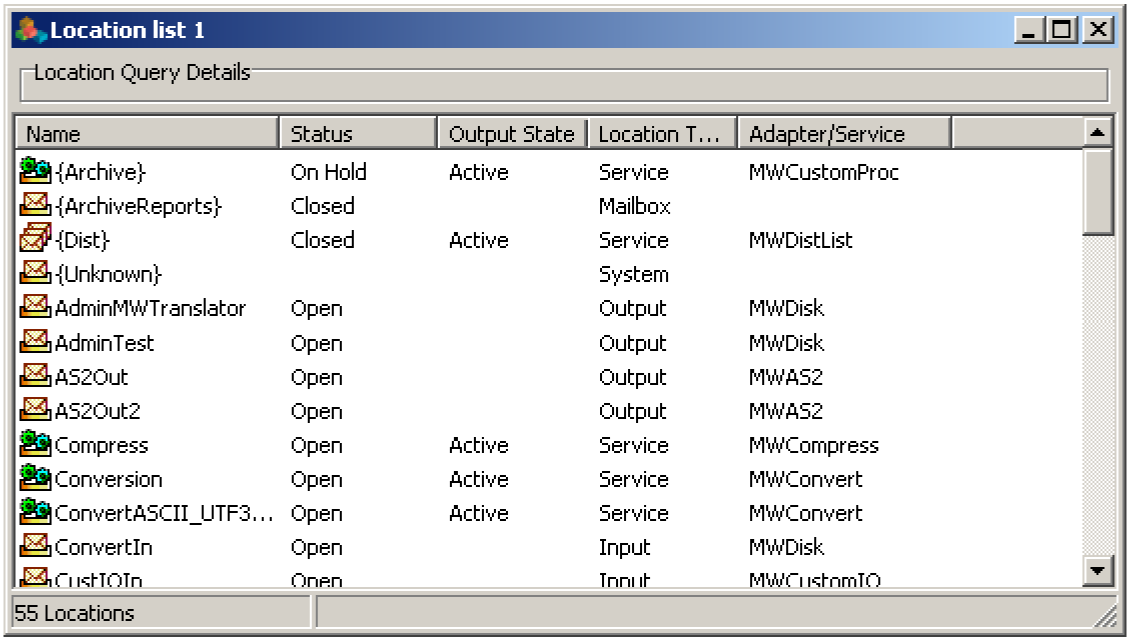


Name	Type
MyCorp SSH key	SSH Private Key
MyImportedKey	SSH Private Key
MyNewKey	SSH Private Key
XYZco SSH key	SSH Private Key

Location List Window

The Location List window appears when you use the **Find Locations** command to search for locations. When you search through multi-system environments, a System Name column also appears.

To sort by column content, click the column heading. For more information, refer to the topic, ***Locations (MessageWay Explorer)*** (on page 1218).



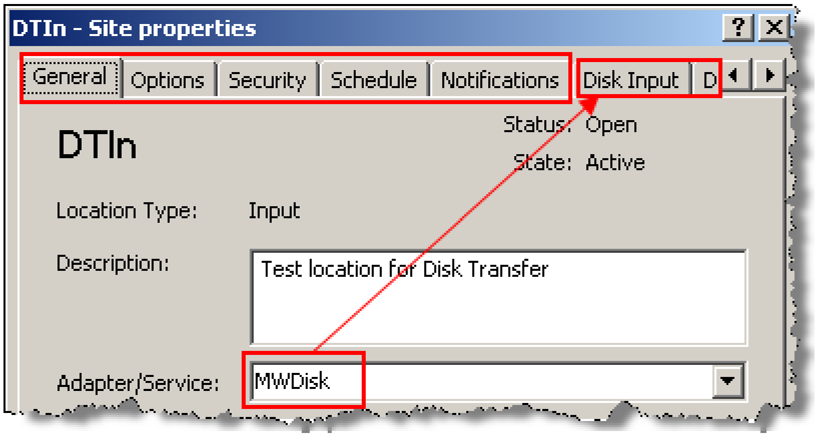
Name	Status	Output State	Location T...	Adapter/Service
{Archive}	On Hold	Active	Service	MWCustomProc
{ArchiveReports}	Closed		Mailbox	
{Dist}	Closed	Active	Service	MWDistList
{Unknown}			System	
AdminMWTranslator	Open		Output	MWDisk
AdminTest	Open		Output	MWDisk
AS2Out	Open		Output	MWAS2
AS2Out2	Open		Output	MWAS2
Compress	Open	Active	Service	MWCompress
Conversion	Open	Active	Service	MWConvert
ConvertASCII_UTF3...	Open	Active	Service	MWConvert
ConvertIn	Open		Input	MWDisk
CustIOIn	Open		Input	MWCustomIO

55 Locations

Location (Service Location, Site, Mailbox) Properties Window

The location (Service Location, Site, Mailbox) Properties window allows users to specify configurations that control the transfer of messages to and from MessageWay. Adapters and services are the means by which messages are transferred automatically. Since adapters and services require different types of information, a location is associated with only one adapter or service at any given time. Locations that do not use auto-delivery, such as the system mailbox, {Unknown} and collection mailboxes, are not associated with an adapter or service.

Generic information that controls processing of messages appears on the first five pages: **General**, **Options**, **Security**, **Schedule**, and **Notifications**. To the right of these is information specific to the adapter or service that is selected on the **General** page.



DTIn

Status: Open

State: Active

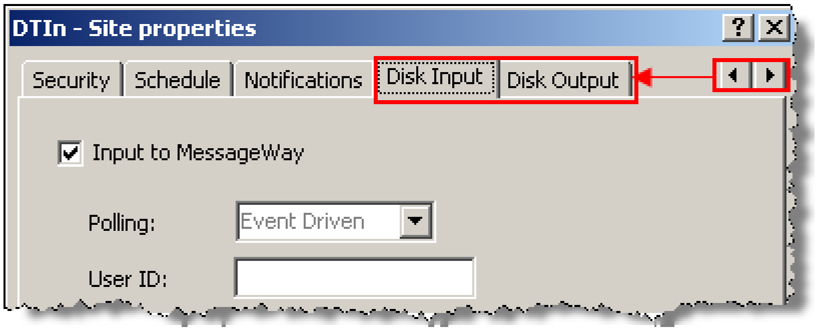
Location Type: Input

Description: Test location for Disk Transfer

Adapter/Service: MWDisk

Arrangement of Pages for Locations Associated with Adapter or Service (Site Properties Window)

Use the tab scroll buttons, ◀▶, to view other tabs.



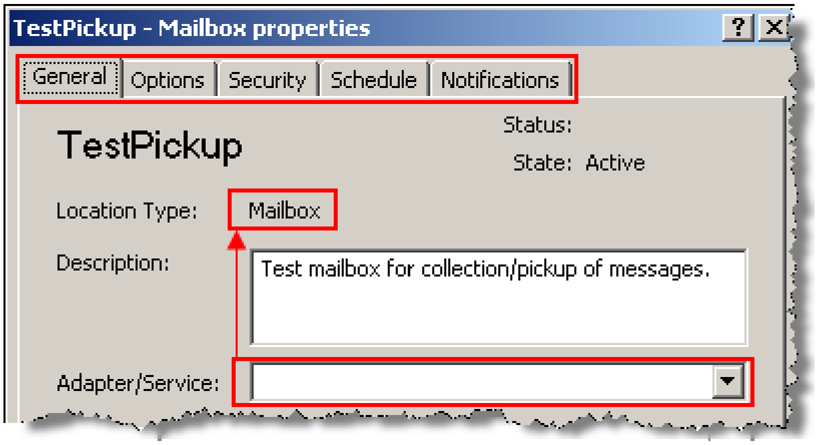
☑ Input to MessageWay

Polling: Event Driven

User ID:

Tab Scroll Buttons (Location Properties Window)

The Location Type listed on the **General** Page shows when the location has been configured for input only (*Input*), output only (*Output*), or both input and output (*I/O*). Service locations, such as Rules Processing or MWTranslator, will have a location type of *service*. Locations used for collection (*Mailbox*) hold messages until someone picks them up.



TestPickup

Status:

State: Active

Location Type: Mailbox

Description: Test mailbox for collection/pickup of messages.

Adapter/Service:

Arrangement of Pages for Locations Not Associated with Adapter or Service (Mailbox Properties Window)

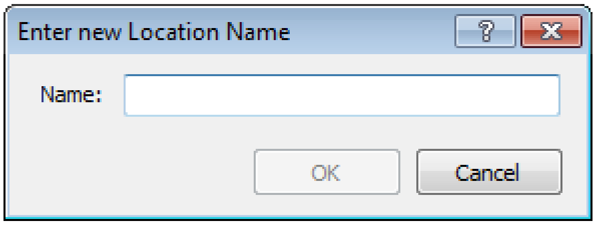
Mailboxes, such as those used for collection and system locations, are not associated with adapters or services. The location, {Unknown}, is a system mailbox that holds messages in error when the destination location does not exist.

NOTE: MessageWay now supports a traditional hierarchical or directory view of messages for FTP and SFTP clients. To support this feature, as of MessageWay version 6.1, there are two systems for locations: the original one that displays the locations in the *Locations* folder and the hierarchical message store that displays the locations in the *File System* folder. The two systems are separate, distinguished by the initial forward slash (/) required for directory names in the File System folder. You can move locations between systems, but they must meet the naming conventions and requirements of that system.

For a description of the differences between locations in the Locations folder and locations in the File System folder, refer to the topic ***Overview of Location Properties*** (on page 453).

Enter New Location Name

The **Enter New Location Name** dialog box appears when you add a location.

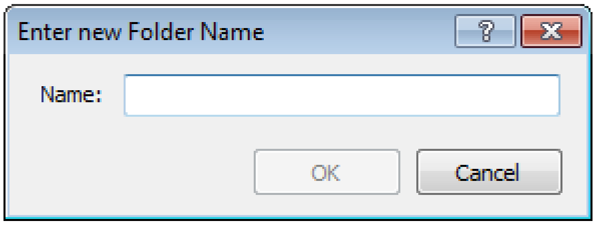


For instructions to create locations in the Locations folder, refer to the topic, ***Adding Locations and Folders to the Locations Folder*** (on page 461).

For instructions to create locations in the File System folder, refer to the topic, ***Adding Locations and Directories to the File System Folder*** (on page 465).

Enter New Folder Name

The **Enter New Folder Name** dialog box appears when you add a user folder to the Locations folder.



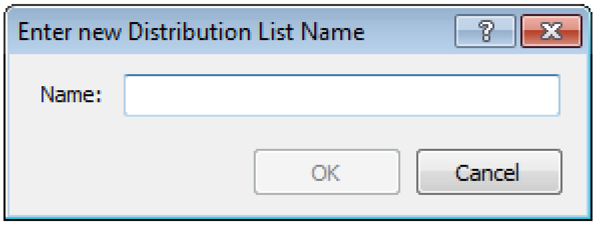
Type a folder name with up to 64 displayable characters. To add a location to this folder, right-click the folder in the right pane of MessageWay Explorer, and select **Add Location**, or drag and drop an existing location on the folder. Note that you can only create folders to organize locations under the *Locations* folder, not under the *File System* folder.

IMPORTANT: Since location names must be unique within the Locations folder, you cannot add a location that exists elsewhere to a folder.

For instructions to create a folder, refer to the topic,***Adding Locations and Group Folders*** (on page 461).

Enter New Distribution List Name

The Enter New Distribution List Name dialog box appears when you add a distribution list.



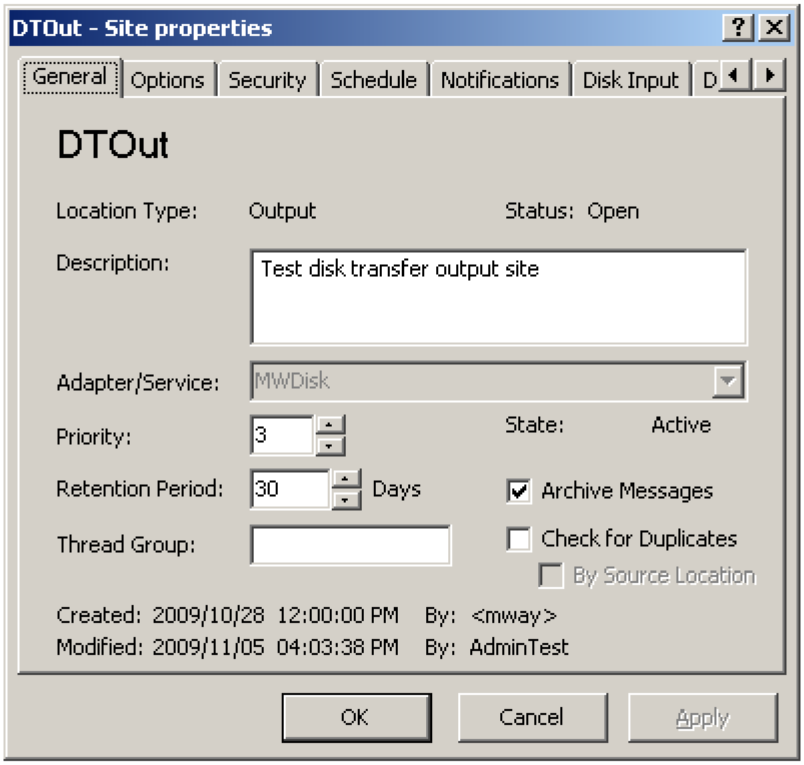
Type a distribution list name with up to 64 displayable characters, excluding the comma (,) and colon (:).

For instructions to configure a distribution list, refer to the topic, ***Specifying Distribution List Location Parameters.*** (on page 596)

(Location Properties) General Page

The **General** page of the location (Service Location, Site, Mailbox) Properties windows shows the adapter or service currently associated with the location. A location is associated with a single adapter or service at any given time. When you do not specify an adapter or service, this location holds messages until users collect them.

This page shows other processing requirements for messages transferred from MessageWay using this location, such as the priority, retention period, thread group assignments, whether to archive messages or to check for duplicates.



DTOut

Location Type: Output

Status: Open

Description: Test disk transfer output site

Adapter/Service: MWDisk

Priority: 3

State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

☐ Check for Duplicates

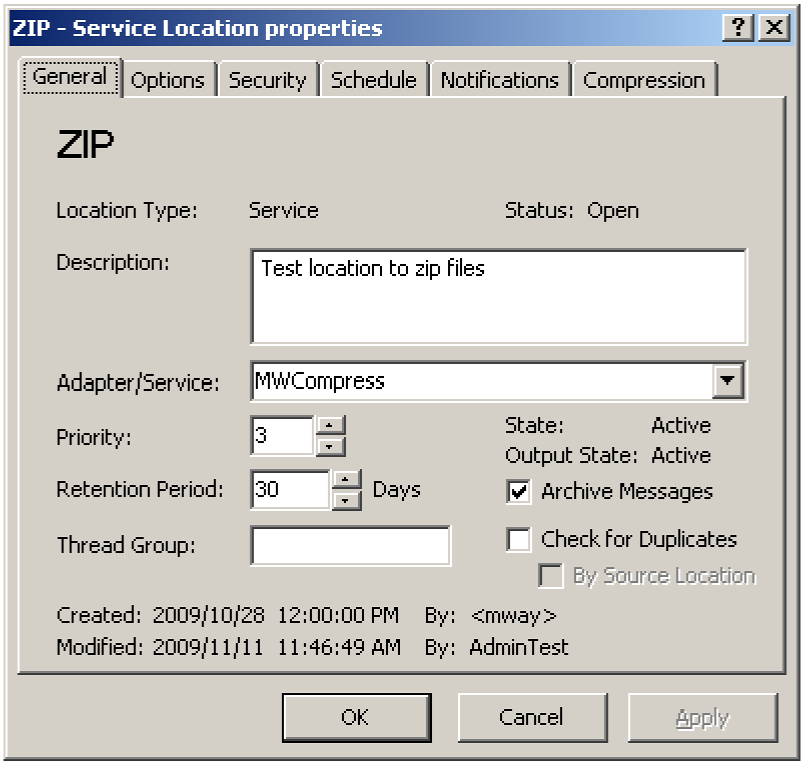
☐ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/05 04:03:38 PM By: AdminTest

General Page, Site (Site Properties)

The following example shows all statuses available for a service location, which includes *Output State*.



ZIP

Location Type: Service Status: Open

Description: Test location to zip files

Adapter/Service: MWCompress

Priority: 3

State: Active

Output State: Active

Retention Period: 30 Days

☑ Archive Messages

Thread Group:

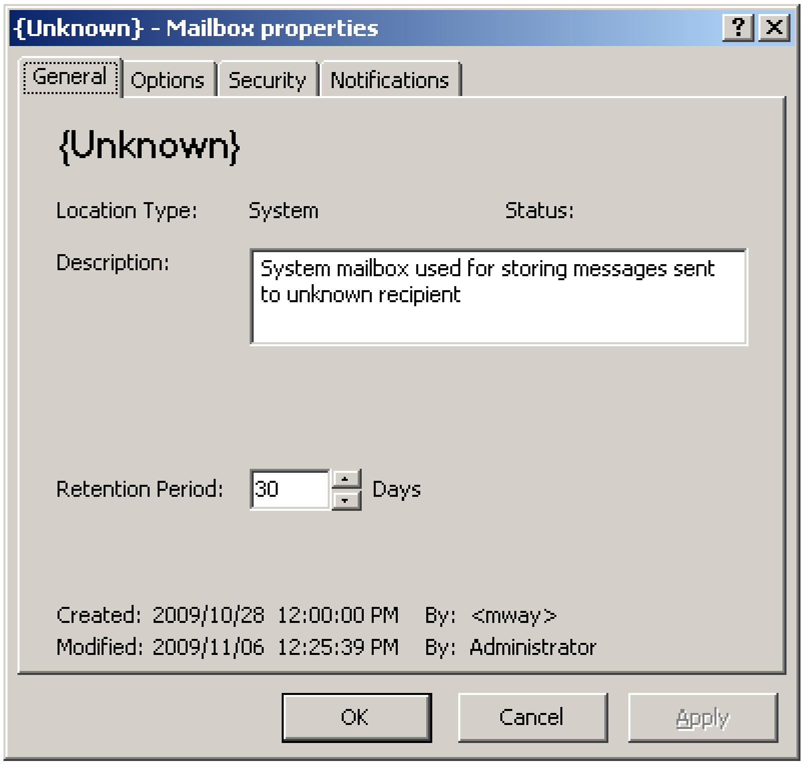
□ Check for Duplicates

□ By Source Location

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/11 11:46:49 AM By: AdminTest

A system mailbox called **{Unknown}** is created during installation. Messages are sent here when the destination location does not exist. It does not have an adapter or service, but it does assign a retention date to the messages.



{Unknown}

Location Type: System

Status:

Description: System mailbox used for storing messages sent to unknown recipient

Retention Period: 30 Days

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/06 12:25:39 PM By: Administrator

Unknown Location (Mailbox Properties Window)

Location Name (display only)

This is the name of the location you created from MessageWay Explorer. All location names must be unique, whether they are in a location group folder or not. A location name has a maximum length of 256 characters and must not contain any of the following characters: **\ / : * ? " < > | ! & ( ) ` ' ; ,** nor be only one period (**.**) or two periods (**..**).

Location Type (display only)

MessageWay determines the type of location when you have completed your configuration. The type depends on what is selected in Adapter/Service and whether it is configured for input or output.

The following table describes the types of locations:

Location Type	Location Category	Description
Folder	N/A	This is a folder to organize locations. It has no affect on processing. All location names must be unique, whether they are in a group or not.

Location Type	Location Category	Description
Service	Service location	This location is associated with a service, such as MWRules or MWTranslator, that receives and processes input messages and delivers output to various locations. When in the File System folder, a service location also functions as a container/directory node.
Input	Site	This location is associated with an adapter and is configured to automatically transfer messages into MessageWay.
Output	Site	This location is associated with an adapter and is configured to automatically transfer messages from MessageWay.
I/O	Site	This location is associated with an adapter and is configured to automatically transfer messages both to and from MessageWay.
System	Mailbox	The system mailboxes, called {Unknown} and {Quarantine}, this latter is created when you use the option Content Validation to check for viruses), are created by the system during installation. They are not associated with any adapter or service. {Unknown} contains messages in error when they cannot be delivered, for example, when the destination location does not exist. {Quarantine} contains messages that have failed validation, and are believed to contain a virus, or that are incomplete, for example, when the validation server is unavailable.
Mailbox	Mailbox	This mailbox is not associated with an adapter or service. It holds messages until they are picked up or collected by an external user through a supported interface, such as the Web Client or MessageWay FTP Perimeter Server. When in the File System folder, a mailbox also functions as a container/directory node.

Status (display only)

This is the primary status of all locations, both service locations and sites. It is calculated from a combination of the location State (**Active** or **On Hold**), the Schedule State (**Open** or **Closed**) and Threshold Release.

Status	Description	Schedule and Location States
On Hold	The location is not available to send or receive messages. This overrides the schedule.	Schedule: open or closed Location: on hold
Open	The location is currently available to send or receive messages.	Schedule: open Location: active

Status	Description	Schedule and Location States
Closed	The location is not currently available to send or receive messages.	Schedule: closed Location: active
Threshold: *nn*	The location schedule is controlled by threshold release rules. The *nn* is the number of messages that must accumulate before the schedule is opened and messages are delivered.	Schedule: closed, uses threshold release Location: active

The status of the location is determined as follows:

Location State	Schedule State	Threshold Release Count	Location Status
Hold	N/A	N/A	On Hold
Active	Open	N/A	Open
Active	Closed	0	Closed
Active	Closed	>0	Threshold

Description

Enter a brief description to help you identify the purpose of this location.

Adapter/Service

What you put here determines whether MessageWay uses this configuration to automatically deliver messages or to hold messages for users to pick up. To automatically deliver messages, select an existing adapter or service from the drop-down box. To hold messages for users to pick up, leave this field blank. To allow users to pick up messages, you must use a MessageWay option, such as the FTP Server, the SFTP Server or AS2. For outbound site or service locations, this value will be dimmed and disabled when the location contains messages.

Priority

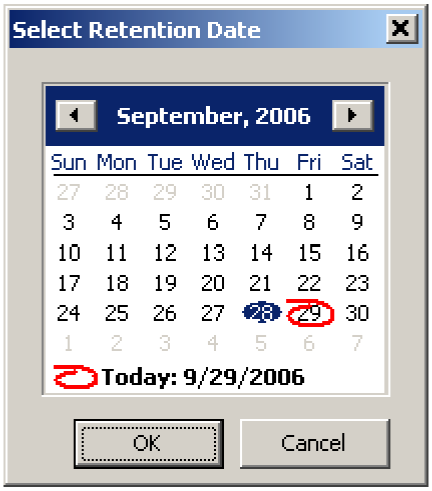
Type or select a priority from 1 (lowest) to 5 (highest). This is the default priority assigned to output messages for delivery. Output messages sent to a service location typically have the same priority as the input message. One exception is a rules processing service, where you can override the priority.

When an outbound message already has a priority assigned, then the new priority will be the higher of the assigned or the default priority. The adapter or service associated with this location will deliver higher priority messages first. Changes to the priority field take effect for messages that are not currently being processed or transferred. However, changes will be applied to any future output messages generated by services, such as MWTranslator. The priority assigned to a message may be changed using the **Change Priority** command.

IMPORTANT: For MWCustomProc (MessageWay Custom Processing Service) service locations configured for trigger messages, the priority must be less than 5 and the number of threads must be greater than 1. This is because trigger messages are assigned a default priority of 5. Other messages should not compete with this priority and there must be a reserved thread available for these messages so they will always appear in the queue. Otherwise, the trigger messages may not be added to the queue and, therefore, not be processed.

Retention Period

Enter a retention period indicating the number of days that must pass before an outbound message is available for archiving or deletion. The retention date assigned to a given message appears in the Message Properties window. The archive/delete process will act on a message beginning one day after the retention date. To manually change the retention period for a given message, select the message and then right-click to select **Modify Retention Date** from the menu. When the **Select Retention Date** dialog box appears, use the navigation options to select the month and day of the new retention date, and click **OK**.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

Today: 9/29/2006

Select Retention Date Dialog Box

Thread Group

To enforce sequential processing of messages, type the name of a thread group, using any MessageWay tokens as necessary to uniquely identify the group. Some useful tokens might be: %sender%, %recipient%, %classid%, %filename%, %inputname%, %outputname%, %contenttype%, %filebase% or %fileext%.

Some MessageWay services or external sites may require serial processing, such as a translation location that has to process an original purchase order before it processes a purchase order change or an FTP site that allows only one logon per user. Adapters and services typically process input and output messages using parallel processing with multiple threads. In order to force serial processing of input or output messages, you may configure a thread group for the location. The thread group is assigned at runtime, when a message is available for receipt or delivery. It processes messages in the queue sequentially until no more messages are available. Multiple locations may share a thread group.

NOTE: Thread groups for Custom IO sites and Email sites are only valid for output, since Custom IO and Email adapters receive messages as they are detected.

State (display only)

The state of a location indicates whether messages are allowed to be transferred to or from the location. A location state can be **Active**, which allows messages to be transferred, or **On Hold**, which does not allow messages to be transferred.

Output State (display only)

The output state only appears for service locations. It indicates whether output messages that result from a processing service can be transferred from the location. A location state of *Active* allows messages to be transferred. A location state of *On Hold* transfers output to a destination location, but the message is not released for delivery or made available for collection. When output is placed on hold, it shows in the Adapter table in parentheses under the Queued column for the adapter that will deliver the message or in the Mailbox table in parentheses under the Available column for messages held for a pickup mailbox.

Archive Messages

Select this box to have messages archived that are delivered to this location, otherwise messages will be deleted. The Archive program archives or deletes messages based on the datetime stamp and the setting of this option. To archive messages, this option must be selected when the Archive program runs.

For more information about archive/delete, refer to the section, ***Maintaining Message Information*** (on page 783).

Check for Duplicates

This check box appears only for locations capable of receiving output, such as service locations, sites configured for output and pickup mailboxes. Select this box to look for duplicate messages before attempting delivery. Any message that has been resent to the same location in MessageWay might be a duplicate. To further limit possible duplicate matches, you can specify that the source location also match.

Two messages are defined as duplicates when they have all the characteristics explained in the following table. Messages of zero length are ignored as possible matches.

Duplicate Criteria	Explanation
Different Original Message IDs	Messages with different Original Message IDs as shown on the Message Properties window, have been sent to MessageWay separately and each has been assigned a unique Original Message ID. Messages resent with the Resubmit command will have the same Original Message IDs, so they will not be considered duplicates.
Same destination location	The destination location is the same for both messages. Messages resent with the **Redirect** command will probably have different locations, so they would not be considered duplicates.
Duplicate data content	The content of the two messages has been compared and they contain exactly the same data.
Same source location	When **By Source Location** is checked, the source location of the messages must be the same.

By Source Location

Check this box to limit possible matches by including the source location as a criterion.

Created

Created is the date and time this location was created.

By (Created)

For system locations, such as {Unknown}, the system service itself creates this value, which appears in angle brackets, <mwmsg>, to distinguish it from a MessageWay user. For other locations, this value is the MessageWay user that created the location. Imported definitions will use <mwimp>.

Modified

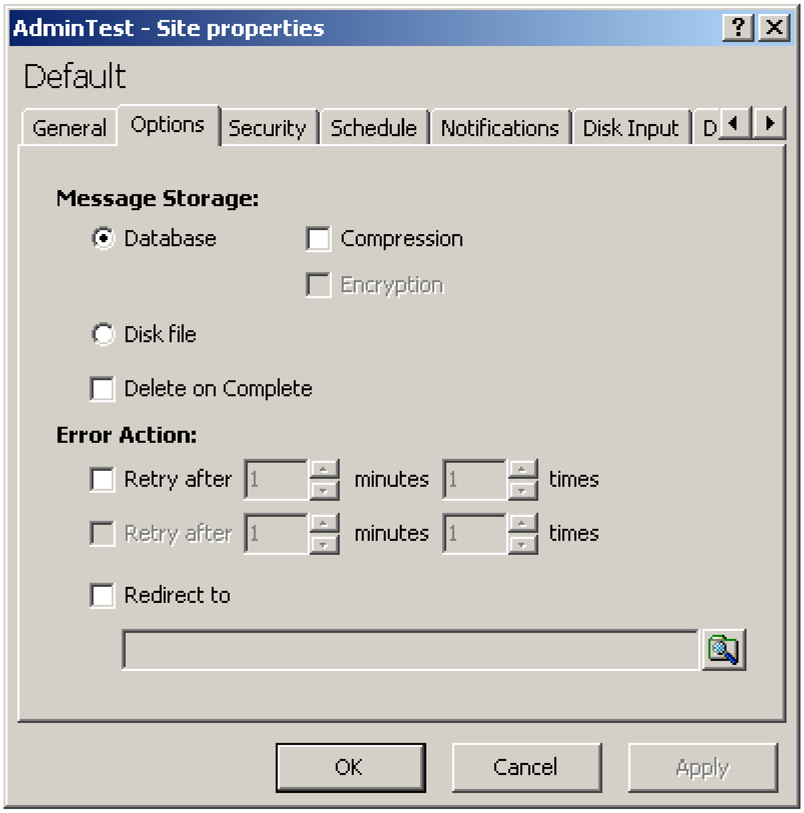
Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

(Location Properties) Options Page

The **Options** page of the location (Service Location, Site, Mailbox) Properties window allows users to select the type of message storage for message content files: database or on disk. Information about messages is always stored in the database. The default is disk. However, users may compress and/or encrypt files stored in the database. The **Encryption** field is dimmed until a user ***adds a master key*** (on page 834).


AdminTest - Site properties

Default

General | Options | Security | Schedule | Notifications | Disk Input | D

Message Storage:

● Database □ Compression

□ Encryption

○ Disk file

□ Delete on Complete

Error Action:

□ Retry after 1 minutes 1 times

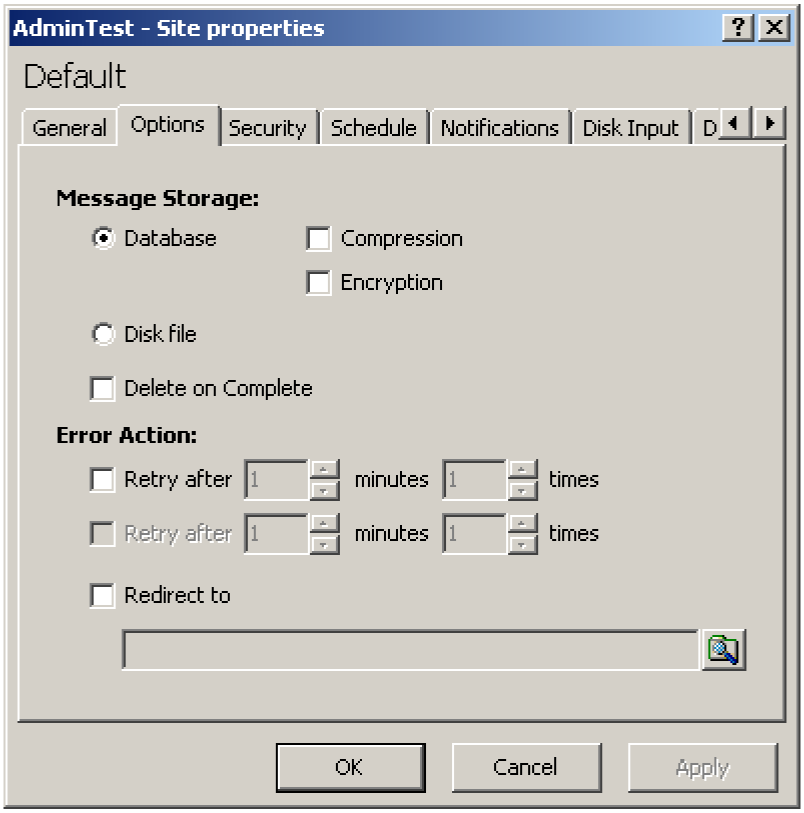
□ Retry after 1 minutes 1 times

□ Redirect to

OK | Cancel | Apply

Options Page, Encryption Dimmed (Site Properties Window)

The **Encryption** field is available after a user adds a master key.



Default

Message Storage:

● Database □ Compression

□ Encryption

○ Disk file

□ Delete on Complete

Error Action:

□ Retry after 1 minutes 1 times

□ Retry after 1 minutes 1 times

□ Redirect to

Options Page, Encryption Clear (Site Properties Window)

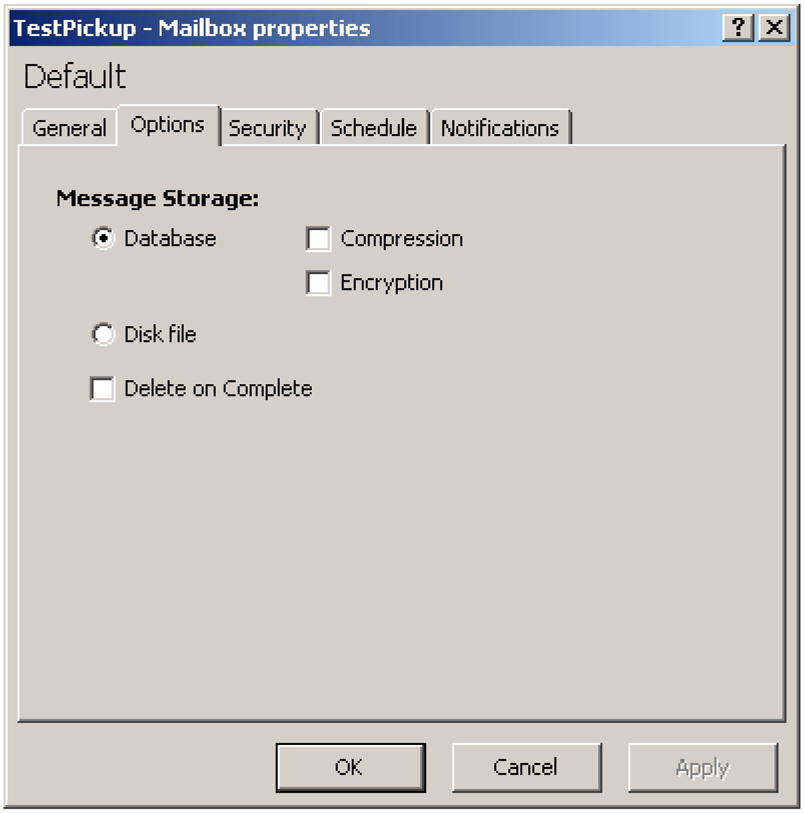
These configurations override the message storage configurations shown on the **Options** page of the MessageWay Server Properties window.

IMPORTANT: When you send messages to a distribution list for delivery to multiple locations, the storage option on the Distribution List Service Location is what determines how a message is stored, not the option on the final destination location. This is because the message is stored once, and the final destination locations point back to the original message sent to the distribution list.

The *Delete on Complete* option is only available for output locations for auto-delivery or pickup. It is not available for input locations.

For locations configured to automatically deliver messages, this page also allows users to select up to two tiers of retry strategies and an option to redirect the messages in case all retries fail. Retries attempt to send the entire file. For FTP output, when the **Restartable** option is checked to allow restarts from a checkpoint, it overrides the retries configured here.

For pickup mailboxes, you do not have an *Error Action* option to redirect messages to another location.



Message Storage:

● Database □ Compression

□ Encryption

○ Disk file

□ Delete on Complete

IMPORTANT: For input locations, users should specify an Error Action. For input messages that go to an error state because they are not properly received, MessageWay will only attempt to input the message again when an error action is configured for the input location or when the adapter is restarted.

Database

Select the *Database* option to store messages sent to this location in the MessageWay database, rather than on disk. This selection overrides the one for the MessageWay Server, visible on the **Options** page of the MessageWay Server Properties window.

Compression Check Box

Check this box to compress the data for storage in the MessageWay database. This selection overrides the one for the MessageWay Server, visible on the **Options** page of the MessageWay Server Properties window.

Encryption Check Box

Check this box to encrypt the content data when it is stored in the MessageWay database. Data is encrypted using the Advanced Encryption Standard (AES). This field is dimmed until a user adds a master key using the mwadmin utility. This selection overrides the one for the MessageWay Server, visible on the **Options** page of the MessageWay Server Properties window.

CAUTION (UNIX/Linux): For MessageWay systems configured to encrypt data content in the database, if you run the archive process from a custom processing service location, as we do from the {Archive} location, instead of from the command line, you must have a ***passphrase file*** (on page 835). To initiate the archive process, the encryption password must be saved as a file, because this process cannot be prompted for the password.

Disk File

Select the *Disk* option to store the content of messages sent to this location on disk. This selection overrides the one for the MessageWay Server, visible on the **Options** page of the MessageWay Server Properties window.

Delete on Complete

This option is only valid for output locations for auto-delivery or pickup. It is useful for large files that may be sent to a string of processes where users only want to retain the content from the last location. This option removes the content of all messages that are delivered to this location from the MessageWay message store after successful delivery and the message is marked *Complete* or *Canceled,* but the detail information for the messages remain in the message store. Since this process deletes the content of the message, only the detail record will be available to archive. Note that it is possible to remove all traces of the content from MessageWay if this option is selected for all locations to which it is delivered.

Messages whose content has been removed from MessageWay by *Delete on Complete* will show a special icon on the **General** page of the Message Properties window to indicate the content has been removed. On message lists, messages whose content has been removed will be dimmed, and when you attempt to view the content, the content window will display a message that the content was deleted.

CAUTION: To use Delete on Complete (DOC) with a distribution list, all configurations associated with that distribution list must also have DOC set, including the distribution list itself. And if you are using dynamic distribution lists, which are locations separated by commas, the system location {Dist} must also have DOC set. Also, during runtime, all messages must be marked *Complete* or *Canceled*. If any message *does not* have a status of *Complete* or *Canceled* or one of the location configurations *does not* have DOC configured, *no* message will be deleted.

Retry After Check Box

This setting affects both input and output locations. Check this box to define up to two sets of rules to re-retrieve a message or to re-deliver a message in case it is not delivered on the first try. For input locations, this applies only to sites that are capable of polling. For output locations, this applies only to sites and service locations that perform auto-delivery, not to pickup mailboxes.

Minutes

Type or select the number of minutes to wait before the next attempt to deliver the message, which is valid when the value in retry times is greater than zero.

Times

Type or select the number of times to attempt to redeliver the message.

This field only applies to automatic transfers initiated by MessageWay. It does not apply to pickup mailboxes, where the transfer is initiated by the user. When the first attempt to transfer the message fails, this is the number of additional times the service or adapter associated with this location may try. When this value is zero or the **Retry After** box is not checked, the service or adapter makes no additional attempts to transfer the message.

Redirect To Check Box

Check this box to send the message to another location, in case it cannot be delivered to its original destination.

Redirect To

Type or select one or more different locations. When you do not enter a location, the message will go to the system mailbox, {Unknown}.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

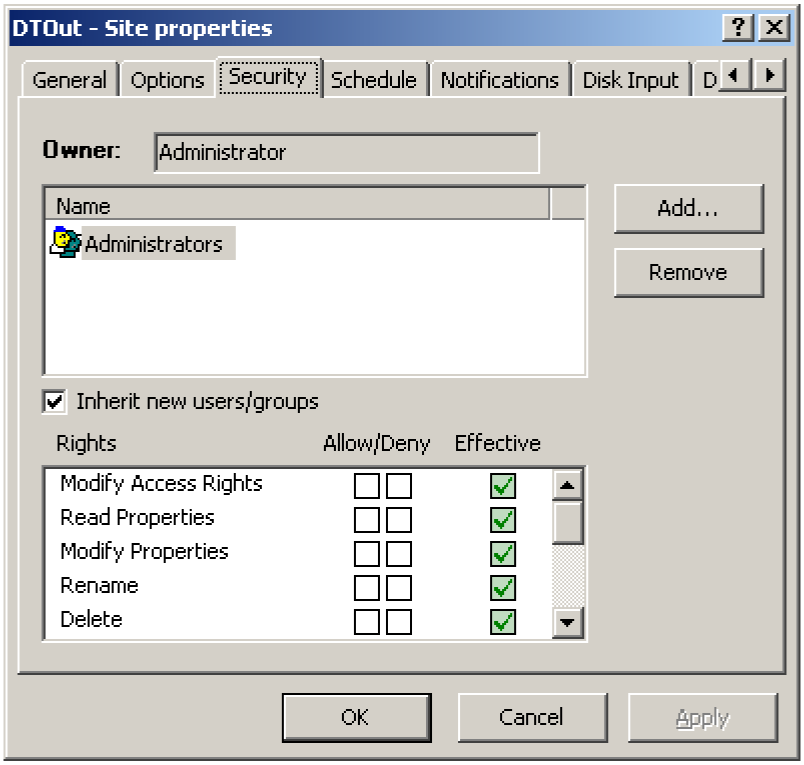
CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

(Location Properties) Security Page

The **Security** page of the location (Service Location, Site, Mailbox) Properties window shows the owner of the location, which users or user groups are allowed access to the location and what actions these users or user groups may perform.

The access list controls access to a location. It consists of a list of users or user groups and the rights that each one has. The location may inherit users and user groups and their rights from the **Locations** folder or one of its subfolders. These rights appear in the **Effective** column when you select the user or user group in the **Name** box.

IMPORTANT: To perform any functions for a location, users must also have appropriate rights set on their **Rights** page of the User Properties window.



Owner: Administrator

Name
Administrators

☑ Inherit new users/groups

Rights	Allow/Deny		Effective
Modify Access Rights	□	□	☑
Read Properties	□	□	☑
Modify Properties	□	□	☑
Rename	□	□	☑
Delete	□	□	☑

Security Page (Location Properties Window)

IMPORTANT: When you copy or move this object, the affect on access rights varies. When you copy and paste an existing object (location, rules profile or key), MessageWay will remove all access rights that have been inherited from the object's current parent folder and update all inherited access rights from the object's new parent folder. When you cut and paste/move an existing object (folder, location, rules profile or key), MessageWay will retain all access rights that have been inherited from the object's current parent folder. To update the inherited access rights to those of the object's new parent folder, for each user and group on the list, you must first clear the Inherit new users/groups box and then recheck the box. After moving a folder, the access rights must be correctly updated for the folder itself and for all of its offspring (sub-folders, locations, rules profiles and keys).

For more information about users and user security, refer to the topic, ***Configuring User Security*** (on page 375).

Owner

Initially, the owner is the user that created the object. The owner may transfer ownership to another user. Owners have complete access rights to the object, regardless of other configurations. Owners always have the right to change the names on the access list and the right to read and change the properties of the object.

Browse Button

When you are the owner, click this button to give ownership to another user.

Name

The Name list contains users or user groups that are permitted to access this object. Use the **Add** and **Remove** buttons to maintain this list. The Name list and the Rights list compose the access list used by MessageWay to determine who has what rights to this object.

Add Button

Select this button to add names of users or user groups to the Name list.

Remove Button

Select this button to delete names of users or user groups from the access list.

Inherit new users or groups

This box refers to different entities depending on whether the location is in the *Locations* folder or the *File System* folder. When this box is checked, any users or user groups that are added to the Name list of the parent folder under the Locations folder or to the Name list of the containing location/directory under the File Systems folder will also be added to the Name list of this object. To remove users or user groups from the list, you must clear this box first.

Rights

The Rights list contains the functions that the users or user groups in the Name list may perform. The Rights list and the Name list compose the access list to determine who has what rights to this object. Objects may inherit rights from their parent folder. These rights appear in the Effective Rights column when you select the user or user group in the Name list.You may override these effective rights by checking the Allow/Deny boxes. To check or clear all rights at once, hold **SHIFT** while you click one of the boxes.

The rights for an individual location are as follows:

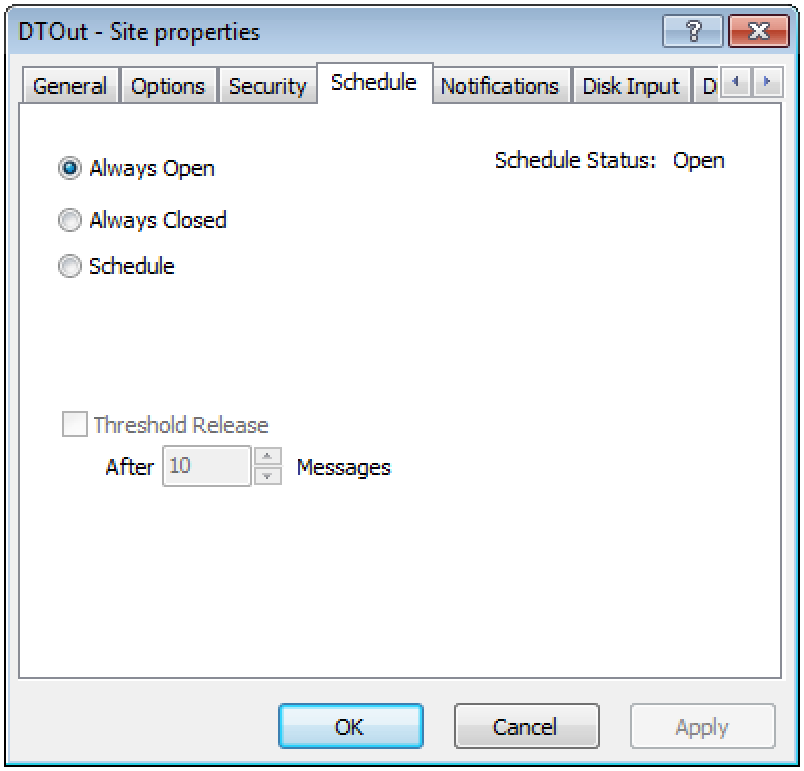
Right	Description
Modify Access Rights	Change values on **Security** page of the Location (Service, Site, Mailbox) Properties window. Also requires the right, **Read Properties**.
Read Properties	View properties of the location.
Modify Properties	Change properties of the location. Also requires the right, **Read Properties**.

Right	Description
Rename	Change the name of the location. Also requires the right, **Read Properties**.
Delete	Delete the location. Also requires the right, **Read Properties**.
Perform Location Actions	Controls user ability to hold messages, release messages, hold outputs or release outputs. Also requires the right, **Read Properties**.
Resubmit Messages	Controls user ability to resubmit messages. Also requires the right, **Read Properties** and **Modify Message Properties**.
Redirect Messages	Controls user ability to redirect messages. Also requires the right, **Read Properties** and **Modify Message Properties**.
Release Messages	Controls user ability to release messages. Also requires the right, **Read Properties** and **Modify Message Properties**.
Restart Receive	Controls user ability to restart transfer of messages only partially received. Also requires the right, **Read Properties** and **Modify Message Properties**.
Cancel Messages	Controls user ability to cancel messages. Also requires the right, **Read Properties** and **Modify Message Properties**.
Retrieve Archive Messages	Controls user ability to retrieve messages from archive. Also requires the right, **Read Properties** and **Modify Message Properties**.
Resubmit Archive Messages	Controls user ability to resubmit messages retrieved from archive. Also requires the right, **Read Properties** and **Modify Message Properties**.
Delete Archive Message Content	Controls user ability to delete messages retrieved from archive. Also requires the right, **Read Properties** and **Modify Message Properties**.
Read Message Properties	View the properties of messages. Also requires the right, **Read Properties**.
Modify Message Properties	Controls user ability to: modify retention date and change priority; mark for archive and mark for deletion. Also requires the rights, **Read Properties** and **Read Message Properties**.
View Messages	Read message content. Also requires the rights, **Read Properties** and **Read Message Properties**.
Upload Messages	Send messages to MessageWay. Required for the user or user group on the access list when this is the destination location. Also requires the rights, **Read Properties** and **Read Message Properties**.
Download Messages	Retrieve messages from MessageWay. Required for the user or user group on the access list when this is the sending location or the destination location. Also requires the rights, **Read Properties** and **Read Message Properties**.

(Location Properties) Schedule Page

The **Schedule** page of the location (Service Location, Site, Mailbox) Properties window allows users to specify a weekly schedule when the location is available for its adapter to poll for input messages or for its adapter or service to deliver output messages. Users may select preset options of **Always Open** or **Always Closed**, or they may set their own schedule. Location schedules determine whether the adapter polls for messages for individual locations. The schedule must be open to allow polling.

When the state of the schedule is **Closed**, the Threshold Release option will open the schedule after a specified number of messages have accumulated. When the state of the schedule is **Open**, then Threshold Release will have no effect, because messages will not accumulate. For this reason, when **Always Open** is selected on the **Schedule** tab, these fields are dimmed.



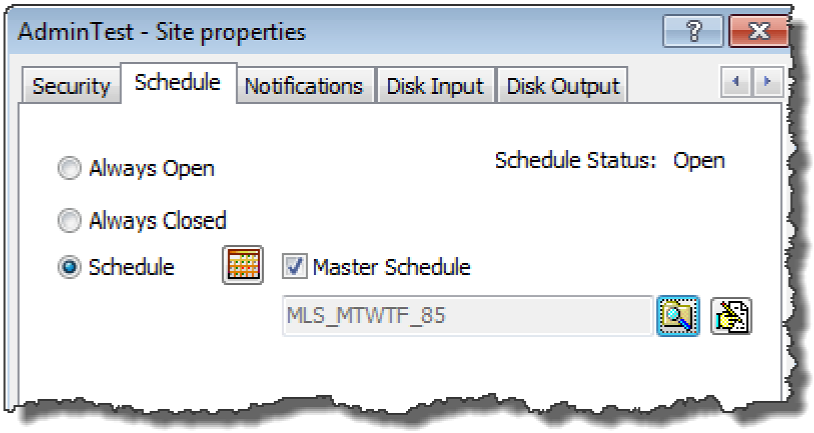
● Always Open
○ Always Closed
○ Schedule

Schedule Status: Open

□ Threshold Release
After 10 Messages

Schedule Page (Location Properties Window)

When you select Schedule, more options appear.



AdminTest - Site properties

○ Always Open

Schedule Status: Open

○ Always Closed

● Schedule

☑ Master Schedule

MLS_MTWTF_85

You can choose to use a master location schedule or create a local, custom schedule. The schedules are either repeating, daily, weekly, monthly or yearly, or absolute, which is non-repeating. You can also select a time zone to which the schedule applies. The default time zone is that of the MessageWay server. You can choose a different time zone to control when MessageWay delivers messages, based on logical or physical requirements. For more information, refer to the topic, ***Specifying Scheduling Strategies*** (on page 494).

Schedule Status

This is the current status of the schedule: open or closed. Open means that the schedule will allow the adapter or service to send and receive messages for this location. Closed means that the schedule will not allow the adapter or service to send and receive messages for this location. A closed schedule might open briefly when a trigger message is sent or when threshold release is activated.

Always Open

Select **Always Open** to allow the adapter or service associated with the location the ability to poll for input and deliver output as appropriate without schedule constraints.

Always Closed

Select **Always Closed** to not allow the adapter or service associated with the location the ability to poll for input and deliver output.

Schedule

Select **Schedule** to control by date and time when the adapter or service associated with this location may poll for input or deliver output. Users may create a local, custom schedule that applies to only this site or service location or select one that is already defined, called a Master Location Schedule, which is stored in the **Master Location Schedules** folder.

Create Schedule Button

Click this button to create a custom schedule, edit a custom schedule, select a master location schedule or view a master location schedule.

Master Schedule Check Box

Check this box to select a master location schedule from the dialog box that appears. This removes any local custom schedule, if you had one. Clear this box to create a local schedule that is not tied to a master location schedule.

Master Location Schedule

This box displays a shared master location schedule, if you have selected one. To remove a master schedule, clear the Master Location Schedule check box.

Select Master Location Schedule Button

Click this button to display the Select Schedule dialog box from which you can select a master schedule.

Customize Schedule Button

Click this button after you have selected a master schedule to use it as a base for a customized, local schedule. If you want to clear the master location schedule items completely, clear the Master Schedule check box.

Threshold Release Check Box

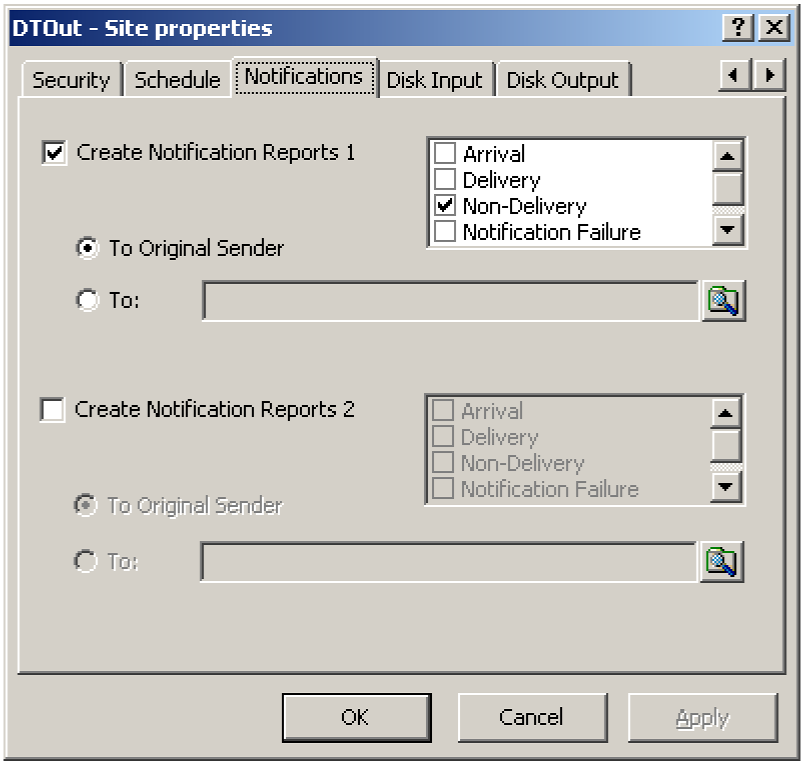
Threshold Release is a strategy to deliver messages from output locations. Check this box to specify when a location will release messages that are queued for transfer from MessageWay. The state of the schedule must be **Closed** to allow messages to accumulate. If the state of the schedule were **Open**, then Threshold Release would have no affect, because messages would not accumulate. This field is dimmed when the **Always Open** option is selected on the **Schedule** page.

After Messages

Type or select a number of messages, such that when this many accumulate in the location, they will be released to the adapter or service for delivery. This field is dimmed when the **Threshold Release** is not selected or when the **Always Open** option is selected on the **Schedule** page.

(Location Properties) Notifications Page

The **Notifications** page of the location (Service Location, Site, Mailbox) Properties window allows users to specify whether to create a notification message, under what circumstances, and the location to which it should be sent. Notification reports are short text messages identifying the event that occurred. Notice that the events that you can select to generate a notification report vary depending on the type of location. For more information about notifications, refer to the topic ***Specifying Notification Strategies*** (on page 501).



☑ Create Notification Reports 1

□ Arrival
□ Delivery
☑ Non-Delivery
□ Notification Failure

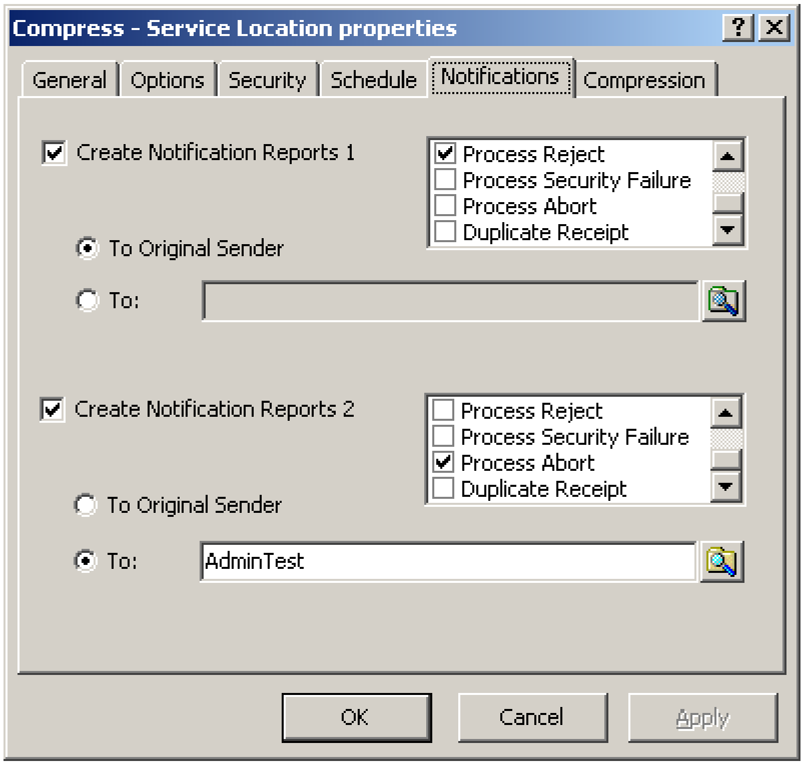
● To Original Sender
○ To:

□ Create Notification Reports 2

□ Arrival
□ Delivery
□ Non-Delivery
□ Notification Failure

● To Original Sender
○ To:

Notifications Page for An Output Site (Site Properties Window)



☑ Create Notification Reports 1

☑ Process Reject
□ Process Security Failure
□ Process Abort
□ Duplicate Receipt

● To Original Sender

○ To:

☑ Create Notification Reports 2

□ Process Reject
□ Process Security Failure
☑ Process Abort
□ Duplicate Receipt

○ To Original Sender

● To: AdminTest

Notifications Page for A Service Location (Service Location Properties Window)

Create Notification Reports 1 or 2

Check one or both boxes and choose events to request that a notification be sent to the specified location when the selected events occur. Users may configure up to two notification options, typically to send different types to different locations.

Notification Event Check Boxes

Select any of the notification events for which you want to send a notification report. Whenever one of the selected events occurs, MessageWay sends a notification.

Location Type	Valid Notification Events
Input	Receipt Receipt Failure **NOTE:** For pickup mailboxes, receipt notifications should be set on the default location of the sender.

Location Type	Valid Notification Events
Output or Mailbox	Arrival Delivery Non-Delivery Notification Failure Duplicate Receipt **NOTE:** For pickup mailboxes, arrival notifications should be set on the default location of the recipient.
System Mailbox	Arrival Receipt Failure Notification Failure Duplicate Receipt
I/O	Receipt Receipt Failure Arrival Delivery Non-Delivery Notification Failure Duplicate Receipt
Service	Receipt Receipt Failure Arrival Process Accept Process Accept w(ith) Errors Process Partial Accept Process Reject Process Security Failure Process Abort Duplicate Receipt

To Original Sender

Select this option to send the report of the selected event(s) to the original sending location. This original sender is determined by MessageWay. This is not the original sender as determined by MWTranslator, for example to return acknowledgments.

To

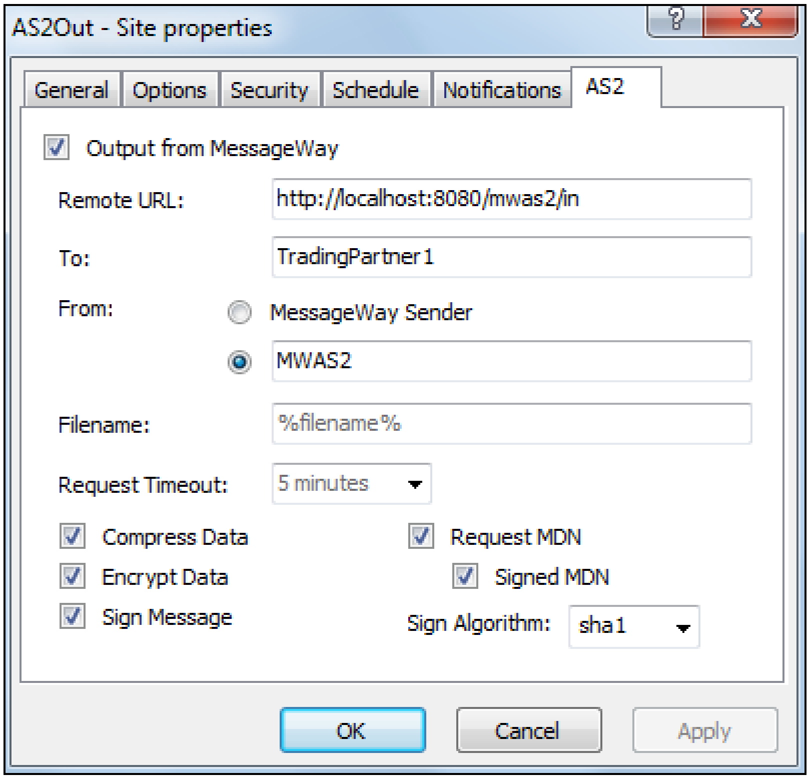
Select this option to specify a location to which the notification reports will be sent.

Location Name

Type or select the location name to which the notification report(s) will be sent when an appropriate event occurs. Select or type one or more locations, separated by commas. To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

(AS2 Site Properties) AS2 Page

The **AS2** page of the Site Properties window allows users to specify how to send data to an AS2 server and whether to receive a Message Disposition Notification (MDN) in return. This page identifies the URL to connect to the AS2 server, the recipient of the message, the sender of the message, the time to keep the connection open, and options to compress or encrypt the data, to sign the message and to request an unsigned or a signed MDN, including sign algorithm to be used.



☑ Output from MessageWay

Remote URL: http://localhost:8080/mwas2/in

To: TradingPartner1

From: ○ MessageWay Sender

● MWAS2

Filename: %filename%

Request Timeout: 5 minutes

☑ Compress Data

☑ Encrypt Data

☑ Sign Message

☑ Request MDN

☑ Signed MDN

Sign Algorithm: sha1

NOTE: The MessageWay AS2 server and the AS2 adapter require a license from Progress. For more information, contact MessageWay Technical Support.

Output from MessageWay

Check this box to configure the site for outbound delivery.

Remote URL

This address is required to connect to the remote AS2 server where MessageWay will send messages to an AS2 trading partner. Type the remote URL. The default port for AS2 servers is 8080.

To

This required field identifies the receiving system or trading partner. Type the name for the recipient, upon which both parties agree, such as a DUNS number or company name. This value will appear as the AS2-To address on the AS2 message.

For encryption, the alias string on the recipient's certificate within the MessageWay Java key store (JKS) must match the value in this box.

A compound address on a service location that forwards messages to this output site will override the value in this box.

From MessageWay Sender

This field identifies the sender. Select this radio button, which is the default, to use the value identified within MessageWay as the sender. The sender name appears on the Message Properties window or a Message List window. This value will be the AS2-From address on the AS2 message.

For messages that will be signed, this value must uniquely match part of the sender's private key subject within the Java key store (JKS). A private key subject includes the common name (CN), organizational unit (OU), organization (O), location (L), state (ST), and country (C), for example:

CN=MWayAS2, OU=AS2 Testing, O="Progress", L=Livonia, ST=MI, C=US

From

This field identifies the sender. Select this radio button, and type a value that identifies the sender to the remote AS2 server. This value will be the AS2-From address on the AS2 message.

For messages that will be signed, this value must uniquely match part of the sender's private key subject within the Java keystore (.jks). A private key subject includes the common name (CN), organizational unit (OU), organization (O), location (L), state (ST), and country (C), for example:

CN=MWayAS2, OU=AS2 Testing, O=Progress, L=Livonia, ST=MI, C=US

Filename

You may specify tokens to create a file name. Use any combination of constants and MessageWay tokens. This value overrides the one for the AS2 Adapter, mwas2, visible on the AS2 page of the AS2 Adapter Properties window. For new installations, the default mask is **%filebase%<[msgid]>.%fileext%**. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name, for example, **MW%msgid%.txt**.

Request Timeout

Select the amount of time in seconds or minutes to allow the AS2 outbound processing cycle to complete. Initially, this default value comes from the value defined on the AS2 adapter, which users can override here.

The elapsed time of the AS2 outbound processing cycle starts when the AS2 Outbound Servlet posts the AS2 message to the recipient and ends when the AS2 Outbound Servlet receives the response indicating that the AS2 message has been received. When an MDN is not required, the response is a returned HTTP status code, where a success code would be in the 200 range. When an MDN is required, the response is the returned MDN.

Ensure enough time to receive a response. If a response is not returned within the timeout limit, the message will be placed in an error state. The error description will appear on the **Error** tab of the Message Properties window for the message.

In order to allow the AS2 Outbound Servlet to timeout before the AS2 Adapter times out, the adapter adds 15 seconds to the configured timeout value to use as its timeout limit when a response has not been received from the AS2 Outbound Servlet.

Compress Data

Check this box to compress the data before sending messages. The default is not to compress data.

Encrypt Data

Check this box to encrypt the data before sending messages. The default is not to encrypt data.

Sign Message

Check this box to add a digital signature to messages before sending them. The default is not to sign messages.

Request MDN

Check this box to always request a Message Disposition Notification (MDN) from the recipient. The default is to always request an MDN, for both success and failure.

NOTE: In production, always request an MDN. Failure to request an MDN may result in the message being marked delivered within MessageWay when the AS2 message was actually rejected by the recipient.

Sign MDN

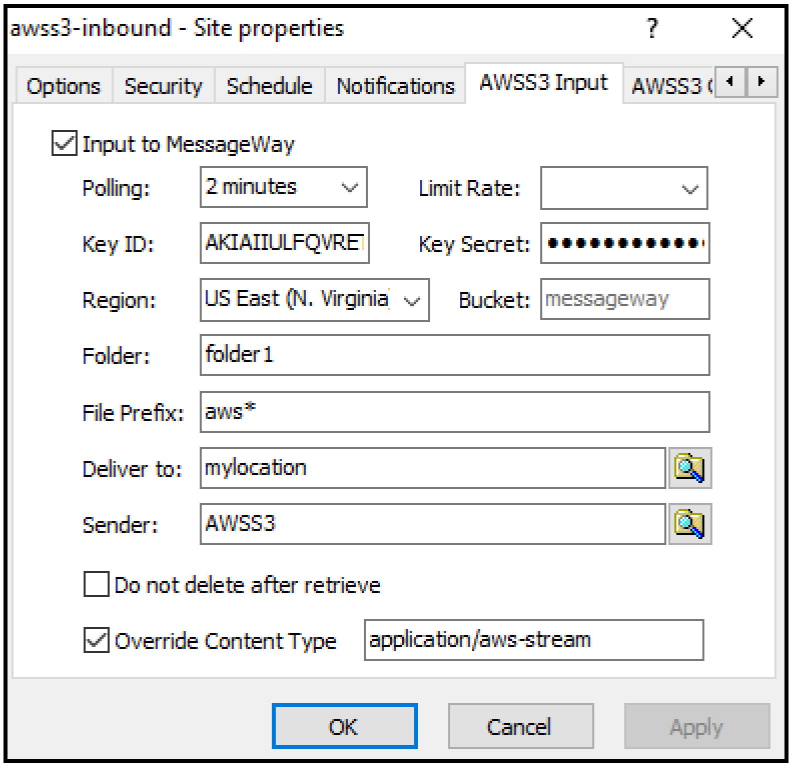
When the Request MDN box is checked, you may also check this box to request a signed MDN (Message Disposition Notification) from the recipient. The default is not to request a signed MDN.

Sign Algorithm

Specifies the algorithm used for signing the MDN. Select one of the options, **sha1**, **md5**, **sha-256**, **sha-384**, **sha-512**, or **sha-224**, to determine which signing algorithm is used. The default is **sha1**.

(MWAWSS3 Site Properties) AWSS3 Input Page

The **AWSS3 Input** tab of the Site Properties window allows users to specify how to transfer messages from an AWSS3 site into MessageWay.



☑ Input to MessageWay

Polling: 2 minutes

Limit Rate:

Key ID: AKIAIIULFQVRET

Key Secret: ●●●●●●●●●●●●

Region: US East (N. Virginia

Bucket: messageway

Folder: folder1

File Prefix: aws*

Deliver to: mylocation

Sender: AWSS3

☐ Do not delete after retrieve

☑ Override Content Type application/aws-stream

AWSS3 Input Page (Site Properties Window)

Input to MessageWay

Check this box to allow the adapter associated with this site to transfer messages from the specified AWSS3 site into MessageWay. The MWAWSS3 adapter only polls for input messages when the schedule for the site is open.

Polling

This value overrides the polling value set for the MWAWSS3 adapter.

The polling interval is used for the transfer of messages from an AWSS3 bucket into MessageWay. This is the amount of time that the AWSS3 client will wait before checking the bucket for files to transfer to the site. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

Select an interval from the list or type the number of hours, minutes or seconds between polling cycles. The option **Never** stops polling for this adapter. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

CAUTION: Polling causes a LIST request to be sent to AWS. Since there is a charge in AWS for a LIST request, setting a lower polling interval can cause excessive charges to be incurred. For example, if there are several hundred AWS S3 inbound locations all configured to poll at 5 second intervals, excessive charges may be incurred. When possible, set polling to hours or minutes, not seconds.

The **Schedule** option requires that the schedule type be *Trigger (Input or Execute Now)*, which polls at the time specified. You identify the schedule on the **Schedule** tab, and from there you can drill down to create or edit a schedule item.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds
30m	means 30 minutes
2 h	means 2 hours

Key ID

This value overrides the key id value set for the MWAWSS3 adapter.

Enter your AWS Identity and Access Management (IAM) access key id value here. This key, along with your AWS IAM secret access key, allow you to control and secure your AWS S3 account. Key ID can be found on your AWS S3 IAM account by selecting **My Security Credentials**, then choosing **Get Started with IAM Users**, then clicking on User name followed by **Security Credentials**. These keys are equivalent to user id and password in some applications.

Key Secret

Enter your AWS Identity and Access Management (IAM) secret access key value here. This key, along with your AWS IAM access key id, allow you to control and secure your AWS S3 account. Key Secret is only available when it is initially created, so make sure it is saved accordingly. These keys are equivalent to user id and password in some applications.

CAUTION: When the key secret is created using your AWS S3 IAM account, this is the only time that you will be able to see what the actual value is, so make sure you **Download Key File** when prompted by AWS and store the resulting file in a secure place for future reference.

Region

This value overrides the region (Default Regions/Inbound) value set for the MWAWSS3 adapter.

Click the down arrow to the right of the **Region** field and select the appropriate AWS region name for inbound transfers. To reduce data latency in your applications, AWS offers multiple independent world-wide regional endpoints to make your upload/download requests to/from. Typically you would select a region closes to your physical location. A region is equivalent to a server in some applications.

Bucket

This value overrides the bucket (Default Buckets/Inbound) value set for the MWAWSS3 adapter.

Enter your AWS bucket value here. Bucket values are case-sensitive. Buckets in AWS are used to store objects, which consist of data and any metadata that describes the data. A bucket is equivalent to a disk drive in some applications.

Folder

Enter your AWS folder value here. Folder values are case-sensitive. Folders in AWS are used to further partition objects within buckets, and can be considered nothing more that empty objects or files. Typical wildcards like * and ? are supported here, or this field can be left blank. A folder is equivalent to a directory in some applications.

NOTE: Entering any value, including a wildcard (*), in the folder field will cause files in the root (files not in any folder) to not be downloaded. To download files from the root, leave the folder field blank.

File Prefix

Enter a file prefix that matches the objects that you want to download from your AWS account. File names are case-sensitive. Typical wildcards like * and ? are supported here, and this field cannot be left blank. An object is equivalent to a file in some applications.

NOTE: To download all files from a bucket (including all files in folders as well as all files in root), put a wildcard (*) in the file prefix field and leave folder field blank. To download all files from folders only (no root files will be downloaded), put a wildcard (*) in both file prefix field and folder field.

Deliver To

Type or select a location to which the adapter associated with this site will transfer the messages. This may be a site for auto-delivery, a service location, such as MWTranslator, or a pickup mailbox. When the location does not exist, the message is sent to the system mailbox, {Unknown}.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

Sender

Select or type a location to represent the sender of the message. This overrides the sender that may or may not have been passed by the AWSS3 server. This feature is useful for testing, where the input site is already defined, but currently inaccessible, such as at a customer site whose connection is unavailable. You can use a test location that has a different name, but when you put the name of the original customer location here, the message will be marked as if it were from the customer location.

Do Not Delete after Retrieve

Check this box to leave the input file on the source AWSS3 site after successful retrieval. When a file has been retrieved from an AWSS3 site into MessageWay, the default behavior is to delete the file from the source AWSS3 site.

Override Content Type Check Box

Check this box to override the content type specified for the input message.

Override Content Type

Enter the content type here. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.

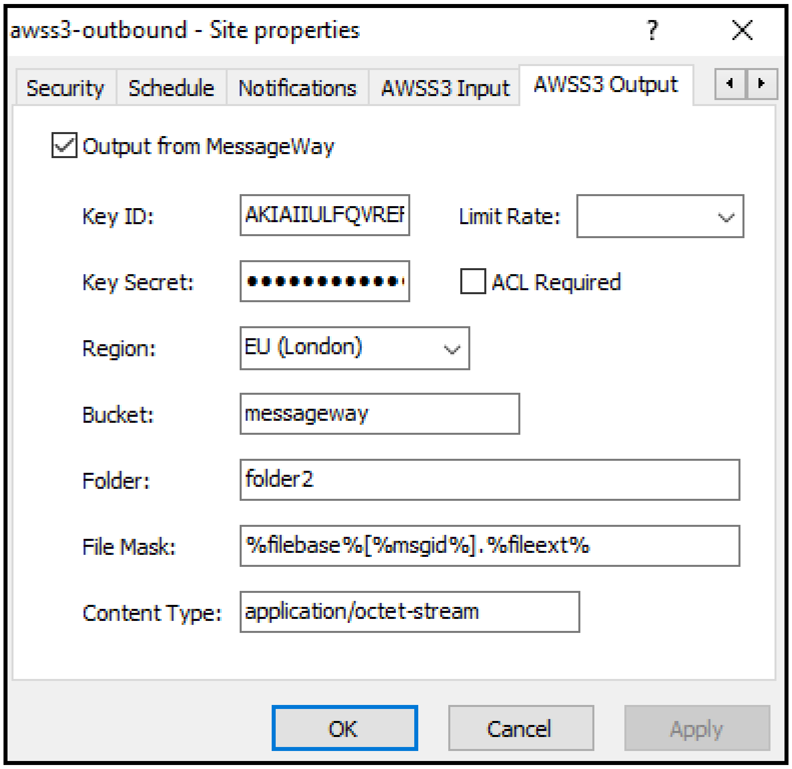
The following table shows the content types that MessageWay supports:

Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png

Type	Content Type	File Extension
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

(MWAWSS3 Site Properties) AWSS3 Output Page

The **AWSS3 Output** tab of the Site Properties window allows users to specify how to transfer messages from MessageWay to an AWSS3 site.


awss3-outbound - Site properties

☑ Output from MessageWay

Key ID: AKIAIIULFQVREF

Limit Rate:

Key Secret: ●●●●●●●●●●●●

□ ACL Required

Region: EU (London)

Bucket: messageway

Folder: folder2

File Mask: %filebase%[%msgid%].%fileext%

Content Type: application/octet-stream

AWSS3 Output Page (Site Properties Window)

Output From MessageWay

Check this box to allow the adapter associated with this location to transfer messages from MessageWay to the specified AWSS3 site. The AWSS3 adapter will deliver messages only when the schedule for this site is open.

Key ID

This value overrides the key id value set for the MWAWSS3 adapter.

Enter your AWS Identity and Access Management (IAM) access key id value here. This key, along with your AWS IAM secret access key, allow you to control and secure your AWS S3 account. Key ID can be found on your AWS S3 IAM account by selecting **My Security Credentials**, then choosing **Get Started with IAM Users**, then clicking on User name followed by **Security Credentials**. These keys are equivalent to user id and password in some applications.

Key Secret

Enter your AWS Identity and Access Management (IAM) secret access key value here. This key, along with your AWS IAM access key id, allow you to control and secure your AWS S3 account. Key Secret is only available when it is initially created, so make sure it is saved accordingly. These keys are equivalent to user id and password in some applications.

CAUTION: When the key secret is created using your AWS S3 IAM account, this is the only time that you will be able to see what the actual value is, so make sure you **Download Key File** when prompted by AWS and store the resulting file in a secure place for future reference.

Region

This value overrides the region (Default Regions/Outbound) value set for the MWAWSS3 adapter.

Click the down arrow to the right of the **Region** field and select the appropriate AWS region name for outbound transfers. To reduce data latency in your applications, AWS offers multiple independent world-wide regional endpoints to make your upload/download requests to/from. Typically you would select a region closes to your physical location. A region is equivalent to a server in some applications.

Bucket

This value overrides the bucket (Default Buckets/Outbound) value set for the MWAWSS3 adapter.

Enter your AWS bucket value here. Bucket values are case-sensitive. Buckets in AWS are used to store objects, which consist of data and any metadata that describes the data. A bucket is equivalent to a disk drive in some applications.

Folder

Enter your AWS folder value here. Folder values are case-sensitive. Folders in AWS are used to further partition objects within buckets, and can be considered nothing more that empty objects or files. This field can be left blank. A folder is equivalent to a directory in some applications.

File Mask

This value overrides the Default Output Mask value set for the MWAWSS3 adapter.

This is a template to create a file name or object name for outbound transfers. Use any combination of constants and MessageWay tokens. For new installations, the default mask is **%filebase%[%msgid%].%fileext%**. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name, for example, **MW%msgid%.txt**.

Use two percent (%) signs to enclose the tokens. MessageWay replaces the tokens with appropriate values. Add constants outside of these signs as required.

CAUTION: When a file of the same name already exists, it will be overlaid by default. Note that file names are case-sensitive.

TIP: The file mask can also be used to create or write to folder names using tokens. The folder name and file name must be separated with a "/". For example, %yyyymmdd%/Testfile.txt will create or write to a folder name of today's date and write the file named Testfile.txt into the folder.

The valid tokens are:

Token	Description
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: MyClassID@MyLocationName To assign a class ID to a mask for a file name, type: MyClassID%yyyymmdd%.txt
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).

Token	Description
inputmsgid	Input Message Id of the message.
inputname	Input Name.
location	The MessageWay location where the message resides. Replaces mailbox.
msgid	The Message Id of the message. Replaces msg.
ms	Milliseconds (000-999). NOTE: The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.
yyyy	Four digit year.
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name

Token	Description
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

MW%msgid%.txt

TR%yyyymmddhhnnss#%.txt

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml

TIP: On systems that allow file names longer than 8 characters, use the msgid token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the filename token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

Content Type

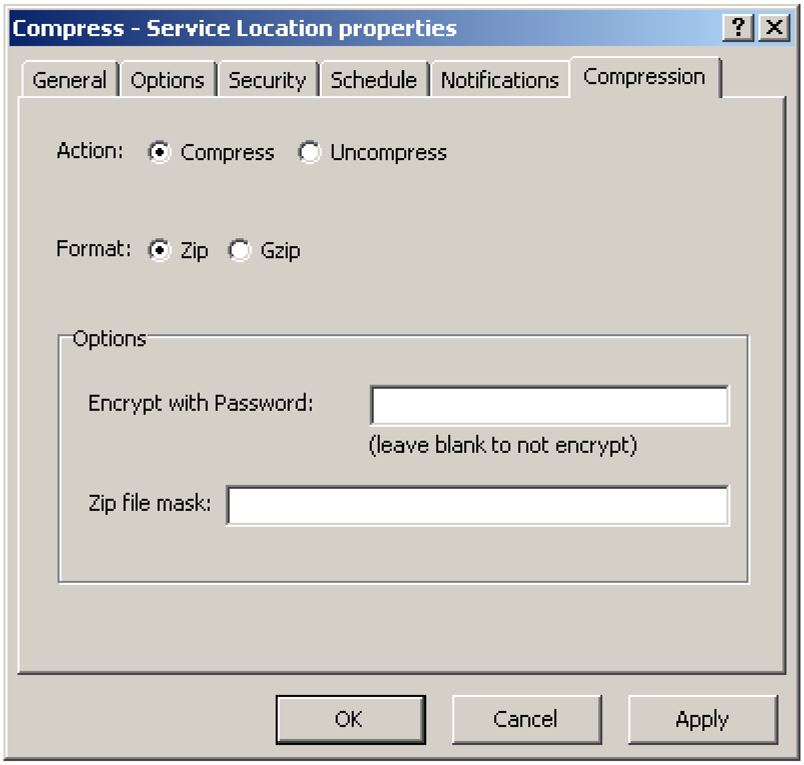
This value overrides the Default Output Content Type value set for the MWAWSS3 adapter.

Enter the content type value that you want to associate with the file or object created in AWS S3 here. Although this value can be any characters that you choose, following is a list of typical content types that MessageWay supports:

Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

(Compression Service Location Properties) Compression Page

The **Compression** page of the Service Location Properties window allows users to specify whether to compress (zip) or uncompress (unzip) the input file. For compressed files, users must enter a mask, which is used to create the name of the file that is contained in the compressed file.



Compress - Service Location properties

Action: ● Compress ○ Uncompress

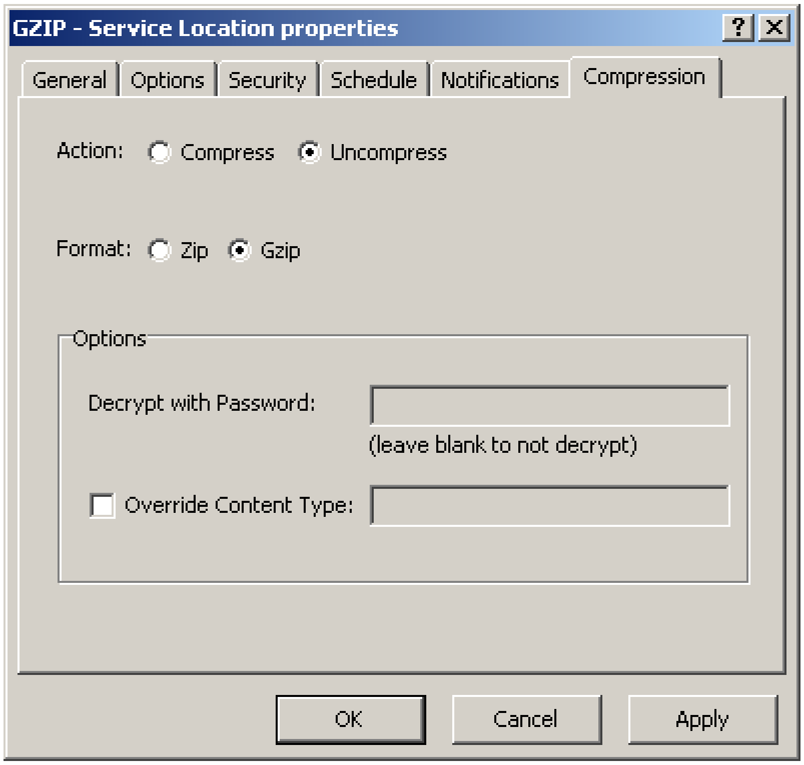
Format: ● Zip ○ Gzip

Options

Encrypt with Password:

(leave blank to not encrypt)

Zip file mask:


GZIP - Service Location properties

Action: ○ Compress ● Uncompress

Format: ○ Zip ● Gzip

Options

Decrypt with Password:

(leave blank to not decrypt)

□ Override Content Type:

Compress

Click this option to compress incoming files. With this option, you also specify the name of the file to be placed inside the zip file. Since there is no routing with this option, you must have specified the routing directions on the input location using a compound address. This option supports the PKWARE zip file format using the DEFLATE compression algorithm (RFC 1951) and the GZIP file format, conforming to RFC1952.

Uncompress

Click this button to unzip incoming files. Since there is no routing with this option, you must have specified the routing directions on the input location using a compound address. This option currently supports the PKWARE zip file format using the DEFLATE compression algorithm (RFC 1951) and the GZIP file format, conforming to RFC1952.

Zip

From the *Format* group of options, choose the type of compression format you want: Zip or Gzip. The zip format can both compress and archive multiple files in one zipped file, which typically has an extension of *.zip*.

Gzip

From the *Format* group of options, choose the type of compression format you want: **Zip** or **Gzip**. The gzip format only compresses one or more concatenated files and has an extension of *.gz*. Typically, however, multiple files will be archived in a tarball and then compressed. The resulting file will have an extension of *.tar.gz* or *.tgz.*

Encrypt/Decrypt Password

Specify a password required to encrypt or decrypt the message. Leave this field blank if you do not want to encrypt or decrypt the message. When you specify a password for files that are to be uncompressed, and files are sent to this location without a password, the password specified for this location is ignored, and the files will be uncompressed. If a file is decrypted correctly, you will be able to view the contents. When there is an error in decryption, information appears on the **Error** tab of the Message Properties window. Currently, this feature is only available for the zip format, not for gzip.

Zip File Mask

Type the name of the file to be placed inside the zip file. This field is ignored for gzip formats. When the field is blank, the Filename property of the input message provides the name of the file. You may use a combination of MessageWay tokens and constants. Enclose the tokens in percent (%) signs. Add constants outside of the percent signs as required.

The valid tokens are:

Token	Description
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: **MyClassID@MyLocationName** To assign a class ID to a mask for a file name, type: **MyClassID%yyyymmdd%.txt**
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).

Token	Description
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).
inputmsgid	Input Message Id of the message.
inputname	Input Name.
location	The MessageWay location where the message resides. Replaces *mailbox*.
msgid	The Message Id of the message. Replaces *msg*.
ms	Milliseconds (000-999). **NOTE:** The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).

Token	Description
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.
yyyy	Four digit year.
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

```
MW%msgid%.txt

TR%yyyymmddhhnnss#%.txt
```

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)

Token	Description
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

```
%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml
```

TIP: On systems that allow file names longer than 8 characters, use the *msgid* token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the *filename* token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  \ / : * ? " < > | ! & ` ' ;

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

- Duplicate Filename values are allowed within the same location within the Locations folder.

Duplicate Filenames are *not* allowed within the same location within the File System folder, unless one has been canceled.

Override Content Type Check Box

Check this box to override the content type specified for the input file.

Override Content Type

Type the content type. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.

The following table gives a list content types that MessageWay supports:

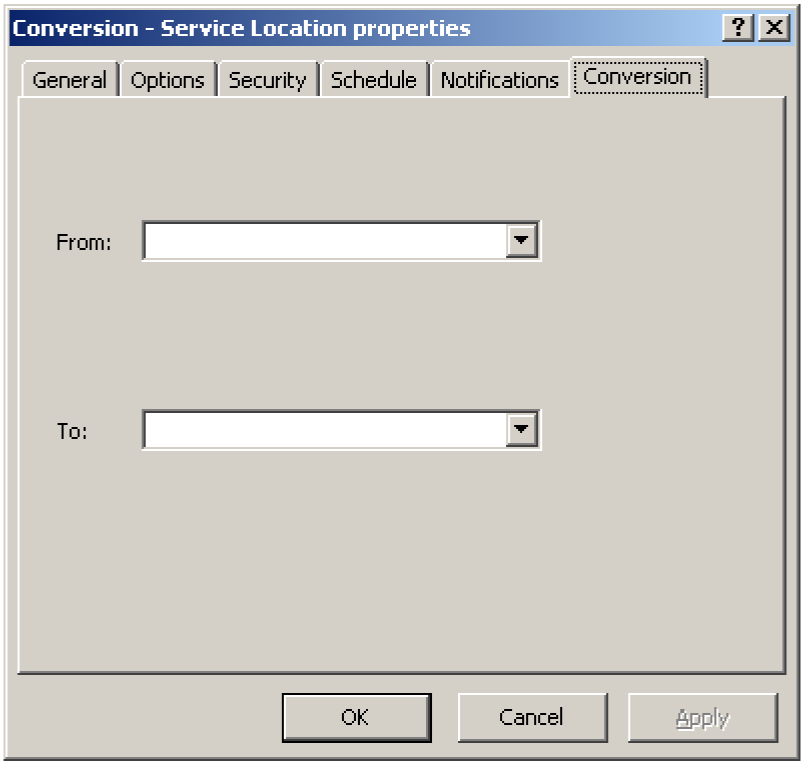
Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi

Type	Content Type	File Extension
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

(Conversion Service Location Properties) Conversion Page

The **Conversion** page of the Site Properties window allows users to specify the type of conversion to perform. The encoding schemes, algorithms and tables are from the ***International Components for Unicode (ICU)*** (***http://site.icu-project.org/***).

IMPORTANT: When data cannot be converted from the input encoding to the output, ICU uses a replacement character of 0x1A in the output to mark the location of the invalid value, including the byte order mark (BOM) if present.



From

Select the character set of the input data from the drop-down list. The value defaults to ASCII (equivalent to ISO/IEC 646, 1991), the original 128 characters. MWConvert does not determine the encoding of the message, so users must determine that before they attempt to send it to a location for conversion.

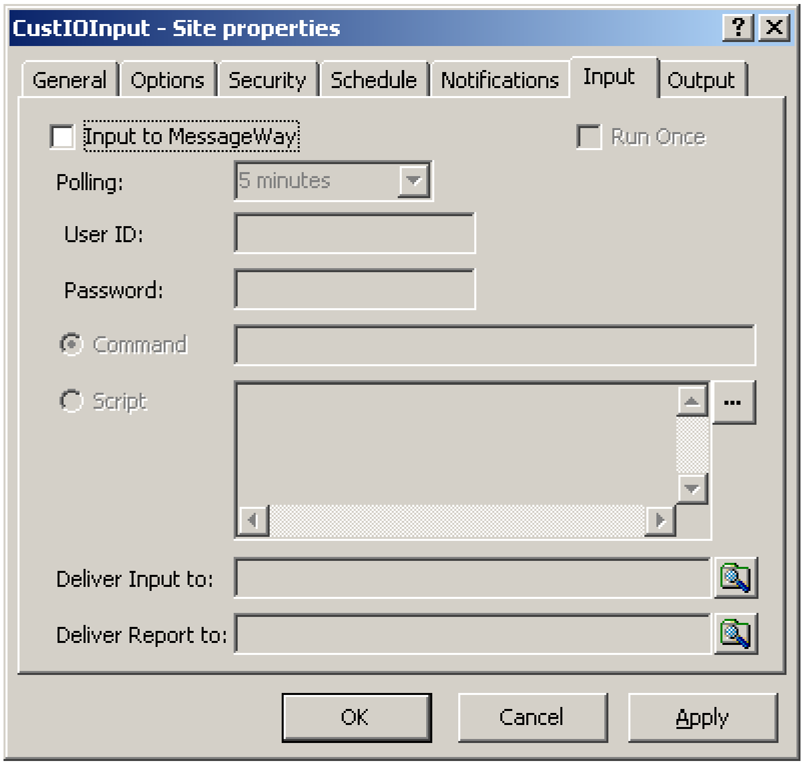
To

Select the character set of the output data from the drop-down list. The default encoding is ASCII (equivalent to ISO/IEC 646, 1991), the original 128 characters.

(Custom IO Site Properties) Input Page

For a custom IO site, the **Input** tab of the Site Properties window allows users to specify parameters to execute a command or run a script to send a file to MessageWay. By default, the name of this site becomes the source of the input message. To override the default source, enter a different source in the status file for a script. For more information, refer to the topic, ***Configuring a Custom I/O Location*** (on page 539).

Note that MessageWay does not support input filenames that contain backslashes, \. For operating systems, such as UNIX, that allow backslashes in filenames, the filename property will be whatever follows the final backslash.



☐ Input to MessageWay

☐ Run Once

Polling: 5 minutes

● Command

○ Script

Input Page, (Site Properties Window)

Input to MessageWay

Check this box to configure this site to transfer messages into MessageWay.

Polling

This value overrides the polling value set for the Custom IO adapter.

The polling interval is used to transfer messages into MessageWay. Enter the number of seconds, minutes, or hours that the adapter will wait before running commands or scripts specified on the **Input** tab of a Custom IO site.

Select an interval from the list. The option **Never** stops polling for this adapter. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

The **Schedule** option requires that the schedule type be *Trigger (Input or Execute Now)*, which polls at the time specified. You identify the schedule on the **Schedule** tab, and from there you can drill down to create or edit a schedule item.

Run Once

Check this box to run simple commands and programs only once per poll interval. Typically, commands or programs exit with a zero completion code. If the box is *not* checked and the executed command or program always exits with a zero completion code, the adapter will immediately re-execute the script, which will cause an infinite loop.

Checking this box has the same effect as exiting a Custom IO Input script with a **100**, which tells the Custom IO adapter not to re-execute the script until the next poll interval.

User ID

When necessary, enter a valid user ID to connect to a process that will transfer messages into MessageWay.

Password

When necessary, enter a valid password for the user ID to connect to a process that will transfer messages into MessageWay.

Command

Select the **Command** option, and type a command line. The first item should be the file name of the external process, which defaults to the script directory specified on the **IO** tab of the Custom I/O Adapter. When the script or program does not reside in the default directory, you must specify the full path name. The process name should be followed by any necessary parameters, such as MessageWay replaceable parameters or parameters required by the process. MessageWay will resolve the replaceable parameters within memory and execute the script. The process should transfer files to MessageWay, and it must return a completion code or a completion status in a status file.

Script

Select the **Script** option, and enter script commands to transfer files to MessageWay. On the first line, you enter the extension of the script to indicate the type of scripting language you want to execute for the commands that follow. On subsequent lines, you enter commands using the MessageWay tokens and specific command parameters as required. You may use any scripting language installed on and supported by the operating system. For example, when the first line contains .bat the subsequent lines would contain batch file commands, or .vbs followed by Visual Basic script or .js followed by Java script. MessageWay will resolve the replaceable parameters and write the script to the /tmp directory where it will be executed. You should place a complex script in an external file and invoke it from the **Command** field.

Edit Button

Click this button to open a separate edit window, which will give you better editing control.

CAUTION: The **Save** command on the Edit window only saves the script to the script box. To save the changes in MessageWay, you must then select **Apply** or **OK** before you exit the properties window.

Deliver Input To

Enter the name of the default location to which input files will be sent.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

When the field is blank or the location does not exist, the message is sent to the system mailbox, {Unknown}. When a status file is used that specifies a destination location, this value is ignored.

Browse Button for Locations

Click this button to select from a list of valid locations.

Deliver Report To

Enter the name of the default location to which reports will be sent. To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

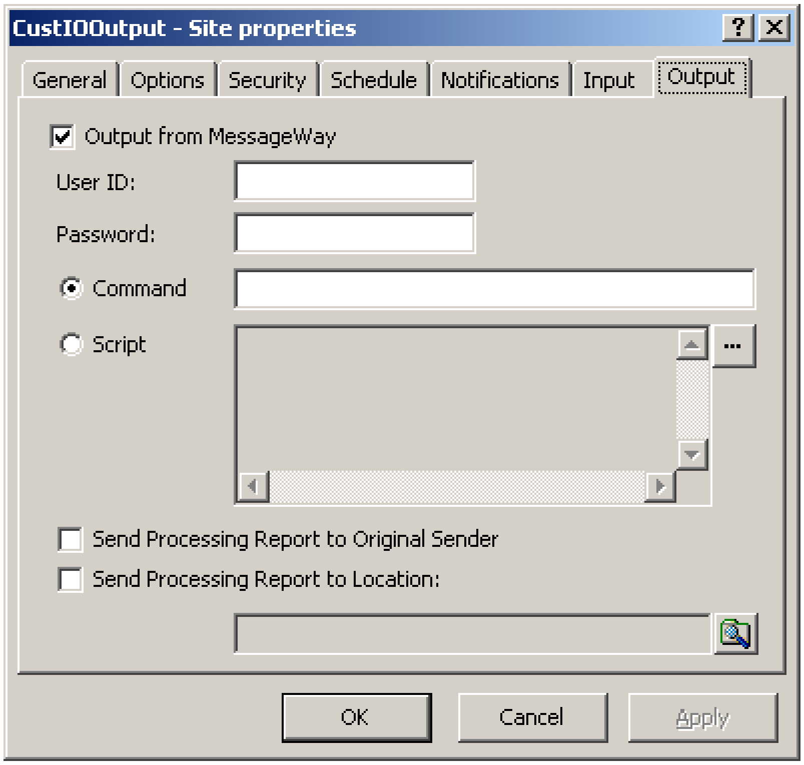
To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

When the field is blank or the location does not exist, the message is sent to the system mailbox, {Unknown}. When a status file is used that specifies a report location, this value is ignored.

(Custom IO Site Properties) Output Page

For a custom IO site, the **Output** tab of the Site Properties window allows users to specify parameters to execute a command or run a script to transfer a file from MessageWay.



Output Page, (Site Properties Window)

Output from MessageWay

Select this box to configure this site to transfer messages from MessageWay or act as a trigger to run a script, without passing a message. Use the latter to start an external process from MessageWay.

User ID

When necessary, enter a valid user ID to connect to a process to transfer messages from MessageWay.

Password

When necessary, enter a valid password for the user ID to connect to a process to transfer messages from MessageWay.

Command

Select the **Command** option, and enter a command line. The first item should be the file name of the external process, which defaults to the script directory specified on the **IO** tab of the Custom I/O adapter. When the script or program does not reside in the default directory, you must specify the full path name. The process name should be followed by any necessary parameters, such as MessageWay replaceable parameters or parameters required by the process. MessageWay will resolve the replaceable parameters within memory and execute the script. The process should transfer files from MessageWay, and it should also return a completion code or a completion status in a status file.

Script

Select the **Script** option, and type a script to transfer files from MessageWay. On the first line, you enter the extension of the script to indicate the type of scripting language you want to execute for the commands that follow. On subsequent lines, you enter commands using the MessageWay replaceable parameters and specific command parameters as required. You may use any scripting language installed on and supported by the operating system. For example, when the first line contains .bat the subsequent lines would contain batch file commands, or .vbs followed by Visual Basic script or .js followed by Java script. MessageWay will resolve the replaceable parameters and write the script to the /tmp directory where it will be executed. You should place a complex script in an external file and invoke it from the Command field.

Edit Button

Click this button to open a separate edit window, which will give you better editing control.

CAUTION: The **Save** command on the Edit window only saves the script to the script box. To save the changes in MessageWay, you must then select **Apply** or **OK** before you exit the properties window.

Send Processing Report to Original Sender

Check this box to send the processing report to the location or address of the input message.

CAUTION: When you use the %rpt% token or RPT lines in a status file and a report option is not selected on the **Output** tab of the custom IO Site Properties window, the adapter ignores any generated report files and then deletes them from disk.

Send Processing Report to Location Check Box

Check this option to send the processing report to the specified location.

CAUTION: When you use the %rpt% token or RPT lines in a status file and a report option is not selected on the **Output** tab of the custom IO Site Properties window, the adapter ignores any generated report files and then deletes them from disk.

Send Processing Report to Location

Type or select the location to which the processing report(s) will be sent.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

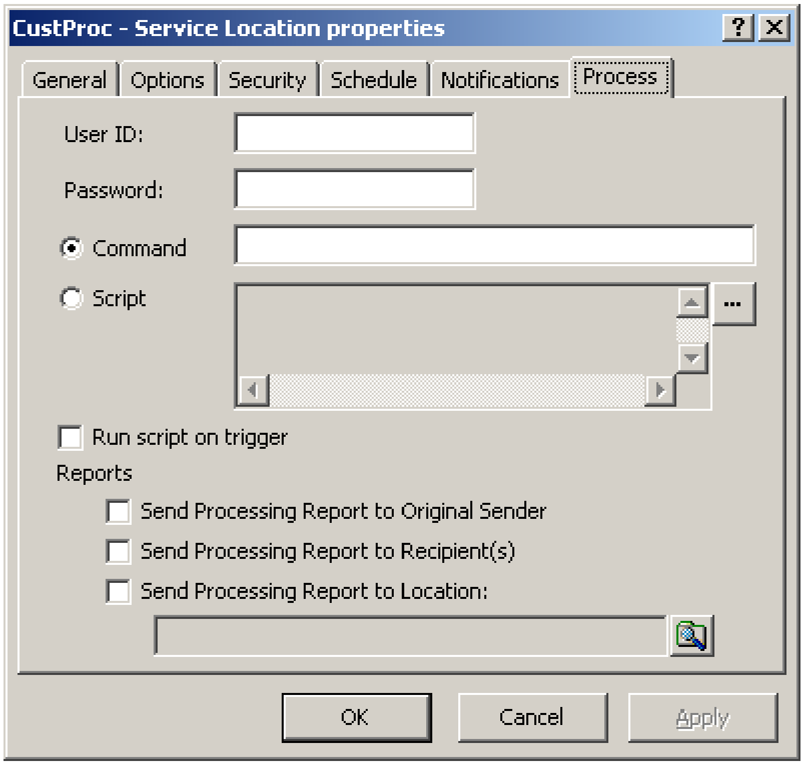
To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

When the location does not exist, the report is sent to the system mailbox, {Unknown}.

(Custom Processing Service Location Properties) Process Page

For a custom processing service location, the **Process** tab of the Service Location Properties window allows users to specify parameters to execute an external script or command outside of MessageWay. By default, the name of this service location becomes the source of the input message. To override the default source, enter a different source in the status file for a script. For more information, refer to the topic, ***Configuring a Custom Processing Location*** (on page 565).


CustProc - Service Location properties
?
General
Options
Security
Schedule
Notifications
Process
User ID:
Password:
● Command
○ Script
...
□ Run script on trigger
Reports
□ Send Processing Report to Original Sender
□ Send Processing Report to Recipient(s)
□ Send Processing Report to Location:
OK
Cancel
Apply

Process Page, (Service Location Properties Window)

User ID

This is a user ID for a local connection from the MessageWay system. When required, this value, together with the password forms the logon to a system within the same LAN or WAN. This value is passed to the script or command with the %user% token. This value must not be blank when the %user% token is used in the Command field or Script box, because it will cause an error.

Password

This is a password for the local connection from the MessageWay system. When needed, this value, together with the local user ID forms the logon to a system within the same LAN or WAN. This value is passed to the script or command with the %password% token. This value must not be blank when the %password% token is used in the Command field or Script box, because it will cause an error.

Command

Select the Command option, and enter a command line that you want to execute from the operating system. The first item should be the file name of the external process, which defaults to the script directory specified on the **Process** tab of the Custom Processing Service. When the script or program does not reside in the default directory, you must specify the full path name. The process name should be followed by any necessary parameters, such as MessageWay replaceable parameters or parameters required by the process. The process must return a completion code and any necessary files to MessageWay.

Script

Select the Script option, and type script commands that you want to execute from the operating system. On the first line, you enter the extension of the script to indicate the type of scripting language you want to execute for the commands that follow. On subsequent lines, you enter commands using the MessageWay tokens and specific command parameters as required. You may use any scripting language installed on and supported by the operating system. For example, when the first line contains .bat the subsequent lines would contain batch file commands for Windows, or use #!/bin/sh for UNIX/Linux systems.

TIP: You should place a complex script in an external file and invoke it from the **Command** field.

Edit Button

Click this button to open a separate edit window, which will give you better editing control.

CAUTION: The **Save** command on the Edit window only saves the script to the script box. To save the changes in MessageWay, you must then select **Apply** or **OK** before you exit the properties window.

Run Script on Trigger

By default, MessageWay runs the specified script when a message is sent to a Custom Processing service location. When this option is checked, MessageWay will run the script when a trigger message is sent to the location. This option also allows users to use the **Execute Now** command, typically to test scripts.

IMPORTANT: Previously, the option, **Run script on trigger or schedule**, ran a script when the state of the schedule changed from closed to open. This option has been deprecated. Beginning with MessageWay 5.0, to allow MessageWay to run a script based on the schedule associated with a service location, you must create a schedule item for the Custom Processing service location, check the box, **Trigger**, and select **Input or Execute Now**. For an example, look at the schedule created for the {Archive} location.

Send Processing Report to Original Sender

Check this box to send the processing report to the location or address of the input message.

CAUTION: When you use the %rpt% token, the report will be uploaded to each report destination defined on the **Process** tab of the custom processing Service Location Properties window, as well as to each destination defined in the status file RPT lines where %rpt% is the report to upload. If no report destinations are defined, the service ignores the generated report file and leaves it on disk.

Send Processing Report to Recipient(s)

Check this option to send the processing report to the recipient of each output created during processing. Duplicate reports will not be sent to a recipient.

CAUTION: When you use the %rpt% token, the report will be uploaded to each report destination defined on the **Process** tab of the custom processing Service Location Properties window, as well as to each destination defined in the status file RPT lines where %rpt% is the report to upload. If no report destinations are defined, the service ignores the generated report file and leaves it on disk.

Send Processing Report to Location

Type or select the location to which the processing report(s) will be sent.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

When the location does not exist, the report is sent to the system mailbox, {Unknown}.

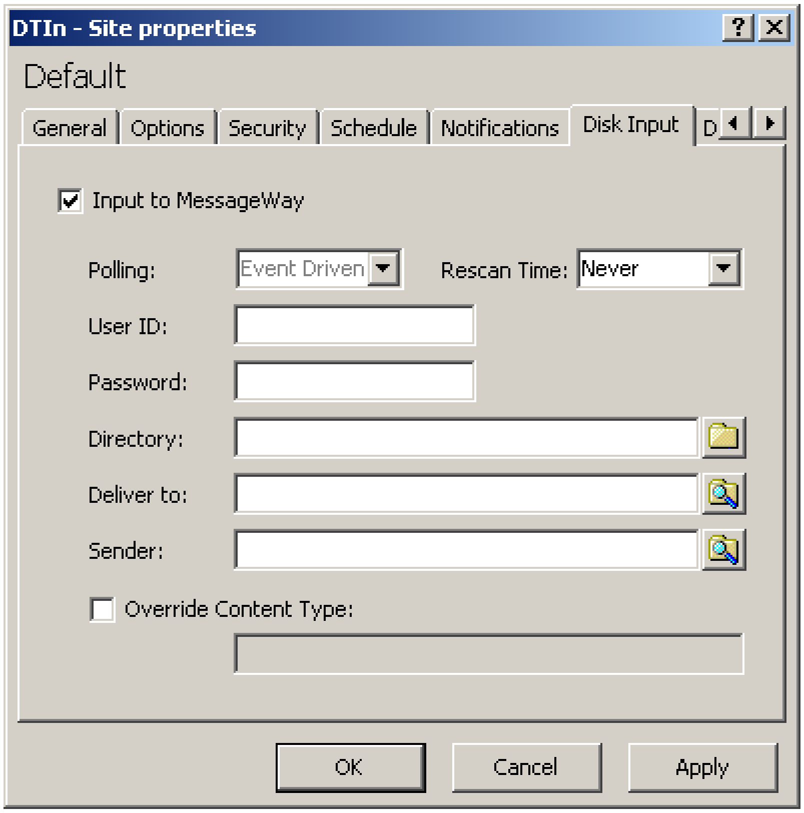
Browse Button for Locations

Click this button to select from a list of valid locations.

(Disk Transfer Site Properties) Disk Input Page

For a disk transfer site, the **Disk Input** page of the Site Properties window allows users to specify when the site is used to transfer messages from a disk location into MessageWay. Users may also specify parameters for the message transfers.

Note that MessageWay does not support input filenames that contain backslashes, \. For operating systems, such as UNIX, that allow backslashes in filenames, the filename property will be whatever follows the final backslash.



☑ Input to MessageWay

Polling: Event Driven

Rescan Time: Never

User ID:

Password:

Directory:

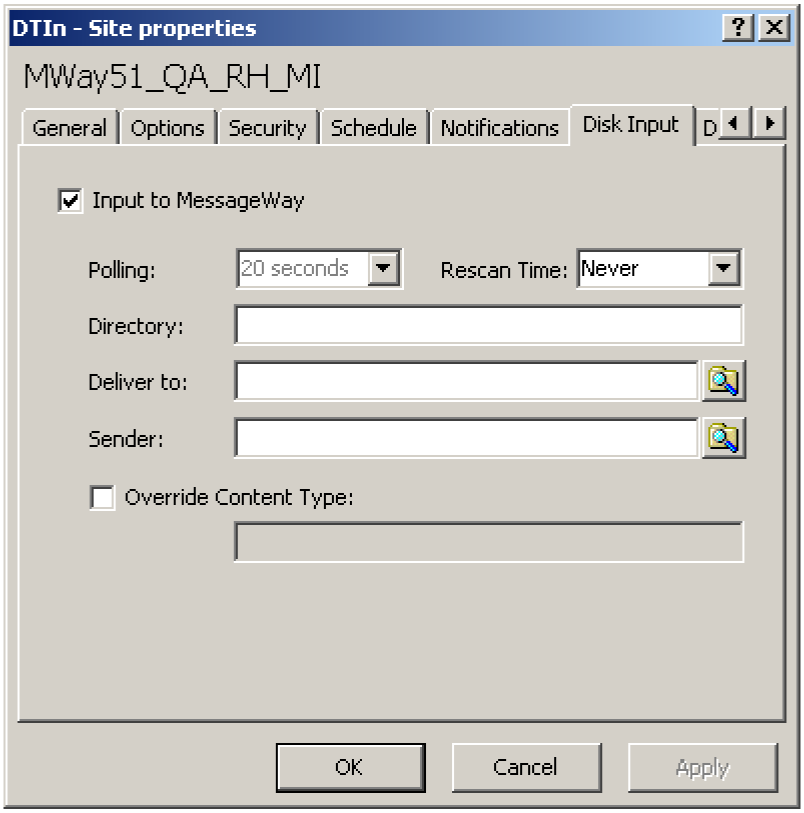
Deliver to:

Sender:

□ Override Content Type:

Disk Input Page on Windows (Site Properties Window)

IMPORTANT: The User ID and Password fields only apply to Windows servers, which require authentication to access remote locations.



MWay51_QA_RH_MI

☑ Input to MessageWay

Polling: 20 seconds

Rescan Time: Never

Directory:

Deliver to:

Sender:

□ Override Content Type:

Disk Input Page on UNIX/Linux (Site Properties Window)

Input to MessageWay

Check this box to allow the adapter associated with this site to transfer messages from the specified directory into MessageWay.

Polling

This value overrides the polling value set for the Disk Transfer Adapter.

The polling interval is used for the transfer of messages from a local directory into MessageWay. Enter the number of seconds, minutes, or hours that the adapter will wait before checking the local directory for files to transfer. The directory to be polled and the location to which the inbound files will be transferred are on the page for the adapter of the Site Properties window. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

Select an interval from the list. The option **Event-Driven** ensures that messages are passed to MessageWay as soon as they appear in the subdirectory. Event-driven polling is not available on UNIX/Linux systems. The option **Never** stops all input for this adapter.

Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

The **Schedule** option requires that the schedule type be *Trigger (Input or Execute Now)*, which polls at the time specified. You identify the schedule on the **Schedule** tab, and from there you can drill down to create or edit a schedule item.

User ID

When required, enter a valid user ID to connect to the system where you poll for input files. This is valid only for Windows servers. Polling remote locations is not supported for UNIX/Linux servers.

Password

When required, enter a valid password to connect to the system where you poll for input files. This is valid only for Windows servers. Polling remote locations is not supported for UNIX/Linux servers.

Rescan Time

This is the interval in seconds that Disk Transfer adapter waits before it rereads the size of the input message. Set this interval for locations that receive large files to assure that MessageWay only inputs complete messages. The alternative to avoid having MessageWay input partial files is to write to a temporary directory, and then rename the file to the primary directory. When the polling interval finds messages to bring into MessageWay, the adapter reads the size of the message. Then it rescans the size of the message until if finds that it has no longer changed. When it determines that the file is stable, it initiates the transfer of the file into MessageWay. Since this feature will input files only after at least three readings of the file properties, it will slow down input for smaller files as well. This setting only works when the polling interval is explicitly set to a value, and the *Input Now* command is disabled when a rescan time is specified. It is ignored when the polling interval is set to *Event Driven*, *Schedule* or *None*. If the rescan time is greater than or equal to the polling time, the polling time will act as the rescan of the previous poll.

CAUTION: When rescan is set to a low number, such as 5 seconds, a remote server may not have enough time to update the file size before 2 consecutive rescans. In this case MessageWay will think the file is complete and input the file, which may result in an incomplete file transfer. Make sure that the rescan time is set high enough to allow remote servers to update the file statistics between scans. We recommend a higher interval, at least 60 seconds.

Directory (Input)

Enter a valid directory that the Disk Transfer adapter will scan for messages to transfer into MessageWay. Do not use mapped drive letters to access network resources. Use full Universal Naming Convention (UNC) names instead. You may also add a file name at the end of the directory path. The file name may be static or dynamic with the * wildcard. If you want to pull a static filename you still have to put an asterisk after it, for example *abc.txt**. Otherwise, MWDisk will interpret it as a directory name.

CAUTION: When you fail to enter a drive letter, the operating system will attempt to create a subdirectory of this name in its default location where services are started, such as \Windows\System32 on Windows XP or /opt/messageway/init on Linux.

Deliver To

Select or type locations where the adapter will transfer the messages. When the location does not exist, the message is sent to the system mailbox, {Unknown}.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

Sender

Select or type a location to represent the sender of the message. This overrides the default sender, which is the name of the input location. This feature is useful for testing, where the input location is already defined, but currently inaccessible, such as at a customer site whose connection is unavailable. You can use a test location that has a different name, but when you put the name of the original customer location here, the message will be marked as if it were from the customer location.

Override Content Type Check Box

Check this box to override the content type specified for the input message.

Override Content Type (Site Properties, Disk Input)

Enter the content type. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.

The following table lists the content types that MessageWay supports:

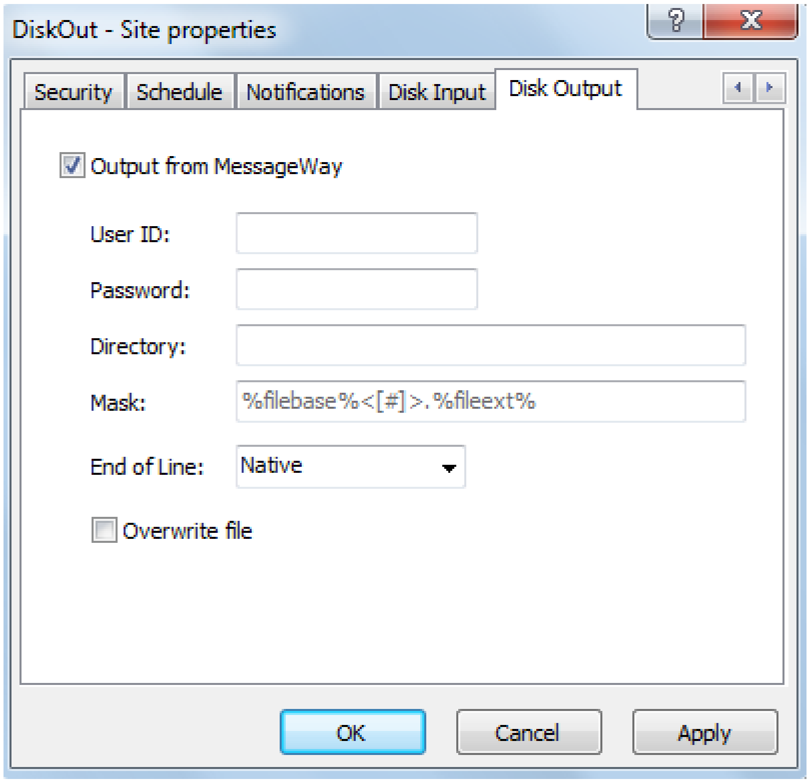
Type	Content Type	File Extension
ZIP	application/zip	zip

Type	Content Type	File Extension
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

(Disk Transfer Site Properties) Disk Output Page

For a disk transfer site, the **Disk Output** tab of the Site Properties window allows users to specify when the site is used to transfer messages from MessageWay to a disk location. Users may also specify parameters for the message transfer. The parameters vary depending on the operating system. For example, *Create Mode* is only valid for UNIX/Linux servers.

IMPORTANT: The User ID and Password fields only apply to Windows servers, which require authentication to access remote locations.



☑ Output from MessageWay

User ID:

Password:

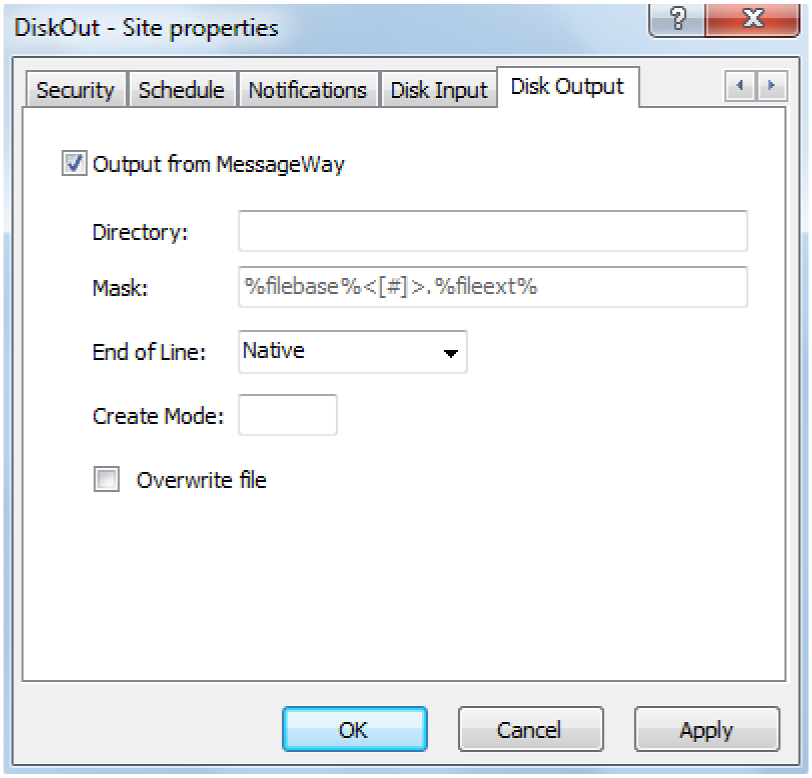
Directory:

Mask: %filebase%<[#]>.%fileext%

End of Line: Native

□ Overwrite file

Disk Output Page, Windows (Site Properties Window)



DiskOut - Site properties

☑ Output from MessageWay

Directory:

Mask: %filebase%<[#]>.%fileext%

End of Line: Native

Create Mode:

□ Overwrite file

Disk Output Page, UNIX/Linux (Site Properties Window)

Output from MessageWay

Select this box to allow the adapter to send messages from MessageWay to the specified directory.

User ID

When required, enter a valid user ID to connect to the system where you send the output file. This is valid only for Windows servers.

Password

When required, enter a valid password to connect to the system where you send the output file. This is valid only for Windows servers.

Directory (Output)

Enter a valid directory where the Disk Transfer adapter will transfer a message from MessageWay. Do not use mapped drive letters to access network resources. Use full Universal Naming Convention (UNC) names instead.

If the directory does not exist, the MessageWay Server will attempt to create one. The server will first attempt to write the file to the \temp directory specified for the Disk Transfer adapter, or if this is blank, then to a directory beneath this directory. When the server successfully completes writing the file to the temporary directory, it moves the file to this directory. This ensures that the file is complete.

CAUTION: If MessageWay finds a file already exists in this directory by the same name as the file it is attempting to rename\move from the \temp directory the rename\move of the file will fail.

You can specify another location for the temporary directory on the **Disk Transfer** tab of the Disk Transfer Adapter Properties window.

Mask

Enter a mask that will be used to create the file name of the file transferred from MessageWay to the specified directory. Use two percent (%) signs to enclose the tokens. Add constants outside of these signs as required. This value overrides any system default set on the **Options** tab of the MessageWay Server Properties window. For new installations, the default mask is **%filebase%<[#]>.%fileext%**. For upgrades from previous versions of MessageWay, the default mask remains **MW%yyyymmddhhnnss#%.dat**.

NOTE: The special <[#]> notation in the default file mask uses a pair of greater-than and less-than signs (< and >) to number each occurrence after the first with a numeric value beginning with 1 in square brackets, for example NewFile, NewFile[1]. Alternatively, if you were to use the normal notation [%#%] instead of <[#]>, all file names would have a number appended in square brackets, beginning with one, for example NewFile[1], NewFile[2].

The valid tokens are:

Token	Description
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: **MyClassID@MyLocationName** To assign a class ID to a mask for a file name, type: **MyClassID%yyyymmdd%.txt**
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.

Token	Description
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).
inputmsgid	Input Message Id of the message.
inputname	Input Name.
location	The MessageWay location where the message resides. Replaces *mailbox*.
msgid	The Message Id of the message. Replaces *msg*.
ms	Milliseconds (000-999). **NOTE:** The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient

Token	Description
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.
yyyy	Four digit year.
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

```
MW%msgid%.txt

TR%yyyymmddhhnnss#%.txt
```

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)

Token	Description
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

```
%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml
```

TIP: On systems that allow file names longer than 8 characters, use the *msgid* token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the *filename* token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  \ / : * ? " < > | ! & ` ' ;

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

- Duplicate Filename values are allowed within the same location within the Locations folder.

Duplicate Filenames are *not* allowed within the same location within the File System folder, unless one has been canceled.

When MessageWay does not explicity receive a value for the Filename, it constructs one using the following rules:

- The value assigned to Input Name will be validated using the previous rules.
- When the validation process does not return a value, MessageWay uses the result of the mask, MW%msgid%.dat.

End of Line

Many different systems change the end-of-line (EOL) character when transferring data. Where possible, MessageWay retains the carriage return/linefeed (CRLF) as the EOL character for text files, that is where the context type starts with **text/**. This may not always be possible, such as when a file is received as binary and later has its context type changed to **text/**. To change the character, select the appropriate value. The options are CRLF, Native, NL and Unchanged.

The following table describes the end-of-line character options.

End-of-Line Character	Description
Native	When the output operating system is known, MessageWay uses the EOL character native to that system.
CRLF	Always use carriage-return/line-feed, which is the native EOL character combination for Windows operating systems.
NL	Always use newline, which is the native EOL character for UNIX/Linux operating systems
Unchanged	Do not change the EOL character.

Create Mode

Type a 3-digit numeric value to set the default file permissions when MessageWay creates a file. This value overrides the default settings for the Disk Transfer adapter.

Each digit may be from 0 to 7, representing permissions, from left to right, for owner/user, group, and all other users. To set the rights for each entity, add the total of the values assigned to each right, where, 4 = read (r), 2 = write (w), 1 = execute (x) and 0 = none (-). For example, 644 would give read and write (4+2=6) permissions to the owner/user, for example *mway*, and 4 would give read permissions to the group and others.

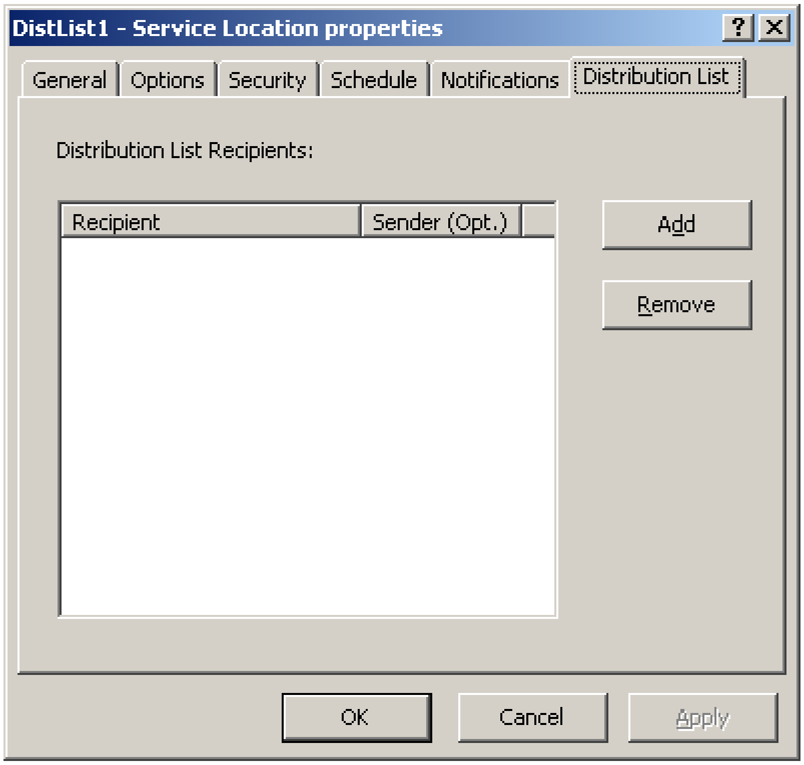
Overwrite file (Site Properties, Disk Output)

Check this box to overwrite the output file if it already exists.   The Disk Adapter must have permission to overwrite files.

(Distribution List Service Location Properties) Distribution List Page

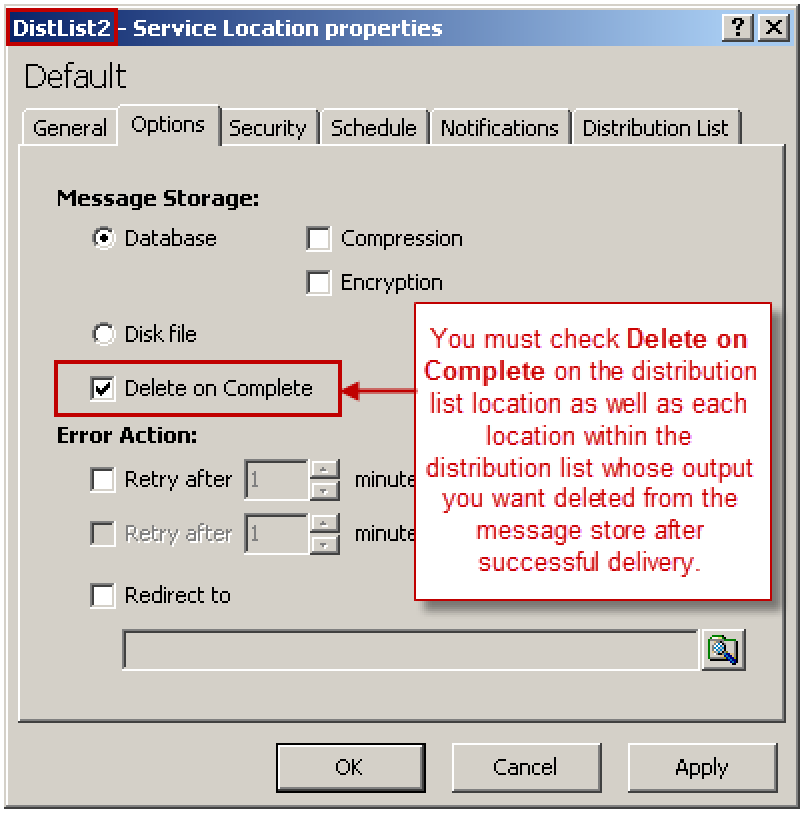
For the Distribution List Service, the **Distribution List** page of the Service Location Properties window allows users to specify multiple destination locations to send the message. Users can send a report to configured output or I/O locations and to other distribution lists.

IMPORTANT: When you send messages to a distribution list for delivery to multiple locations, the storage option on the Distribution List Service Location is what determines how a message is stored, not the option on the final destination location. This is because the message is stored once, and the final destination locations point back to the original message sent to the distribution list.



Distribution List Page (Service Location Properties Window)

CAUTION: To use Delete on Complete (DOC) with a distribution list, all configurations associated with that distribution list must also have DOC set, including the distribution list itself. And if you are using dynamic distribution lists, which are locations separated by commas, the system location {Dist} must also have DOC set. Also, during runtime, all messages must be marked *Complete* or *Canceled*. If any message *does not* have a status of *Complete* or *Canceled* or one of the location configurations *does not* have DOC configured, *no* message will be deleted.



Message Storage:

● Database □ Compression

□ Encryption

○ Disk file

☑ Delete on Complete

Error Action:

□ Retry after 1 minute

□ Retry after 1 minute

□ Redirect to

You must check **Delete on Complete** on the distribution list location as well as each location within the distribution list whose output you want deleted from the message store after successful delivery.

Distribution List Recipients

This list shows the locations to which messages will be forwarded.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

You can optionally specify a sender for each item on the list. The optional sender overrides the default sender, which is the sender of the original message. Use the **Add** and **Remove** buttons to maintain this list.

Add button

Click **Add** to add destination locations or other distribution lists to the list.

Remove button

Click **Remove** to delete destination locations or other distribution lists from the list.

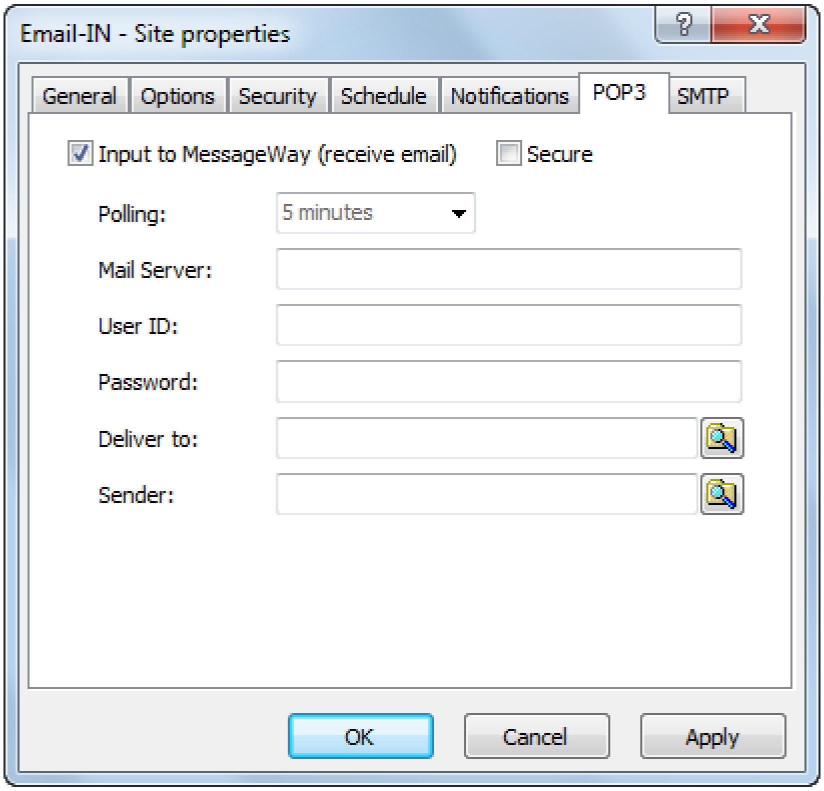
(E-mail Site Properties) POP3 Page

For e-mail sites, the **POP3** page of the Site Properties window allows users to specify how to transfer e-mail messages using POP3 into MessageWay. Users may override the polling interval defined for the E-mail Adapter.

The purpose of this client's input option is to extract the payload, either from the body or from an attachment. It does not preserve the e-mail headers. It delivers the payload as a message as follows:

- If there is an attachment, it delivers the attachment as a message and discards the body text of the e-mail
- If there is no attachment, it delivers the text in the body as a message

IMPORTANT: This e-mail client preserves the content/payload when it transfers text-only messages into MessageWay. Do not try to accept messages that have anything other than text in the body.



☑ Input to MessageWay (receive email) □ Secure

Polling: 5 minutes

Mail Server:

User ID:

Password:

Deliver to:

Sender:

POP3 Page (Site Properties Window)

Input to MessageWay (receive email)

Check this box to allow the adapter associated with this site to transfer messages from the specified e-mail server into MessageWay.

Secure

Check this box to enable a secure POP3 connection to the e-mail server.

Polling

This value overrides the polling value set for the Email adapter.

The polling interval is used for the transfer of messages from a POP3 mail server into MessageWay. Enter the number of seconds, minutes or hours that the e-mail client will wait before checking all of the e-mail type sites for files to transfer. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

Select one of the polling options from the list. The option **NEVER** stops all polling for this adapter, effectively stopping message transfers into MessageWay. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

The **Schedule** option requires that the schedule type be *Trigger (Input or Execute Now)*, which polls at the time specified. You identify the schedule on the **Schedule** tab, and from there you can drill down to create or edit a schedule item.

Mail Server

Type the name of the e-mail server to which you want to connect. Leave this blank to accept the default value for the e-mail adapter.

User ID

Type a valid user ID to connect to the mail server from which you want to transfer e-mail messages.

Password

Type a valid password to connect to the e-mail server.

Deliver To

Type or select a location to which the adapter associated with this location will transfer the messages. This may be a site for auto-delivery or a service location, such as MWTranslator. When the location does not exist, the message is sent to the system mailbox, {Unknown}.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

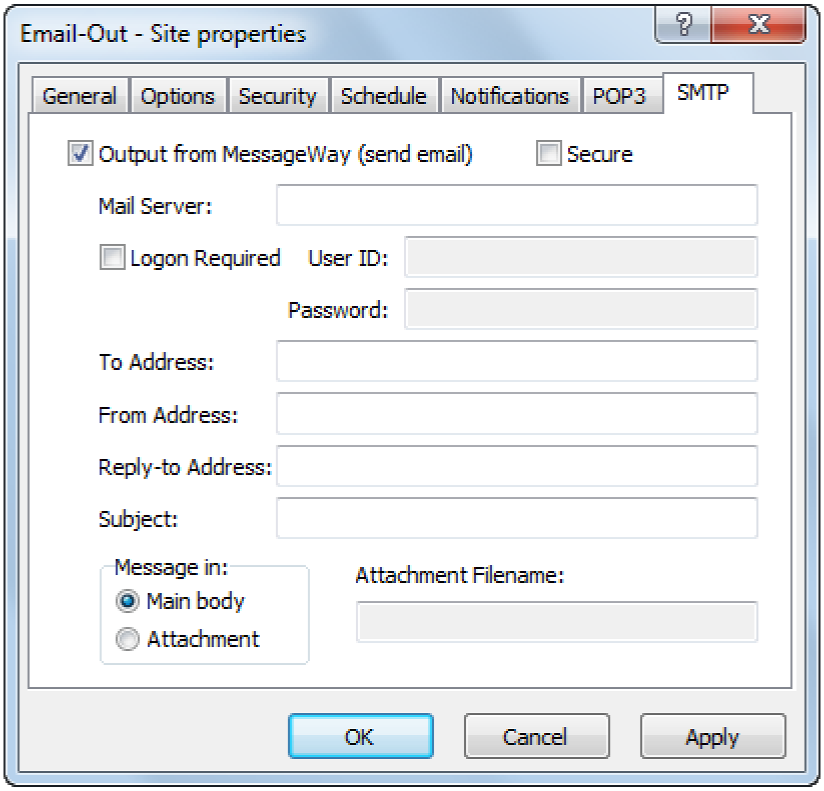
Sender

Select or type a location to represent the sender of the message. This overrides the default sender of the e-mail message.

(E-mail Site Properties) SMTP Page

For e-mail sites, the **SMTP** page of the Site Properties window allows users to specify how to transfer e-mail messages using SMTP from MessageWay.

IMPORTANT: If necessary, users must first establish a connection that provides access to the mail server before a transfer occurs. The e-mail adapter does not make such connections.



☑ Output from MessageWay (send email) □ Secure

Mail Server:

□ Logon Required User ID:

Password:

To Address:

From Address:

Reply-to Address:

Subject:

Message in:
● Main body
○ Attachment

Attachment Filename:

SMTP Page (Site Properties Window)

Output from MessageWay (send email)

Check this box to allow the adapter associated with this location to transfer messages from MessageWay to the specified e-mail server.

Secure

Check this box to enable a secure SMTP connection to the e-mail server.

Mail Server

Type the name of the e-mail server to which you want to connect. Leave this blank to accept the default value from the e-mail adapter configuration.

Logon Required

Check **Logon Required** when the mail server to which you want to transfer messages requires you to log on. You must then supply appropriate values for the **User ID** and **Password** fields.

User ID

When the **Logon Required** box is checked, type a valid user ID to connect to the mail server to which you want to transfer messages. Leave this blank to accept the default value from the e-mail adapter configuration.

Password

When the **Logon Required** box is checked, type a valid password to connect to the mail server to which you want to transfer messages.

To Address

Type a valid e-mail address to which this message will be sent. You may use the enhanced SMTP e-mail format, such as, **recipientname <recipient@domain.com>**. You may also request delivery notification with an additional parameter, **notify=success**, for example, **recipientname <recipient@domain.com> notify=success**. The notify parameter should be used with the delivery notification parameters on the **From address**, **ret=hdrs** and **envid=***token*.For a generic e-mail site, this will be a default address to collect e-mails that were not properly addressed. In accordance with industry practice, e-mail output via SMTP does not accept Unicode e-mail addresses. Unicode characters can only be present in the e-mail's mask, for example, κόσμε <you@yourcompany.com>.

From Address

Type a valid e-mail address from which this message will be sent. You may use the enhanced SMTP e-mail format, such as **sendername <sender@domain.com>**. You may also request delivery notification with optional parameters, **ret=hdrs** or **envid=%msgid%**, for example, **sendername <sender@domain.com> ret=hdrs envid=%msgid%**. You may use any MessageWay tokens for the envelope ID parameter. For more information about tokens, refer to the Mask field on the **Disk Output** tab of Disk Transfer site. The first parameter, **ret=hdrs**, returns the header information from the original e-mail, and the second, **envid=***token*, returns information about the MessageWay message. These should be used with the delivery notification parameter on the **To address**, **notify=success**. In accordance with industry practice, e-mail output via SMTP does not accept Unicode e-mail addresses. Unicode characters can only be present in the e-mail's mask, for example, ジェイソン <me@mycompany.com>.

Reply-to Address

Type a valid e-mail address to which replies will be sent when different from the sender address. In accordance with industry practice, e-mail output via SMTP does not accept Unicode e-mail addresses. Unicode characters can only be present in the e-mail's mask, for example, 素晴らしい男 <anyone@anywhere.com>.

Subject

Type a subject for this message using any combination of literals and tokens.

Message in

Select how the message will be sent with the e-mail: as part of the main body or as an attachment. Messages sent in the body of the e-mail are encoded as quoted-printable, which is best for text. Messages sent as an attachment are encoded as base64, which is best for binary data. When you select **Attachment**, you must also supply an attachment name. There is a maximum of one attachment per e-mail message.

Attachment Filename

Enter the name of the attached file. You may use tokens to create the file name. Enclose the tokens between percent (%) signs. Add constants outside of these signs as required. For new installations, the default mask is blank. For upgrades from previous versions of MessageWay, the default mask is the same as **%filename%**.

The valid tokens are:

Token	Description
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: **MyClassID@MyLocationName** To assign a class ID to a mask for a file name, type: **MyClassID%yyyymmdd%.txt**
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.

Token	Description
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).
inputmsgid	Input Message Id of the message.
inputname	Input Name.
location	The MessageWay location where the message resides. Replaces *mailbox*.
msgid	The Message Id of the message. Replaces *msg*.
ms	Milliseconds (000-999). **NOTE:** The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.

Token	Description
yyyy	Four digit year.
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

```
MW%msgid%.txt

TR%yyyymmddhhnnss#%.txt
```

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

```
%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml
```

TIP: On systems that allow file names longer than 8 characters, use the *msgid* token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the *filename* token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  \ / : * ? " < > | ! & ` ' ;

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

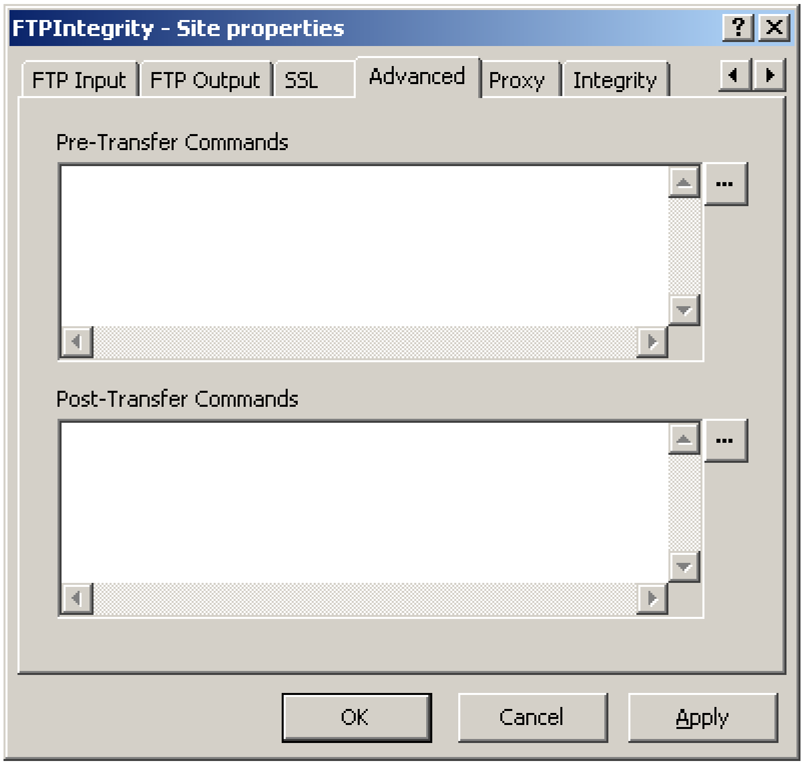
- Duplicate Filename values are allowed within the same location within the Locations folder.

Duplicate Filenames are not allowed within the same location within the File System folder, unless one has been canceled.

(FTP Site Properties) Advanced Page

For an FTP output site, the **Advanced** tab of the Site Properties window allows users to specify additional commands to be executed before or after the transfer for input or output.

NOTE: A special token %remotefile% is available only for pre and post transfer commands. This token resolves to the name of a file on a remote system, not in MessageWay. The token %remotefile% is replaced with the filename that is picked up for inbound transfers or replaced with the filename that is sent for outbound transfers, and it can be used in either Pre-Transfer or Post-Transfer command boxes. The token %filename% cannot be used this way, because it refers to the filename of a message in MessageWay. For some examples, refer to the topic ***Changing Remote Files with Pre and Post Transfer Commands*** (on page 614).



FTP Advanced Page (Site Properties Window)

Pre-transfer Commands

Enter commands that will be sent: for input files, before the RETR/get of the file; for output files, before the STOR/put of the file.

Enter **QUOT**, **SITE**, **PUTFILE** or **PUTLINE** commands, one per line, by typing in the window. The **SITE** command may be included on the same line as the **QUOT** command. For more editing control, click the **Edit** button to open a separate edit window.

The **QUOT** command allows you to enter any standard FTP command, which is sent to the server without change. The **SITE** command allows you to enter a command that is specific to the current FTP server site.

The FTP adapter ignores FTP commands that require a data channel when they are used with a **QUOT** command. FTP commands that are ignored with a **QUOT** command are **LIST**, **NLST**, **RETR** and **STOR**.

The **PUTFILE** and **PUTLINE** commands are MessageWay versions of PUT commands that may use MessageWay tokens. These commands permit the following types of transfers:

- Out(s) before in
- Out(s) after in
- Out(s) before out
- Out(s) after out

NOTE: When the adapter ignores a command, a warning event appears in the event log.

You may also use the keywords **strict** or **relaxed**. The following table describes the behavior for the options:

STRICT	The command is not case-sensitive. All commands defined in the following lines will require verbose (positive) responses from the remote server. When verbose responses are not received, the transfer is aborted. Positive responses are in the 200 range.
RELAXED	The command is not case-sensitive. Treats any response, verbose (positive) or non-verbose (negative) from the server as valid. This type of transfer ignores case.
QUOT or **QUOTE**	The command is not case-sensitive. **QUOT** may optionally end with an **E** (**QUOTE**). The **QUOT** command must be followed by an FTP command, or the adapter will ignore the command. Parameters may optionally be enclosed in single or double quotes.
SITE	The command is not case-sensitive. **SITE** may be embedded in a **QUOT** command or it may be on a separate line. When on a separate line, the **SITE** command must be followed by parameters, or the adapter will ignore the command. Parameters may optionally be enclosed in single or double quotes.
PUTFILE	The command is not case-sensitive. Use it to transfer files from the local disk file system. Syntax: **PUTFILE**[**+**] *local file* [*remote file*] where: ▪ **PUTFILE** generates STOR command ▪ **PUTFILE+** generates APPE command

PUTLINE	The command is not case-sensitive. Use it to transfer a single line of data to a remote system. Syntax: **PUTLINE**[**+**] *remote file* [*data*] where: ▪ **PUTLINE** generates STOR command ▪ **PUTLINE+** generates APPE command The following post-transfer example appends a line of data to the remote file testftp.log, which is derived from *%sender%.log*. **PUTLINE+ %sender%.log Location: [%sender%] Sent message: [%msgid%] On: %mm%-%dd%-%yyyy% At: %hh%:%nn%:%ss%** This pre-transfer example creates a file derived from *M%msgid%.log* and adds the transfer started time. **PUTLINE M%msgid%.log Message: [%msgid%] Transfer started: %mm%-%dd%-%yyyy% At: %hh%:%nn%:%ss%**

CAUTION: When a file of the name exists, it will be overlaid by default. Also, there is only one instance per output session (pre-transfer commands, transfer commands and post-transfer commands) of the persistent counter symbol, #. This means that when you use the # token as part of your mask name, and you also use the same name, including the # token in pre-transfer and post-transfer **PUTFILE** or **PUTLINE** commands, the pre-transfer file will be overlaid by the output file, which in turn will be overlaid by the post-transfer file.

Post-transfer Commands

Enter commands that will be sent: for input files, after a file is successfully received from the remote server; for output files, after a message is successfully sent to the remote server.

Enter **QUOT, SITE**, **PUTFILE** or **PUTLINE** commands, one per line, by typing in the window. The **SITE** command may be included on the same line as the **QUOT** command. For more editing control, click the **Edit** button to open a separate edit window.

The **QUOT** command allows you to enter any standard FTP command, which is sent to the server without change. The **SITE** command allows you to enter a command that is specific to the current FTP server site.

The FTP adapter ignores FTP commands that require a data channel when they are used with a **QUOT** command. FTP commands that are ignored with a **QUOT** command are **LIST**, **NLST**, **RETR** and **STOR**.

The **PUTFILE** and **PUTLINE** commands are MessageWay versions of PUT commands that may use MessageWay tokens. These commands permit the following types of transfers:

- Out(s) before in
- Out(s) after in
- Out(s) before out
- Out(s) after out

NOTE: When the adapter ignores a command, a warning event appears in the event log.

You may also use the keywords **strict** or **relaxed**. The following table describes the behavior for the options:

STRICT	The command is not case-sensitive. All commands defined in the following lines will require verbose (positive) responses from the remote server. When verbose responses are not received, the transfer is aborted. Positive responses are in the 200 range.
RELAXED	The command is not case-sensitive. Treats any response, verbose (positive) or non-verbose (negative) from the server as valid. This type of transfer ignores case.
QUOT or **QUOTE**	The command is not case-sensitive. **QUOT** may optionally end with an **E** (**QUOTE**). The **QUOT** command must be followed by an FTP command, or the adapter will ignore the command. Parameters may optionally be enclosed in single or double quotes.
SITE	The command is not case-sensitive. **SITE** may be embedded in a **QUOT** command or it may be on a separate line. When on a separate line, the **SITE** command must be followed by parameters, or the adapter will ignore the command. Parameters may optionally be enclosed in single or double quotes.
PUTFILE	The command is not case-sensitive. Use it to transfer files from the local disk file system. Syntax: **PUTFILE**[**+**] *local file* [*remote file*] where: ▪ **PUTFILE** generates STOR command ▪ **PUTFILE+** generates APPE command

PUTLINE	The command is not case-sensitive. Use it to transfer a single line of data to a remote system. Syntax: **PUTLINE**[**+**] *remote file* [*data*] where: ▪ **PUTLINE** generates STOR command ▪ **PUTLINE+** generates APPE command The following post-transfer example appends a line of data to the remote file testftp.log, which is derived from *%sender%.log*. **PUTLINE+ %sender%.log Location: [%sender%] Sent message: [%msgid%] On: %mm%-%dd%-%yyyy% At: %hh%:%nn%:%ss%** This pre-transfer example creates a file derived from *M%msgid%.log* and adds the transfer started time. **PUTLINE M%msgid%.log Message: [%msgid%] Transfer started: %mm%-%dd%-%yyyy% At: %hh%:%nn%:%ss%**

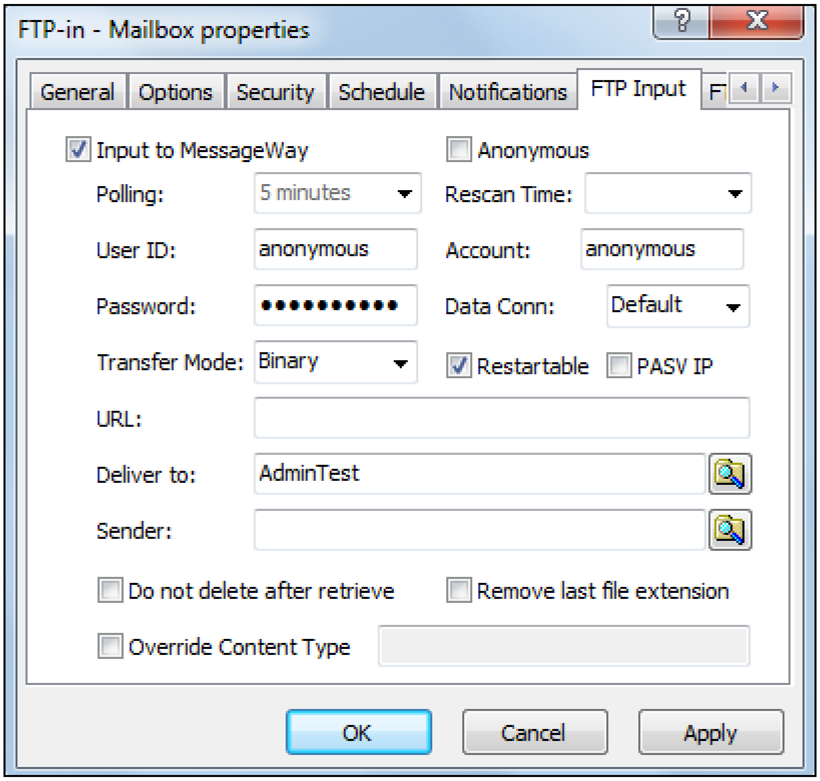
CAUTION: When a file of the name exists, it will be overlaid by default. Also, there is only one instance per output session (pre-transfer commands, transfer commands and post-transfer commands) of the persistent counter symbol, #. This means that when you use the # token as part of your mask name, and you also use the same name, including the # token in pre-transfer and post-transfer **PUTFILE** or **PUTLINE** commands, the pre-transfer file will be overlaid by the output file, which in turn will be overlaid by the post-transfer file.

(FTP Site Properties) FTP Input Page

The **FTP Input** tab of the Site Properties window allows users to specify how to transfer messages from an FTP site into MessageWay.

Note that MessageWay does not support input filenames that contain backslashes, \. For operating systems, such as UNIX, that allow backslashes in filenames, the filename property will be whatever follows the final backslash.

IMPORTANT: Note that these parameters control the connection to an FTP server. When the adapter connects to the MessageWay FTP Perimeter Server first, the URL to connect to the server and the transfer mode and data connection from the FTP adapter to the FTP perimeter server are controlled by values on the **Proxy** tab of the Site Properties window.



☑ Input to MessageWay ☐ Anonymous

Polling: 5 minutes Rescan Time:

User ID: anonymous Account: anonymous

Password: •••••••••• Data Conn: Default

Transfer Mode: Binary ☑ Restartable ☐ PASV IP

URL:

Deliver to: AdminTest

Sender:

☐ Do not delete after retrieve ☐ Remove last file extension

☐ Override Content Type

Input to MessageWay

Check this box to allow the adapter associated with this site to transfer messages from the specified site into MessageWay. The FTP adapter only polls for input messages when the schedule for the site is open.

Polling

This value overrides the polling value set for the FTP adapter.

The polling interval is used for the transfer of messages from an FTP directory into MessageWay. This is the amount of time that the FTP client will wait before checking the directory for files to transfer to the site. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

The URL to be polled and the location to which the inbound files will be transferred are on the **FTP** page of the Site Properties window under **Input to MessageWay**.

Select an interval from the list or type the number of hours, minutes or seconds between polling cycles. The option **Never** stops polling for this adapter. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

The **Schedule** option requires that the schedule type be *Trigger (Input or Execute Now)*, which polls at the time specified. You identify the schedule on the **Schedule** tab, and from there you can drill down to create or edit a schedule item.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds
30m	means 30 minutes
2 h	means 2 hours

User ID

Enter a valid user ID to connect to the remote FTP site. If you check the box *Anonymous* to connect to the FTP server as an anonymous user, this field defaults to **anonymous** and cannot be changed.

IMPORTANT: To connect to a MessageWay FTP Perimeter Server as an anonymous user, the User ID must be **Anonymous**, and it must exist as a valid user ID in the MessageWay environment where the perimeter server connects.

Password

Enter a valid password to connect to the FTP site. If you check the box *Anonymous* to connect to the FTP server as an anonymous user, this field is ignored.

Anonymous

Some FTP sites allow users to connect without a unique user ID or password. Such a user is called *anonymous*. Check this box if you want to connect to the FTP site as an anonymous user. The *User ID*, *Password* and *Account* fields are filled with default values that cannot be changed.

IMPORTANT: To connect to a MessageWay FTP Perimeter Server as an anonymous user, the User ID must be **Anonymous**, and it must exist as a valid user ID in the MessageWay environment where the perimeter server connects.

Rescan Time

This is the interval in seconds that FTP adapter waits before it rereads the properties of the input message. Set this interval for locations that receive large files to assure that MessageWay only inputs complete messages. The alternative to avoid having MessageWay input partial files is to write to a temporary directory, and then rename the file to the primary directory. When you use this feature, as the polling interval finds messages to bring into MessageWay, the adapter reads the properties returned from the LIST command. These properties may include message size and date/time stamps, as transferred by the FTP input stream. Then it rescans the properties of the message at the rescan time until if finds that the properties have no longer changed. When it determines that the file is stable, it initiates the transfer of the file into MessageWay. Since this feature will input files only after at least three readings of the file properties, it will slow down input for smaller files as well. This setting only works when the polling interval is explicitly set to a value, and the *Input Now* command is disabled when a rescan time is specified. It is ignored when the polling interval is set to *Event Driven*, *Schedule* or *None*. If the rescan time is greater than or equal to the polling time, the polling time will act as the rescan of the previous poll.

CAUTION: When rescan is set to a low number, such as 5 seconds, a remote server may not have enough time to update the file size before 2 consecutive rescans. In this case MessageWay will think the file is complete and input the file, which may result in an incomplete file transfer. Make sure that the rescan time is set high enough to allow remote servers to update the file statistics between scans. We recommend a higher interval, at least 60 seconds.

Account

Enter a valid account for the FTP site, which is sent only when the server requests it.

Transfer Mode

Select one of the options, **Binary** or **Text** or for UNIX/Linux only, **Strict**, to determine in which format the message(s) will be transferred.

CAUTION: When the last line in a file transferred as a text file contains no line termination character, then a line terminator is added to the file. The line terminator depends on the system default values. For example, for Windows, a line terminator is carriage return/linefeed (CRLF), and for UNIX/Linux it is a newline (NL).

The options are as follows:

Transfer Mode	Description
Binary	A file that appears to be data, an executable, or compressed should be transferred in binary mode. Binary mode should also be used if there is no file extension or the file extension is not registered.
Text	A file that appears to be text or other ASCII format should be transferred in text mode. Typically, the FTP server will automatically convert end-of-line markers and end-of-text markers to the format required for the system where the file is written.
Strict (UNIX/Linux only)	All commands will require verbose (positive) responses from the remote server. When verbose responses are not received, the transfer is aborted. Positive responses are in the 200 range.

CAUTION: Transferring a binary file in text format may damage the file. Never transfer both binary and text data in the same file.

Data Connection

FTP clients determine the type of connection used with an FTP server when the adapter collects messages from an FTP site. Since the FTP adapter is an FTP client, this is where you determine the type of connection when the adapter connects to an FTP server or the FTP perimeter server, acting as a client, connects to an FTP server.

IMPORTANT: Note that this parameter controls the connection to an FTP server. The type of connection from the FTP adapter to an FTP perimeter server is controlled by the Data Connection value on the **Proxy** tab of the Site Properties window.

Select one of the options, **Default**, **Active**, **Passive** or **Ext-Passive**, to determine how messages are sent to this site.

The options are as follows:

Data Connection	Description
Default	Attempt a passive connection first, and if it fails, try an active connection. This is the default behavior for MessageWay versions prior to 4.2.
Passive	Attempt a passive connection only.
Active	Attempt an active connection only.
Ext-Passive	Attempt an extended passive connection only, using IPv4 protocol. Communicates data connection endpoint information for network protocols through firewalls or network address translators (NATs). Use this extended passive command (*EPSV*) in place of the *PASV* command for FTP transfers where the control and data connection(s) are being established between the same two machines. Since the server only returns a port number, the client must assume the connection is to the same address to which it originally connected. This type of connection does not require the translation of the network address, so it also supports encrypted data.

To avoid problems with client firewalls, among other reasons, the client often initiates a passive connection.

The FTP perimeter server and an FTP client each use at least two ports: a command port and a data port. They exchange commands and responses on the command port, and they receive and send data, including directory listings, on the data port. For active transfers, the server initiates a data connection to a client's data port. For passive transfers, the client initiates a data connection to the server's data port.

Restartable Check Box

Check this box to allow the external FTP server to restart from a check point, rather than resend the entire file when an error occurs during transmission. Restart occurs at the next polling interval, so you must also configure a polling interval. The external FTP server must support check-point restart, either as streaming or block mode. As a best practice, also configure the **Transfer Mode** as **Binary**. Restart preempts configurations for retries, which attempt to receive the file from the beginning. Retry strategies are configured on the **Options** tab under **Error Action**. When the FTP server does not support check-point restart, MessageWay will ask the server to resend the file from the beginning, if retries are configured for this site.

PASV IP

Check this box to force use of the IP Address returned by a PASV response for the data channel connection.

URL (Input)

Enter a valid input location in the form of a URL that the adapter will scan for messages to transfer into MessageWay. Do not use mapped drive letters to access network resources. Use full Universal Naming Convention (UNC) names instead.

The URL uses the following syntax:

- For FTP Output: [*protocol prefix*] *host* [**/***location*]
- For FTP Input: [*protocol prefix*] *host* [**/***location*]

  - or -

  [*protocol prefix*] *host* [**/**location**/**filemask]

Component	Requirement	Description
Protocol prefix	optional	▪ **ftp://** or **//** ▪ When not used, defaults to ftp protocol
Host	required	[*userID* [**:***pw*] [**:***account*] **@**] (*hostname* **|** *IP address*) [**:***port number*] ▪ *Hostname* is standard internet domain name ▪ *IP address* is four decimal values separated by periods ▪ When *port number* is not used, defaults to ftp port When connecting to the dedicated MessageWay FTP Server, you cannot use the *userID*, *pw* or *account* options.
Location	optional	For generic FTP servers: ▪ A valid directory for the URL. For the dedicated MessageWay FTP Server: ▪ A valid MessageWay location where messages reside, which overrides the user's default location

Component	Requirement	Description
Filemask	optional	(FTP Input only) You can construct file names to pull one or more files from a directory as follows: ▪ A static file name with all literal characters, for example, ftp://100.100.1.100:2020/dir/abc.txt ▪ A dynamic file name with wild cards, for example, ftp://100.100.1.100:2020/dir/abc*

Here are some examples of valid URLs:

Description	Example
Basic	For a generic FTP server: ▪ ftp://userID:password@www.ftpserver.com/dir ▪ ftp://100.100.1.100:2020/dir For the dedicated MessageWay FTP Server: ▪ ftp://www.ftpserver.com/mailbox ▪ ftp://100.100.1.100:2020
Basic, shortened	For a generic FTP server: ▪ www.ftpserver.com/dir ▪ 100.100.1.100/dir For the dedicated MessageWay FTP Server: ▪ www.ftpserver.com ▪ 100.100.1.100/mailbox

Deliver To

Type or select a location to which the adapter associated with this site will transfer the messages. This may be a site for auto-delivery, a service location, such as MWTranslator, or a pickup mailbox. When the location does not exist, the message is sent to the system mailbox, {Unknown}.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

Sender

Select or type a location to represent the sender of the message. This overrides the sender that may or may not have been passed by the FTP server. This feature is useful for testing, where the input site is already defined, but currently inaccessible, such as at a customer site whose connection is unavailable. You can use a test location that has a different name, but when you put the name of the original customer location here, the message will be marked as if it were from the customer location.

Do Not Delete after Retrieve

Check this box to leave the input file on the source FTP site after successful retrieval. When a file has been retrieved from a non-MessageWay FTP site into MessageWay, the default behavior is to delete the file from the source FTP site.

When you connect to another MessageWay FTP Perimeter Server to send messages from MessageWay, you must check this box, because MessageWay does not allow messages to be deleted this way. Messages are conditionally archived and then deleted when the archive program runs.

Remove Last File Extension

Some non-traditional FTP servers may provide a directory listing where the last extension on the file name does not actually exist. In order for MessageWay to retrieve the file, it must remove the extension before it issues a GET command. Check this box to allow MessageWay to remove the invalid extension and retrieve the file. You typically determine the discrepancy based on a MessageWay 3002 error saying the file does not exist and a subsequent trace that shows the file name returned by the FTP server is invalid.

Override Content Type Check Box

Check this box to override the content type specified for the input message.

Override Content Type

The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.

The following table shows the content types that MessageWay supports.

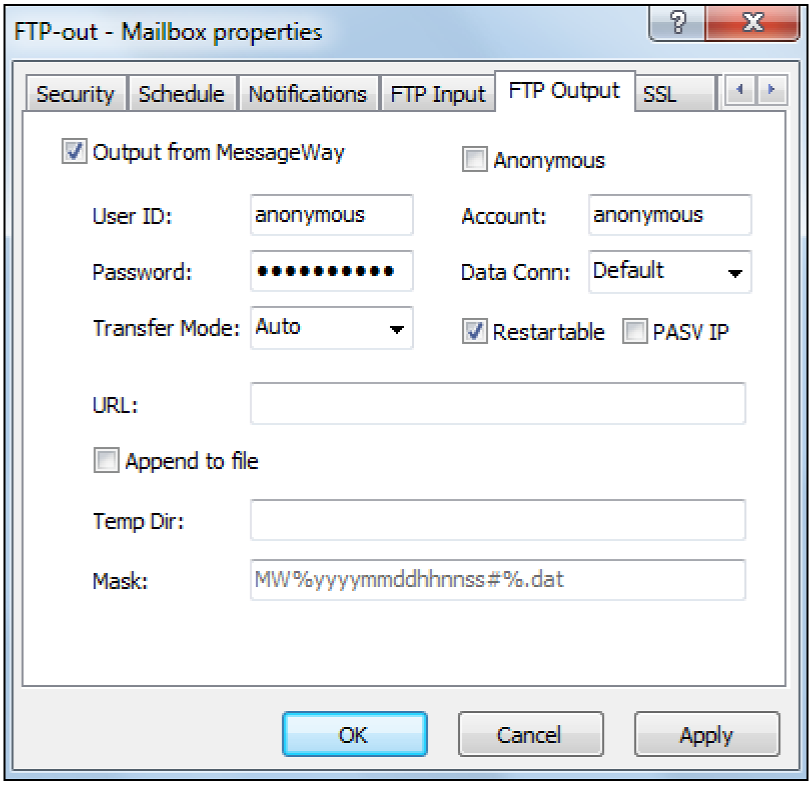
Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf

Type	Content Type	File Extension
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

(FTP Site Properties) FTP Output Page

For an FTP output site, the **FTP Output** tab of the Site Properties window allows users to specify how to transfer messages from MessageWay to an FTP site.

IMPORTANT: Note that these parameters control the connection to an FTP server. When the adapter connects to the MessageWay FTP Perimeter Server first, the URL to connect to the server and the transfer mode and data connection from the FTP adapter to an FTP perimeter server are controlled by values on the **Proxy** tab of the Site Properties window.


FTP-out - Mailbox properties

☑ Output from MessageWay
□ Anonymous
User ID: anonymous
Account: anonymous
Password: ••••••••••
Data Conn: Default
Transfer Mode: Auto
☑ Restartable
□ PASV IP
URL:
□ Append to file
Temp Dir:
Mask: MW%yyyymmddhhnnss#%.dat

FTP Output Page (Site Properties Window)

Output from MessageWay

Check this box to allow the adapter associated with this location to transfer messages from MessageWay. The FTP adapter will deliver messages only when the schedule for this site is open.

User ID

Type a valid user ID to connect to the FTP site. If you check the box *Anonymous* to connect to the FTP server as an anonymous user, this field defaults to **anonymous** and cannot be changed.

IMPORTANT: To connect to a MessageWay FTP Perimeter Server as an anonymous user, the User ID must be **Anonymous**, and it must exist as a valid user ID in the MessageWay environment where the perimeter server connects.

Password

Type a valid password to connect to the FTP site. If you check the box *Anonymous* to connect to the FTP server as an anonymous user, this field is ignored.

Transfer Mode

Select one of the options, **Auto**, **Binary** or **Text** or for UNIX/Linux only, **Strict**, to determine in which format the message(s) will be transferred.

CAUTION: When the last line in a file transferred as a text file contains no line termination character, then a line terminator is added to the file. The line terminator depends on the system default values. For example, for Windows, a line terminator is carriage return/linefeed (CRLF), and for UNIX/Linux it is a newline (NL).

The options are as follows:

Transfer Mode	Description
Auto	MessageWay uses the Content Type of the message to determine the transfer mode. When the content type starts with *text/*, then text mode is used. Otherwise binary mode is used.
Binary	A file that appears to be data, an executable, or compressed should be transferred in binary mode. Binary mode should also be used if there is no file extension or the file extension is not registered.
Text	A file that appears to be text or other ASCII format should be transferred in Text mode.
Strict (UNIX/Linux only)	All commands will require verbose (positive) responses from the remote server. When verbose responses are not received, the transfer is aborted. Positive responses are in the 200 range.

Anonymous

Some FTP sites allow users to connect without a unique user ID or password. Such a user is called *anonymous*. Check this box if you want to connect to the FTP site as an anonymous user. The *User ID*, *Password* and *Account* fields are filled with default values that cannot be changed.

IMPORTANT: To connect to a MessageWay FTP Perimeter Server as an anonymous user, the User ID must be **Anonymous**, and it must exist as a valid user ID in the MessageWay environment where the perimeter server connects.

Account

Type a valid account for the FTP site, which is sent only when the server requests it.

Data Connection

FTP clients determine the type of connection used with an FTP server when the adapter sends messages to an FTP site. Since the FTP adapter is an FTP client, this is where you determine the type of connection when the adapter connects to an FTP server or when the FTP perimeter server connects to an FTP server.

IMPORTANT: Note that this parameter controls the connection to an external FTP server. The type of connection from the FTP adapter to an FTP perimeter server is controlled by the Data Connection value on the **Proxy** tab of the Site Properties window.

Select one of the options, **Default**, **Active**, **Passive** or **Ext-Passive**, to determine how messages are sent from this site.

The options are as follows:

Data Connection	Description
Default	Attempt a passive connection first, and if it fails, try an active connection. This is the default behavior for MessageWay versions prior to 4.2.
Passive	Attempt a passive connection only.
Active	Attempt an active connection only.
Ext-Passive	Attempt an extended passive connection only, using IPv4 protocol. Communicates data connection endpoint information for network protocols through firewalls or network address translators (NATs). Use this extended passive command (*EPSV*) in place of the *PASV* command for FTP transfers where the control and data connection(s) are being established between the same two machines. Since the server only returns a port number, the client must assume the connection is to the same address to which it originally connected. This type of connection does not require the translation of the network address, so it also supports encrypted data.

An FTP Server and an FTP client each use at least two ports: a command port and a data port. They exchange commands and responses on the command port, and they receive and send data, including directory listings, on the data port. For active transfers, the server initiates a data connection to a client's data port. For passive transfers, the client initiates a data connection to the server's data port.

URL (FTP Output)

Type a valid destination location in the form of a URL that the adapter will use to transfer a message from MessageWay. Do not use mapped drive letters to access network resources. Use full Universal Naming Convention (UNC) names instead.

The URL uses the following syntax:

- For FTP Output: [*protocol prefix*] *host* [/*location*]
- For FTP Input: [*protocol prefix*] *host* [/*location*]

  - or -

  [*protocol prefix*] *host* [/location/filemask]

Component	Requirement	Description
Protocol prefix	optional	▪ **ftp:**// or // ▪ When not used, defaults to ftp protocol
Host	required	[*userID* [**:***pw*] [**:***account*] **@**] (*hostname* **|** *IP address*) [**:***port number*] ▪ *Hostname* is standard internet domain name ▪ *IP address* is four decimal values separated by periods ▪ When *port number* is not used, defaults to ftp port When connecting to the dedicated MessageWay FTP Server, you cannot use the *userID*, *pw* or *account* options.
Location	optional	For generic FTP servers: ▪ A valid directory for the URL. For the dedicated MessageWay FTP Server: ▪ A valid MessageWay location where messages reside, which overrides the user's default location
Filemask	optional	(FTP Input only) You can construct file names to pull one or more files from a directory as follows: ▪ A static file name with all literal characters, for example, ftp://100.100.1.100:2020/dir/abc.txt ▪ A dynamic file name with wild cards, for example, ftp://100.100.1.100:2020/dir/abc*

Here are some examples of valid URLs:

Description	Example
Basic	For a generic FTP server: ▪ ftp://userID:password@www.ftpserver.com/dir ▪ ftp://100.100.1.100:2020/dir For the dedicated MessageWay FTP Server: ▪ ftp://www.ftpserver.com/mailbox ▪ ftp://100.100.1.100:2020

Description	Example
Basic, shortened	For a generic FTP server: ▪ www.ftpserver.com/dir ▪ 100.100.1.100/dir For the dedicated MessageWay FTP Server: ▪ www.ftpserver.com ▪ 100.100.1.100/mailbox

Restartable Check Box

Check this box to allow MessageWay to restart from a check point, rather than resend the entire file when an error occurs during transmission. Restart occurs based on the next configured retry interval, so you must also configure retries. Retry strategies are configured on the **Options** tab under **Error Action**. The remote FTP server must support check-point restart, either as streaming or block mode. We strongly recommend that you configure the **Transfer Mode** as **Binary**, because many FTP servers do not support ASCII transfers for restarts. When the remote FTP server does not support check-point restart, MessageWay will attempt to resend the entire file, if retries are configured for this site.

PASV IP

Check this box to force use of the IP Address returned by a PASV response for the data channel connection.

Append to file

Check this box to append the contents of the message to a file of the same name. When this box is not checked, existing files will be replaced with the newer version. Append is not compatible with Integrity checks. If the **Append to** box is checked and integrity checking is mandatory, the transfer will fail, and an error will be logged to the error log and placed on the **Error** tab of the Message Properties window. If the **Append to** box is checked and integrity checking is optional, integrity will be ignored, the transfer will proceed, and a warning will appear on the **Misc** tab of the Message Properties window.

CAUTION: This option allows MessageWay to write directly to the permanent file, so any program that reads the file must ensure the file is complete before accessing it.

Temp Dir (FTP Output)

Type a valid temporary directory for the URL on the remote system to deposit a message from MessageWay. This directory will be added to the URL. The directory name may also be prefixed with the same protocol prefix, host, and directory as the output URL. When using the full directory path, it must match the directory path in the URL exactly. The temporary directory must exist within the URL location.

When the file completes sending, MessageWay renames it to the permanent directory. This avoids programs reading a file before it has been completely transferred.

If the output FTP site does not allow you to create temporary directories, leave this value blank. In this case, you can specify a temporary file name mask and a permanent file name mask in the Mask field. The file will be written to the permanent directory using the temporary file name mask and then will be renamed using the permanent file name mask. For more information, refer to the Mask field.

Mask (FTP Output)

You may specify tokens to create a permanent file name and a temporary file name. The mask for the permanent file name is separated from the mask for the optional temporary file name with a forward slash: *permanent file name mask/temporary file name mask*. When only one mask is configured, the file name is the same for both the temporary and permanent file names. If a temporary directory is used, the file is written to the temporary directory using the temporary file mask and renamed to the permanent directory using the permanent file mask. If a temporary directory is not used, the file is written to the permanent directory using the temporary file mask and then renamed using the permanent file mask.

Use any combination of constants and MessageWay tokens. This value overrides the one for the FTP Adapter, mwftp, visible on the **FTP** page of the FTP Adapter Properties window. For new installations, the default mask is **%filebase%<[msgid]>.%fileext%**. For upgrades from previous versions of MessageWay, the default mask is the same as **%filename%**. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name, for example, **MW%msgid%.txt**. If you use both permanent and temporary masks, your entry might look as follows: **CO1%yyyymmddhhnnss#%/CO1temp%yyyymmddhhnnss#%**.

CAUTION: When users have a program that scans for files to pick up after they appear in the target directory, and when you do not use a temporary directory, make sure the program scans for files by name rather than scan a directory. Otherwise, it may read the temporary file before it is renamed, which will likely be a partial file.

Use two percent (%) signs to enclose the tokens. MessageWay replaces the tokens with appropriate values. Add constants outside of these signs as required.

CAUTION: When a file of the name exists, it will be overlaid by default. Also, there is only one instance per output session (pre-transfer commands, transfer commands and post-transfer commands) of the persistent counter symbol, #. This means that when you use the # token as part of your mask name, and you also use the same name, including the # token in pre-transfer and post-transfer **PUTFILE** or **PUTLINE** commands, the pre-transfer file will be overlaid by the output file, which in turn will be overlaid by the post-transfer file.

To append data to an existing file, check **Append to file**.

CAUTION: Do not specify both a temporary mask and check the box, **Append to file**, because the new file will be appended to the temporary file and then renamed to the permanent file. If you want to use the append option, only specify a permanent mask.

The valid tokens are:

Token	Description
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: **MyClassID@MyLocationName** To assign a class ID to a mask for a file name, type: **MyClassID%yyyymmdd%.txt**
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).
inputmsgid	Input Message Id of the message.
inputname	Input Name.

Token	Description
location	The MessageWay location where the message resides. Replaces *mailbox*.
msgid	The Message Id of the message. Replaces *msg*.
ms	Milliseconds (000-999). **NOTE:** The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.
yyyy	Four digit year.
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

```
MW%msgid%.txt

TR%yyyymmddhhnnss#%.txt
```

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

```
%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml
```

TIP: On systems that allow file names longer than 8 characters, use the *msgid* token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the *filename* token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  `\ / : * ? " < > | ! & ` ' ;`

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

- Duplicate Filename values are allowed within the same location within the Locations folder.

Duplicate Filenames are *not* allowed within the same location within the File System folder, unless one has been canceled.

By default, the file attributes used to create a file on NonStop are from the default TACL parameters of the UserID used to log on to the NonStop system specified on this page. You may specify alternative attributes after the mask as a series of values separated by commas. The values you may enter depend on whether you want to create Edit, Structured, or Unstructured files. The following table shows the <attributes> separated by commas and their order for each file type. Commas are required, but you may leave a value blank to allow it to default. For appropriate values to use in each position, refer to your NonStop documentation. The *HP NonStop TCP/IP Application and Utilities User Guide* contains this information.

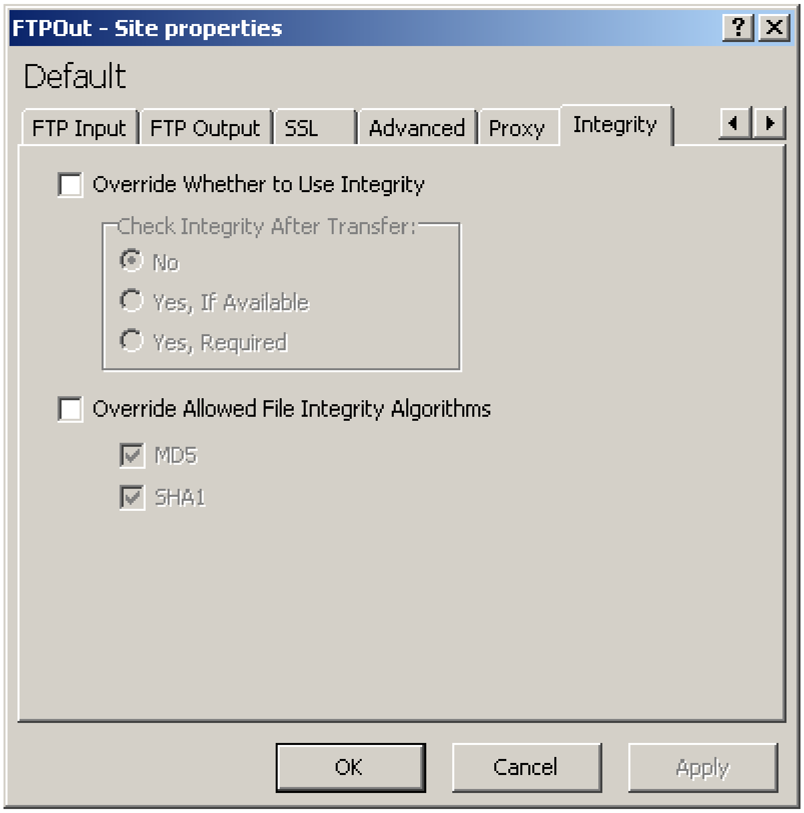
File Type	File Attributes
ASCII or unstructured	<MASK_FILENAME>,<FILECODE>,<PRIMARY_EXTENT>, <SECONDARY_EXTENT>,<MAXEXTENTS>
Structured	<MASK_FILENAME>,<FILETYPE>,<FILECODE>,<PRIMARY_EXTENT>, <SECONDARY_EXTENT>,<MAXEXTENTS>, <RECORD_LENGTH>

The following table provides some examples:

File Type	Example
ASCII or unstructured	Filename, followed by attributes M%hhnn#:3%,0,100,100,25
Structured	Filename, followed by attributes M%hhnn#:3%,U,0,100,100,25,512

(FTP Site Properties) Integrity Page

For an FTP input or output site, the **Integrity** page allows users to configure whether to verify the message by comparing hash totals from an external FTP server with one that MessageWay creates.



□ Override Whether to Use Integrity

Check Integrity After Transfer:
● No
○ Yes, If Available
○ Yes, Required

□ Override Allowed File Integrity Algorithms

☑ MD5
☑ SHA1

Override Whether to Use Integrity

Check this box to override the default setting on the **Integrity** tab of the FTP Adapter Properties window to check the integrity of messages.

No

Select **No** to *not* check the integrity of the message. This overrides the default option on the **Integrity** tab of the FTP Adapter Properties window.

Yes, If Available

Select **Yes, If Available** to check the integrity of the message when possible. MessageWay uses the strongest algorithm selected that the FTP server also supports. When the comparison of hash values succeeds, the algorithm and hash value used appear on the **Misc** tab of the Message Properties window. When the comparison of hash values fails, MessageWay marks the message with a status of *Error*, and displays the error information on the **Error** tab of the Message Properties window. When the FTP server does not support integrity checks or does not support any of the algorithms selected, the adapter does not perform an integrity check. This overrides the default option on the **Integrity** tab of the FTP Adapter Properties window.

Yes, Required

Select **Yes, Required** to check the integrity of the message. MessageWay uses the strongest algorithm selected that the FTP server also supports. When the comparison of hash values succeeds, the algorithm and hash value used appear on the **Misc** tab of the Message Properties window. When the FTP server does not support integrity checks or does not support any of the algorithms selected, or the comparison of hash values fails, MessageWay marks the message with a status of *Error*, and displays the error information on the **Error** tab of the Message Properties window. This overrides the default option on the **Integrity** tab of the FTP Adapter Properties window.

Override Allowed File Integrity Algorithms

Check this box to override the default setting on the **Integrity** tab of the FTP Adapter Properties window for specific algorithms that may be used to check the integrity of messages. When multiple algorithms are checked, MessageWay uses the strongest algorithm that the FTP server also supports.

MD5

Check this box to potentially use the MD5 (Message-Digest algorithm 5) to determine the integrity of the message. This overrides the default option on the **Integrity** tab of the FTP Adapter Properties window.

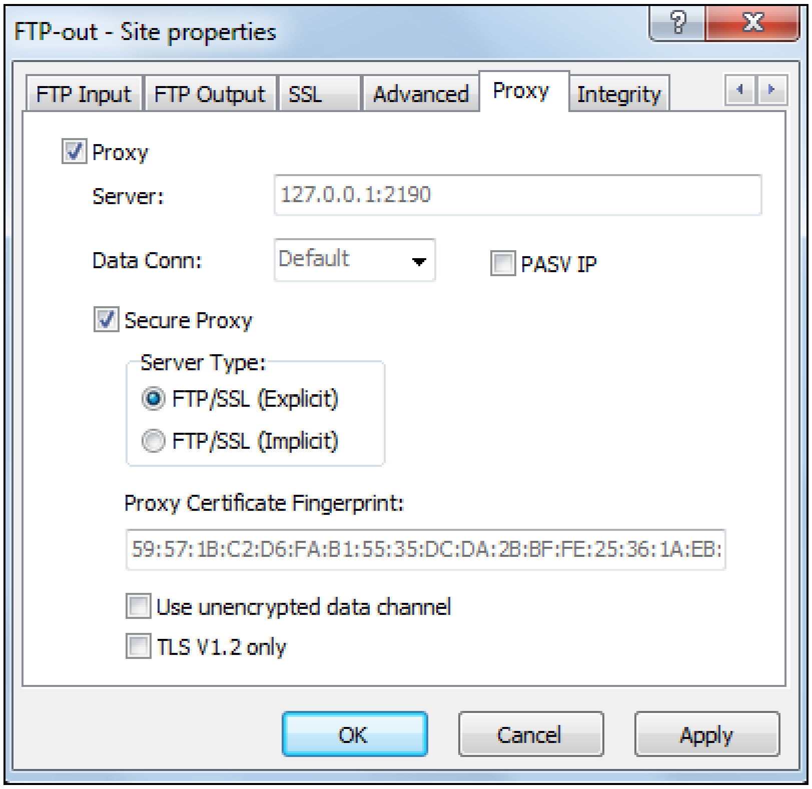
SHA1

Check this box to potentially use the SHA-1 (Secure Hash Algorithm 1) to determine the integrity of the message. This overrides the default option on the **Integrity** tab of the FTP Adapter Properties window.

(FTP Site Properties) Proxy Page

By default, the FTP adapter communicates directly with an FTP server. To communicate with an FTP server through the MessageWay FTP Perimeter Server instead, you must provide information on the **Proxy** tab. The **Proxy** page allows you to specify the type of data connection between the adapter and the perimeter server and, if the connection is to be secure, additional security information.

IMPORTANT: Note that these parameters control the connection between the adapter and the MessageWay FTP Perimeter Server. The type of connection from the perimeter server acting as a client to an external FTP server is controlled by the corresponding values on the **FTP Input** or **FTP Output** tab of the Site Properties window.



☑ Proxy

Server: 127.0.0.1:2190

Data Conn: Default

□ PASV IP

☑ Secure Proxy

Server Type:

● FTP/SSL (Explicit)

○ FTP/SSL (Implicit)

Proxy Certificate Fingerprint:

59:57:1B:C2:D6:FA:B1:55:35:DC:DA:2B:BF:FE:25:36:1A:EB:

□ Use unencrypted data channel

□ TLS V1.2 only

Proxy Page (Site Properties Window)

Proxy

Check this box to send messages from this location through an FTP proxy server rather than directly to an external FTP server.

Server

This setting is inherited from the FTP adapter, which is visible on the **Proxy** tab of the Adapter Properties window. To override the adapter setting, type the URL of the FTP proxy server, and include the host and port.

Data Connection

This setting is inherited from the FTP adapter, which is visible on the **Proxy** tab of the Adapter Properties window. To override the adapter setting, select another option.

IMPORTANT: Note that this parameter controls the connection between the adapter and the FTP proxy server. The type of connection from the proxy server acting as a client to the external FTP server is controlled by the Data Connection value on the **FTP Input** or **FTP Output** tab of the Location Properties window.

The options are as follows:

Data Connection	Description
Default	Attempt a passive connection first, and if it fails, try an active connection. This is the default behavior for MessageWay versions prior to 4.2.
Passive	Attempt a passive connection only.
Active	Attempt an active connection only.
Ext-Passive	Attempt an extended passive connection only, using IPv4 protocol. Communicates data connection endpoint information for network protocols through firewalls or network address translators (NATs). Use this extended passive command (*EPSV*) in place of the *PASV* command for FTP transfers where the control and data connection(s) are being established between the same two machines. Since the server only returns a port number, the client must assume the connection is to the same address to which it originally connected. This type of connection does not require the translation of the network address, so it also supports encrypted data.

PASV IP

Check this box to force use of the IP Address returned by a PASV response for Proxy data channel connection. This setting is inherited from the FTP Adapter, which is visible on the Proxy tab of the Adapter Properties window. To override the adapter setting, check or clear this box.

Secure Proxy

Check this box to enable the fields that allow you to specify the parameters for a TLS/SSL session. This setting is inherited from the FTP adapter, which is visible on the **Proxy** tab of the Adapter Properties window. To override the adapter setting, check or clear this box. Clear this box to not use encryption.

IMPORTANT: This controls security from the adapter to the proxy server. Security from the proxy server acting as a client to the external FTP server is controlled by the corresponding value on the **SSL** tab of the Location Properties window.

Server Type

This setting is inherited from the FTP adapter, which is visible on the **Proxy** tab of the Adapter Properties window. To override the adapter setting, select another option.

IMPORTANT: This controls the server type from the adapter to the proxy server. The server type from the proxy server acting as a client to the external FTP server is controlled by the corresponding value on the **SSL** tab of the Site Properties window.

Check the Secure option that precedes, and then select the type of secure connection for the server. When the Secure option is clear, the default is non-secure FTP.

FTP/SSL (Explicit) The client connects to an unencrypted port on the server, typically 21. To connect to the MessageWay FTP perimeter server, we use 2190 to avoid conflict with other existing FTP servers. After starting a normal session, the client requests that SSL/TLS security be used, and when the appropriate handshake occurs, it sends the data.

FTP/SSL (Implicit) The client connects to an encrypted port, typically 990, and after an appropriate SSL handshake, it sends FTP commands.

Proxy Certificate Fingerprint

This fingerprint is used instead of a full certificate to authenticate the FTP proxy server. This setting is inherited from the FTP adapter, which is visible on the **Proxy** tab of the Adapter Properties window. To override the adapter setting, enter the appropriate fingerprint.

Use unencrypted data channel

This setting is inherited from the FTP adapter, which is visible on the **Proxy** tab of the Adapter Properties window. To override the adapter setting, check this box to use a clear data channel, or uncheck this box to encrypt the data over the data channel.

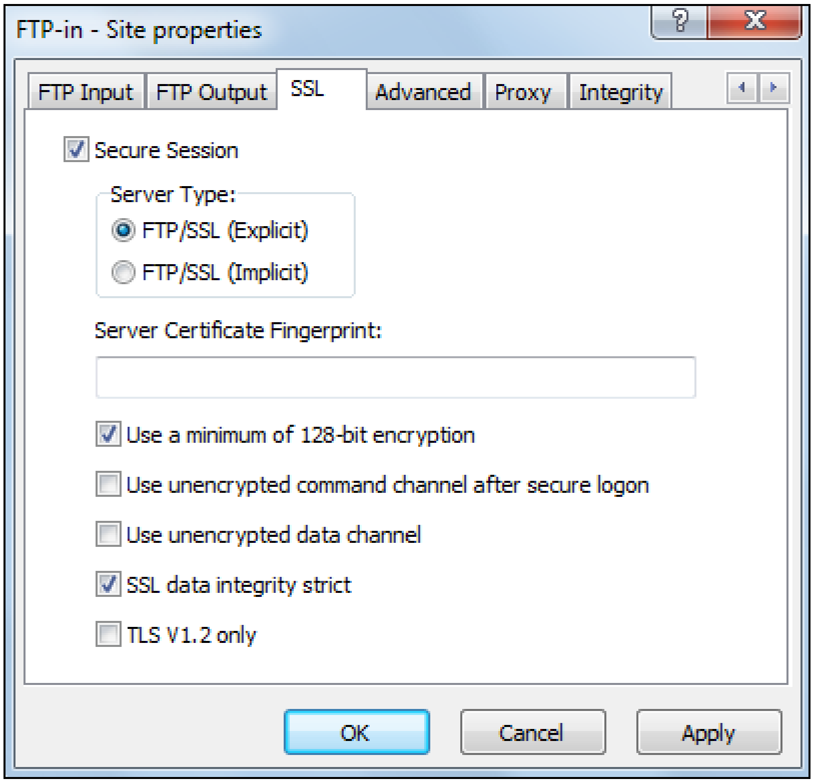
TLS V1.2 only

Check this box to force the use of the TLS V1.2 protocol for the connection to the Proxy. This setting is inherited from the FTP Adapter, which is visible on the Proxy tab of the Adapter Properties window. To override the adapter setting, check or clear this box.

(FTP Site Properties) SSL Page

For an FTP site, the **SSL** tab of the Site Properties window allows users to specify whether to use SSL/TLS security, and which type. It also specifies a fingerprint with which to identify the server. Once a secure connection is made, users may choose to use an unencrypted data channel.

IMPORTANT: Note that these parameters control the connection to an external FTP server. When the adapter connects to the MessageWay FTP Perimeter Server first, the parameters to connect the FTP adapter to an FTP perimeter server are controlled by values on the **Proxy** tab of the Site Properties window.



☑ Secure Session

Server Type:

● FTP/SSL (Explicit)

○ FTP/SSL (Implicit)

Server Certificate Fingerprint:

☑ Use a minimum of 128-bit encryption

□ Use unencrypted command channel after secure logon

□ Use unencrypted data channel

☑ SSL data integrity strict

□ TLS V1.2 only

SSL Page (Site Properties Window)

Secure Session

Check this box to enable the fields that allow you to specify the parameters for the TLS/SSL session.

IMPORTANT: Note that this parameter controls the connection to an external FTP server. The type of connection from the FTP adapter to an FTP perimeter server is controlled by the Secure Proxy value on the **Proxy** tab of the Site Properties window.

Server Type

This is the server type for the FTP adapter that connects to an external FTP server.

IMPORTANT: Note that this parameter controls the connection to an external FTP server. The type of connection from the FTP adapter to an FTP perimeter server is controlled by the Data Connection value on the **Proxy** tab of the Site Properties window.

Check the Secure option that precedes, and then select the type of secure connection for the server. When the Secure option is clear, the default is non-secure FTP.

FTP/SSL (Explicit)	The client connects to an unencrypted port on the server, typically 21. To connect to the MessageWay FTP perimeter server, we use 2190 to avoid conflict with other existing FTP servers. After starting a normal session, the client requests that SSL/TLS security be used, and when the appropriate handshake occurs, it sends the data.
FTP/SSL (Implicit)	The client connects to an encrypted port, typically 990, and after an appropriate SSL handshake, it sends FTP commands.

Server Certificate Fingerprint

To use a fingerprint instead of a full certificate to authenticate the FTP server, enter that fingerprint here. Leave this blank if you always want to authenticate the server with a full certificate.

IMPORTANT: Note that this parameter controls authentication of an external FTP server. The type of authentication of an FTP perimeter server is controlled by the corresponding value on the **Proxy** tab of the Site Properties window.

NOTE: You specify the location of the Certificate Authority certificate bundles or repository on the **FTP** page of the FTP Adapter Properties window.

Use a minimum of 128-bit encryption

Typically each SSL client and server has a list of ciphers, called a cipher suite list, that they will use. When the client first contacts the server, it also sends a list of ciphers it will use. A single cipher suite is a combination of an encryption protocol, the encryption key length and a hash algorithm that is used for integrity checking. The server compares its list with that of the client and usually chooses the strongest cipher that they both support.

Check this box to use a cipher suite list that only supports 128-bit or higher encryption. If the server to which the adapter connects does not support at least 128-bit encryption, the session terminates. When this box is clear, the cipher list allows all ciphers, including those below 128-bit.

Use unencrypted command channel after secure logon

For SSL communication, encryption can occur in the command channel (CC), the data channel (DC), or both. For SSL/implicit or SSL/explicit, users may check this box to not encrypt the command channel after a secure logon, that is, to use a clear command channel (CCC). This selection does not affect the data channel.

Use unencrypted data channel

For SSL communication, encryption can occur in the command channel (CC), the data channel (DC), or both. For SSL/implicit or SSL/explicit, users may check this box to not encrypt the data channel, that is, to use a clear data channel (CDC). This selection does not affect the command channel.

SSL data integrity strict

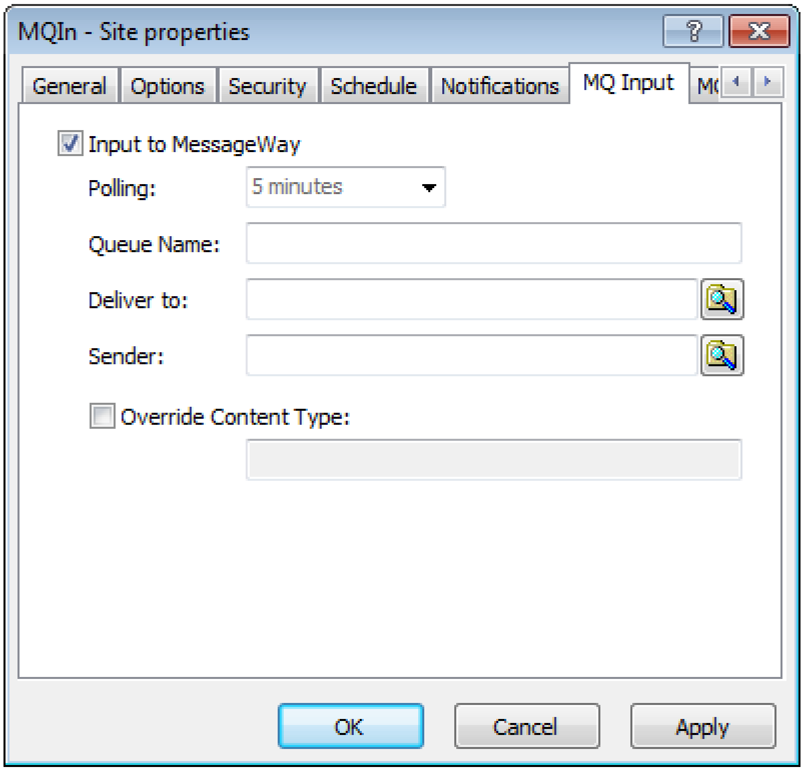
Clear this box to allow transfers to and from FTP servers that do not strictly follow the SSL shutdown protocol. Check this box to enforce strict SSL data integrity.

TLS V1.2 only

Check this box to force the use of the TLS V1.2 protocol for the connection to the external FTP server.

(MQ Site Properties) MQ Input Page

The **MQ Input** tab of the Site Properties window allows users to specify how to transfer messages from a WebSphere MQ server into MessageWay.


MQIn - Site properties

☑ Input to MessageWay

Polling: 5 minutes

Queue Name:

Deliver to:

Sender:

☐ Override Content Type:

NOTE: The MessageWay MQ Adapter requires a license from Progress. You must have a license in order to start the adapter. For more information, contact MessageWay Technical Support.

Input to MessageWay

Check this box to configure this site as an input location to collect messages from a WebSphere MQ server.

Polling

Select a different polling interval to override the default setting on the MWMQ adapter. The polling interval is used to transfer messages from a WebSphere MQ queue manager into MessageWay. Enter the number of seconds, minutes, or hours that the adapter will wait before checking a queue for files to transfer. Location schedules determine when the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

Select an interval from the list. The option **Never** stops all input for this adapter. The **Schedule** option requires that the schedule type be *Trigger (Input or Execute Now)*, which polls at the time specified. You identify the schedule on the **Schedule** tab, and from there you can drill down to create or edit a schedule item. Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds
30m	means 30 minutes
2 h	means 2 hours

Queue Name

Type the queue name from which to collect messages. This queue must be defined for the queue manager that is specified in the MQ adapter.

Deliver to

Specify the name of the MessageWay location where you want to deliver the messages.

Sender

Specify the name of the sender that will override the one determined by MessageWay.

Override Content Type check box

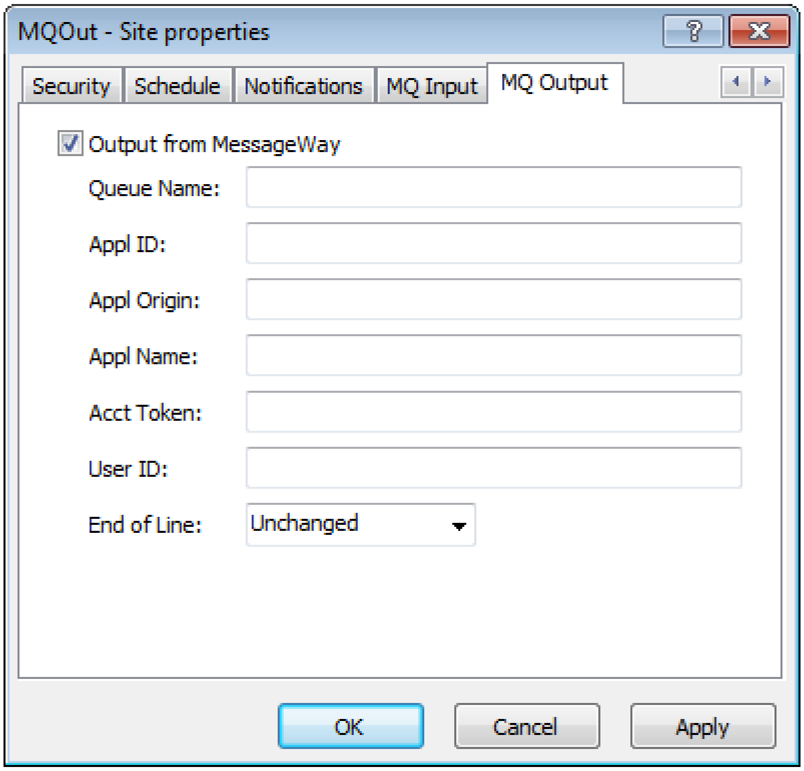
Check this box to override the content type as determined by MessageWay.

Override Content Type

Enter the content type. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.

(MQ Site Properties) MQ Output Page

The **MQ Output** tab of the Site Properties window allows users to specify how to transfer messages from MessageWay to a WebSphere MQ server.


MQOut - Site properties

☑ Output from MessageWay

Queue Name:

Appl ID:

Appl Origin:

Appl Name:

Acct Token:

User ID:

End of Line: Unchanged

NOTE: The MessageWay MQ Adapter requires a license from Progress. You must have a license in order to start the adapter. For more information, contact MessageWay Technical Support.

Output from MessageWay

Check this box to send messages from this site to a WebSphere MQ server.

Queue Name

Type a queue name where you want to send the messages. This queue must be defined for the queue manager that is specified in the MQ adapter.

Appl ID

The Appl ID field contains identity context data that typically refers to the application that originally put the message.

Appl Origin

The Appl Origin field contains identity context data that typically refers to the application that most recently put the message. This may differ from Appl ID, for example, if a message is forwarded from one application to another.

Appl Name

This is the name of the application that issued the API call to MQ to send (put) the data. This value defaults to *mway*.

Acct Token

The Acct Token field is part of the identify context of a message whose content may be used by an application.

User ID

The User ID contains the identity of a valid MQ user that MQ server uses to authenticate the client.

End of Line

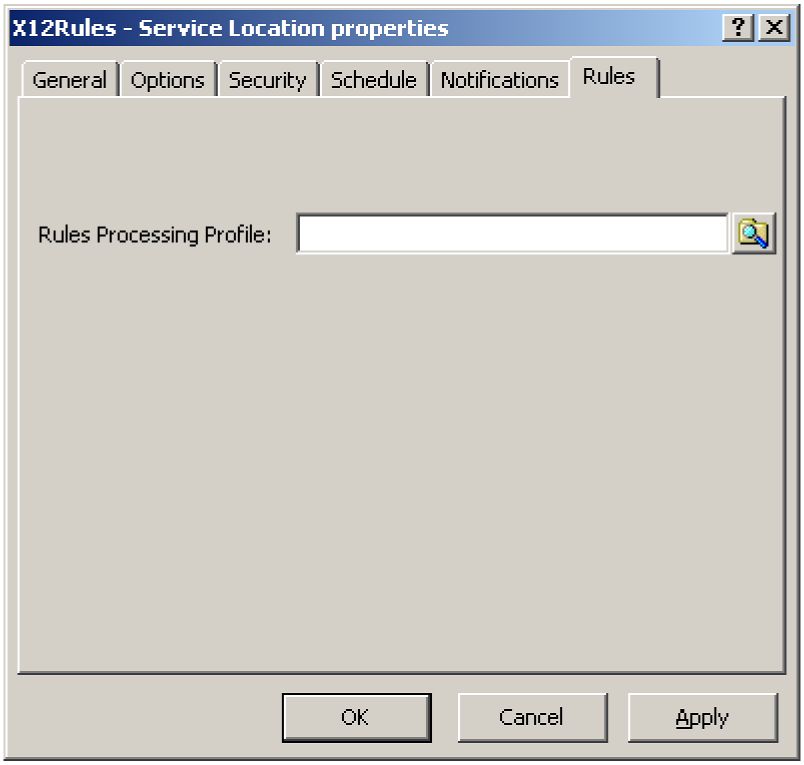
Many different systems change the end-of-line (EOL) character when transferring data. Where possible, MessageWay retains the carriage return/linefeed (CRLF) as the EOL character for text files, that is where the context type starts with text/. This may not always be possible, such as when a file is received as binary and later has its context type changed to text/. To change the character, select the appropriate value. The options are CRLF, NL and Unchanged.

The following table describes the end-of-line character options.

End-of-Line Character	Description
CRLF	Always use carriage-return/line-feed, which is the native EOL character combination for Windows operating systems.
NL	Always use newline, which is the native EOL character for UNIX/Linux operating systems
Unchanged	Do not change the EOL character.

(Rules Processing Service Location Properties) Rules Page

For a rules processing location, the **Rules** page of the Service Location Properties window allows users to specify a rules processing profile that contains the rules to route the inbound message.


X12Rules - Service Location properties
?
X
General
Options
Security
Schedule
Notifications
Rules
Rules Processing Profile:
OK
Cancel
Apply

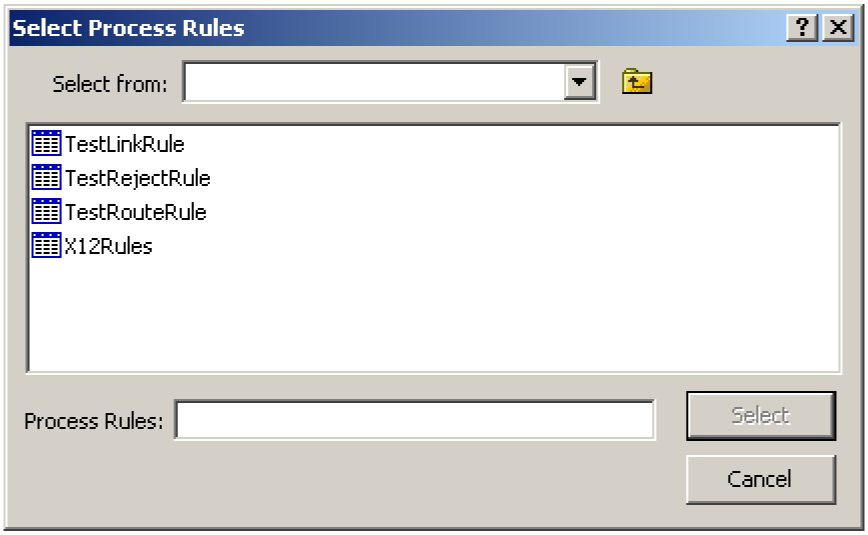
Rules Page (Service Location Properties Window)

Rules Processing Profile Name

Type a name of up to 64 characters for the rules processing profile, or select one using the **Browse** button.

Select Process Rule Dialog Box

The **Select Process Rule** dialog box appears when you select the **Browse** button from the **Rules** page of the Service Location Properties window.



Select From

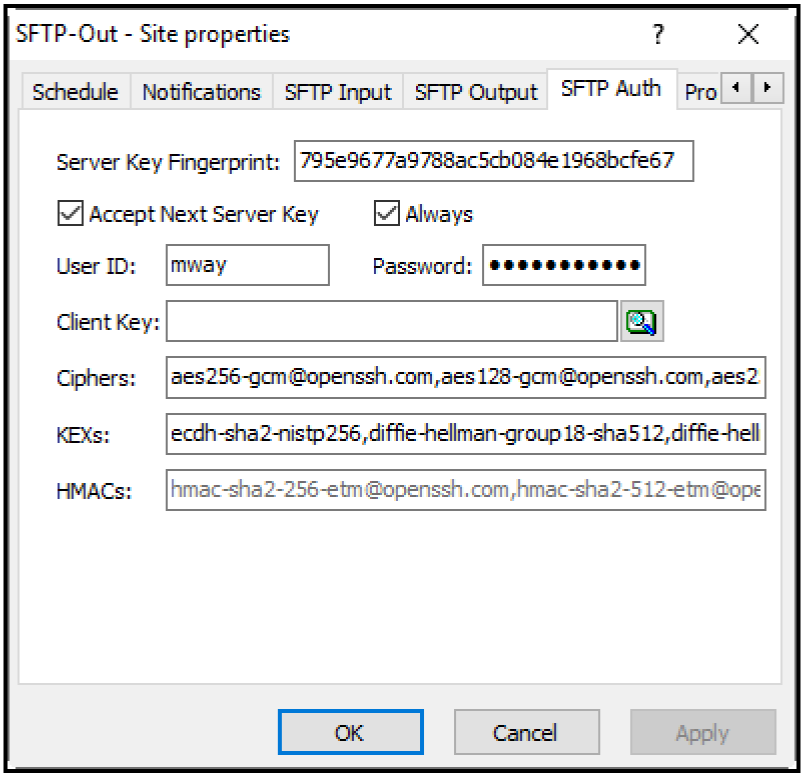
The **Select from** box allows you to specify the location of the rules profiles you want to display. Accept the main **Rules Processing** folder or select any subfolder. Click the down arrow to display subfolders. When you point to subfolders, you can then move up a level by clicking the folder icon to the right of the box.

List of Rules Processing Profiles and Folders

Click any rules profile to select it, which then appears in the **Process Rules** box. Double-click any folder to display the contents of the folder.

(SFTP Site Properties) SFTP Auth Page

The **SFTP Auth** page provides information to support the SSH authentication protocol layer for both input and output. This information includes a fingerprint to identify the SFTP server to the client, which is the SFTP adapter. SSH authentication of the client to the server may be done either with a user ID and password or a client key, which is part of a public key set, and is often called a public key. The SFTP server decides which authentication method it will use.



Server Key Fingerprint: 795e9677a9788ac5cb084e1968bcfe67

☑ Accept Next Server Key ☑ Always

User ID: mway Password: ●●●●●●●●●●●

Client Key:

Ciphers: aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes2

KEXs: ecdh-sha2-nistp256,diffie-hellman-group18-sha512,diffie-hell

HMACs: hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@ope

NOTE: The MessageWay SFTP Adapter is included as part of the license for the SFTP Proxy Server and the SFTP perimeter server, although you install and configure them separately. For more information, contact MessageWay Technical Support.

Server Key Fingerprint

Enter the fingerprint of the key that identifies the SFTP server, or leave the field blank and check the box, **Accept Next Server Key**. There must be a fingerprint value available to validate the SFTP server, whichever method you use, or the adapter will refuse to continue the session. When you check the box, the fingerprint will be replaced by the fingerprint provided during the next connection to the SFTP server. MessageWay uses this value to authenticate the server.

Accept Next Server Key

Check this box when you do not know the server key and you want to accept the connection from the server. The new key fingerprint supplied by the server appears in the **Server Key Fingerprint** box, and the check box is then cleared. There must be a fingerprint value available to validate the SFTP server, whether the SFTP server supplies it or you enter it, or the adapter will refuse to continue the session. So, you must check this box if the value in the **Server Key Fingerprint** field is blank. To accept a different server key, you must recheck this box.

Always Accept Next Server Key

Check this box when you want to ‘always’ accept a new server key from the remote server without operator intervention. The new key is used to update the **Server Key Fingerprint**. Note that checking 'Always' should only be done when it has been confirmed that the remote server regularly changes it’s key. Generally accepting a new server key can be considered a security risk.

User ID

Type the user ID that, together with either the password or the client key, will allow the SFTP server to authenticate the SFTP adapter client. This is a user defined on the SFTP server system.

Password

Type the password that, together with the user ID, will allow the SFTP server to authenticate the user, which is the MessageWay SFTP adapter client.

Client Key

Enter an SSH client key that the server will use for public key authentication. The client key is a more secure option than a password. The key must already be stored in the MessageWay database. Use the search button to the right of the field to select a pre-defined key.

Ciphers

When FIPS is not enabled, overrides the default list of ciphers that the Location will use to negotiate an SSH session with the remote SFTP server. In the SSH protocol, asymmetric ciphers are used to handle encrypt and decrypt functions. Each individual value is separated with a comma, the values are negotiated from left to right in order to determine a match and any invalid or misspelled values are ignored. These values override the ones for the SFTP Adapter, visible on the SFTP tab of the MWSFTP Adapter Properties window.

KEXs

Overrides the default list of Key Exchange algorithms that the Location will use to negotiate an SSH session with the remote SFTP server. KEX algorithms are used to exchange the keys (public and private) that will be used to encrypt and decrypt. Each individual value is separated with a comma, the values are negotiated from left to right in order to determine a match and any invalid or misspelled values are ignored. These values override the ones for the SFTP Adapter, visible on the SFTP tab of the MWSFTP Adapter Properties window.

HMACs

When FIPS is not enabled, overrides the default list of Hashed MAC functions that the Location will use to negotiate an SSH session with the remote SFTP server. HMACs are used to calculate the Message

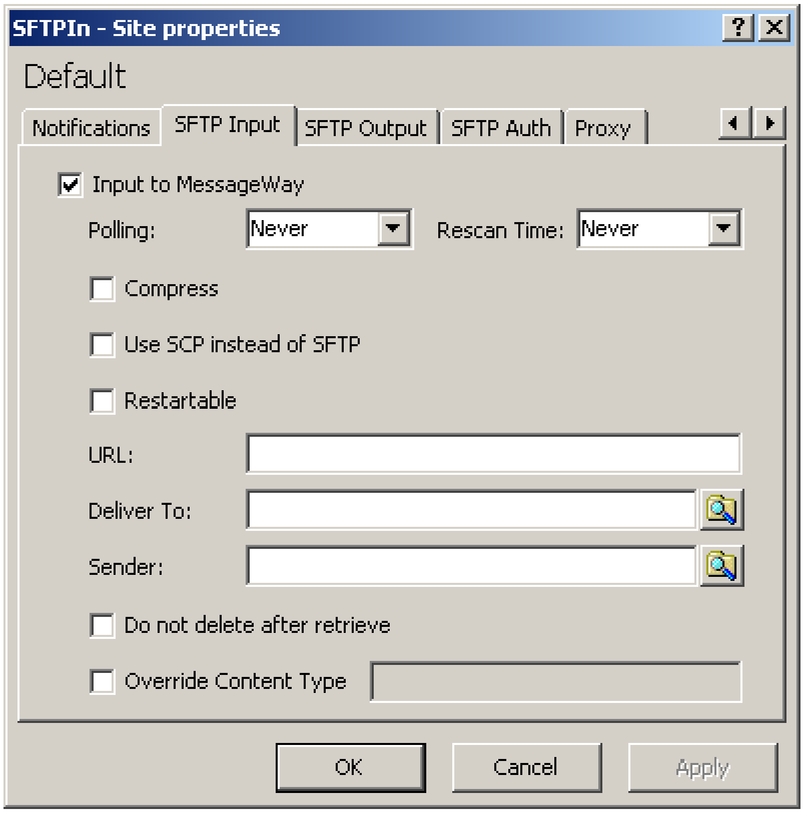
Authentication Code involving a function in combination with a secret key. In the SSH protocol, it is used to verify the integrity and authenticity of a message. Each individual value is separated with a comma, the values are negotiated from left to right in order to determine a match and any invalid or misspelled values are ignored. These values override the ones for the SFTP Adapter, visible on the SFTP tab of the MWSFTP Adapter Properties window.

(SFTP Site Properties) SFTP Input

The **SFTP Input** tab of the Site Properties window allows users to specify how to transfer messages from an SFTP external server into MessageWay. Transfers may be directly from the SFTP server or through the MessageWay SFTP Proxy server.

NOTE: All SFTP transfers are binary.

MessageWay does not support input file names that contain backslashes, \. For operating systems, such as UNIX/Linux, that allow backslashes in file names, the Filename property will be whatever follows the final backslash.



SFTPIn - Site properties

Default

☑ Input to MessageWay

Polling: Never

Rescan Time: Never

☐ Compress

☐ Use SCP instead of SFTP

☐ Restartable

URL:

Deliver To:

Sender:

☐ Do not delete after retrieve

☐ Override Content Type

NOTE: The MessageWay SFTP Adapter is included as part of the license for the SFTP Proxy Server and the SFTP perimeter server, although you install and configure them separately. For more information, contact MessageWay Technical Support.

Input to MessageWay

Check this box to allow the adapter associated with this site to transfer messages from the specified site into MessageWay. The SFTP adapter only polls for input messages when the schedule for the site is open.

Polling

This value overrides the polling value set for the SFTP adapter.

The polling interval is used to transfer of messages from an SFTP directory into MessageWay. This is the amount of time that the SFTP client will wait before checking the directory for files to transfer to the site. Location schedules determine whether the adapter polls for messages for individual locations. The schedule for a location must be open to allow polling.

The URL to be polled and the location to which the inbound files will be transferred are on the **SFTP Input** page of the Site Properties window under **Input to MessageWay**.

Select an interval from the list or enter the number of hours, minutes or seconds between polling cycles. The option **Never** stops polling for this adapter.   Polling is based on the hour of the system time after the adapter has started. For example, when the polling interval is set to every 15 minutes, the adapter will poll on the hour and at 15, 30 and 45 minutes past the hour. If the adapter starts at 2:10, the first polling cycle will be at 2:15.

The **Schedule** option requires that the schedule type be *Trigger (Input or Execute Now)*, which polls at the time specified. You identify the schedule on the **Schedule** tab, and from there you can drill down to create or edit a schedule item.

You may also enter a number followed by an optional unit of time: **s** for seconds, **m** for minutes, and **h** for hours. A space between the number and unit of time is optional. The default unit of time is seconds.

5 or 5s	means 5 seconds
30m	means 30 minutes
2 h	means 2 hours

Rescan Time

This is the interval in seconds that SFTP adapter waits before it rereads the properties of the input message. Set this interval for locations that receive large files to assure that MessageWay only inputs complete messages. The alternative to avoid having MessageWay input partial files is to write to a temporary directory, and then rename the file to the primary directory. When you use this feature, as the polling interval finds messages to bring into MessageWay, the adapter reads the properties returned from the LIST command. These properties may include message size and date/time stamps, as transferred by the SFTP input stream. Then it rescans the properties of the message at the rescan time until if finds that the properties have no longer changed. When it determines that the file is stable, it initiates the transfer of the file into MessageWay. Since this feature will input files only after at least three readings of the file properties, it will slow down input for smaller files as well. This setting only works when the polling interval is explicitly set to a value, and the *Input Now* command is disabled when a rescan time is specified. It is ignored when the polling interval is set to *Event Driven*, *Schedule* or *Never*. If the rescan time is greater than or equal to the polling time, the polling time will act as the rescan of the previous poll.

CAUTION: When rescan is set to a low number, such as 5 seconds, a remote server may not have enough time to update the file size before 2 consecutive rescans. In this case MessageWay will think the file is complete and input the file, which may result in an incomplete file transfer. Make sure that the rescan time is set high enough to allow remote servers to update the file statistics between scans. We recommend a higher interval, at least 60 seconds.

Compress

Check this box to enable SSH data stream compression during upload transmission between the server and the adapter client. This is typically most beneficial on slow links and for large text files, but less so for faster links or binary files.

Use SCP Instead of SFTP

Check this box to use SCP transfer protocol instead of SFTP. This is only supported by SSH servers running on UNIX/Linux servers. SCP is not compatible with the *Restartable* option, which would attempt a check-point restart. Recovery from input failures when you do not use restart depends on the error actions specified on the **Options** tab, which attempts to receive from the beginning.

Restartable

Check this box to allow the external SFTP server to restart from a check-point, rather than resend the entire file when an error occurs during transmission. Restart occurs at the next polling interval, so you must also configure a polling interval. The external SFTP server must support check-point restart, either as streaming or block mode. Restart preempts configurations for retries, which attempt to receive the file from the beginning. Retry strategies are configured on the **Options** tab under **Error Action**. When the SFTP server does not support check-point restart, MessageWay will ask the server to resend the file from the beginning, if retries are configured for this site. You may not use the Restartable option with SCP protocol transfers.

URL

Enter a valid location in the form of a URL that the adapter will scan for messages to transfer into MessageWay. Do not use mapped drive letters to access network resources. Use full Universal Naming Convention (UNC) names instead. The type of connection is determined by the check box, *Use SCP instead of SFTP*, so the protocol prefix, sftp or scp, is accepted but ignored.

The URL uses the following syntax:

- For SFTP Output: [*protocol prefix*] *host* [*/location*]
- For SFTP Input: [*protocol prefix*] *host* [*/location*]

  - or -

  [*protocol prefix*] *host* [**/**location**/**filemask]

Component	Requirement	Description
Protocol prefix	optional	**sftp://** or **scp://** ▪ Either is accepted and ignored; the actual choice of protocol is made via the *Use SCP instead of SFTP* check box. ▪ You may also omit the protocol prefix.
Host	required	(*hostname* **|** *IP address*) [**:***port number*] ▪ *Hostname* is standard internet domain name ▪ *IP address* is four decimal values separated by periods ▪ When *port number* is not used, defaults to 22
Location	optional	A path to the directory or file. ▪ Locations starting with // are absolute. ▪ Locations starting with only / are relative to the user's home directory.
Filemask	optional	(SFTP Input only) You can construct file names to pull one or more files from a directory as follows: ▪ A static file name with all literal characters, for example, sftp://100.100.1.100:2020/dir/abc.txt ▪ A dynamic file name with wild cards, for example, sftp://100.100.1.100:2020/dir/abc*

Here are some examples of valid URLs:

Description	Example
Basic	sftp://www.sftpserver.com//home/user1/dir scp://100.100.1.100:2222/dir
Basic, shortened	www.sftpserver.com//home/user1/dir 100.100.1.100:2222/dir

Deliver To

Type or select a location to which the adapter associated with this site will transfer the messages. This may be a site for auto-delivery, a service location, such as MWTranslator, or a pickup mailbox. When the location does not exist, the message is sent to the system mailbox, {Unknown}.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

Sender

Select or type a location to represent the sender of the message. This overrides the sender that may or may not have been passed by the SFTP server. This feature is useful for testing, where the input site is already defined, but currently inaccessible, such as at a customer site whose connection is unavailable. You can use a test location that has a different name, but when you put the name of the original customer location here, the message will be marked as if it were from the customer location.

Do Not Delete After Retrieve

Check this box to leave the input file on the source SFTP site after successful retrieval. When a file has been retrieved from a non-MessageWay SFTP site into MessageWay, the default behavior is to delete the file from the source SFTP site.

When you connect to a MessageWay SFTP Perimeter Server to send messages from this MessageWay system into another MessageWay system, you must check this box, because MessageWay does not allow messages to be deleted by a client. Messages are conditionally archived and then deleted when the archive program runs.

Override Content Type Check Box

Check this box to override the content type specified for the input message.

Override Content Type

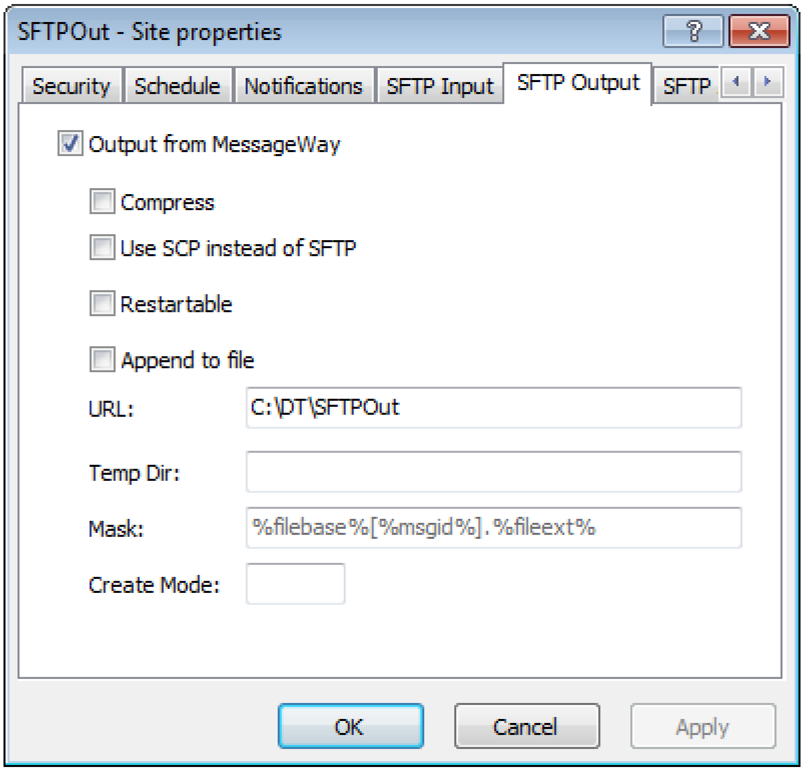
The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.

The following table shows the content types that MessageWay supports.

Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

(SFTP Site Properties) SFTP Output Page

For an SFTP output site, the **SFTP Output** tab of the Site Properties window allows users to specify how to transfer messages from MessageWay to an external SFTP server. The transfer may be directly to an SFTP server or through the MessageWay SFTP Proxy Server.



☑ Output from MessageWay

□ Compress

□ Use SCP instead of SFTP

□ Restartable

□ Append to file

URL: C:\DT\SFTPOut

Temp Dir:

Mask: %filebase%[%msgid%].%fileext%

Create Mode:

NOTE: The MessageWay SFTP Adapter is included as part of the license for the SFTP Proxy Server and the SFTP perimeter server, although you install and configure them separately. For more information, contact MessageWay Technical Support.

Output from MessageWay

Check this box to allow the adapter associated with this location to transfer messages from MessageWay. The SFTP adapter will deliver messages only when the schedule for this site is open.

Compress

Check this box to enable SSH data stream compression during download transmissions between the client and the server. This is typically most beneficial on slow links and for large text files, but less so for faster links or binary files.

Use SCP instead of SFTP

Check this box to use SCP transfer protocol instead of SFTP. This is only valid for SFTP running on UNIX/Linux servers. SCP may use multiple threads to transmit multiple files. SCP is not compatible with the *Restartable* or *Append to file* options. When you do not use restart, recovery from output failures depends on the error actions specified on the **Options** tab, which attempts to send from the beginning.

Restartable

Check this box to allow MessageWay to restart from a check-point, rather than resend the entire file when an error occurs during transmission. Restart occurs based on the next configured retry interval, so you must also configure retries. Retry strategies are configured on the **Options** tab under **Error Action**. The external SFTP server must support check-point restart, either as streaming or block mode. Restart preempts configurations for retries, which attempt to resend the file from the beginning. When the SFTP server does not support check-point restart, MessageWay will ask the server to resend the file from the beginning, if retries are configured for this site. You may not use the *Restartable* option with SCP protocol transfers.

Append to file

Check this box to append the contents of the message to a file of the same name. When this box is not checked, existing files will be replaced with the newer version. The *Append to file* option is incompatible with SCP.

URL

Type a valid location in the form of a URL that the adapter will use to transfer a message from MessageWay. Do not use mapped drive letters to access network resources. Use full Universal Naming Convention (UNC) names instead. The type of connection is determined by the check box, *Use SCP instead of SFTP*, so the protocol prefix, sftp or scp, is accepted but ignored.

The URL uses the following syntax:

▪ For SFTP Output:	[*protocol prefix*] *host* [*/location*]
▪ For SFTP Input:	[*protocol prefix*] *host* [*/location*] - or - [*protocol prefix*] *host* [/location/filemask]

Component	Requirement	Description
Protocol prefix	optional	**sftp:**// or **scp:**// ▪ Either is accepted and ignored; the actual choice of protocol is made via the *Use SCP instead of SFTP* check box. ▪ You may also omit the protocol prefix.
Host	required	(*hostname* **|** *IP address*) [**:***port number*] ▪ *Hostname* is standard internet domain name ▪ *IP address* is four decimal values separated by periods ▪ When *port number* is not used, defaults to 22
Location	optional	A path to the directory or file. ▪ Locations starting with // are absolute. ▪ Locations starting with only / are relative to the user's home directory.
Filemask	optional	(SFTP Input only) You can construct file names to pull one or more files from a directory as follows: ▪ A static file name with all literal characters, for example, sftp://100.100.1.100:2020/dir/abc.txt ▪ A dynamic file name with wild cards, for example, sftp://100.100.1.100:2020/dir/abc*

Here are some examples of valid URLs:

Description	Example
Basic	sftp://www.sftpserver.com//home/user1/dir scp://100.100.1.100:2222/dir
Basic, shortened	www.sftpserver.com//home/user1/dir 100.100.1.100:2222/dir

Temp Dir

Type a valid temporary directory for the URL on the remote system to deposit a message from MessageWay. This directory will be added to the URL. The directory name may also be prefixed with the same protocol prefix, host, and directory as the output URL. When using the full directory path, it must match the directory path in the URL exactly. The temporary directory must exist within the URL location. When the file completes sending, MessageWay renames it to the permanent directory. This avoids programs reading a file before it has been completely transferred. The temporary directory is ignored when you check *Append to file*.

If the output SFTP site does not allow you to create temporary directories, leave this value blank. In this case, you can specify a temporary file name mask and a permanent file name mask in the Mask field. The file will be written to the permanent directory using the temporary file name mask and then will be renamed using the permanent file name mask. For more information, refer to the Mask field.

Mask

You may specify tokens to create a permanent file name and a temporary file name. The mask for the permanent file name is separated from the mask for the optional temporary file name with a forward slash: *permanent file name mask/temporary file name mask*. When only one mask is configured, the file name is the same for both the temporary and permanent file names. If a temporary directory is used, the file is written to the temporary directory using the temporary file mask and renamed to the permanent directory using the permanent file mask. If a temporary directory is not used, the file is written to the permanent directory using the temporary file mask and then renamed using the permanent file mask.

Use any combination of constants and MessageWay tokens. This value overrides the one for the SFTP Adapter, mwsftp, visible on the **SFTP** page of the SFTP Adapter Properties window. For new installations, the default mask is **%filebase%<[msgid]>.%fileext%**. For upgrades from previous versions of MessageWay, the default mask is the same as **%filename%**. To avoid delivery errors because of duplicate file names, make sure you use a default mask here that will assure a unique file name, for example, **MW%msgid%.txt**. If you use both permanent and temporary masks, your entry might look as follows: **CO1%yyyymmddhhnnss#%/CO1temp%yyyymmddhhnnss#%**.

CAUTION: When users have a program that scans for files to pick up after they appear in the target directory, and when you do not use a temporary directory, make sure the program scans for files by name rather than scan a directory. Otherwise, it may read the temporary file before it is renamed, which will likely be a partial file.

Use two percent (%) signs to enclose the tokens. MessageWay replaces the tokens with appropriate values. Add constants outside of these signs as required.

To append data to an existing file, check **Append to file**.

CAUTION: Do not specify both a temporary mask and check the box, **Append to file**, because the new file will be appended to the temporary file and then renamed to the permanent file. If you want to use the append option, only specify a permanent mask.

The valid tokens are:

Token	Description
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.

Token	Description
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: **MyClassID@MyLocationName** To assign a class ID to a mask for a file name, type: **MyClassID%yyyymmdd%.txt**
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).
inputmsgid	Input Message Id of the message.
inputname	Input Name.
location	The MessageWay location where the message resides. Replaces *mailbox*.
msgid	The Message Id of the message. Replaces *msg*.

Token	Description
ms	Milliseconds (000-999). **NOTE:** The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.
yyyy	Four digit year.
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

```
MW%msgid%.txt
```

```
TR%yyyymmddhhnnss#%.txt
```

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

```
%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml
```

TIP: On systems that allow file names longer than 8 characters, use the *msgid* token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the *filename* token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  `\ / : * ? " < > | ! & ` ' ;`

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

- Duplicate Filename values are allowed within the same location within the Locations folder.

Duplicate Filenames are not allowed within the same location within the File System folder, unless one has been canceled.

Create Mode

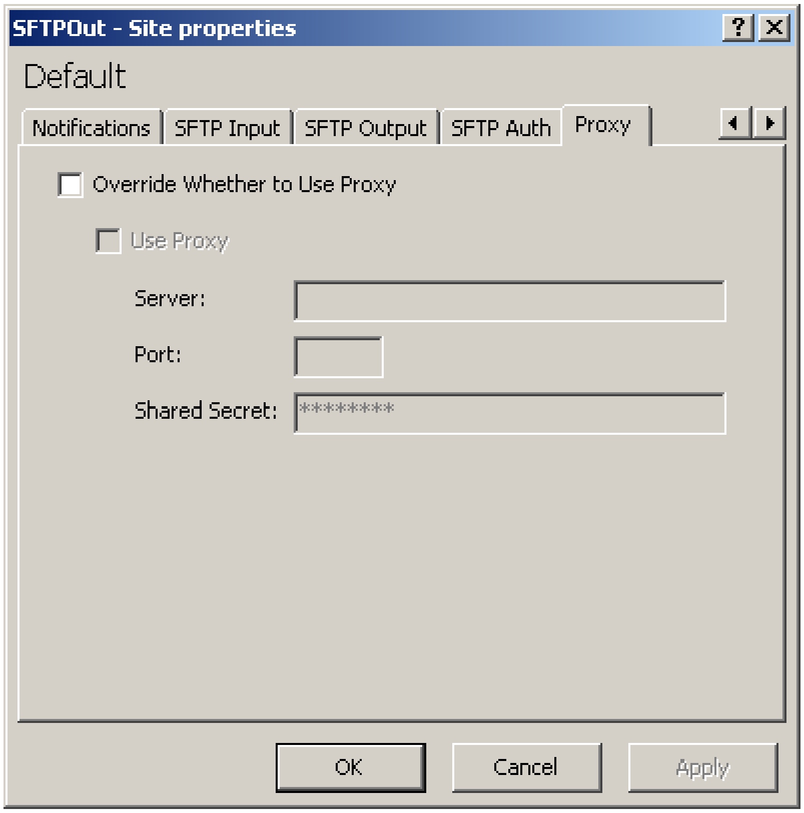
Type a 3-digit numeric value to set the default file permissions when MessageWay creates a file. The default value is **640**. This value overrides the default settings for the SFTP adapter.

Each digit may be from 0 to 7, representing permissions, from left to right, for owner/user, group, and all other users. To set the rights for each entity, add the total of the values assigned to each right, where, 4 = read (r), 2 = write (w), 1 = execute (x) and 0 = none (-). For example, 644 would give read and write (4+2=6) permissions to the owner/user, for example *mway*, and 4 would give read permissions to the group and others.

CAUTION: You may not be able to set the permissions for files on remote systems from the MessageWay SFTP adapter, based on the remote server/system settings for umask. The setting is controlled differently depending on whether you use SFTP or SCP to transfer the files. You should contact the administrator for the remote SFTP server for further information and help.

(SFTP Site Properties) Proxy Page

By default, the SFTP adapter communicates directly with an SFTP server. To communicate with an SFTP server through the MessageWay SFTP Proxy Server instead, you must provide information on the **Proxy** tab. The **Proxy** page allows you to configure the connection between the adapter and the proxy server. The proxy server makes the secure connection with the external SFTP server and then serves as a passthru for the adapter.



□ Override Whether to Use Proxy

□ Use Proxy

Server:

Port:

Shared Secret: *********

NOTE: The MessageWay SFTP Adapter is included as part of the license for the SFTP Proxy Server and the SFTP perimeter server, although you install and configure them separately. For more information, contact MessageWay Technical Support.

Override Whether to Use Proxy

Check this box if you want to override the settings for a proxy server on the SFTP Adapter Properties window.

Use Proxy

Check this box to allow the SFTP adapter to communicate through the MessageWay SFTP Proxy Server, rather than directly with an external SFTP server. Clear this box to communicate directly with an external SFTP server.

Server

Type the URL for the MessageWay SFTP Proxy Server.

Port

Type the port number on which the proxy server listens.

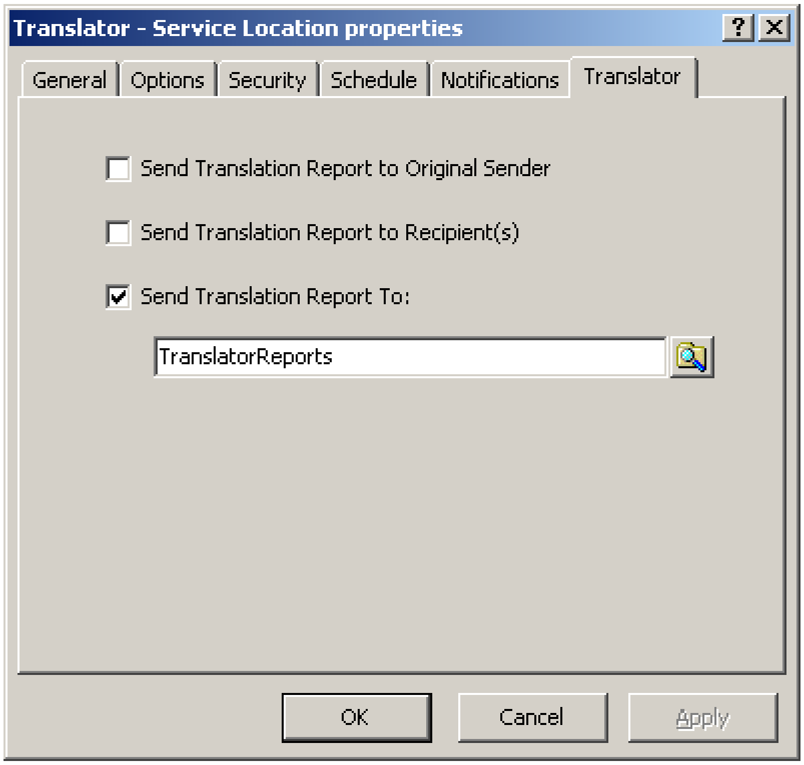
Shared Secret

The SFTP adapter and proxy server authenticate each other with a shared secret key. Type a random ASCII string for the shared secret key here. This value must also be stored in the proxy configuration file, mwproxy.conf.

(Translator Service Location Properties) Translator Page

The **Translator** page of the Service Location Properties window allows users to specify where to send the processing report, also called a translation report. This page appears only for a MWTranslator service location. Users can send a report to any of three locations: to the original sender, to the recipient(s) of the output, and to a specified location.

IMPORTANT: When you do not select a location to send the report, the report is discarded.



□ Send Translation Report to Original Sender

□ Send Translation Report to Recipient(s)

☑ Send Translation Report To:

TranslatorReports

Translator Page (Service Location Properties Window)

Send Translation Report to Original Sender

Select this option to send the processing report to the original sending location or address. This original sender is determined by MessageWay. This is not the original sender as determined by MWTranslator, for example to return acknowledgments.

Send Translation Report to Recipient(s)

Select this option to send the processing report to the recipient(s) of the output created during processing.

Send Translation Report To Check Box

Select this option to send the processing report to the specified address, which may be any valid address type.

Send Translation Report To

Type or select the location name to which the processing report(s) will be sent. When the location does not exist, the report is sent to the {Unknown} system mailbox.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

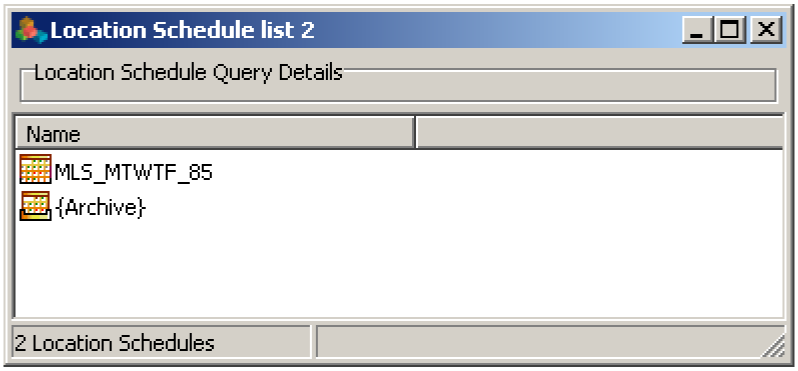
To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

Location Schedule List Window

The Location Schedule List window appears when you use the **Find Location Schedules** command to search for master location schedules and specific location schedules. When you search through multi-system environments, a System Name column also appears.

To sort by column content, click the column heading. For more information, refer to the topics, ***Master Location Schedules*** (on page 1222) and ***Schedule Page (Location Properties)*** (on page 1059).



Name	
MLS_MTWTF_85	
{Archive}	

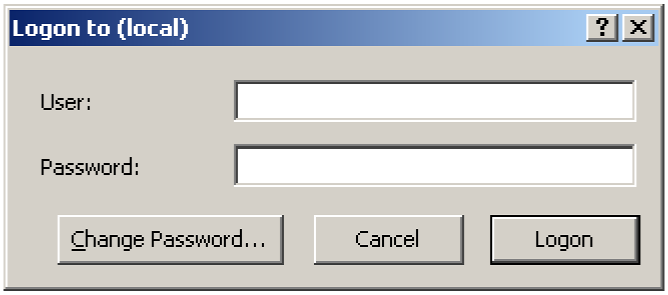
2 Location Schedules

Logon to MessageWay Environment Window

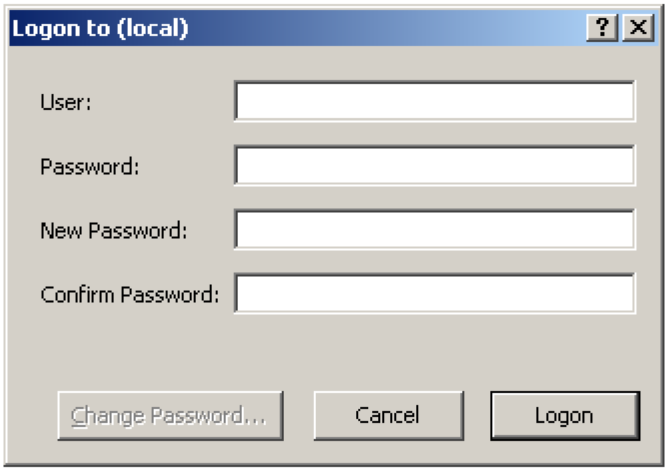
The Logon to *MessageWay environment* window allows users access to a specific database environment through the MessageWay Manager. This window appears after you have started the MessageWay Server. This window also appears when you click the **Logon** button from the toolbar. Use this window to log on as a different user and to change passwords. Click the **Change Password** button to change your password as you log on.

To access the Logon to MessageWay window, select the **Logon** button 🔑 from the toolbar.

There are two versions of the window. One allows you to log on and the other allows you to log on and change your password.



Logon to MessageWay Environment Window



Logon to MessageWay Environment Window with Password Change Option

User

Type a valid user ID.

Password

Type your current password. Contact your MessageWay administrator for the minimum length and other restrictions.

New Password

Type a new password that is different from the current or any previous passwords on your password history list. Contact your MessageWay administrator for the password history depth. Various password options appear on the **Password** tab of the User Policies window.

Confirm Password

Re-enter your password to make sure you did not make an error.

Change Password Button

Click this button to display a window that allows you to change your password.

Cancel Button

Click this button to exit the window without any action.

Logon Button

Click this button to log on to MessageWay.

Message Window

The Message window displays the text of the message. To view the text of a message, right-click the message in a message list, and select **View** from the pop-up menu.

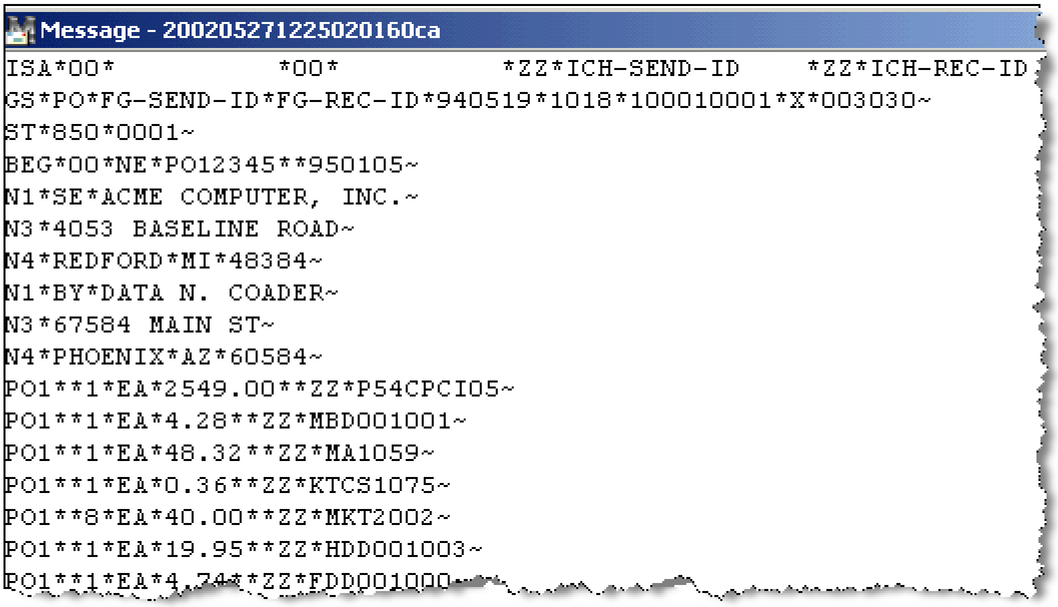
NOTE: Unicode characters will be displayed as non-printable characters and replaced with periods.

When the Message window appears, additional menu options are available to search for values in the data. Under the **Search** menu, users may select **Find** and **Search Again** commands. They can also select the **Find** button, 🔍 , and the **Search Again** button, 🔍 , from the toolbar.

NOTE: It may take some time for messages whose contents are larger than 20 MB to display when you switch between views.

Under the **View** menu, users may select the method of viewing the data, or they may choose the corresponding buttons from the toolbar.

- To display the data using carriage-return/linefeed characters (CR/LF) for line breaks, select **Text** . This is useful when there are CR/LF characters in the data.

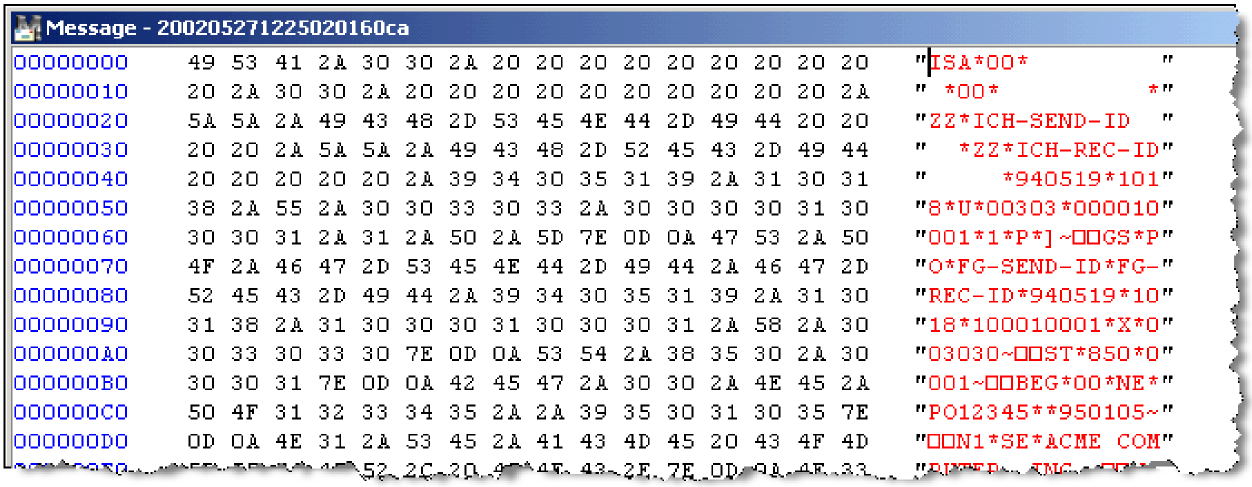


Message - 200205271225020160ca

```
ISA*00*          *00*          *ZZ*ICH-SEND-ID     *ZZ*ICH-REC-ID
GS*PO*FG-SEND-ID*FG-REC-ID*940519*1018*100010001*X*003030~
ST*850*0001~
BEG*00*NE*PO12345**950105~
N1*SE*ACME COMPUTER, INC.~
N3*4053 BASELINE ROAD~
N4*REDFORD*MI*48384~
N1*BY*DATA N. COADER~
N3*67584 MAIN ST~
N4*PHOENIX*AZ*60584~
PO1**1*EA*2549.00**ZZ*P54CPCI05~
PO1**1*EA*4.28**ZZ*MBD001001~
PO1**1*EA*48.32**ZZ*MA1059~
PO1**1*EA*0.36**ZZ*KTCS1075~
PO1**8*EA*40.00**ZZ*MKT2002~
PO1**1*EA*19.95**ZZ*HDD001003~
PO1**1*EA*4.74**ZZ*FDD001000~
```

Text Format (Message Window)

- To display the data as hexadecimal and ASCII characters, select **Hex** .

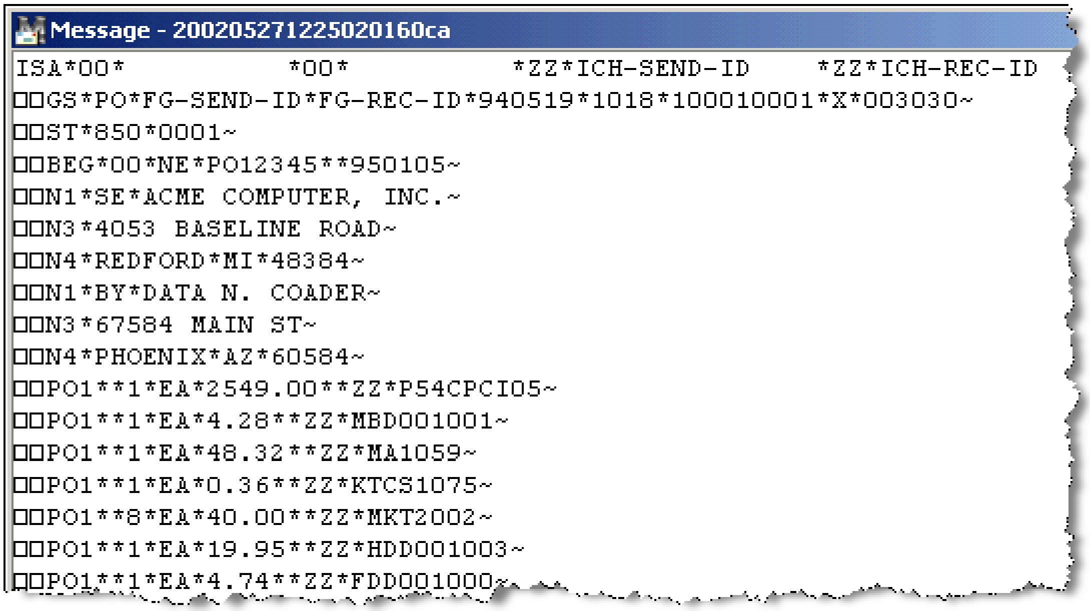


Message - 200205271225020160ca

```
00000000    49 53 41 2A 30 30 2A 20 20 20 20 20 20 20 20 20    "ISA*00*         "
00000010    20 2A 30 30 2A 20 20 20 20 20 20 20 20 20 20 2A    " *00*          *"
00000020    5A 5A 2A 49 43 48 2D 53 45 4E 44 2D 49 44 20 20    "ZZ*ICH-SEND-ID  "
00000030    20 20 2A 5A 5A 2A 49 43 48 2D 52 45 43 2D 49 44    "  *ZZ*ICH-REC-ID"
00000040    20 20 20 20 20 2A 39 34 30 35 31 39 2A 31 30 31    "     *940519*101"
00000050    38 2A 55 2A 30 30 33 30 33 2A 30 30 30 30 31 30    "8*U*00303*000010"
00000060    30 30 31 2A 31 2A 50 2A 5D 7E 0D 0A 47 53 2A 50    "001*1*P*]~□□GS*P"
00000070    4F 2A 46 47 2D 53 45 4E 44 2D 49 44 2A 46 47 2D    "O*FG-SEND-ID*FG-"
00000080    52 45 43 2D 49 44 2A 39 34 30 35 31 39 2A 31 30    "REC-ID*940519*10"
00000090    31 38 2A 31 30 30 30 31 30 30 30 31 2A 58 2A 30    "18*100010001*X*0"
000000A0    30 33 30 33 30 7E 0D 0A 53 54 2A 38 35 30 2A 30    "03030~□□ST*850*0"
000000B0    30 30 31 7E 0D 0A 42 45 47 2A 30 30 2A 4E 45 2A    "001~□□BEG*00*NE*"
000000C0    50 4F 31 32 33 34 35 2A 2A 39 35 30 31 30 35 7E    "PO12345**950105~"
000000D0    0D 0A 4E 31 2A 53 45 2A 41 43 4D 45 20 43 4F 4D    "□□N1*SE*ACME COM"
```

Hex Format (Message Window)

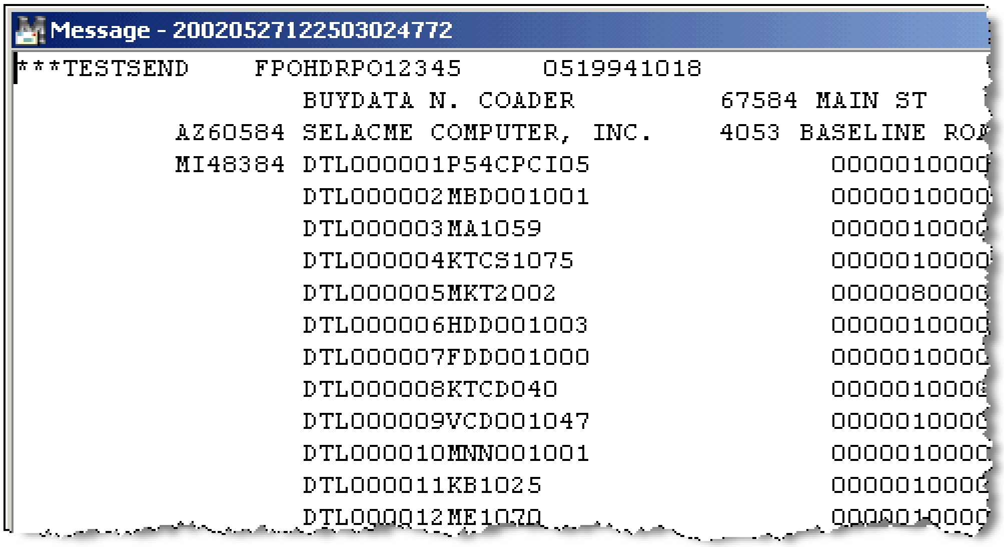
- To display the data using segment terminators and release characters to determine line breaks, select **EDI** EDI※. This is useful for delimited data, such as EDI data.



```
ISA*00*          *00*          *ZZ*ICH-SEND-ID    *ZZ*ICH-REC-ID
□□GS*PO*FG-SEND-ID*FG-REC-ID*940519*1018*100010001*X*003030~
□□ST*850*0001~
□□BEG*00*NE*PO12345**950105~
□□N1*SE*ACME COMPUTER, INC.~
□□N3*4053 BASELINE ROAD~
□□N4*REDFORD*MI*48384~
□□N1*BY*DATA N. COADER~
□□N3*67584 MAIN ST~
□□N4*PHOENIX*AZ*60584~
□□PO1**1*EA*2549.00**ZZ*P54CPCI05~
□□PO1**1*EA*4.28**ZZ*MBD001001~
□□PO1**1*EA*48.32**ZZ*MA1059~
□□PO1**1*EA*0.36**ZZ*KTCS1075~
□□PO1**8*EA*40.00**ZZ*MKT2002~
□□PO1**1*EA*19.95**ZZ*HDD001003~
□□PO1**1*EA*4.74**ZZ*FDD001000~
```

EDI Format (Message Window)

- To display the data using column width to determine line breaks, select **Fixed** ≣. This is useful for data whose records or lines are the same length.



```
***TESTSEND    FPOHDRPO12345     0519941018
                  BUYDATA N. COADER         67584 MAIN ST
          AZ260584 SELACME COMPUTER, INC.    4053 BASELINE ROA
          MI48384 DTL000001P54CPCI05               0000010000
                  DTL000002MBD001001               0000010000
                  DTL000003MA1059                  0000010000
                  DTL000004KTCS1075                0000010000
                  DTL000005MKT2002                 0000080000
                  DTL000006HDD001003               0000010000
                  DTL000007FDD001000               0000010000
                  DTL000008KTCD040                 0000010000
                  DTL000009VCD001047               0000010000
                  DTL000010MNN001001               0000010000
                  DTL000011KB1025                  0000010000
                  DTL000012ME1070                  0000010000
```

Fixed Format (Message Window)

Message List Window

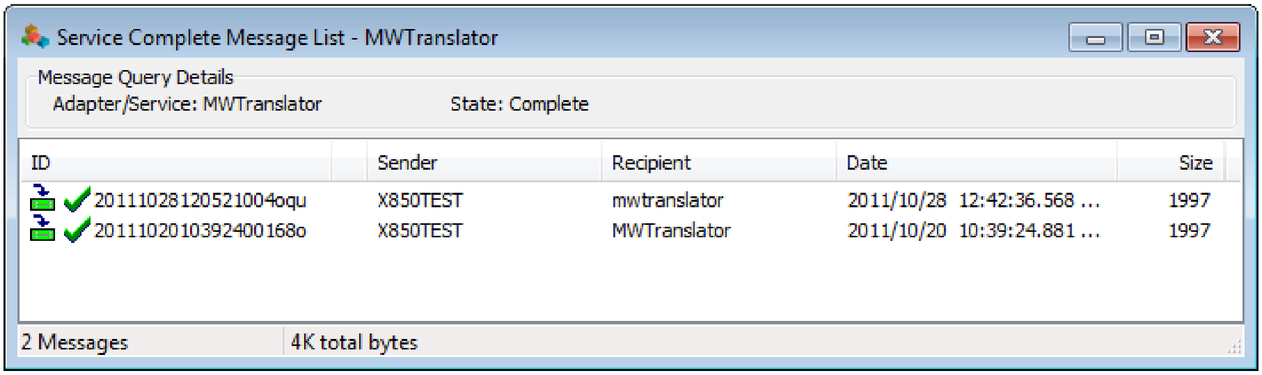
The Message List windows allow users to see pertinent data for selected messages using certain criteria. How you choose to display messages determines the full title of the Message List window. For example, when you select **Show Messages** for a location, the window title is "Location Message List." When you double-click a count in the **Complete** column of the System Monitor for adapters, the title of the window will be "Adapter Complete Message List." This helps you identify the type of messages displayed in a window.

To choose the type of information to display in the Message List window, refer to the topic, ***Displaying More Properties in Message List Window*** (on page 754).

You can display message lists using the following methods:

- To list messages for an adapters/services category, double-click one of the counts in the System Monitor or in the Adapters/Services monitors of MessageWay Explorer.
- To list messages, whose contents reside in the Message Store directory, right click any output, I/O, pickup or processing location in MessageWay Explorer, and select **Show Messages** from the pop-up menu.
- To find specific messages, use the Find Messages window and specify criteria for a search.
- To find all messages related to a MessageWay process, such as the translator, right click a message in a Message List window and select **Get Related Messages** from the pop-up menu.
- To find all messages linked because they share the same content, right-click a message in a Message List window and select **Get Linked Messages** from the pop-up menu.
- To find all messages that depend on the selected location, right-click a message in the Message List window and select **Show Dependent Messages**. This is similar to *Show Messages* but also includes messages that were created in the location but were later redirected to a different location. Use this command to find all messages that must be deleted in order to delete the location.

The Message Query Details area contains the selection criteria for the query that resulted in the list of messages.


Service Complete Message List - MWTranslator

Message Query Details

Adapter/Service: MWTranslator State: Complete

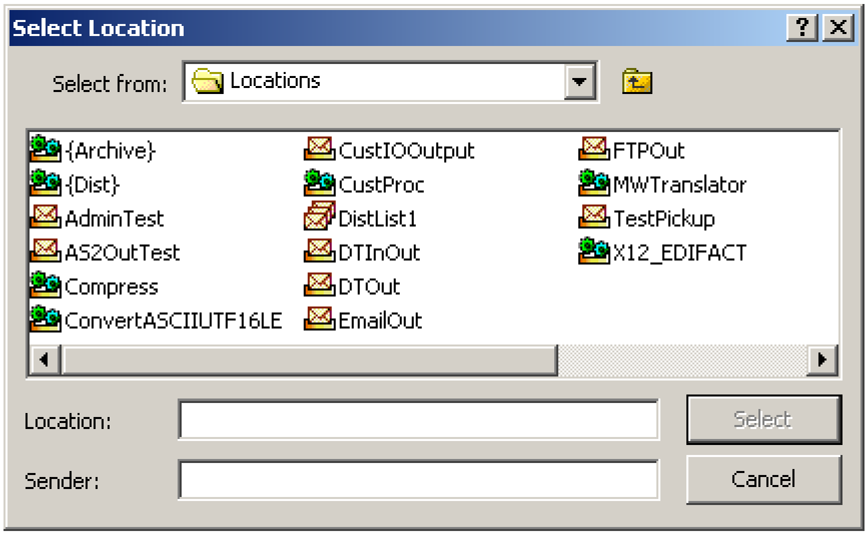
ID	Sender	Recipient	Date	Size
✓ 20111028120521004oqu	X850TEST	mwtranslator	2011/10/28 12:42:36.568 ...	1997
✓ 2011102010392400168o	X850TEST	MWTranslator	2011/10/20 10:39:24.881 ...	1997

2 Messages 4K total bytes

Service Complete Message List Window

Select Location Dialog Box for Redirect

The **Select Location** dialog box appears when you issue a **Redirect** command for a message.



Select From

The **Select from** box allows you to specify the folder that contains the destination locations you want to display. Accept the main **Locations** folder, or click the down arrow to display subfolders. To move up a level, click the folder button to the right of the box.

List of Locations and Folders

Select one or more destination locations. Double-click any folder to display the contents of the folder.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

Location Name

The Location list shows the destination locations you have typed or selected from the list. When you type a name of a location that does not exist, the message is delivered to the system mailbox, {Unknown}.

Broadcast locations, where the message is sent to all locations on the list at once, must be separated by commas. Piped locations, where the message travels sequentially from service to service and where the output of one becomes input to the next, must be separated by colons.

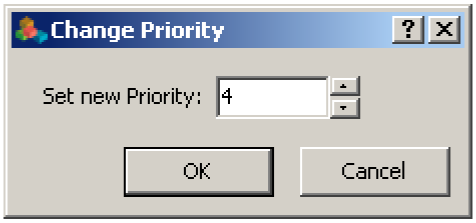
CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

Sender

The **Sender** box allows users to specify a different location as the original sender. This sender does not have to be a valid location. To use the original sender, leave this box blank.

Change Priority Dialog Box

The **Change Priority** dialog box appears when you select **Change Priority** from the pop-up menu in the Message List window.


Change Priority

Set new Priority: 4

Type or select a priority from 1 (lowest) to 5 (highest). This is the default priority assigned to output messages for delivery. Output messages sent to a service location typically have the same priority as the input message. One exception is a rules processing service, where you can override the priority.

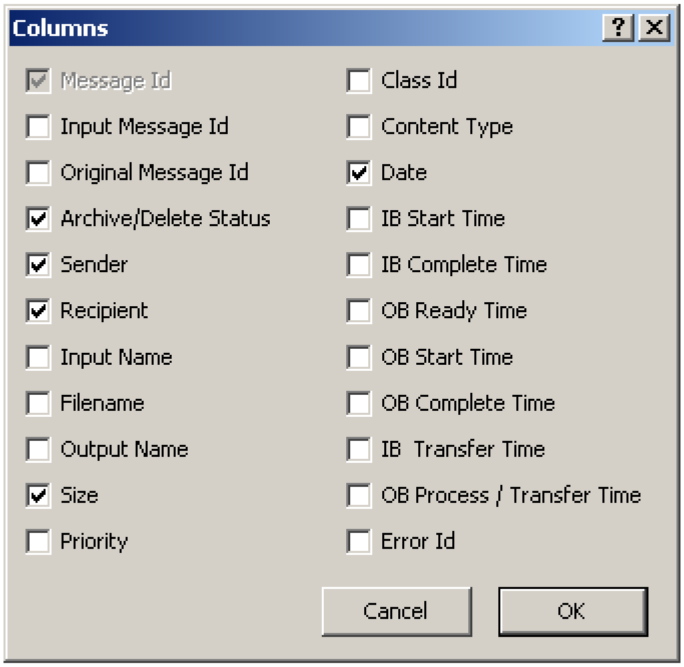
When an outbound message already has a priority assigned, then the new priority will be the higher of the assigned or the default priority. The adapter or service associated with this location will deliver higher priority messages first. Changes to the priority field take effect for messages that are not currently being processed or transferred. However, changes will be applied to any future output messages generated by services, such as MWTranslator. The priority assigned to a message may be changed using the **Change Priority** command.

IMPORTANT: For MWCustomProc (MessageWay Custom Processing Service) service locations configured for trigger messages, the priority must be less than 5 and the number of threads must be greater than 1. This is because trigger messages are assigned a default priority of 5. Other messages should not compete with this priority and there must be a reserved thread available for these messages so they will always appear in the queue. Otherwise, the trigger messages may not be added to the queue and, therefore, not be processed.

Columns Dialog Box

The **Columns** dialog box appears when you right-click in the Message List Window and select **Select Columns** from the menu. This dialog allows you to select the message information you want to display.

Message ID is required. For instructions, refer to the topic, ***Displaying More Properties in a List Window*** (on page 754).

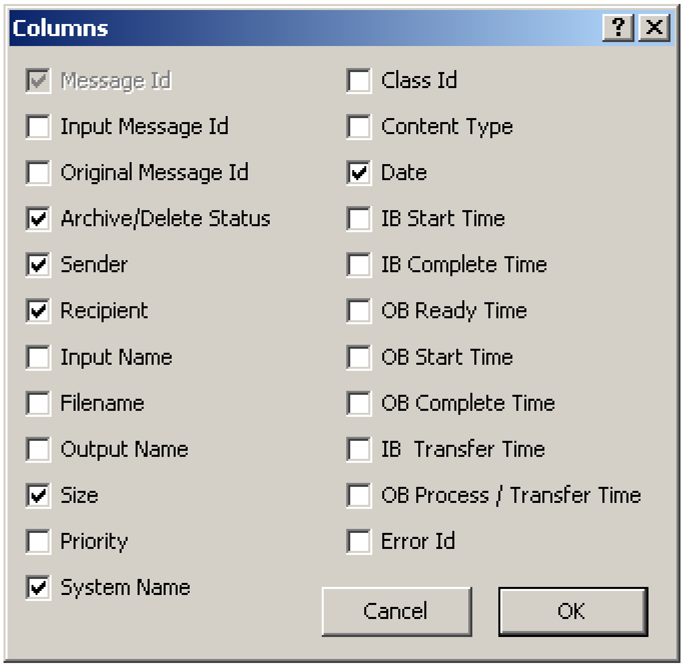


Columns

☑ Message Id
☐ Input Message Id
☐ Original Message Id
☑ Archive/Delete Status
☑ Sender
☑ Recipient
☐ Input Name
☐ Filename
☐ Output Name
☑ Size
☐ Priority

☐ Class Id
☐ Content Type
☑ Date
☐ IB Start Time
☐ IB Complete Time
☐ OB Ready Time
☐ OB Start Time
☐ OB Complete Time
☐ IB Transfer Time
☐ OB Process / Transfer Time
☐ Error Id

When you monitor a multi-system environment, you can also select to display the System Name.



Columns

☑ Message Id
☐ Input Message Id
☐ Original Message Id
☑ Archive/Delete Status
☑ Sender
☑ Recipient
☐ Input Name
☐ Filename
☐ Output Name
☑ Size
☐ Priority
☑ System Name

☐ Class Id
☐ Content Type
☑ Date
☐ IB Start Time
☐ IB Complete Time
☐ OB Ready Time
☐ OB Start Time
☐ OB Complete Time
☐ IB Transfer Time
☐ OB Process / Transfer Time
☐ Error Id

ID

The message ID column contains three components:

- an icon indicating the type of message
- an icon indicating the status of the message
- a system-generated name that uniquely identifies the message.

Descriptions of the message types are listed in the following table:

Message Type	Icon	Description
Input	⤵	An input message is any message sent into MessageWay for processing, automatic delivery or pickup. Input messages may also be cloned from other messages by services such as Distribution List or Rules Processing, or by resubmitting or redirecting a message that has a status of *Canceled* or *Complete*.
Output	⤴	An output message is one possible type of output from a service.
Acknowledgment	↩	An acknowledgment is a message returned to the sender acknowledging some aspect of the input message. Whether a service returns an acknowledgment depends on the service application.
Report	📜	A report is a processing report generated by a service, such as MWTranslator.
Notification Report	✓	A notification report is a brief message describing an event regarding a message transfer or message processing. It may be created by a service or auto-generated by MessageWay, based on configurations for a location. Trigger messages, a type of notification, may be auto-generated by MessageWay or by operator action.

Descriptions of the message statuses are listed in the following table:

Message State	Icon	Description	Possible Cause
Available for Download	👍	The message is waiting in a pickup type location for a user to collect it.	Normal processing for locations not associated with an adapter or service. User must collect messages through the optional services, such as the FTP Server, SFTP Server, AS2.
Canceled	🚫	This message is canceled.	Operator has canceled the message.

Message State	Icon	Description	Possible Cause
Complete	✓	This message has been delivered or picked up/collected.	Normal processing for all locations.
Downloading	⬇	A user is receiving the message from MessageWay through the AS2 interface, FTP Server, SFTP Server or Web Client.	The message is being downloaded by one of the MessageWay perimeter servers.
Error	✗	The message has not been delivered from MessageWay, because it has an error.	▪ Invalid output location ▪ (Translator) Translation abort ▪ (Rules Processing) Reject or abort
Hold, Hold Output, Schedule Wait	✋	This message is currently on hold or waiting for a closed schedule to open, and will be processed when it is released.	▪ Destination location is on hold ▪ Service Location is holding its outputs ▪ Schedule is closed; may use threshold release
Receive Error	✕	Adapter was not able to complete input of message in Message Store. This may contain partial data.	▪ Protocol problems with connecting site ▪ Adapter or service was stopped during transfer
Sending	⚙	An adapter or service is in the process of sending the message	Normal processing.
Queued	⏳	The message is queued awaiting delivery to a process or out from MessageWay.	▪ Adapter or service is busy processing other messages ▪ Adapter or service is stopped or suspended
Uploading	⬆	A user is sending the message to MessageWay through the AS2 interface, FTP Server, SFTP Server or Web Client.	The message is being uploaded by one of the MessageWay perimeter servers.

Input Message Id

The Input Message ID is the link to the input message. For messages received or sent by adapters or rules processing, this is the same as the message ID. For messages sent from services other than Rules Processing, this relates generated outputs with the original input message. To view all related messages, select one of the messages from a message list, right-click, and then choose **Get Related Messages**.

Original Message Id

This is the same as the Message ID, unless this message was created by resubmitting or redirecting a completed message. All messages that have the same original message ID share the same message content file. To view all messages that share the same content, select one of the messages from a message list, right-click, and then select **Get Linked Messages**.

Blank Column (Message List)

The column without a title provides the status for archive/delete. This typically includes the calculated retention date for archive or delete. On the specified date, an icon appears to indicate that this file will be a candidate for archiving or deletion on the following day. When the archive program runs after this date, it will determine whether to archive or delete the messages. By default, the retention date is hidden from view. To view the retention date, widen the column to the right.

Descriptions of the message archive and delete statuses are listed in the following table:

Archive/Delete Status	Icon	Description
Ready for Archive	🗄	Message will be a candidate for archive on the day after the associated retention date when the MessageWay Archive program runs.
	🚫	(Translator option using Reconciliation) Message is ready for archive, but it cannot be archived, because it is awaiting a return acknowledgment.
Ready for Delete	🗑	Message will be a candidate for deletion on the day after the associated retention date when the MessageWay Archive program runs.
	🚫	(Translator option using Reconciliation) Message is ready for delete, but it cannot be deleted, because it is awaiting a return acknowledgment.

Sender

The **Sender** column shows the address of the sender of the message. When this message is output from a service location, the sender may be determined during processing, based on configurations for the application, such as the translator. When this message is transferred by an adapter, this address is the inbound (source) location. When this message is generated by MessageWay, such as a notification report, MessageWay is defined as the sender, followed, in parentheses, by the original sending location or address, as in the case of an e-mail, for example, *MessageWay(X850Test)* or *MessageWay (My Name <my.name@mycompany.com>)*.. The sender may be either a MessageWay location or an external address, such as smtp:myself@mymail.com.

Recipient

The **Recipient** column shows the address of the recipient of the message. It may be either a MessageWay location or an external address, such as smtp:myself@mymail.com. When the destination is specified as a compound address, and there are more destination locations remaining in the address, these additional addresses follow the current location address separated by colons. For example, the address, Unzip:MWTranslator:AdminTest, shows that this message has been sent to the Unzip service location, and it will then be sent to the Translator service location and finally to the AdminTest I/O site. The last location is typically an output site or pickup mailbox.

Input Name

This is the name for the input message, assuming one is known. This name differs depending on the type of adapter or service for the location that passes the name to MessageWay. For Disk Transfer or the FTP adapter sites, this would be a file name with the directory path. For an E-mail adapter site, the name might represent the name of an attached file. Since the Message ID is only useful within MessageWay, this name may be used in lieu of the Message ID to relate a message to an external system.

Filename

Filename is a consistent name that may be assigned directly or generated from either the name of the input file or, when no input file name exists, from a mask that uses the message ID. Its purpose is to provide a name that does not depend on the requirements of the adapter or service that receives the message, as does input name, nor on the requirements of the adapter or service that delivers the message, as does output name. A filename does not have to be unique in MessageWay, and it may be changed when it is sent to a Rules Processing service location.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  \ / : * ? " < > | ! & ` ' ;

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

- Duplicate Filename values are allowed within the same location within the Locations folder.
- Duplicate Filenames are *not* allowed within the same location within the File System folder, unless one has been canceled.

IMPORTANT (UNIX): Note that MessageWay does not support input filenames that contain backslashes, \. For operating systems, such as UNIX, that allow backslashes in filenames, the filename property will be whatever follows the final backslash.

Output Name

This is the name for the output message, assuming one is known. This name differs depending on the type of adapter or service for the location that generates the name. For Disk Transfer or the FTP sites, this would include a full path with a file name generated by a mask. For an E-mail site, the name might represent the name of an attached file. Since the Message ID is only useful within MessageWay, this name may be used in lieu of the Message ID to relate a message to an external system.

Size

This is the size of the message in bytes.

Priority

This is the priority that is assigned by the service location or the outbound site.

System Name

This column is available for multi-system environments, so you can determine to which system items on a list belong. If your environment contains only one system, this option is not available.

Class ID

Class IDs allow users to assign a category to a message. Use them to find and route groups of messages. Users may assign a class ID to a message in MessageWay using the syntax *classid***@** or *classid***@***recipient* in the various destination options, such as the **Deliver to** field in input sites, the Rules Processing Profile **Recipient** field or MWTranslator destination fields. Recipient is typically a valid destination location. Users may change class ID values by using the **Redirect** command for messages that have not yet been marked complete.

Content Type

The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream. Content types can be used with FTP output to dynamically determine the transfer mode, either Text or Binary, when the Transfer Mode on Site Properties is set to AUTO.

MessageWay is able to detect the following content types:

Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm

Type	Content Type	File Extension
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

Date

This is the date and time the message was received or when the last delivery was completed.

IB Time Started

The inbound time started is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the adapter or service allocated a thread to start the transfer of the message into MessageWay.

IB Time Complete

The inbound time complete is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message completed transfer to MessageWay. You may see a status of queued, waiting, processing or hold, indicating the inbound process has completed its work and the next stage of the message is to be passed to the outbound process.

OB Time Ready

The outbound time ready is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message was available to be delivered or picked up from MessageWay. For a service location, this is the time the message is available for processing by the associated service, such as MWTranslator or Rules Processing.

OB Time Started

The outbound time started is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message was allocated a thread by the adapter or service to be transferred from a MessageWay location. If retries are used, this is the latest retry. For messages downloaded from pickup mailboxes, this is the first time the file was downloaded.

OB Time Complete

The outbound time complete is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message completed processing, either by successful delivery or exhausted retries. When retries are used, this is the time of the final retry. For messages downloaded from pickup mailboxes, this is the first time the file was downloaded.

IB Transfer Time

The inbound transfer time is the lapsed time (hh:mm:ss:ms) for the message to transfer to MessageWay, calculated by subtracting the IB Time Complete from the IB Time Started.

OB Transfer Process Time

The outbound transfer process time is the lapsed time (hh:mm:ss:ms) for the message to complete processing. It is calculated by subtracting the OB Time Complete from the OB Time Started.

Error ID

When messages have a status of *Error*, this column displays the error ID.

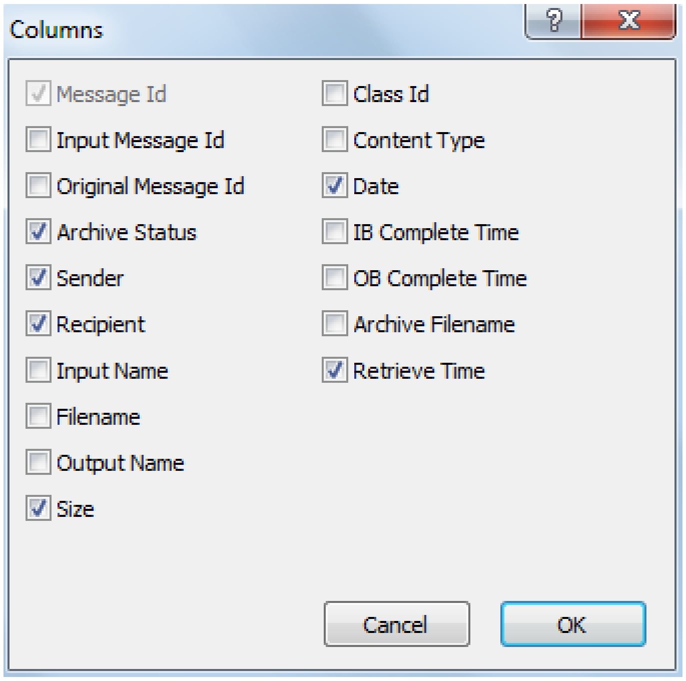
Archive Message List Window

The Archive Message List window allows users to see pertinent data for selected archive messages using certain criteria. The only way to display archive messages is by using the **Find Archive Messages** window and specify criteria for a search.

To choose the type of information to display in the Archive Message List window, refer to the topic, ***Displaying More Properties in Message List Window*** (on page 754).

Columns Dialog Box

The **Columns** dialog box appears when you right-click in the Archive Message List Window and select **Select Columns** from the menu. This dialog allows you to select the archive message information you want to display. Message ID is required. For instructions, refer to the topic, ***Displaying More Properties in a List Window*** (on page 754).



Columns

☑ Message Id
☐ Input Message Id
☐ Original Message Id
☑ Archive Status
☑ Sender
☑ Recipient
☐ Input Name
☐ Filename
☐ Output Name
☑ Size

☐ Class Id
☐ Content Type
☑ Date
☐ IB Complete Time
☐ OB Complete Time
☐ Archive Filename
☑ Retrieve Time

ID (Archive Message List)

The message ID column contains three components:

- an icon indicating the type of message
- an icon indicating the status of the message
- a system-generated name that uniquely identifies the message.

Descriptions of the message types are listed in the following table:

Message Type	**Icon**	**Description**
Input		An input message is any message sent into MessageWay for processing, automatic delivery or pickup. Input messages may also be cloned from other messages by services such as Distribution List or Rules Processing, or by resubmitting or redirecting a message that has a status of *Canceled* or *Complete*.

Message Type	Icon	Description
Output	↪	An output message is one possible type of output from a service.
Acknowledgment	↩	An acknowledgment is a message returned to the sender acknowledging some aspect of the input message. Whether a service returns an acknowledgment depends on the service application.
Report	📜	A report is a processing report generated by a service, such as MWTranslator.
Notification Report	✓	A notification report is a brief message describing an event regarding a message transfer or message processing. It may be created by a service or auto-generated by MessageWay, based on configurations for a location. Trigger messages, a type of notification, may be auto-generated by MessageWay or by operator action.

Descriptions of the message statuses are listed in the following table:

Message State	Icon	Description	Possible Cause
Available	👍	The message is waiting in a pickup type location for a user to collect it.	Normal processing for locations not associated with an adapter or service. User must collect messages through the optional services, such as the FTP Server, SFTP Server, AS2.
Canceled	⊘	This message is canceled.	Operator has canceled the message.
Complete	✓	This message has been delivered or picked up/collected.	Normal processing for all locations.
Error	✗	The message has not been delivered from MessageWay, because it has an error.	▪ Invalid output location ▪ (Translator) Translation abort ▪ (Rules Processing) Reject or abort

Input Message Id (Archive Message List)

The Input Message ID is the link to the input message. For messages received or sent by adapters or rules processing, this is the same as the message ID. For messages sent from services other than Rules Processing, this relates generated outputs with the original input message. To view all related messages, select one of the messages from a message list, right-click, and then choose **Get Related Messages**.

Original Message Id (Archive Message List)

This is the same as the Message ID, unless this message was created by resubmitting or redirecting a completed message. All messages that have the same original message ID share the same message content file. To view all messages that share the same content, select one of the messages from a message list, right-click, and then select **Get Linked Messages**.

Blank Column (Archive Message List)

The column without a title provides the status of a message in the archive.

Descriptions of the status of messages in the archive are listed in the following table:

Archive Status	Icon	Description
Message in Archive	A	Message is in archive. The next step is to mark it for retrieve from archive.
Message marked for Retrieve	M	Message has been marked for retrieve from archive. It will be retrieved the next time the Archive Retrieve program is run.
Message Retrieved from Archive	R	Message has been retrieved from archive and can now be viewed or resubmitted back into MessageWay.

Sender (Archive Message List)

The **Sender** column shows the address of the sender of the message. When this message is output from a service location, the sender may be determined during processing, based on configurations for the application, such as the translator. When this message is transferred by an adapter, this address is the inbound (source) location. When this message is generated by MessageWay, such as a notification report, MessageWay is defined as the sender, followed, in parentheses, by the original sending location or address, as in the case of an e-mail, for example, *MessageWay(X850Test)* or *MessageWay (My Name <my.name@mycompany.com>)*. The sender may be either a MessageWay location or an external address, such as smtp:myself@mymail.com.

Recipient (Archive Message List)

The **Recipient** column shows the address of the recipient of the message. It may be either a MessageWay location or an external address, such as smtp:myself@mymail.com. When the destination is specified as a compound address, and there are more destination locations remaining in the address, these additional addresses follow the current location address separated by colons. For example, the address, Unzip:MWTranslator:AdminTest, shows that this message has been sent to the Unzip service location, and it will then be sent to the Translator service location and finally to the AdminTest I/O site. The last location is typically an output site or pickup mailbox.

Input Name (Archive Message List)

This is the name for the input message, assuming one is known. This name differs depending on the type of adapter or service for the location that passes the name to MessageWay. For Disk Transfer or the FTP adapter sites, this would be a file name with the directory path. For an E-mail adapter site, the name might represent the name of an attached file. Since the Message ID is only useful within MessageWay, this name may be used in lieu of the Message ID to relate a message to an external system.

Filename (Archive Message List)

Filename is a consistent name that may be assigned directly or generated from either the name of the input file or, when no input file name exists, from a mask that uses the message ID. Its purpose is to provide a name that does not depend on the requirements of the adapter or service that receives the message, as does input name, nor on the requirements of the adapter or service that delivers the message, as does output name. A filename does not have to be unique in MessageWay, and it may be changed when it is sent to a Rules Processing service location.

- When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:
- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
- \ / : * ? " < > | ! & ( ) ` ' ;
- NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.
- Duplicate Filename values are allowed within the same location within the Locations folder.
- Duplicate Filenames are not allowed within the same location within the File System folder, unless one has been canceled.

IMPORTANT (UNIX): Note that MessageWay does not support input filenames that contain backslashes, \. For operating systems, such as UNIX, that allow backslashes in filenames, the filename property will be whatever follows the final backslash.

Output Name (Archive Message List)

This is the name for the output message, assuming one is known. This name differs depending on the type of adapter or service for the location that generates the name. For Disk Transfer or the FTP sites, this would include a full path with a file name generated by a mask. For an E-mail site, the name might represent the name of an attached file. Since the Message ID is only useful within MessageWay, this name may be used in lieu of the Message ID to relate a message to an external system.

Size (Archive Message List)

This is the size of the message in bytes.

Class ID (Archive Message List)

Class IDs allow users to assign a category to a message. Use them to find and route groups of messages. Users may assign a class ID to a message in MessageWay using the syntax classid@ or classid@recipient in the various destination options, such as the Deliver to field in input sites, the Rules Processing Profile Recipient field or MWTranslator destination fields. Recipient is typically a valid destination location. Users may change class ID values by using the Redirect command for messages that have not yet been marked complete.

Content Type (Archive Message List)

The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream. Content types can be used with FTP output to dynamically determine the transfer mode, either Text or Binary, when the Transfer Mode on Site Properties is set to AUTO.

MessageWay is able to detect the following content types:

Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff

Type	Content Type	File Extension
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

Date (Archive Message List)

This is the date and time the message was received or when the last delivery was completed.

IB Time Complete (Archive Message List)

The inbound time complete is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message completed transfer to MessageWay.

OB Time Complete (Archive Message List)

The outbound time complete is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message completed processing, either by successful delivery or exhausted retries. When retries are used, this is the time of the final retry. For messages downloaded from pickup mailboxes, this is the first time the file was downloaded.

Archive Filename (Archive Message List)

Name of the archive zip file where the message was archived to or retrieved from.

Retrieve Time (Archive Message List)

The retrieve time is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message was retrieved from archive.

Message Properties Window

The Message Properties window displays information about a specific message. The **General** page shows basic information about the message: message IDs, message attributes, locations, sender and receiver IDs, file names and the current state. The **Timestamps** page contains information about various message processing times. The **Misc**(miscellaneous) page contains information about the processing. When the message is in error, an **Error** page also appears to display the error message. Users may copy the value of any fields to the clipboard using the key combination **CTL+C**. If you have a license for the antivirus server, a **Data Validation** page shows the results of a content scan of the message.

To access the window:

1. Right-click a message from a message list, and click **Properties** from the menu.

   All message values are for display only and are valid at the time the query is made.
2. Since the values are not updated dynamically, press **F5** to update the contents of the window

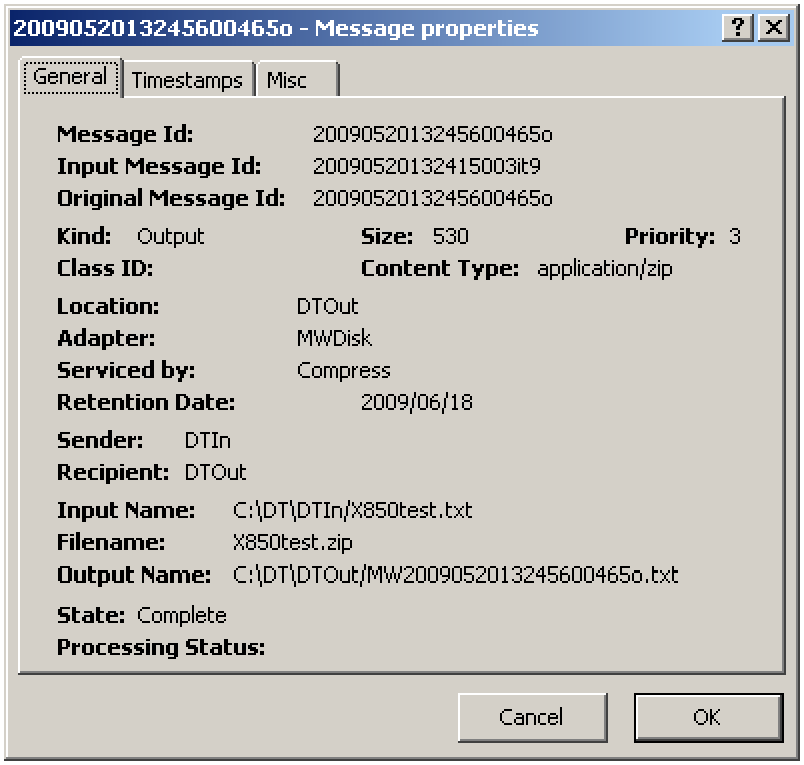
(Message Properties) General Page

The **General** page shows basic information about the message: message IDs, message attributes, locations, sender and receiver IDs, file names and the current state. Users may copy the value of any fields to the clipboard using the key combination **CTL+C**.

Icons may appear to the right of the message ID, to indicate where and how the message content is stored. The options for content storage and their representative icons are:

Icon	Storage Option
None	SQL database, no encryption, no compression
🔑	SQL database, Encrypted
🗜	SQL database, Compressed
💾	Disk
❌	Deleted from Message Store after successful delivery

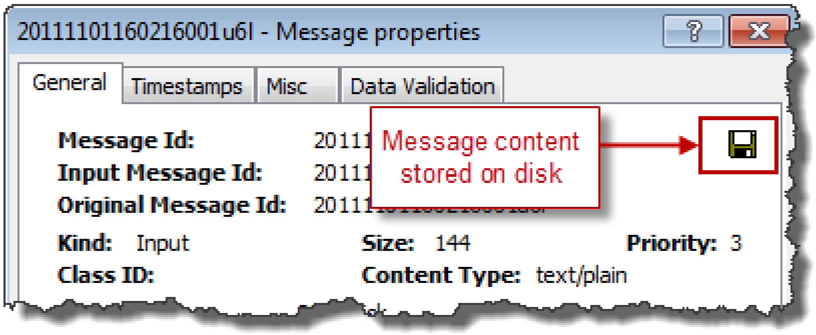
Note that when no icons appear, the message content is stored in the database, without encryption or compression, as shown in the following figure.



Message Id: 2009052013245600465o
Input Message Id: 20090520132415003it9
Original Message Id: 2009052013245600465o
Kind: Output **Size:** 530 **Priority:** 3
Class ID: **Content Type:** application/zip
Location: DTOut
Adapter: MWDisk
Serviced by: Compress
Retention Date: 2009/06/18
Sender: DTIn
Recipient: DTOut
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.zip
Output Name: C:\DT\DTOut/MW2009052013245600465o.txt
State: Complete
Processing Status:

Message Properties Window without Error (General Page)

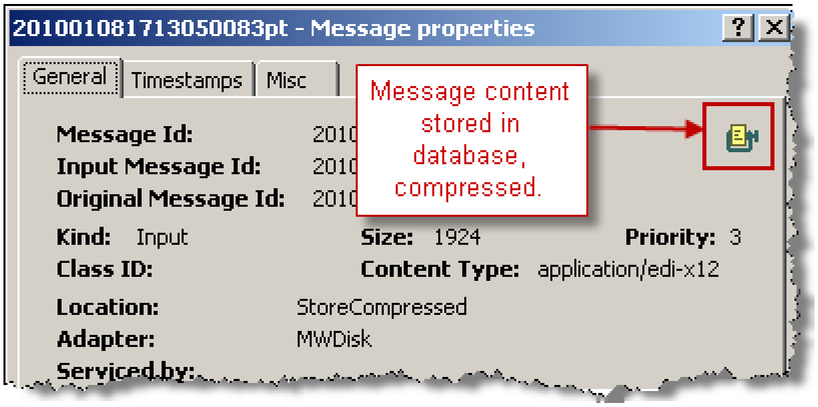
The following figure shows an example of a message whose content was stored on disk:


20111101160216001u6l - Message properties

Message Id: 20111
Input Message Id: 20111
Original Message Id: 20111
Kind: Input
Size: 144
Priority: 3
Class ID:
Content Type: text/plain

Message content stored on disk

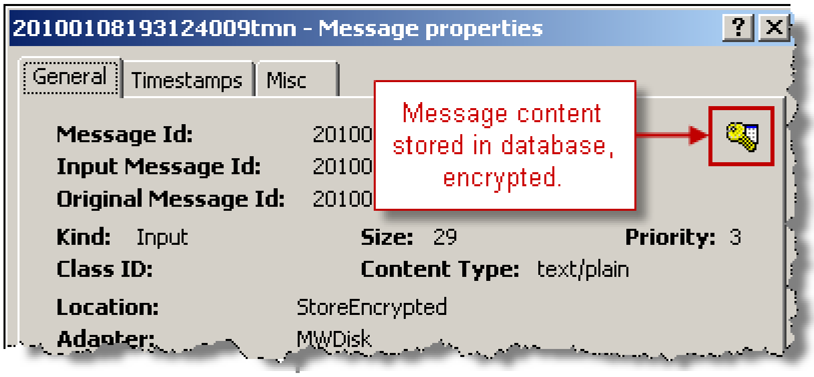
This figure shows an example of a message whose content was stored in the database, compressed.


201001081713050083pt - Message properties

Message Id: 2010
Input Message Id: 2010
Original Message Id: 2010
Kind: Input
Size: 1924
Priority: 3
Class ID:
Content Type: application/edi-x12
Location: StoreCompressed
Adapter: MWDisk
Serviced by:

Message content stored in database, compressed.

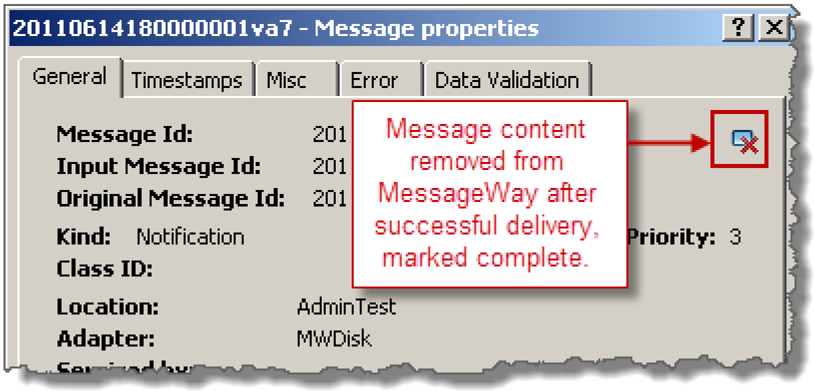
This figure shows an example of a message whose content was stored in the database, encrypted.


201001081931240009tmn - Message properties

Message Id: 20100
Input Message Id: 20100
Original Message Id: 20100
Kind: Input
Size: 29
Priority: 3
Class ID:
Content Type: text/plain
Location: StoreEncrypted
Adapter: MWDisk

Message content stored in database, encrypted.

This figure shows an example of a message whose content was deleted after the message was successfully delivered and marked complete. Note that only the content is removed. The message detail information remains in the database.



Message Id: 201
Input Message Id: 201
Original Message Id: 201
Kind: Notification
Class ID:
Priority: 3
Location: AdminTest
Adapter: MWDisk

Message content removed from MessageWay after successful delivery, marked complete.

Message Id

The Message ID is a unique message identifier assigned by the MessageWay Server.

Input Message Id

The Input Message ID is the link to the input message. For messages received or sent by adapters or rules processing, this is the same as the message ID. For messages sent from services other than Rules Processing, this relates generated outputs with the original input message. To view all related messages, select one of the messages from a message list, right-click, and then choose **Get Related Messages**.

Original Message Id

This is the same as the Message ID, unless this message was created by resubmitting or redirecting a completed message. All messages that have the same original message ID share the same message content file. To view all messages that share the same content, select one of the messages from a message list, right-click, and then select **Get Linked Messages**.

Kind

The message kind or type can be Input, Output, Acknowledgment, Report, or Notification. Input message types may be received through adapters, perimeter servers or generated by some services, such as Distribution List or Rules Processing, or by operator action on messages that have already been marked Complete, such as Resubmit or Redirect. Acknowledgment message types may be created by services. Notification message types may be created by services or auto-generated by MessageWay. Trigger messages are a special type of message that can trigger a service. Operator action, Execute Now, and location schedule configurations can create trigger messages.

The following table describes the various types of messages:

Message Type	Icon	Description
Input	↳	An input message is any message sent into MessageWay for processing, automatic delivery or pickup. Input messages may also be cloned from other messages by services such as Distribution List or Rules Processing, or by resubmitting or redirecting a message that has a status of *Canceled* or *Complete*.
Output	↱	An output message is one possible type of output from a service.
Acknowledgment	↰	An acknowledgment is a message returned to the sender acknowledging some aspect of the input message. Whether a service returns an acknowledgment depends on the service application.
Report	📜	A report is a processing report generated by a service, such as MWTranslator.
Notification Report	✓	A notification report is a brief message describing an event regarding a message transfer or message processing. It may be created by a service or auto-generated by MessageWay, based on configurations for a location. Trigger messages, a type of notification, may be auto-generated by MessageWay or by operator action.

Size

This is the size of the message in bytes.

Priority

This is the priority that is assigned by the service location or the outbound site.

Class ID

Class IDs allow users to assign a category to a message. Use them to find and route groups of messages. Users may assign a class ID to a message in MessageWay using the syntax *classid@* or *classid@recipient* in the various destination options, such as the **Deliver to** field in input sites, the Rules Processing Profile **Recipient** field or MWTranslator destination fields. Recipient is typically a valid destination location. Users may change class ID values by using the **Redirect** command for messages that have not yet been marked complete.

Content Type

The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream. Content types can be used with FTP output to dynamically determine the transfer mode, either Text or Binary, when the Transfer Mode on Site Properties is set to AUTO.

MessageWay is able to detect the following content types:

Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff

Type	Content Type	File Extension
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

Location

This is the destination location for the message.

Adapter

This is the adapter that delivered the message. When a message is sent to a pickup mailbox, there is no adapter used to auto-deliver the message, so this field does not appear.

Serviced By

For messages that are output created by a service, this is the name of the service location. If the message was not sent to a service location, this will be blank.

Retention Date

This message may be archived and deleted beginning one day after this date. It is set when the message first enters the system. The date is calculated from the retention period of the destination location. When the destination location is invalid, the message will appear in the system mailbox, {Unknown}, which has no retention period. In this case the Retention Date will be that of its last service location or a default of 30 days. Input messages also have a default retention date of 30 days.

Operators may change the retention date. Operators may also mark messages for delete or archive to override the retention date, and then the Retention Date will say **Ready for Delete** or **Ready for Archive**, respectively.

The following icons appear to indicate the current archive or delete status of the message:

Archive/Delete Status	Icon	Description
Ready for Archive	🗄	Message will be a candidate for archive on the day after the associated retention date when the MessageWay Archive program runs.
	🚫	(Translator option using Reconciliation) Message is ready for archive, but it cannot be archived, because it is awaiting a return acknowledgment.
Ready for Delete	🗑	Message will be a candidate for deletion on the day after the associated retention date when the MessageWay Archive program runs.
	🚫	(Translator option using Reconciliation) Message is ready for delete, but it cannot be deleted, because it is awaiting a return acknowledgment.

Sender

This is the sender of the message. It is typically a MessageWay location. When a message is generated by MessageWay, such as a notification, MessageWay is defined as the sender, followed, in parentheses, by the original sending location or address, as in the case of an e-mail, for example, *MessageWay(X850Test)* or *MessageWay (My Name <my.name@mycompany.com>)*.

Recipient

This is the destination MessageWay location. When the destination is specified as a compound address, and there are more destination locations remaining in the address, these additional locations appear separated by colons, for example, Unzip:MWTranslator:AdminTest. The last location is typically an output site or pickup mailbox.

Input Name

This is the name for the input message, assuming one is known. This name differs depending on the type of adapter or service for the location that passes the name to MessageWay. For Disk Transfer or the FTP adapter sites, this would be a file name with the directory path. For an E-mail adapter site, the name might represent the name of an attached file. Since the Message ID is only useful within MessageWay, this name may be used in lieu of the Message ID to relate a message to an external system.

Filename

Filename is a consistent name that may be assigned directly or generated from either the name of the input file or, when no input file name exists, from a mask that uses the message ID. Its purpose is to provide a name that does not depend on the requirements of the adapter or service that receives the message, as does input name, nor on the requirements of the adapter or service that delivers the message, as does output name. A filename does not have to be unique in MessageWay, and it may be changed when it is sent to a Rules Processing service location.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  \ / : * ? " < > | ! & ` ' ;

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

- Duplicate Filename values are allowed within the same location within the Locations folder.
- Duplicate Filenames are *not* allowed within the same location within the File System folder, unless one has been canceled.

IMPORTANT (UNIX): Note that MessageWay does not support input filenames that contain backslashes, \. For operating systems, such as UNIX, that allow backslashes in filenames, the filename property will be whatever follows the final backslash.

Output Name

This is the name for the output message, assuming one is known. This name differs depending on the type of adapter or service for the location that generates the name. For Disk Transfer or the FTP sites, this would include a full path with a file name generated by a mask. For an E-mail site, the name might represent the name of an attached file. Since the Message ID is only useful within MessageWay, this name may be used in lieu of the Message ID to relate a message to an external system.

State (Message Properties)

The state of the message is a current description of where the message is in its processing cycle. Examples of possible statuses are Canceled, Complete and Error.

The possible message states are as follows:

State	Description
Available for download	The message is waiting to be picked up by a user.
Canceled	The message has been canceled.
Complete	The message has been delivered.

State	Description
Downloading	A user is receiving the message from MessageWay through the AS2 interface, FTP Server, SFTP Server or Web Client.
Error	The message has an error that occurred during processing or delivery.
Hold	The message is on hold awaiting further action by an operator.
Incomplete Output	The process was interrupted and the output may be incomplete.
Output Hold	The message is output from a service location and is on hold at its destination location awaiting further action by an operator.
Processing	The message has been received by a service location and is currently being processed.
Queued	The message is currently queued for processing or delivery action.
Receiving	The message is being received by an inbound location.
Scheduled	The schedule is currently closed and the message is on hold.
Sending	The message is in a send and perhaps retry cycle.
Uploading	A user is sending the message to MessageWay through the AS2 interface, FTP Server, SFTP Server or Web Client.

Processing Status

Input messages sent to a service location, such as MWTranslator, will have a processing status.

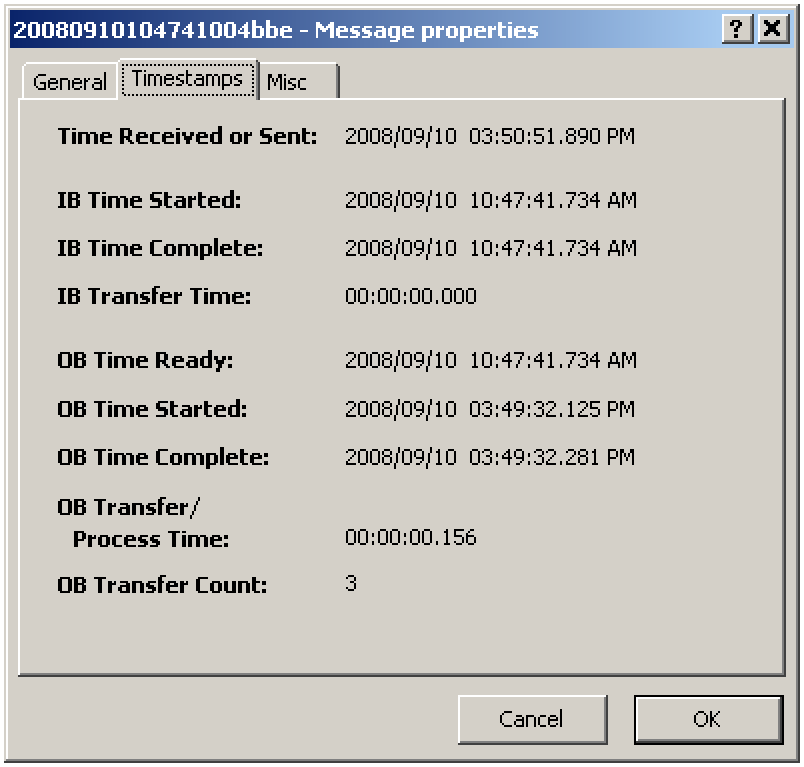
The following table describes the possible statuses:

Processing Status	Description
Accept	The process accepted the message.
Accept w(ith) Errors	The process detected errors but accepted the message.
Partial Accept	The process rejected part of the message and accepted the rest. This is usually the result of one document in an interchange or functional group being rejected, but the remaining documents were accepted, so the message was partially accepted.
Reject	The process rejected the entire message.
Security Failure	The process detected a security error.
Abort	The process aborted processing the message.
Duplicate Receipt	Duplicate messages were received while the **Check for Duplicates** box was checked. For information about how MessageWay determines that messages are duplicates, refer to the help for the check box on the **General** tab of the location (Service Location, Site, Mailbox) Properties window.

(Message Properties) Timestamps Page

The Timestamps page contains date and time information for the various states of the message. When the message is in error, an **Error** page also appears to display the error message. Users may copy the value of any fields to the clipboard using the key combination **CTL+C**.

NOTE: The OB Transfer Count field appears only when users download a message from a pickup mailbox more than once.



Time Received or Sent:	2008/09/10 03:50:51.890 PM
IB Time Started:	2008/09/10 10:47:41.734 AM
IB Time Complete:	2008/09/10 10:47:41.734 AM
IB Transfer Time:	00:00:00.000
OB Time Ready:	2008/09/10 10:47:41.734 AM
OB Time Started:	2008/09/10 03:49:32.125 PM
OB Time Complete:	2008/09/10 03:49:32.281 PM
OB Transfer/ Process Time:	00:00:00.156
OB Transfer Count:	3

Message Properties Window without Error (Timestamps Page)

Time Received or Sent

This is the date and time the message was received or when the last delivery was completed.

IB Time Started

The inbound time started is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the adapter or service allocated a thread to start the transfer of the message into MessageWay.

IB Time Complete

The inbound time complete is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message completed transfer to MessageWay. You may see a status of queued, waiting, processing or hold, indicating the inbound process has completed its work and the next stage of the message is to be passed to the outbound process.

IB Transfer Time

The inbound transfer time is the lapsed time (hh:mm:ss:ms) for the message to transfer to MessageWay, calculated by subtracting the IB Time Complete from the IB Time Started.

OB Time Ready

The outbound time ready is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message was available to be delivered or picked up from MessageWay. For a service location, this is the time the message is available for processing by the associated service, such as MWTranslator or Rules Processing.

OB Time Started

The outbound time started is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message was allocated a thread by the adapter or service to be transferred from a MessageWay location. If retries are used, this is the latest retry. For messages downloaded from pickup mailboxes, this is the first time the file was downloaded.

OB Time Complete

The outbound time complete is the date (yyyy/mm/dd) and time (hh:mm:ss:ms) when the message completed processing, either by successful delivery or exhausted retries. When retries are used, this is the time of the final retry. For messages downloaded from pickup mailboxes, this is the first time the file was downloaded.

OB Transfer Process Time

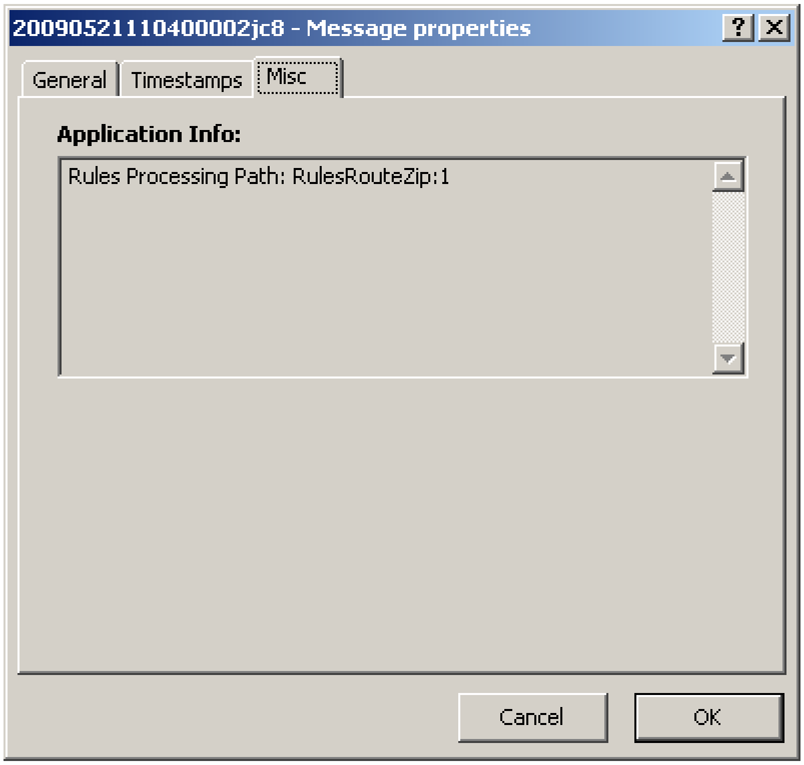
The outbound transfer process time is the lapsed time (hh:mm:ss:ms) for the message to complete processing. It is calculated by subtracting the OB Time Complete from the OB Time Started.

OB Transfer Count

For messages from pickup mailboxes, this is the number of times the file was downloaded. This field appears only when you have downloaded the message more than once.

(Message Properties) Misc Page

The **Misc**(ellaneous) page contains information about an application that processed the message, such as the Rules Processing service. When the message is in error, an **Error** page also appears to display the error message. Users may copy the value of any fields to the clipboard using the key combination **CTL+C**.



Rules Processing Path: RulesRouteZip:1

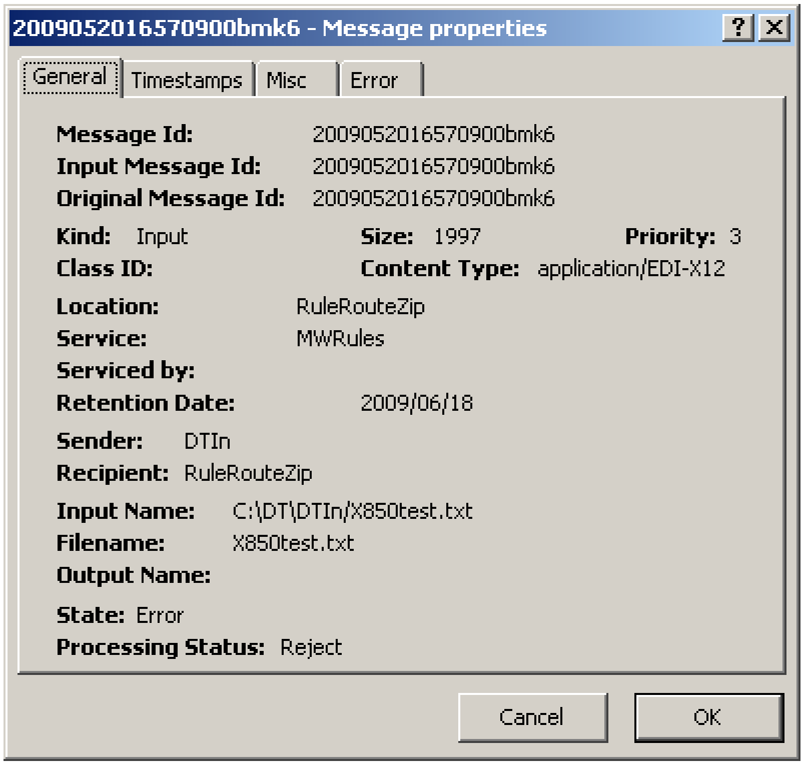
Message Properties Window (Misc Page)

Application Information

This box displays any information that is pertinent to an application that has processed the message. For example, for the Rules Processing service, which routes messages based on message content and other rules, the information shows the profiles and specific rules that were used to route the message.

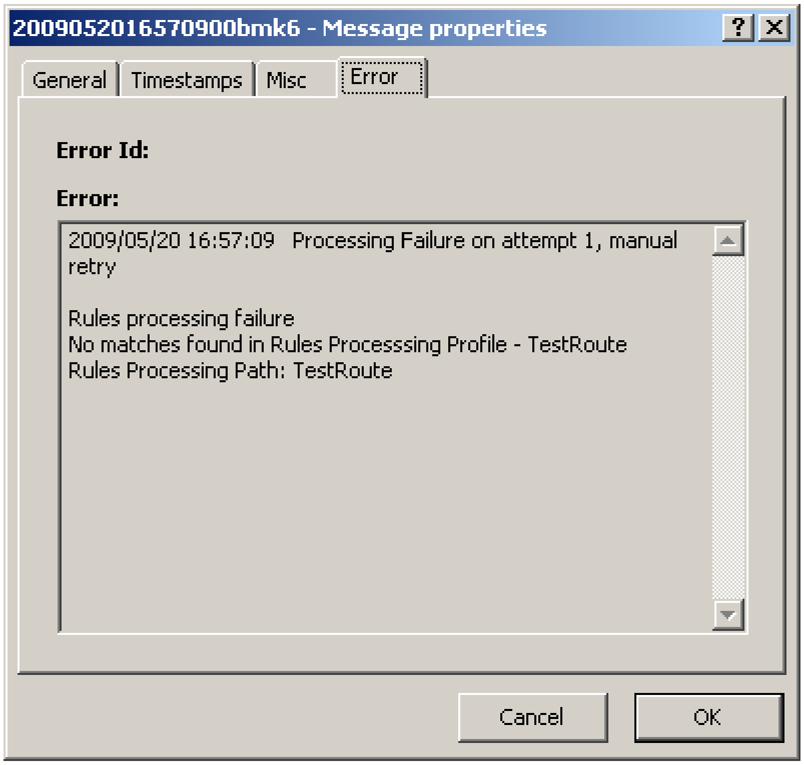
(Message Properties) Error Page

An **Error** page appears when required to display an error message. The state of the message at the bottom of the **General** page is **Error**. Users may copy the value of any fields to the clipboard using the key combination **CTL+C**.



Message Id: 2009052016570900bmk6
Input Message Id: 2009052016570900bmk6
Original Message Id: 2009052016570900bmk6
Kind: Input Size: 1997 Priority: 3
Class ID: Content Type: application/EDI-X12
Location: RuleRouteZip
Service: MWRules
Serviced by:
Retention Date: 2009/06/18
Sender: DTIn
Recipient: RuleRouteZip
Input Name: C:\DT\DTIn/X850test.txt
Filename: X850test.txt
Output Name:
State: Error
Processing Status: Reject

Message Properties Window with Error (General Page)



Error Id:

Error:

2009/05/20 16:57:09 Processing Failure on attempt 1, manual retry

Rules processing failure
No matches found in Rules Processsing Profile - TestRoute
Rules Processing Path: TestRoute

Message Properties Window with Error (Error Page)

Error ID

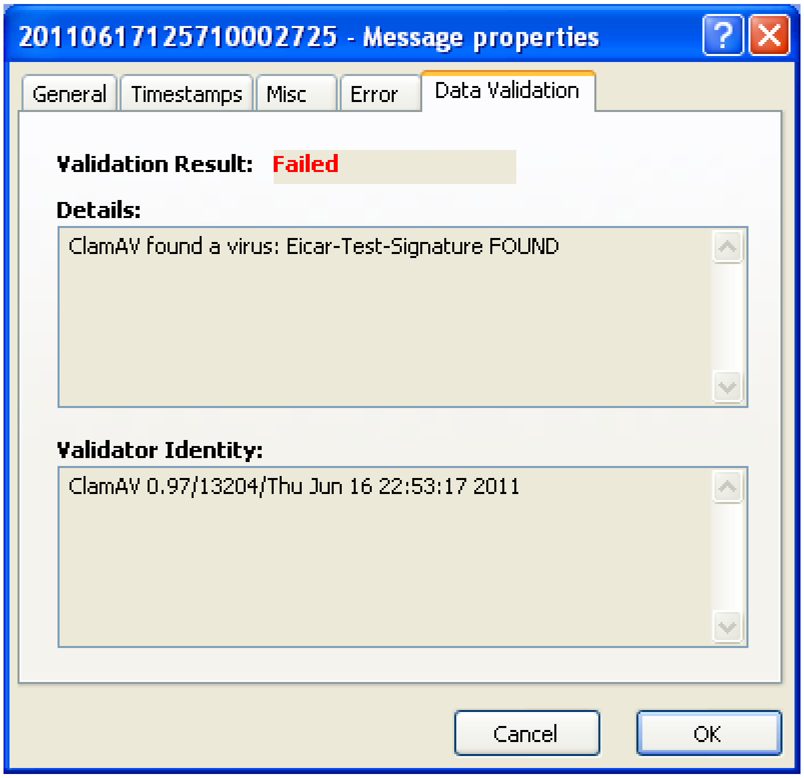
When the message has a state of Error, this is the ID of the error. For more information about the error, refer to the Troubleshooting section in help.

Error

This is a brief description of the error.

Data Validation (Message Properties)

A **Data Validation** page appears when required to display the results of a validation process, for example, results from a virus scanner.



Validation Result: Failed

Details:

ClamAV found a virus: Eicar-Test-Signature FOUND

Validator Identity:

ClamAV 0.97/13204/Thu Jun 16 22:53:17 2011

Validation Result (Message Properties)

The **Validation Result** shows the result from the validation process. For example, for the embedded anti-virus (AV) engine, this shows one of the following:

- Passed: Validation succeeded, no viruses found.
- Failed: Validation failed, which means a virus was found.
- Incomplete: Validation was not finished due to various reasons, such as the message exceeded the maximum size set in the MessageWay Server Properties, Content Validation page; or because MessageWay could not connect to the anti-virus service.
- Not Required: Content Validation, in the MessageWay Server Properties, was not enabled; or the message was a 0 byte file. (0 bytes files can be used as part of a message flow to indicate that a process is completed or is ready to start).

Details (Message Properties)

Shows the status message returned by the validation process. For example, if a virus is found in a message, this would show the name of the virus found and any associated details.

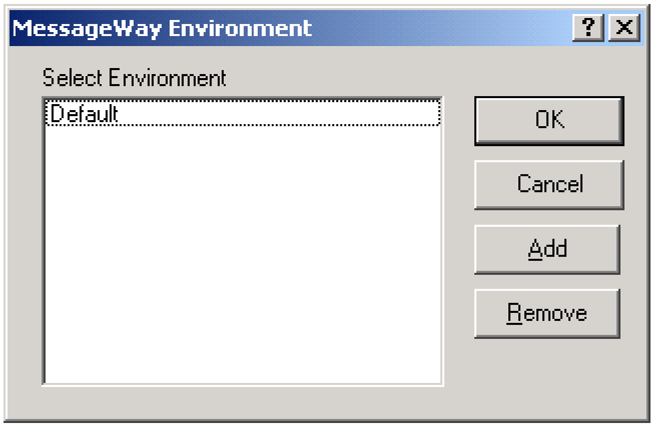
Validator Identity (Message Properties)

Shows the version of the validation service. For example, for the embedded anti-virus engine, this shows the engine version and virus definition version.

MessageWay Environment Window

The MessageWay Environment window allows users to specify remote environments that they are able to access. These environments then appear on a list that you can select from the Connection Options window and then the MessageWay Manager. From the Connection Options window, you can specify up to 4 MessageWay systems that are part of the environment and that you can then monitor from a single instance of the Manager.

To access the MessageWay Environment window, click the **Select Environment** button from the toolbar.



Environment List Box

The MessageWay Environment window allows users to create a name specifying configurations for Connections Options.

This is the list of environments that have been added to specify configurations for remote Connections Options.

OK Button

Click **OK** to save your environment configurations and exit the window.

Cancel Button

Click **Cancel** to exit the window without saving your configurations.

Add Button

Click **Add** to create an environment. The **Add Environment** dialog box appears to enter the environment name. When you type the new environment name and click **OK**, the Connection Options window appears.

Remove Button

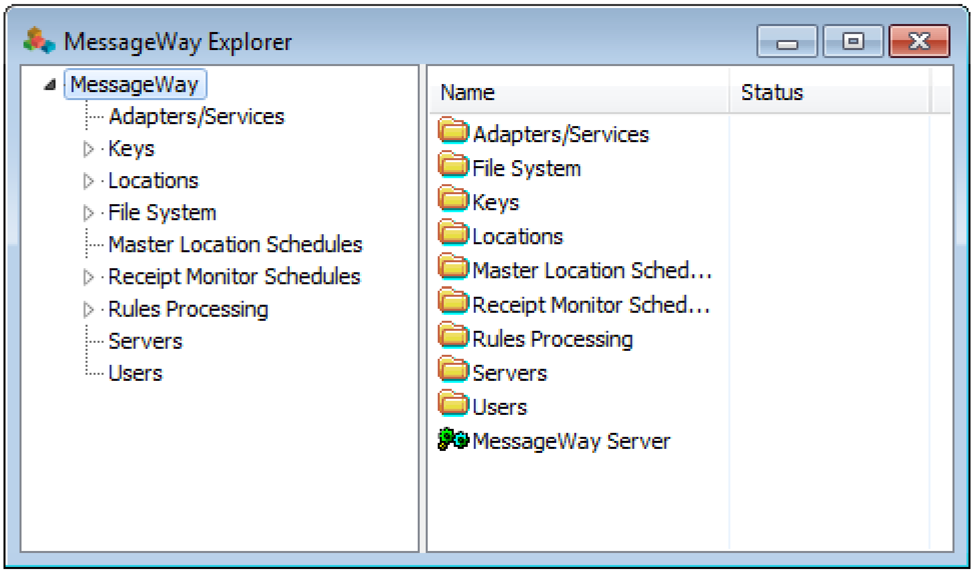
Click **Remove** to remove an environment configuration from the list, which you no longer need to access a MessageWay server database from a remote MessageWay Manager.

MessageWay Explorer Window

The MessageWay Explorer window allows users to display the following:

- Adapters and services
- Keys
- Locations
- File System
- Master Location Schedules
- Receipt Monitor Schedules
- Rules Processing
- Servers
- Users
- Properties for the MessageWay Server

It shows relevant statuses and statistics for adapters and services and statuses for locations. Adapters and services provide communications and processing options. Locations and File System provide addresses to route messages and processing parameters for the messages. Master location schedules allow locations to share the same schedule. Receipt Monitor schedules allow users to monitor inbound messages based on schedules. Processing rules allow users to route messages based on message content or properties. Properties for MessageWay servers may be set here. User security controls internal and external user access to MessageWay definitions and processes.



How to View Properties

To access the properties of an object, such as a folder or other object:

1 In the left pane of the MessageWay Explorer window, do one of the following:

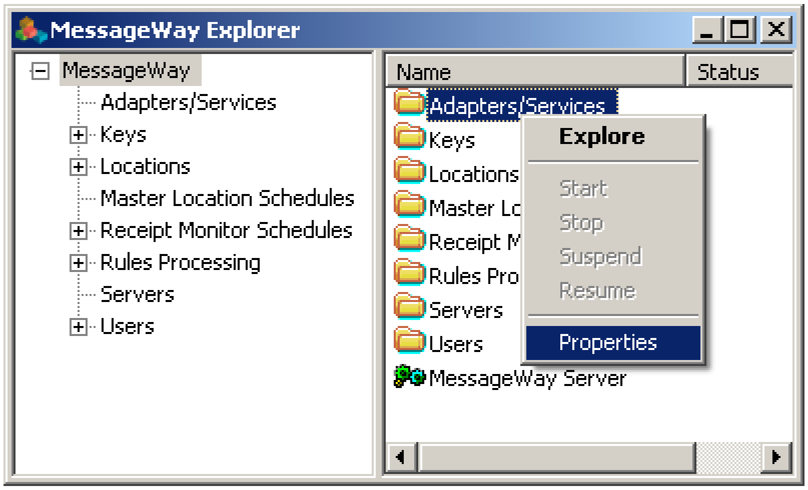
- To access properties for the highest-level folders, select the highest node, **MessageWay**.
- To access properties for other types of folders or objects, select the parent node, such as A**dapters/Services**.

2 In the right pane, select the object whose properties you want to access. This might be another folder or an object such as a location.

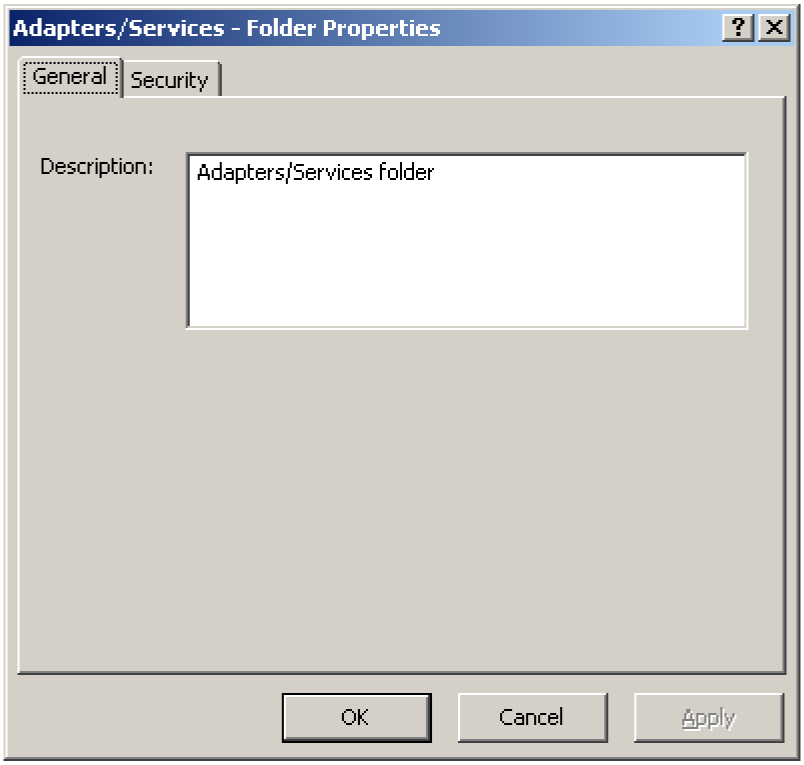
3 Then do one of the following:

- From the task bar, select the **Properties** button, or

- Right click the mouse, and select **Properties** from the menu.



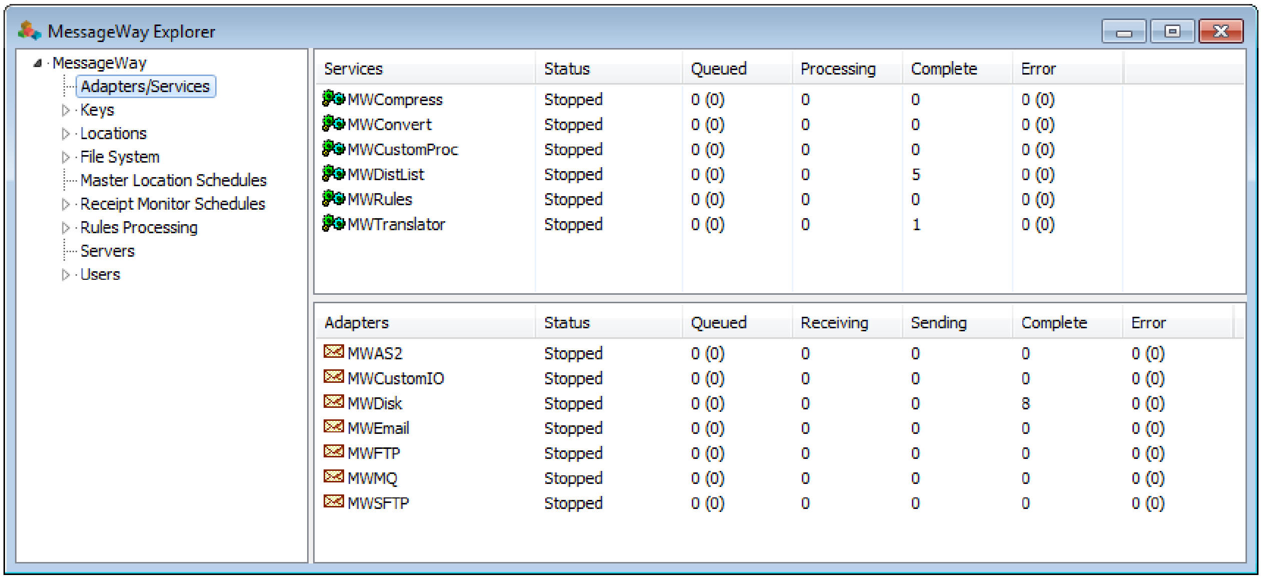
The properties window appears for the object you selected. Properties windows will have different pages of information, depending on what object you have selected.



Description: Adapters/Services folder

Adapters/Services

The **Adapters/Services** folder in the left pane of the MessageWay Explorer window displays all adapters and services configured for your system. The function of an adapter is to do input and output (I/O). The function of services is to provide special processing for messages. Statuses and statistics appear for each adapter and service. You can use the System Monitor to show a consolidated view of statistics for all adapters and services. For more information, refer to ***System Monitor Bar*** (on page 1332).



Services	Status	Queued	Processing	Complete	Error
MWCompress	Stopped	0 (0)	0	0	0 (0)
MWConvert	Stopped	0 (0)	0	0	0 (0)
MWCustomProc	Stopped	0 (0)	0	0	0 (0)
MWDistList	Stopped	0 (0)	0	5	0 (0)
MWRules	Stopped	0 (0)	0	0	0 (0)
MWTranslator	Stopped	0 (0)	0	1	0 (0)

Adapters	Status	Queued	Receiving	Sending	Complete	Error
MWAS2	Stopped	0 (0)	0	0	0	0 (0)
MWCustomIO	Stopped	0 (0)	0	0	0	0 (0)
MWDisk	Stopped	0 (0)	0	0	8	0 (0)
MWEmail	Stopped	0 (0)	0	0	0	0 (0)
MWFTP	Stopped	0 (0)	0	0	0	0 (0)
MWMQ	Stopped	0 (0)	0	0	0	0 (0)
MWSFTP	Stopped	0 (0)	0	0	0	0 (0)

Adapters and Services (MessageWay Explorer Window)

Services provide access to processing services, such as the Compression, Rules Processing and the Distribution List services. Processing services may modify the inbound data and produce separate outbound messages, or they may provide validation services or sophisticated routing without modifying the data.

Adapters provide access to message routing services that are interfaces between external systems or services and MessageWay or between services within MessageWay.

Services

The following status information appears for each service. This information is updated dynamically.

Column	Description
Services	Short name used by the operating system and appears on the **License** page of the MessageWay Server Properties window.
Status	**Running** means that the service has been started. **Stopped** means that the service is not running. **Suspended** means that the service will complete processing current messages, but it will not receive new messages.

Column	Description
Queued ( )	Displays the total number of messages awaiting processing. Numbers in parentheses show the total number of messages awaiting processing that are currently on hold, which includes the message states of **Hold**, **Hold Output** and **Schedule Wait**.
Processing	Displays the total number of messages currently being processed.
Complete	Displays the total number of messages that have been delivered.
Error ( )	Displays the total number of messages that have an error status. Numbers in parentheses show the total number of messages that have been canceled. Operators may cancel any messages that do not have the state of **Receiving**, **Complete** or **Error**.

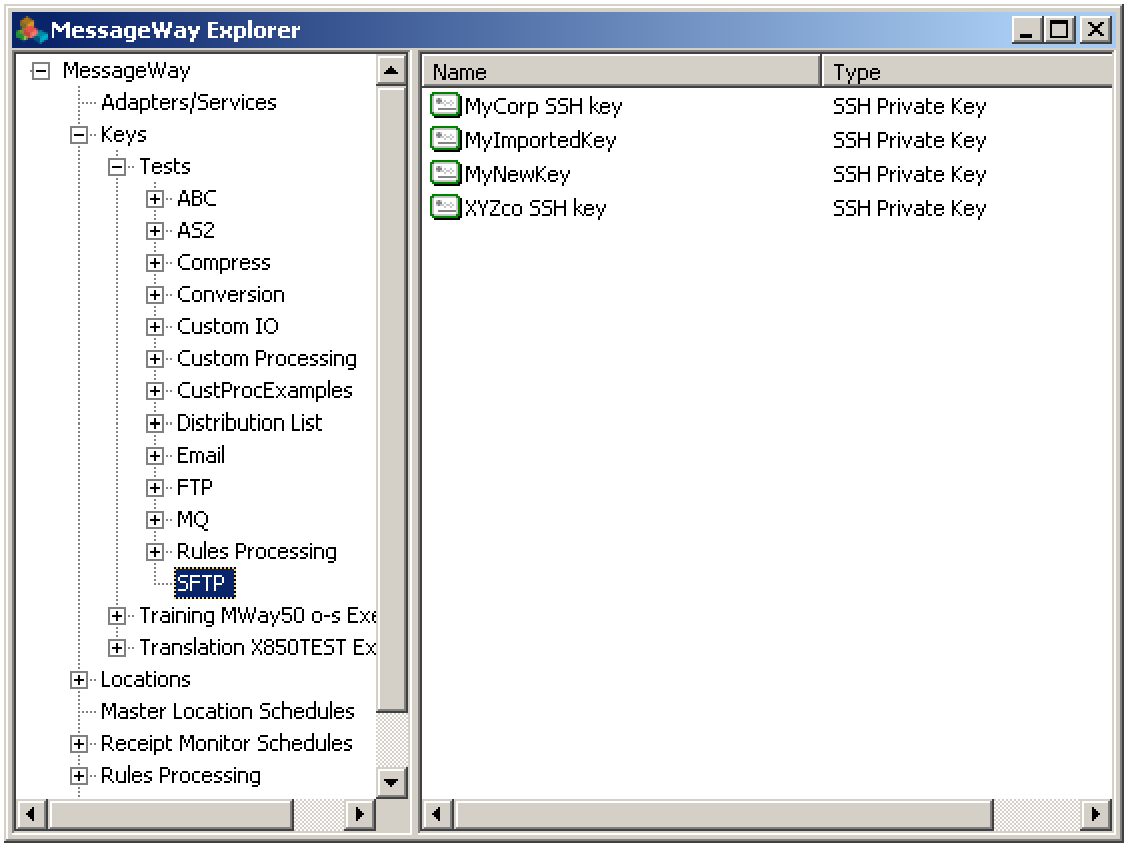
Adapters

The following status information appears for each adapter. This information is updated dynamically.

Column	Description
Adapters	Short name used with the operating system and on the **License** page of the MessageWay Server Properties window.
Status	**Running** means that the adapter has been started. **Stopped** means that the adapter is not running. **Suspended** means that the adapter will complete delivering current messages, but it will not receive new messages.
Queued ( )	Displays the total number of messages that are awaiting delivery. Numbers in parentheses show the total number of messages awaiting delivery that are currently on hold, which includes the message states of **Hold**, **Hold Output** and **Schedule Wait**.
Receiving	Displays the total number of messages currently being received into MessageWay.
Sending	Displays the total number of messages currently being sent to their destination.
Complete	Displays the total number of messages that have been sent to their destination.
Error ( )	Displays the total number of messages that have an error status and are not yet delivered. Messages in the {Unknown} mailbox are not included in the count of any of the individual adapters. Numbers in parentheses show the total number of messages that have been canceled. Operators may cancel any messages that do not have the status of **Receiving**, **Complete** or **Error**.

Keys

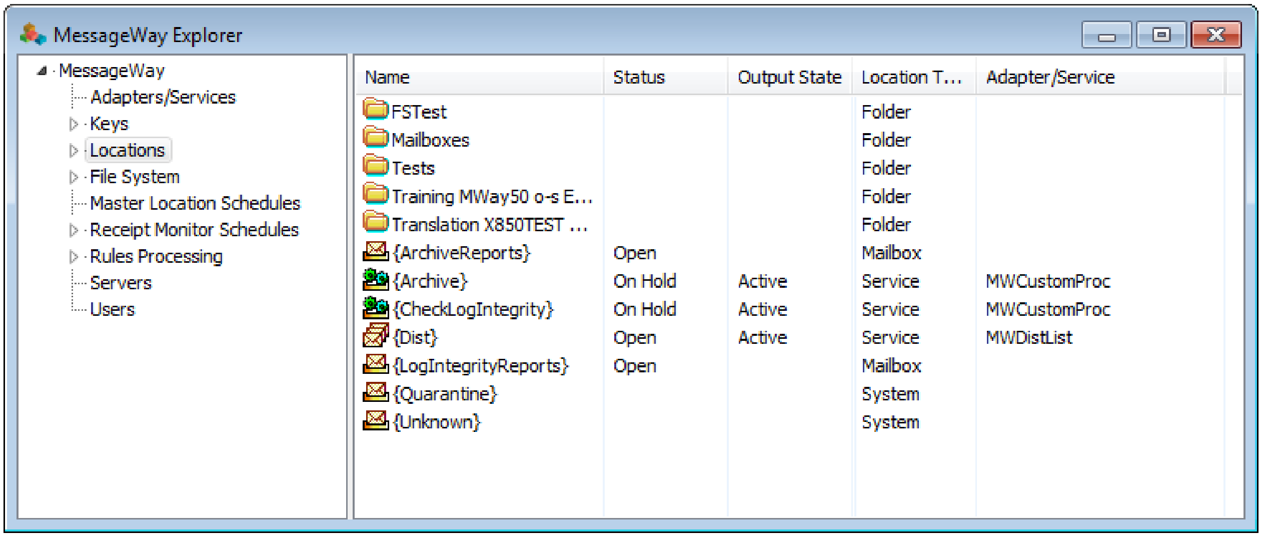
The **Keys** folder in the left pane of the MessageWay Explorer window displays SSH keys for the optional SFTP adapter that are configured for your system. The Keys folder replicates the location folders, since keys are typically associated with specific locations. For more reference information, refer to ***Key Properties Window*** (on page 1032).



Name	Type
MyCorp SSH key	SSH Private Key
MyImportedKey	SSH Private Key
MyNewKey	SSH Private Key
XYZco SSH key	SSH Private Key

Locations

The **Locations** folder in the left pane of the MessageWay Explorer window displays locations configured for your system. Locations here can be displayed individually or within a folder, but each location may be listed only once. Locations can also be created under the File System folder. Locations in the two folders are distinct and separate. For more reference information, refer to ***Location Properties Window*** (on page 1040).



Name	Status	Output State	Location T...	Adapter/Service
FSTest			Folder	
Mailboxes			Folder	
Tests			Folder	
Training MWay50 o-s E...			Folder	
Translation X850TEST ...			Folder	
{ArchiveReports}	Open		Mailbox	
{Archive}	On Hold	Active	Service	MWCustomProc
{CheckLogIntegrity}	On Hold	Active	Service	MWCustomProc
{Dist}	Open	Active	Service	MWDistList
{LogIntegrityReports}	Open		Mailbox	
{Quarantine}			System	
{Unknown}			System	

Each location in the Locations folder, except a system mailbox or a pickup mailbox, is associated with one adapter or service at a time. The icons distinguish between two types of locations, sites, service locations, and folders as shown in the following table.

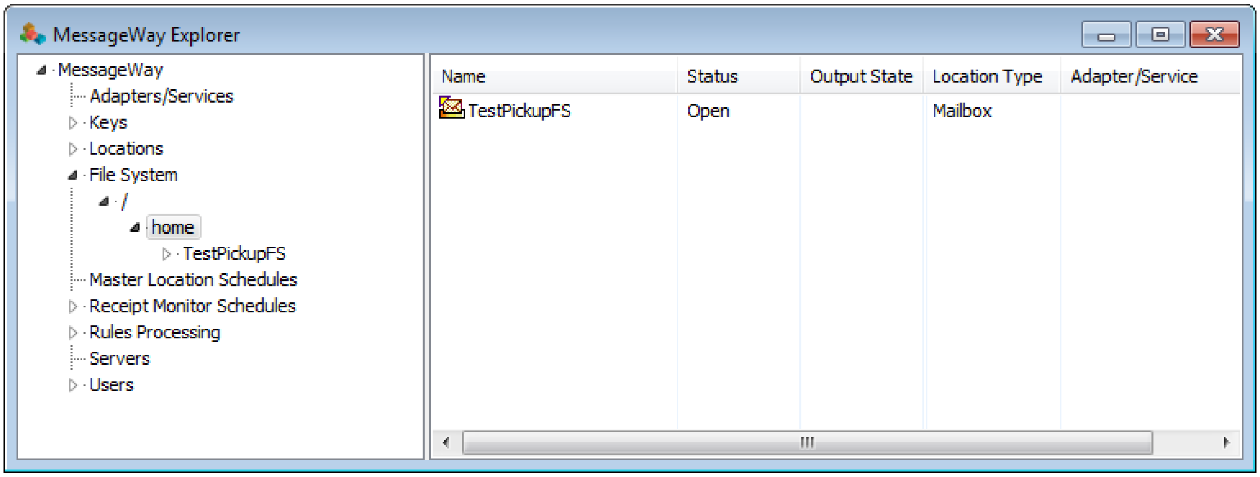
Icon	Location Function (Locations Folder)
⚙	Service location (Compression, Conversion, Custom Processing, Rules Processing, Translator)
✉	Service location (Distribution List)
✉	Sites and mailboxes (system mailboxes and pickup mailboxes)
📁	Folder to organize locations

Location information is current at the time of display. Press **F5** to refresh the display with the most current information. The following table explains the location information:

Column	Description
Status	This is the primary status of all auto-delivery locations, sites and service locations. It is calculated from a combination of the location's state (*Active* or *On Hold*), the schedule state (*Open* or *Closed*) and threshold release. ▪ *Open* means that the schedule will allow the adapter or service to send and receive messages for this location. ▪ *Closed* means that the schedule will not allow the adapter or service to send and receive messages for this location. ▪ *On Hold* means that the location is not available to send or receive data. ▪ *Threshold: nn* means that the schedule is controlled by threshold release rules.
Output State	Valid for service locations only. It is blank for all other types of locations. ▪ *Active* means that the service location will send output for delivery. ▪ *On Hold* means that the service location will send output to the appropriate adapter or service, but the output will be placed on hold in the queue for the service or adapter.
Location Type	▪ *Input* means that the site is configured to send messages into MessageWay. ▪ *Output* means that the site is configured to deliver messages from MessageWay. ▪ *I/O* means that the site is configured to send messages into and deliver messages from MessageWay. ▪ *Mailbox* means that the location waits for users to collect their messages, rather than having them delivered by an adapter. ▪ *Service* means that the location is associated with a service, rather than an adapter. ▪ *System* means that this is the system mailbox, {Unknown}, used for messages that are in error, because the destination location does not exist. This location may not be deleted. ▪ *Folder* means that this item is a folder, which you can use to organize your locations. It has no effect on configurations or processing.
Adapter/Service	The location is currently associated with this adapter or service. This value is blank for group folders, system mailboxes and pickup mailboxes.

File System

The **File System** folder in the left pane of the MessageWay Explorer window displays locations configured for your system to support hierarchical view of the MessageWay Message Store for FTP and SFTP clients. Locations here appear within a directory structure, and the location name can be reused at different levels of the structure. Locations can also be created under the Locations folder. Locations in the two folders are distinct and separate. For more reference information, refer to ***Location Properties Window*** (on page 1040).



MessageWay Explorer

- MessageWay
  - Adapters/Services
  - Keys
  - Locations
  - File System
    - /
      - home
        - TestPickupFS
  - Master Location Schedules
  - Receipt Monitor Schedules
  - Rules Processing
  - Servers
  - Users

Name	Status	Output State	Location Type	Adapter/Service
✉ TestPickupFS	Open		Mailbox	

In the File System folder, a location may be associated with a service that performs a processing service or simply be a pickup mailbox. The icons distinguish between the types of locations, as shown in the following table.

Icon	Location Function
⚙	Service location (Compression, Conversion, Custom Processing, Rules Processing, Translator)
🗂	Service location (Distribution List)
✉	Mailboxes (pickup mailboxes)

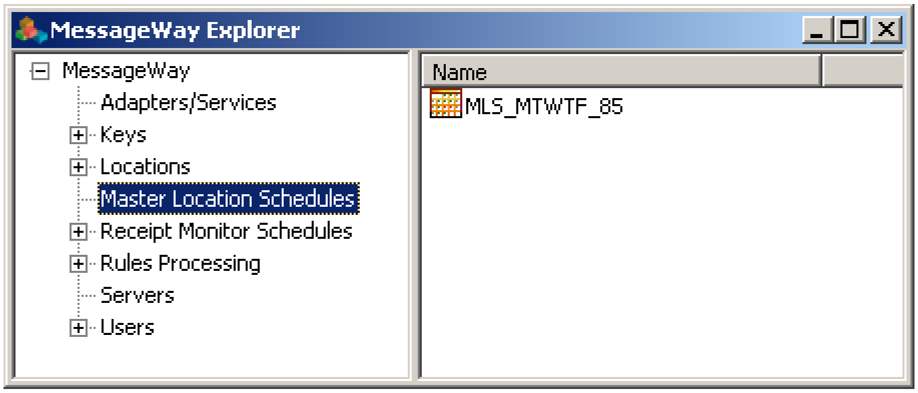
Location information is current at the time of display. Press **F5** to refresh the display with the most current information. The following table explains the location information.

Column	Description
Status	This is the primary status of service locations. It is calculated from a combination of the location's state (*Active* or *On Hold*), the schedule state (*Open* or *Closed*) and threshold release. *Open* means that the schedule will allow the service to send and receive messages for this location. *Closed* means that the schedule will not allow the service to send and receive messages for this location. *On Hold* means that the location is not available to send or receive data. *Threshold: nn* means that the schedule is controlled by threshold release rules.
Output State	Valid for service locations only. It is blank for all other types of locations. *Active* means that the service location will send output for delivery. *On Hold* means that the service location will send output to the appropriate adapter or service, but the output will be placed on hold in the queue for the service or adapter.

Column	Description
Location Type	*Mailbox* means that the location waits for users to collect their messages, rather than having them delivered by an adapter. *Service* means that the location is associated with a service.
Adapter/Service	The location is currently associated with this service. This value is blank for pickup mailboxes.

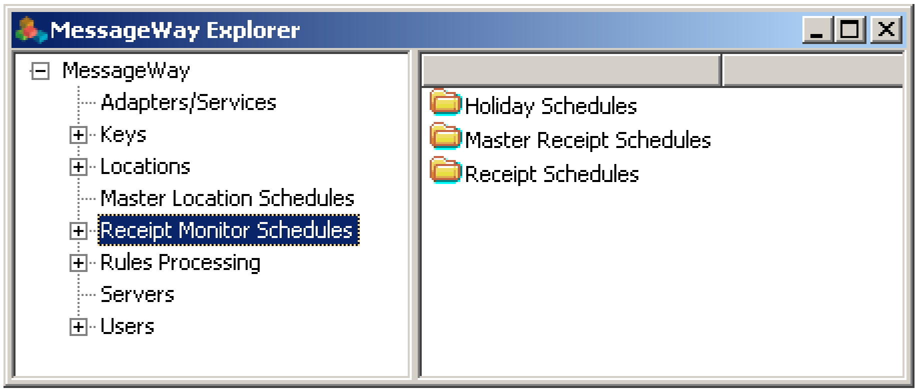
Master Location Schedules

Master Location Schedules may be shared by many locations. They may also be used as a template, which can then be modified for a specific location. This creates a new location schedule which is no longer associated with the original master location schedule.



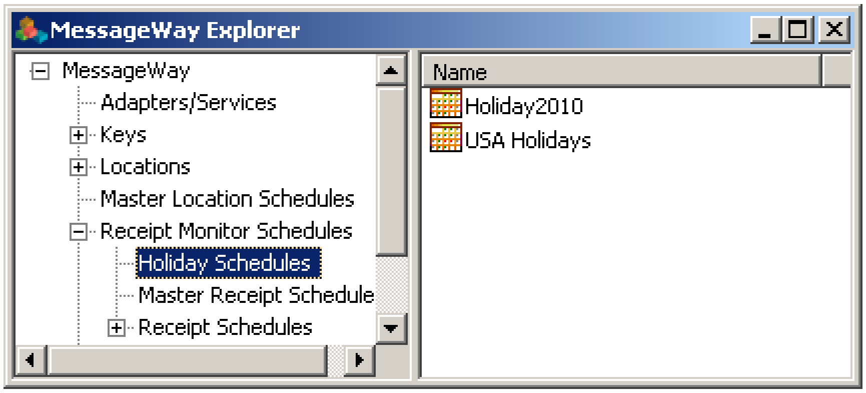
Receipt Monitor Schedules

The **Receipt Monitor Schedules** folder includes folders for the three types of schedules associated with the Receipt Monitor: **Holiday Schedules**, **Master Receipt Schedules** and **Receipt Schedules**.



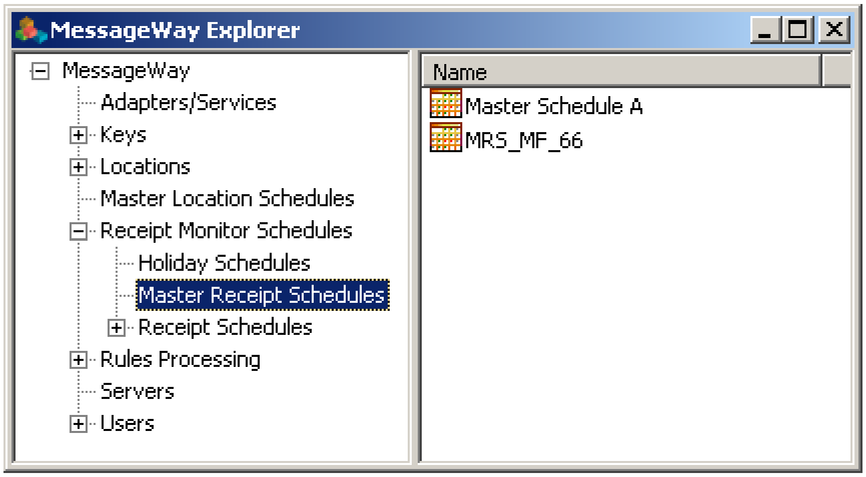
Holiday Schedules

For Receipt Monitor, holiday schedules may be used by many receipt schedules to identify dates and times when the receipt schedule is inactive because of a holiday.



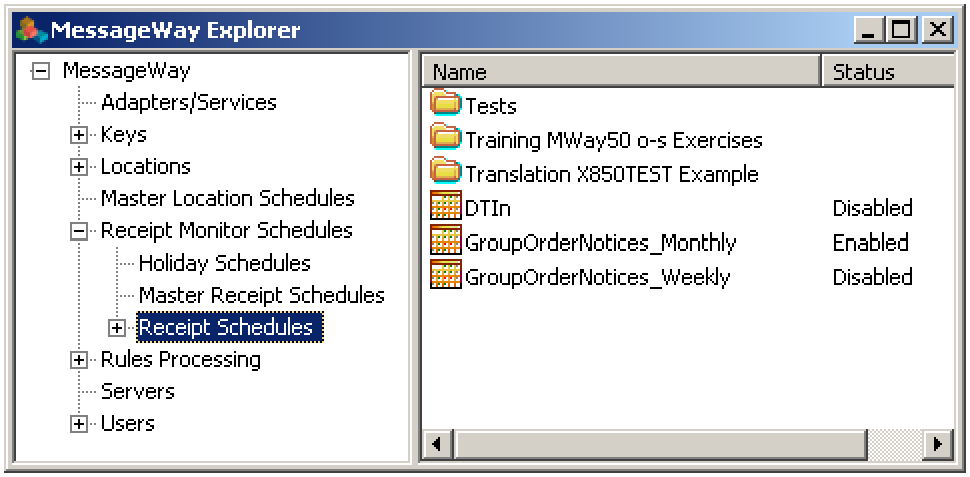
Master Receipt Schedules

For Receipt Monitor, master receipt schedules may be used by many receipt schedules associated with different locations.



Receipt Schedules

For Receipt Monitor, receipt schedules allow users to monitor the number of messages delivered to a location within a specific date and time window. Receipt schedules may be unique or they may use shared master receipt schedules and holiday schedules.

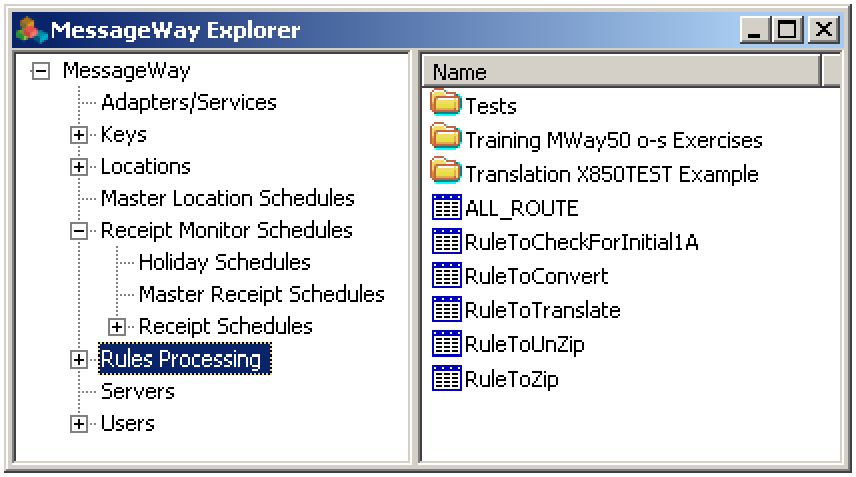


Name	Status
Tests	
Training MWay50 o-s Exercises	
Translation X850TEST Example	
DTIn	Disabled
GroupOrderNotices_Monthly	Enabled
GroupOrderNotices_Weekly	Disabled

Rules Processing

The **Rules Processing** folder in the left pane of the MessageWay Explorer window displays all rules profiles configured for your system. Profiles can be displayed individually or within a group folder, but each profile may be listed only once.

The Rules Processing Service uses rules profiles to deliver messages based on the content or properties of the message. Each profile contains rules to determine where to send the message. Profiles may send messages to a destination location or another profile. When users create locations that use the Rules Processing Service, they specify the profile used for messages sent to this location.

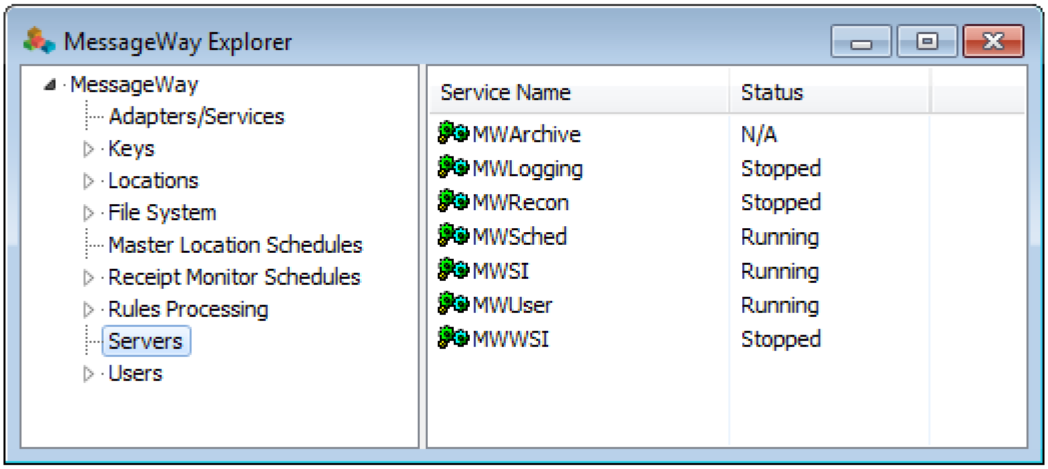


Name
Tests
Training MWay50 o-s Exercises
Translation X850TEST Example
ALL_ROUTE
RuleToCheckForInitial1A
RuleToConvert
RuleToTranslate
RuleToUnZip
RuleToZip

Servers

The Servers folder contains the internal MessageWay servers for which you can configure various options. These include:

- MessageWay Archive/Delete/Maintenance Program
- MessageWay Logging Server (valid only for the MessageWay Translator)
- MessageWay Reconciliation Server (valid only for the MessageWay Translator)
- MessageWay Scheduling Server
- MessageWay Service Interface
- MessageWay User Server
-



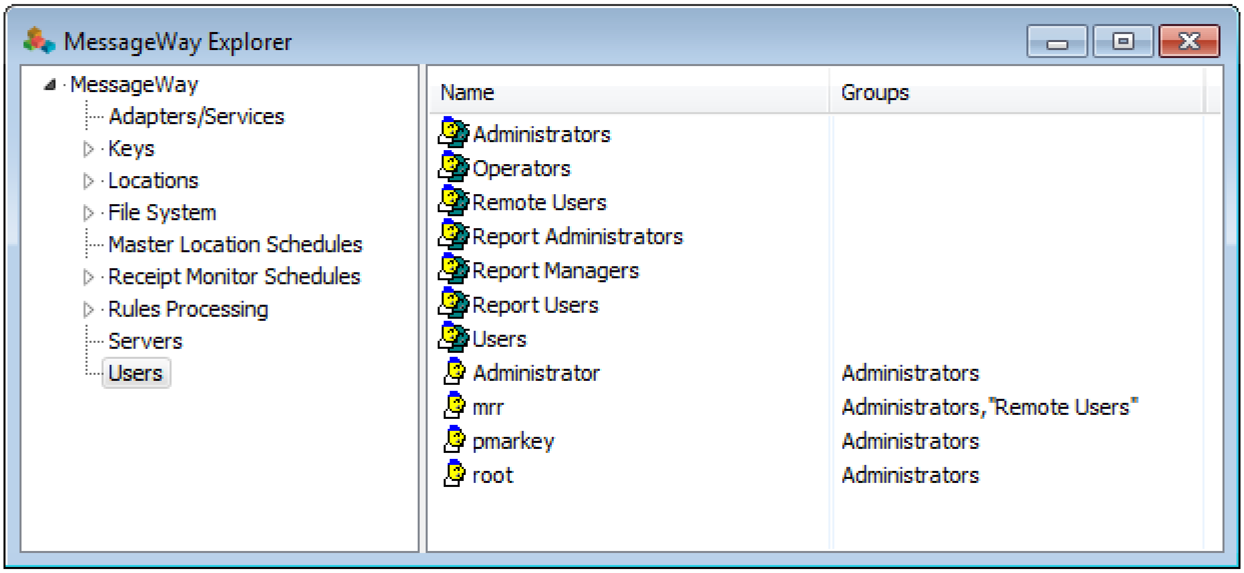
Service Name	Status
MWArchive	N/A
MWLogging	Stopped
MWRecon	Stopped
MWSched	Running
MWSI	Running
MWUser	Running
MWWSI	Stopped

Servers (MessageWay Explorer)

Users

The **Users** folder contains all users and user groups configured for your system. Users and user groups can be displayed individually or within a group folder that you have created, but each user or user group may occur only once.

Users and user groups provide the security to log on and manipulate entities in MessageWay. Each user group has a list of rights for functions they can perform. User configurations contain logon information. They also contain a rights list. Users may optionally belong to groups. When members of groups, users inherit the rights of the groups to which they belong. The rights list for a user shows the combined rights of all groups to which the user belongs. For reference information, refer to the topics, ***User Properties Window*** (on page 1351) and ***User Group Properties Window*** (on page 1335).



Name	Groups
Administrators	
Operators	
Remote Users	
Report Administrators	
Report Managers	
Report Users	
Users	
Administrator	Administrators
mrr	Administrators,"Remote Users"
pmarkey	Administrators
root	Administrators

MessageWay Server

The MessageWay Server displays a properties window with a series of options that the MessageWay uses during startup to validate the license and set the operating parameters.

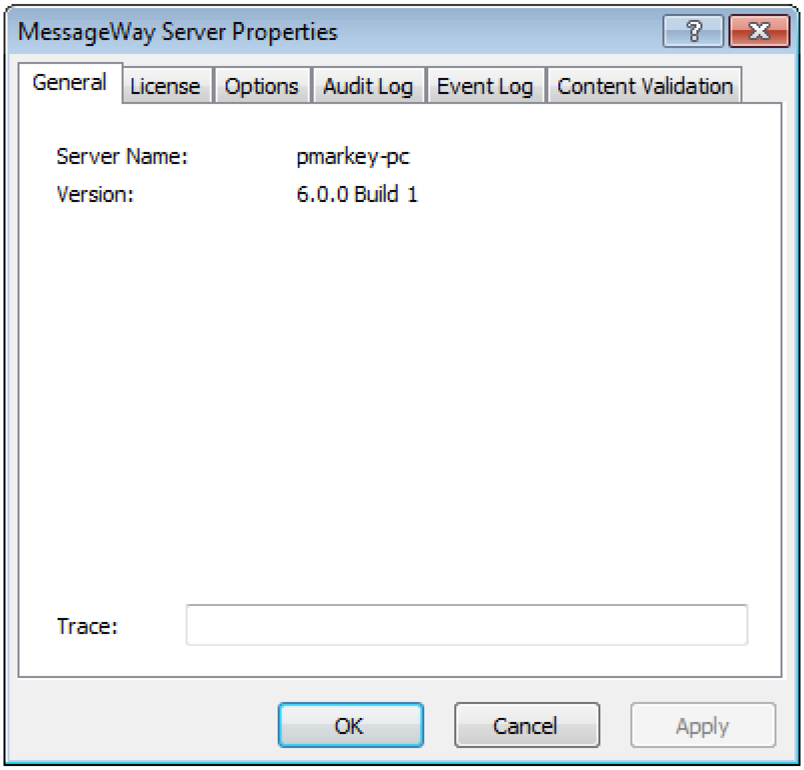
For more reference information, refer to the topic ***MessageWay Server Properties Window*** (on page 1226) and the subsequent definitions of each of its pages.

MessageWay Server Properties Window

The MessageWay Server Properties window allows users to view information about MessageWay and to set default properties. Here you find the server name, the current version of the server, trace capability, message storage option and the active licenses. If a system has the option for virus checking, there will also be configurations for content validation.

(MessageWay Server Properties) General Page

The **General** page of the MessageWay Server Properties window shows the name of the system on which the MessageWay Messaging Server is installed and the version of the current server.



Server Name: pmarkey-pc

Version: 6.0.0 Build 1

Trace:

Server Name (display only)

This is the name of the server on which the MessageWay Server is installed. This name may be different from where the Manager or database is installed.

Version

This is the current version and build of the MessageWay Server.

Trace

This option specifies the type of activity to log to the MessageWay database for the server. Then you can filter and view the information using the Search Trace Logs feature, or using the trace utility. Enter a list of types, separated by commas, that you want to use to appear in the trace log. The types available vary by server. You may also type an asterisk (*) to trace all activity. You can limit the log information further by location, message ID, user and/or IP address.

The trace utility, mwtrace, allows you to view trace information, online or from a disk file, and to delete trace records from the database. For information about how to use the trace utility, in the Troubleshooting section, refer to the topic, ***Tracing Activity for an Adapter, Service or Server*** (on page 877).

CAUTION: The trace process may have a significant impact on performance, especially when you use the asterisk * to trace everything, and particularly for the MessageWay User Server, mwuser. Except for the

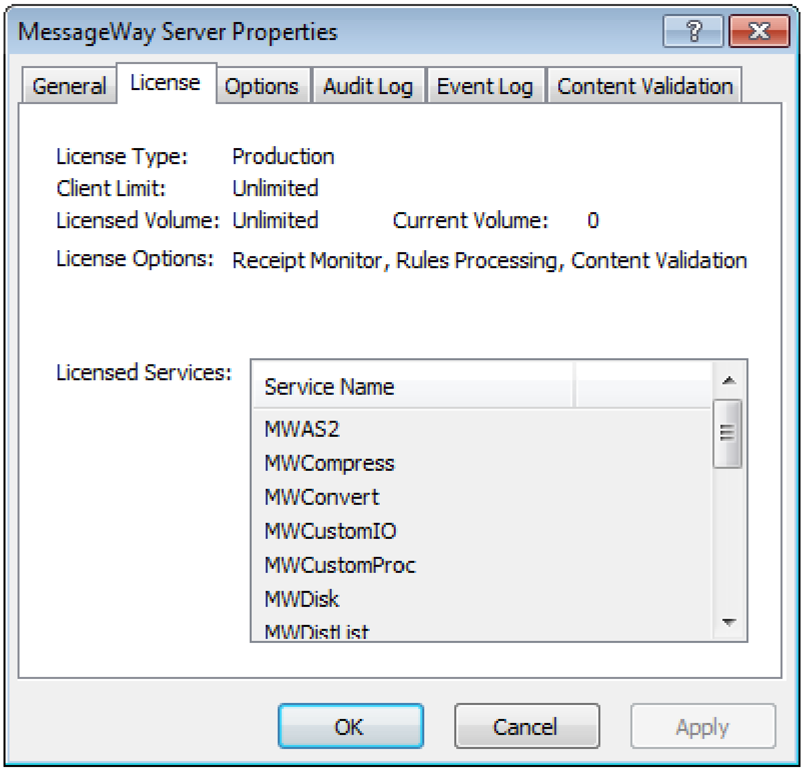
MessageWay Messaging Server, tracing starts as soon as you enter your trace options and click **Apply** or **OK**. When you have finished debugging, clear the field of all text to turn off the trace. If there is an asterisk in a trace field of core or other active servers when MessageWay starts, you risk overwhelming your system with trace activity.

For more information, refer to the topic for servers in general, ***Trace*** (on page 1315).

NOTE: To trace activity for the MessageWay Server, you must stop and start the server.

(MessageWay Server Properties) License Page

The **License** page of the MessageWay Server Properties window allows users to view license information. All fields are display-only.



License Type: Production
Client Limit: Unlimited
Licensed Volume: Unlimited Current Volume: 0
License Options: Receipt Monitor, Rules Processing, Content Validation

Licensed Services:

Service Name
MWAS2
MWCompress
MWConvert
MWCustomIO
MWCustomProc
MWDisk
MWDistList

License Type

This is the type of license currently in use. For various options available, contact technical support.

Client Limit

This is the maximum number of output characters per month that you can process through the MessageWay Manager. Depending on the type of contract you have, this may have a number or the word, **Unlimited**.

Licensed Volume

This is the maximum number of output characters per month that you can process through MessageWay. Depending on the type of contract you have, this may have a number or the word **unlimited**.

Current Volume

This is the current number of output bytes that you have processed through MessageWay.

Licensed Options

Options that have been purchased or otherwise activated for MessageWay appear on the **Licenses** page. For more information about purchasable options that are available, refer to the topic, "Features" in the "Getting Started" section.

Licensed Services

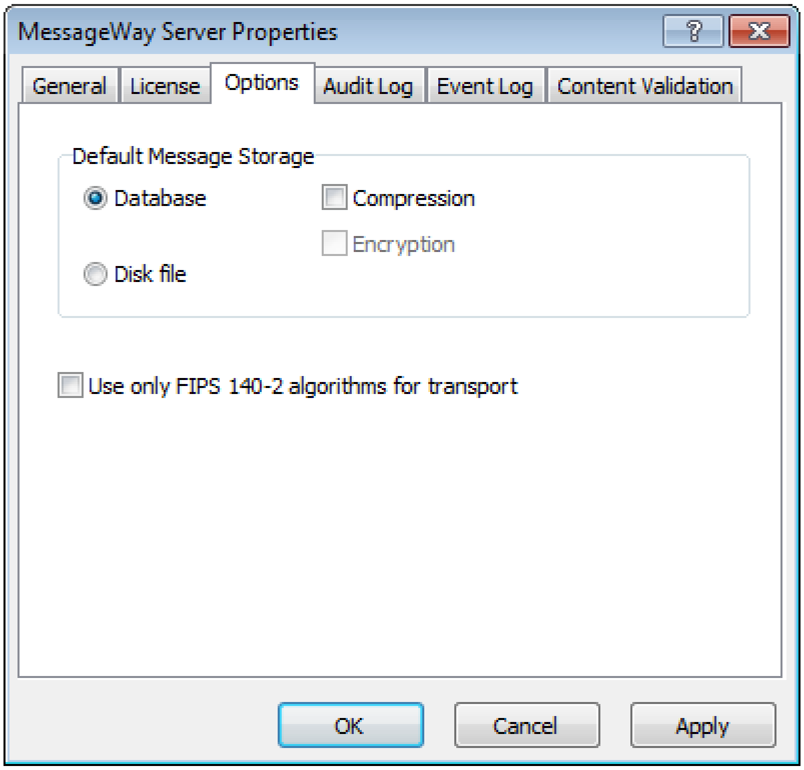
This is a list of licenses provided in the license file.

(MessageWay Server Properties) Options Page

The **Options** page of the MessageWay Server Properties window allows users to choose where they want to store message content, in the database or on disk, and if in the database, whether to compress or encrypt the data.

IMPORTANT: When you send messages to a distribution list for delivery to multiple locations, the storage option on the Distribution List Service Location is what determines how a message is stored, not the option on the final destination location. This is because the message is stored once, and the final destination locations point back to the original message sent to the distribution list.

The **Encryption** field is dimmed until a user ***adds a master key*** (on page 834).



Default Message Storage

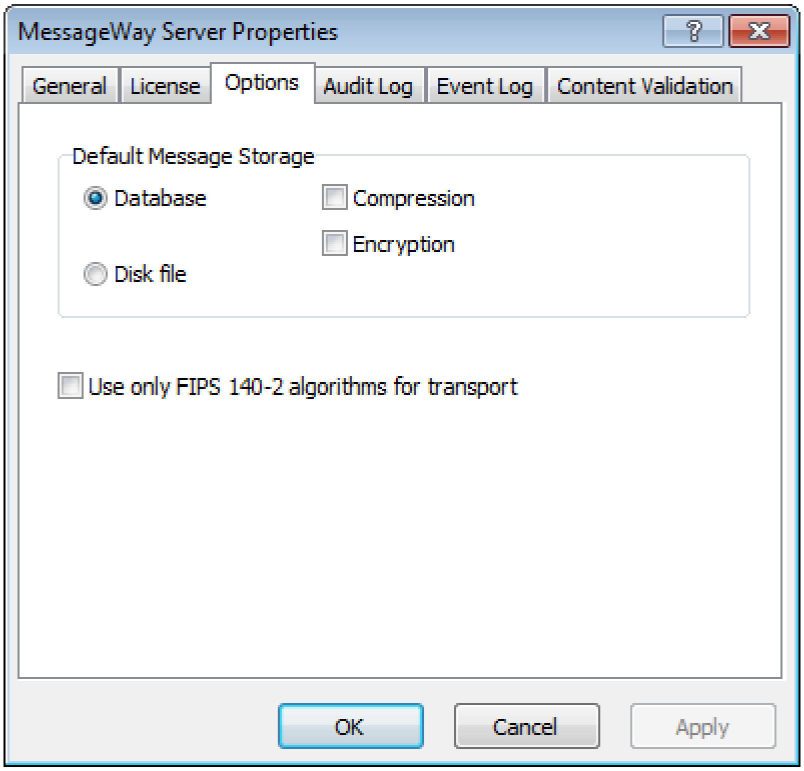
● Database □ Compression

□ Encryption

○ Disk file

□ Use only FIPS 140-2 algorithms for transport

The **Encryption** field is available after a user adds a master key.



Default Message Storage

● Database □ Compression

□ Encryption

○ Disk file

□ Use only FIPS 140-2 algorithms for transport

Database

Select the *Database* option to store the content of messages in the MessageWay database, rather than on disk. You may override this default for a specific location.

Compression

Check this box to compress the data for storage in the MessageWay database. You may override this default for a specific location.

Encryption

Check this box to encrypt the content data when it is stored in the MessageWay database. Data is encrypted using the Advanced Encryption Standard (AES). This field is dimmed until a user adds a master key using the mwadmin utility. You may override this default for a specific location.

CAUTION (UNIX/Linux): For MessageWay systems configured to encrypt data content in the database, if you run the archive process from a custom processing service location, as we do from the {Archive} location, instead of from the command line, you must have a ***passphrase file*** (on page 835). To initiate the archive process, the encryption password must be saved as a file, because this process cannot be prompted for the password.

Disk File

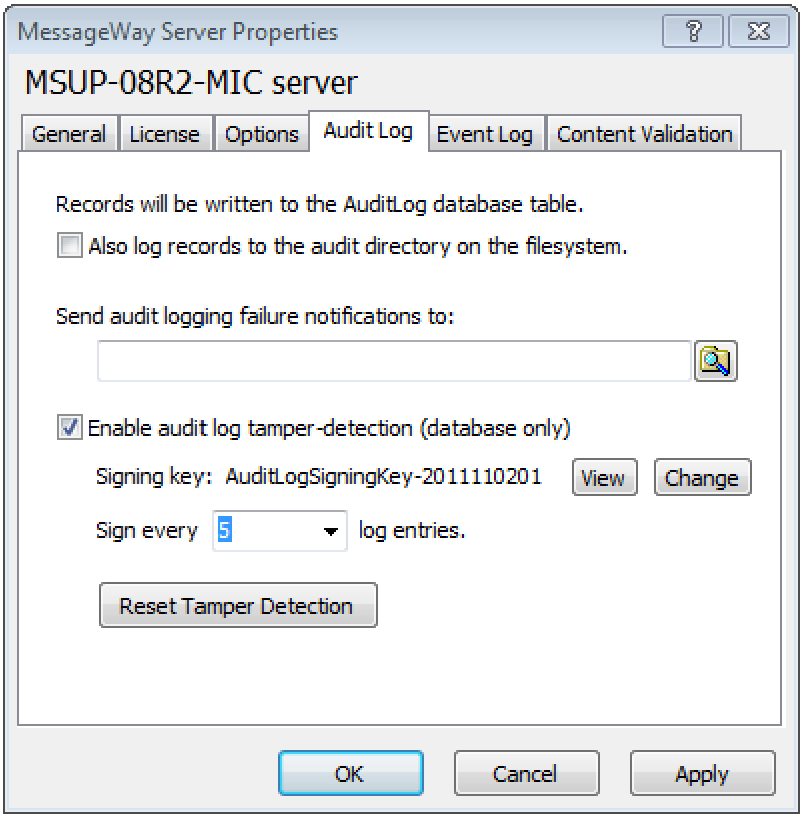
Select the *Disk* option to store the content of messages on disk. You may override this default for a specific location.

Use only FIPS 140-2 algorithms for tranport

When this box is checked, which is the default for new installations of MessageWay, all secure FTP, HTTP, and SFTP message transfers to and from MessageWay will use FIPS 140-2 encryption algorithms. This setting overrides any other encryption algorithm settings for adapters and MessageWay servers.

(MessageWay Server Properties) Audit Log Page

The **Audit Log** page of the MessageWay Server Properties window allows users to configure logging settings for the Audit Log.



Records will be written to the AuditLog database table.

□ Also log records to the audit directory on the filesystem.

Send audit logging failure notifications to:

☑ Enable audit log tamper-detection (database only)

Signing key: AuditLogSigningKey-2011110201

Sign every 5 log entries.

You can select an option to also log entries to the audit directory (C:\MessageWay\Audit), which is the pre-v6.0 method.

Log tables will be periodically pruned, and old entries optionally archived via the MWArchive custom process.

Also log records to the audit directory on the filesystem (MessageWay Server Properties, Audit Log)

In addition to logging to the database table, also logs records to the audit directory. The default for a new install is to log to the database only. The default for an upgrade install is to select this option, for backwards compatibility.

Send audit logging failure notifications to (MessageWay Server Properties, Audit Log)

If Messageway fails to log an audit record, send a notification to the selected location. In most cases, this failure would occur only if the MessageWay database is down. The location can be configured as an email distribution to send the notification to appropriate email addresses.

Enable audit log tamper-detection (database only) (MessageWay Server Properties, Audit Log)

This is a security feature that enables the hashing and signing of audit logs, to allow for detection of log record tampering.

Signing Key (MessageWay Server Properties, Audit Log)

This shows which signing key (a randomly- generated RSA key) is currently being used to sign audit log records.

View Key (MessageWay Server Properties, Audit Log)

Opens the properties dialog for the current signing key, allowing the user to view the public portion of the key. The public portion of this key can be used to verify the audit log hash signatures if desired.

Change Key (MessageWay Server Properties, Audit Log)

Triggers MessageWay to automatically generate a new signing key. After a new key is generated, a system restart is required. MessageWay will not notify the currently running servers to switch keys.

Sign every nn log entries (MessageWay Server Properties, Audit Log)

Determines how often a log entry will be signed. The larger the number, the more records will be logged between signatures, improving performance, but increasing the potential number of log records that will not be verifiable in the event of a system failure.

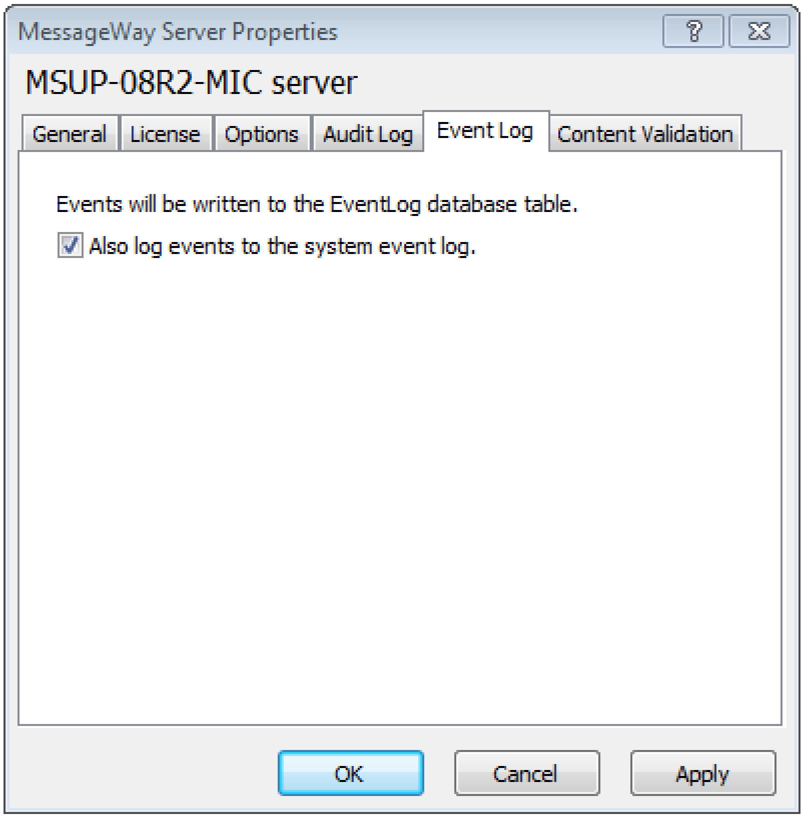
Reset Tamper Detection (MessageWay Server Properties, Audit Log)

Triggers MessageWay to close the current hash chains, log a special "Tamper Detection Reset" record indicating that tamper detection has been reset, and begin a new hash chain. The special record indicates to the validation program that audit records prior to this record should not be checked. This might be used in case tampering is found, to reset the detection so previous errors are not rediscovered.

(MessageWay Server Properties) Event Log Page

To support the centralized logging feature (new with v6.0), events reported to the operating system, such as server startup and shutdown, are logged to the MessageWay database, in the EventLog Table.

The **Event Log** page of the MessageWay Server Properties window allows users to configure logging settings.



Events will be written to the EventLog database table.

☑ Also log events to the system event log.

In addition to the database table, by default, events are also logged to the system log (syslog on UNIX, Event Log on Windows), which is the pre-v.6.0 method. We recommend this default setting so that events continue to be written to the system log, particularly in the event of a MessageWay database failure.

Log tables will be periodically pruned, and old entries optionally archived via the {Archive} custom process and reports written to the {ArchiveReports} location.

You can search for and view log entries using the ***Search, Find Logs, Find Event Logs*** (on page 777) features.

Also log events to the system even log (MessageWay Server Properties, Event Log)

In addition to the database table, also logs events to the system log (syslog on UNIX, Event Log on Windows). The default setting is to select this option, so that events continue to be written to the system log, particularly in the event of a MessageWay database failure.

(MessageWay Server Properties) Content Validation Page

The Content Validation page of the MessageWay Server Properties allows users to configure MessageWay to scan messages for viruses by integrating a third-party virus scanner.

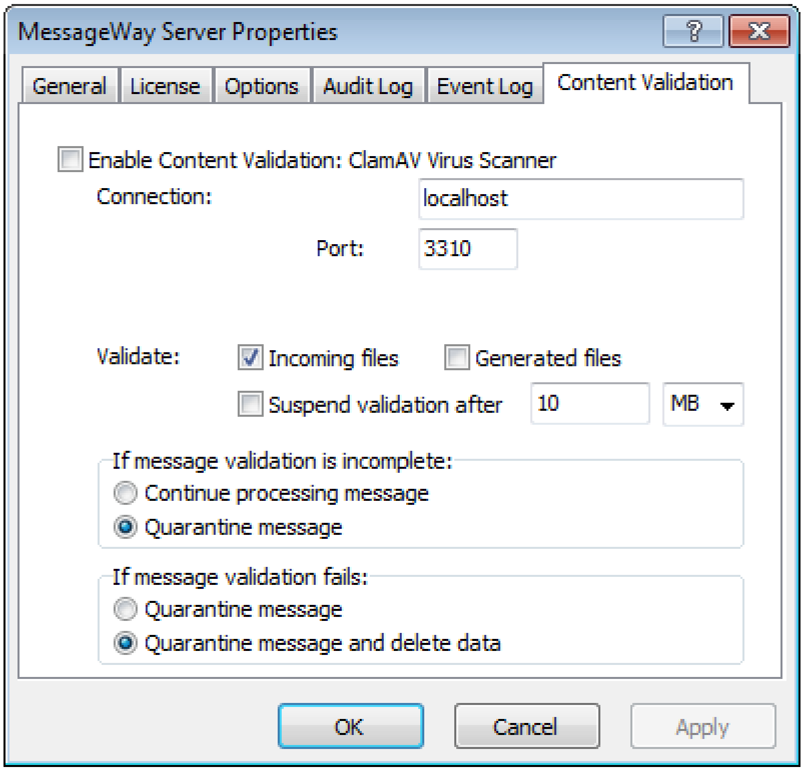
After you enable content validation and configure the connection to the antivirus scanner, MessageWay will scan messages for viruses using the default settings on this page. By default, MessageWay will scan incoming messages (files), if message validation succeeds, the message moves to the next step in the message flow. If message validation fails (indicating a virus was found), MessageWay will quarantine the message, and (optionally) delete the associated data. If message validation is incomplete, MessageWay will (optionally) quarantine the message by moving it to the system-level {Quarantine} mailbox.

You can change the default settings as required.

Best Practice

By default, when message validation fails, the data associated with the message is deleted. This setting (**Quarantine message and delete data**) is recommended. If the **Quarantine message** alternative is selected, the message is quarantined, but the associated data is delivered to the destination. The message header information can always be found in the {Quarantine} mailbox.

The only difference between the Windows and UNIX/Linux environments are the Connection properties. The following is a Windows example.



□ Enable Content Validation: ClamAV Virus Scanner

Connection: localhost

Port: 3310

Validate: ☑ Incoming files □ Generated files

□ Suspend validation after 10 MB

If message validation is incomplete:

○ Continue processing message

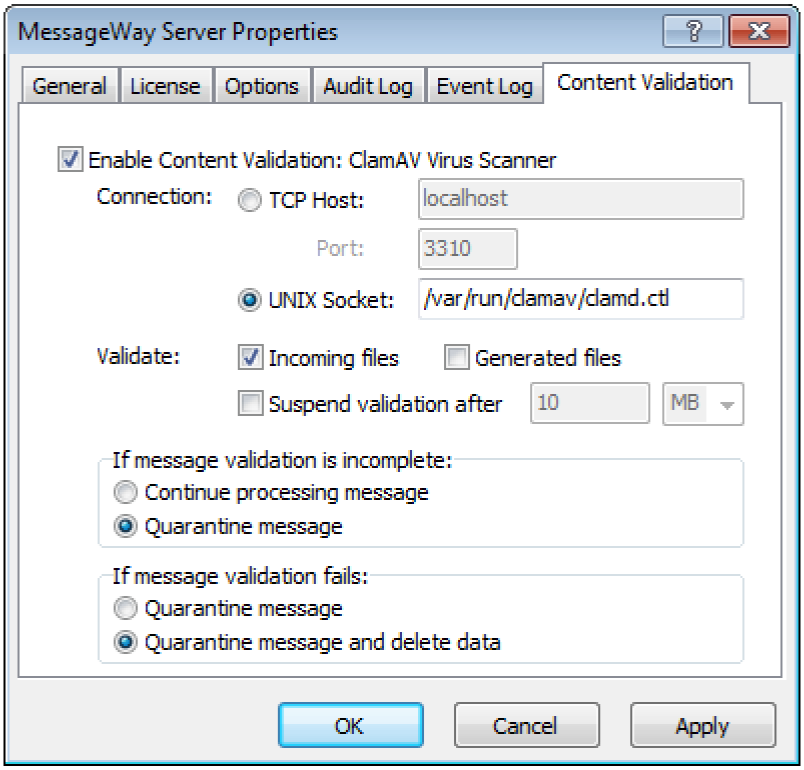
● Quarantine message

If message validation fails:

○ Quarantine message

● Quarantine message and delete data

With UNIX/Linux environments, you also have the choice of connecting using a UNIX socket.



☑ Enable Content Validation: ClamAV Virus Scanner

Connection: ○ TCP Host: localhost

Port: 3310

● UNIX Socket: /var/run/clamav/clamd.ctl

Validate: ☑ Incoming files ☐ Generated files

☐ Suspend validation after 10 MB

If message validation is incomplete:

○ Continue processing message

● Quarantine message

If message validation fails:

○ Quarantine message

● Quarantine message and delete data

NOTE: MessageWay Content Validation requires a license from Progress. This tab appears when you have the licensed option. For more information, contact MessageWay Technical Support.

Enable Content Validation (MessageWay Server Properties, Content Validation)

Check the *Enable Content Validation* box to enable scanning of messages for viruses. When you first enable Content Validation, you will need to configure the *Connection* to the antivirus server.

Connection (MessageWay Server Properties, Content Validation)

The *Connection* specifies the location where the embedded anti-virus engine will listen for a request to scan messages. Depending on your operating system, you will see one or both of these options:

- **UNIX Socket**: Enter the file location of the embedded anti-virus engine
- **TCP Host and Port**: Enter the IP address and port number for the embedded anti-virus engine; for example: TCP Host: localhost Port: 3310

Validate (MessageWay Server Properties, Content Validation)

Select which types of files you want to scan for viruses, and whether you want to limit the scan based on file size.

- **Incoming**: Select this option to enable scanning of files (messages) coming into MessageWay via an adapter or the Service Interface, for example, files uploaded via FTP, SFTP, AS2.
- **Generated Files**: Select this option to enable scanning of files generated within MessageWay, for example files that are transformed by the compression service or the translation service.
- **Suspend validation after**: If enabled, a file will be scanned until the specified byte size is reached. When the limit is reached, MessageWay stops submitting data to the scanner and sets the file's validation status to "Incomplete."

By default, an Incomplete file (message) is quarantined, as set in the **If message validation is incomplete** option.

Note: The **Suspend validation after** size can also be set in the embedded anti-virus configuration file by using the StreamMaxLength option. If the option is set here and in the configuration file, the lesser of the two settings will be used.

Note: A message that is a 0 byte file will not be scanned and the validation status will be set to "Not Required." (0 bytes files can be used as part of a message flow to indicate that a process is completed or is ready to start).

If message validation is incomplete (MessageWay Server Properties, Content Validation)

If MessageWay is unable to complete validation of a message, the validation status is set to "Incomplete." Examples of messages with validation status of "Incomplete" include messages that are larger than the size set in the **Suspend validation after** option; and messages not scanned because MessageWay could not connect to the antivirus service.

If message validation is incomplete, MessageWay can take one of these actions:

- **Continue processing message**: Select this option if you want to ignore the incomplete validation status of the message and continue to the next step in the message flow.
- **Quarantine message**: By default, the message is placed in the {Quarantine} location, which is a system-level mailbox.

Message status and validation results are reported on the Message Properties, Data Validation tab.

If message validation fails (MessageWay Server Properties, Content Validation)

If message validation fails, MessageWay can take one of these actions:

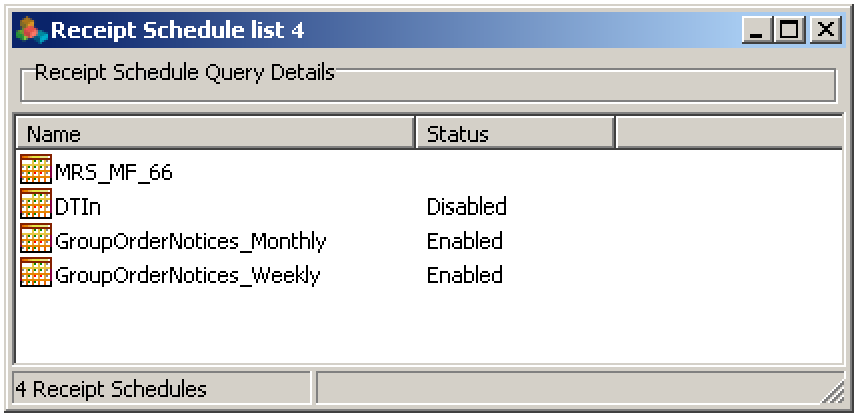
- **Quarantine message and delete data**: By default, if a message has a virus, MessageWay quarantines the message and deletes the content data associated with the message. The message detail record remains on the system.
- **Quarantine message**: Select this option if you want MessageWay to put the message in the {Quarantine} location (a system-level mailbox), but not delete the message content data.

Message status and validation results are reported on the Message Properties, Data Validation tab.

Receipt Schedule List Window

The Receipt Schedule List window appears when you use the **Find Receipt Schedules** command to search for receipt schedules, which include holiday schedules, master receipt schedules and receipt schedules. When you search through multi-system environments, a System Name column also appears.

To sort by column content, click the column heading. For more information about the columns, refer to the topic, ***Receipt Monitor Schedules (MessageWay Explorer)*** (on page 1222).



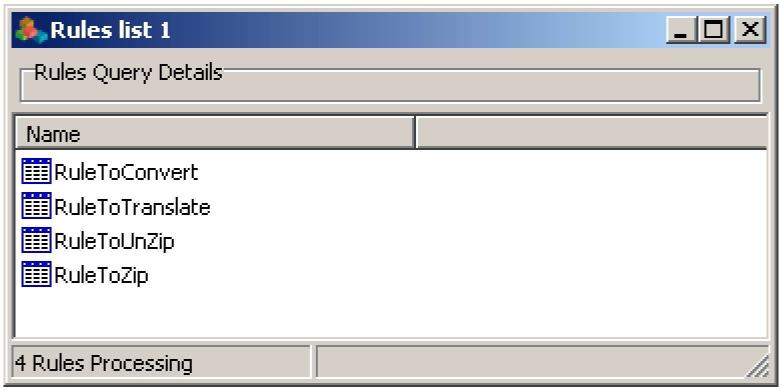
Name	Status
MRS_MF_66	
DTIn	Disabled
GroupOrderNotices_Monthly	Enabled
GroupOrderNotices_Weekly	Enabled

4 Receipt Schedules

Rules List Window

The Rules List window appears when you use the **Find Rules** command. When you search through multi-system environments, a System Name column also appears.

To sort by column content, click the column heading. For more information about the columns, refer to the topic, ***Rules Processing Profile Window*** (on page 1262).



Name
RuleToConvert
RuleToTranslate
RuleToUnZip
RuleToZip

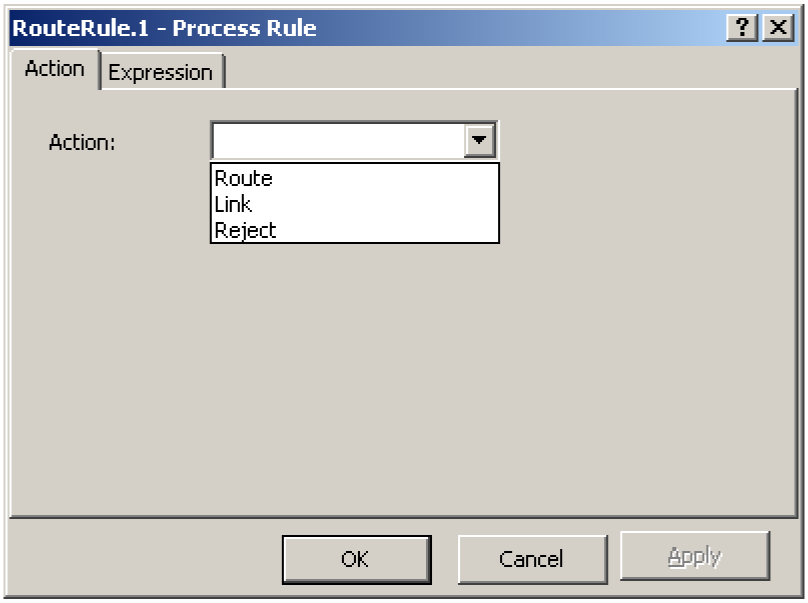
4 Rules Processing

(Rules Processing) Process Rule Window

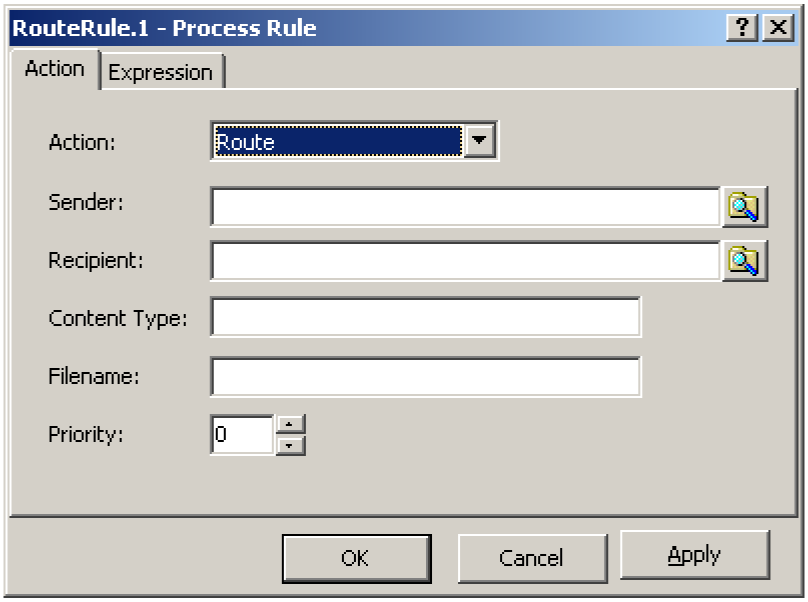
You access the Process Rule window from the **General** page of the Rules Processing Profile window. When you select the **Add** button or select a definition and the **Edit** button, the Process Rule window appears.

(Process Rule) Action Page

The **Action** page of the Process Rule window specifies the action that will be performed when one of the definitions matches. What appears on the page depends on the action selected, since each action requires different settings.



Action Page (Process Rule Window)



Action: Route

Sender:

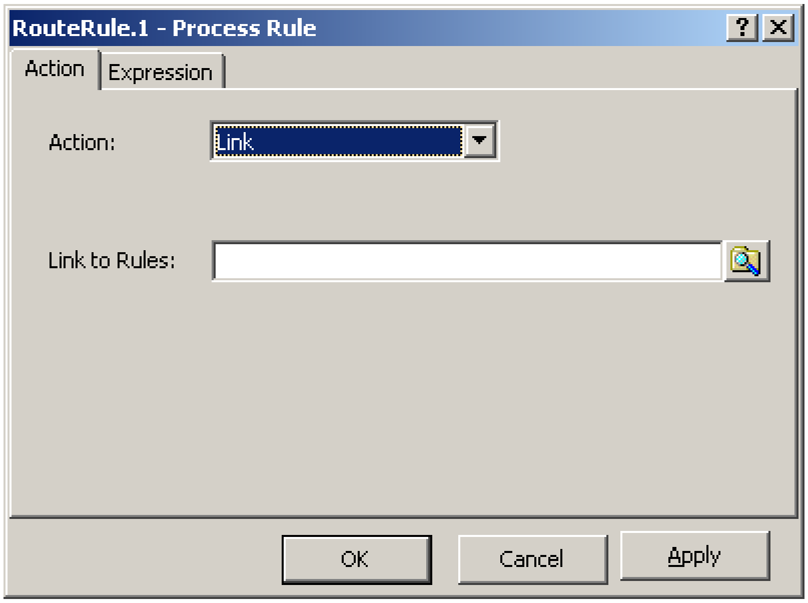
Recipient:

Content Type:

Filename:

Priority: 0

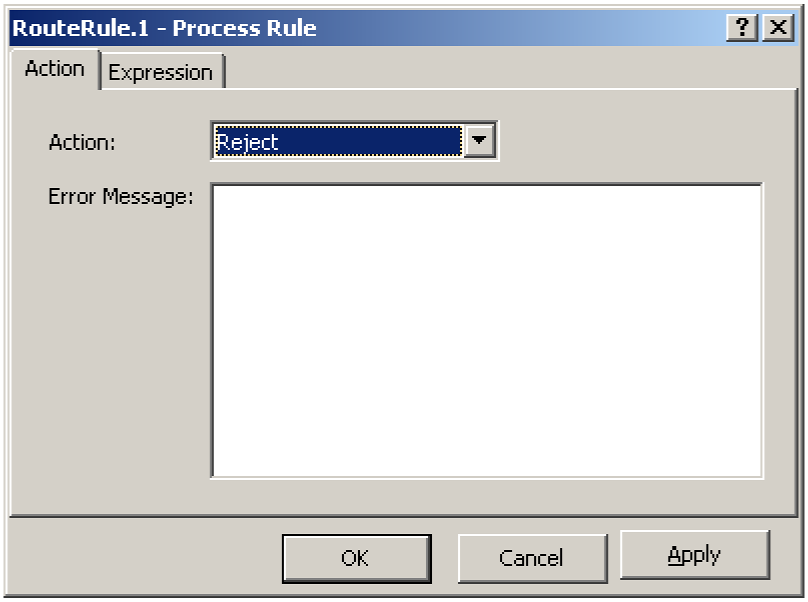
Action Page with Route Action (Process Rule Window)



Action: Link

Link to Rules:

Action Page with Link Action (Process Rule Window)



Action: Reject

Error Message:

Action Page with Reject Action (Process Rule Window)

Action

Select the routing action that you want to perform when this definition applies: Route, Link or Reject.

Action	Description
Route	Route this message to the specified location.
Link	Link to another table to apply additional definitions.
Reject	Reject this message and notify the sender using the specified text. When a message is rejected, no output message is created, and the input message has a status of error.

Sender

When you select the Route action, you may specify a location representing the sender that will override the current source location. You may also use any available tokens to specify the sender. This might be useful when you are sending files to MWTranslator, which may be configured to receive files from specified source locations.

Select Location Button

Click this button to select from a list of valid locations.

Recipient

When you select the Route action, you may specify a destination location. However, this will not override a recipient/to compound address defined on the input location. You may also use any available tokens to specify the recipient. Be aware that when the location does not exist, MessageWay sends the message to the system mailbox, {Unknown}. You may also use this field to assign a class ID, using the notation, *classID***@***recipient*.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

Content Type

You may assign or override an existing content type for the message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.

The following is a list of content types that MessageWay supports.

Type	Content Type	File Extension
ZIP	application/zip	zip
GZIP	application/gzip	gz
PDF	application/pdf	pdf
BMP	image/bmp	bmp
JPEG	image/jpeg	jpeg
PNG	image/png	png
TIFF	image/tiff	tiff
GIF	image/gif	gif
X12	application/edi-x12	x12
EDIFACT	application/edifact	edf
TEXT	text/plain	txt
XML	application/xml	xml
MPEG	video/mpeg	mpeg

Type	Content Type	File Extension
Lotus 123	application/vnd.lotus-1-2-3	wk4
MS Powerpoint	application/vnd.ms-powerpoint	ppt
MS Excel	application/vnd.ms-excel	xls
Real Media	application/vnd.realmedia	rm
Real Audio	audio/vnd.rn-realaudio	ra
Sun audio files	audio/basic	au
MS WMV, WMA, ASFfiles	video/x-ms-wmv	wmv
Photoshop files	image/x-psd	psd
BZIP	application/x-bzip	bz2
Shockwave flash	application/x-shockwave-flash	swf
AIFF	audio/x-aiff	aiff
MP3	audio/mpeg	mp3
HP Laser printer-compatible file (Printer Control Language)	application/vnd.hp-pcl	pcl
AVI	video/x-msvideo	avi
WAV	audio/x-wav	wav
Quicktime	video/quicktime	mov

Filename

Type a name to override the filename for the message. You may also use any available tokens to specify the filename. Note that when you use these tokens to form a filename, the values will come from the input message where they exist. For example, %classid% will resolve to the class ID from the input message. If you have assigned a class ID to the output message in the Recipient box, and you also want to assign this class ID to the filename, use the same literals you used for the class ID in the Recipient box. For example where *abc* is the class ID, if you typed *abc@mylocation* in the Recipient box, also type *abc@%yyyymmdd%.txt* in the Filename box.

The valid tokens are:

Token	Description
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.

Token	Description
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: **MyClassID@MyLocationName** To assign a class ID to a mask for a file name, type: **MyClassID%yyyymmdd%.txt**
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).
inputmsgid	Input Message Id of the message.
inputname	Input Name.
location	The MessageWay location where the message resides. Replaces *mailbox*.
msgid	The Message Id of the message. Replaces *msg*.

Token	Description
ms	Milliseconds (000-999). **NOTE:** The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.
yyyy	Four digit year.
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

```
MW%msgid%.txt
```

```
TR%yyyymmddhhnnss#%.txt
```

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

```
%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml
```

TIP: On systems that allow file names longer than 8 characters, use the *msgid* token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the *filename* token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  `\ / : * ? " < > | ! & ` ' ;`

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

- Duplicate Filename values are allowed within the same location within the Locations folder.

Duplicate Filenames are *not* allowed within the same location within the File System folder, unless one has been canceled.

Priority

When you select the Route action, you may specify a priority to override the current priority of the message, which typically is the default priority specified on the destination location. Enter or select a priority from 1 (lowest) to 5 (highest).

Link to Rules

When you select the Link action, you must specify a process rule that will provide additional filters to apply to this message. Type or select the rule to which you want to link.

Browse Button for Rules

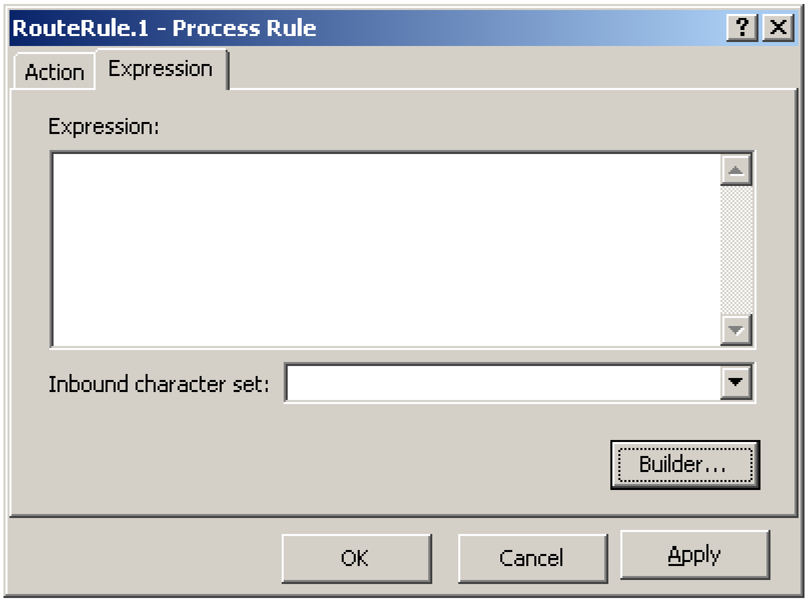
Click this button to select from a list of current rules.

Error Message

When you select the Reject action, you may provide text that will appear on the Misc page of the Message Properties window. This should be something useful for operators to troubleshoot the problem.

(Process Rule) Expression Page

The **Expression** page of the Process Rule window shows the syntax of the rule that will be executed to perform the action on the **Action** page. You may type the syntax directly in the Routing Expression box or select the **Builder** button to use the Expression Builder window.



Expression Page (Process Rule Window)

Expression

If you are familiar with the syntax of process rules, you may type them in this box. You may also select the **Builder** button to let the syntax builder create the syntax based on your selections. To delete a rule, select it and press **Delete**.

EDIT TIP: Expressions can become very complex, with hundreds of routing rules with multiple AND/OR conditions each. The best way to reorder the routing rules or conditions, delete individual routing rules or conditions, or insert new routing rules or conditions is with a text editor. Copy the entire contents of the expression window to a text file and use a text editor to make changes to the routing rules or conditions. Once changes are complete, copy the entire contents of the text file back into the expression window and save the changes. Best practice would be to save the contents of the expression window before making any changes.

Inbound Character Set

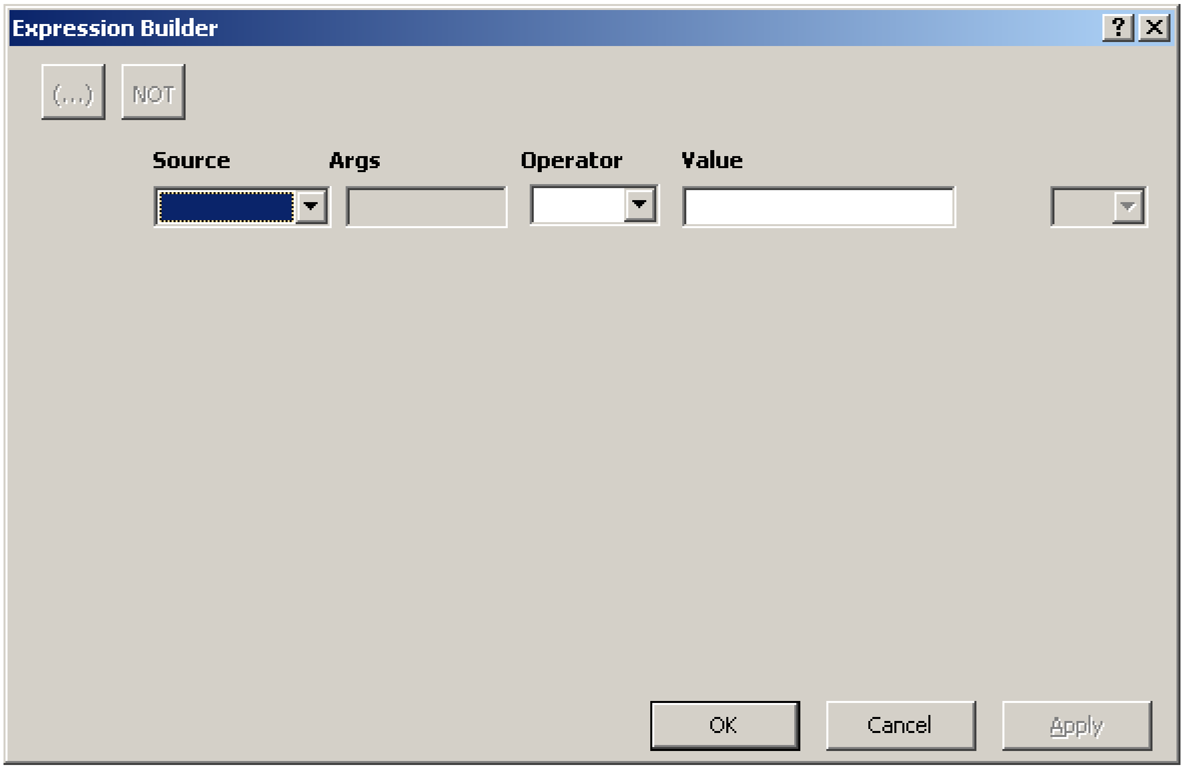
Select the character set for the input data. ASCII is the default when no character set is selected. This character set will be used to match any data you have used in a rule, either by typing a value directly in the **Expression** box or by typing it in the **Value** box of the Expression Builder. To see that you have typed the correct value, you should use the same character set for your keyboard as selected in this field when you type the value.

Builder Button

Click the **Builder** button to let the expression builder create the syntax of a rule based on your choices. This opens the Expression Builder window.

(Rules Processing) Expression Builder Window

The Expression Builder window allows you to create expressions for MessageWay to route a message based on the content or characteristics of a message. When you use the Expression Builder, you may choose among various options to create the expression. The expression is then generated using correct syntax and added to the **Expression** box on the Rules Processing Profile window.



You access the Expression Builder window from the **Expression** page of the Process Rule window. When you select the **Builder** button, the Expression Builder window appears.

Source

Select the type of input you want to use for comparison.

The options are as follows:

Source	**Description**
Data Type	Based on message content, MessageWay will automatically identify one of the following data types: X12, EDIFACT, XML, ZIP, UNKNOWN, UTF-8, UTF-16BE, UTF-16LE, UTF-32BE, and UTF-32LE. MessageWay uses the basic syntax rules of these standards or conventions to identify the data.
Size	Length of the message in bytes
Sender	MessageWay determines the sender, which might be the input location, or it might be a value sent by the input adapter, or it might have been determined by a service, such as MWTranslator. **CAUTION:** This value is case-sensitive. The sender will not match the data unless the case is correct. If you are not sure of the case, use a lowercase *i* before the sender, which itself should be within double quotation marks, for example, **i"x850test"**.
Recipient	MessageWay determines the recipient from a compound address when it is used on the input location. Recipient may only be used when the input location contains a compound address in the **Deliver To** or **Recipient** box. **CAUTION:** This value is case-sensitive. The recipient will not match the data unless the case is correct. If you are not sure of the case, use a lowercase *i* before the recipient, which itself should be within double quotation marks, for example, **i"mwtranslator"**.
Filename	The MessageWay filename of the input message
InputName	The MessageWay input filename of the input message
ClassID	The class ID assigned to the input message
ContentType	The content type assigned to the message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream. For more information about content types that MessageWay recognizes, refer to the topic, ***Content Type (Process Rule)*** (on page 1242)
Data	Input data content at a fixed offset and length
Ele	Input data content for a specific segment/element/subelement position, which would typically be X12 or EDIFACT data.
XPath	XML data content using a subset of XPath notation

Args

When MessageWay parses the data, the only assumptions it can make are those based on specific standards, such as X12 or EDIFACT, or conventions, such as XML or ZIP. When you enter arguments for comparison, remember that MessageWay will use syntax rules if it knows the standard or convention or it will count bytes.

Enter the arguments for the type of input you want to use for comparison. The square brackets [and] enclose optional items. The signs < and > enclose names that describe the type of value actually used. Special characters that are part of the syntax, such as brackets or commas, are highlighted.

The options are as follows:

Source	Arguments	Example
Data Type	None	
Size	None	
Sender	None	
Recipient	None	
Filename	None	
InputName	None	
Data	<offset>**,** <length>	0, 1023
Ele	<SegmentNum>**,** <ElementNum>**,** <SubElementNum> [**,** **"**<SegmentTerminatorVal>**",** **"**<ElementDelimiterVal>**",** **"**<SubElementSeparatorVal>**"**] **IMPORTANT:** The double quotation marks around the values are required.	5, 1, 0 2,1,0, "~","*",":"
XPath	Subset of XPath notation: [**/**<ElementName>] [**//**<ElementName>] **/**<ElementName> [**[**<Predicate>**]**] [**/@**<AttributeName>]	/Document/Line/@ID /PO/Address[@ID='SE']/Name

Operator

Enter the operator you want to use for comparison.

The options are as follows:

Operator	Description
=	Input data must equal the value.
>	Input data must be greater than the value.

Operator	Description
>=	Input data must be greater than or equal to the value.
<	Input data must be less than the value.
<=	Input data must be less than or equal to the value.
<>	Input data must not be equal to the value.
contains	Input data must contain the value (not valid when Source is **Size**).
beginswith	Input data must begin with the value (not valid when Source is **Size**).
endswith	Input data must end with the value (not valid when Source is **Size**).
matches	Input data must match a regular expression in the value (RegEx).

RegEx Examples (matches)

Following are a few examples using the MWRules 'matches' operator with regular expressions (RegEx). For a complete list of supported RegEx metacharacters, operators and character classes, refer to the following URL:

https://presstige.io/p/Regular-Expressions-ICU-User-Guide-0eff0feb3f9f4cceb4428c00c5662e97

NOTE: All backslash (\) characters must be preceded by an additional backslash (\) character to escape it.

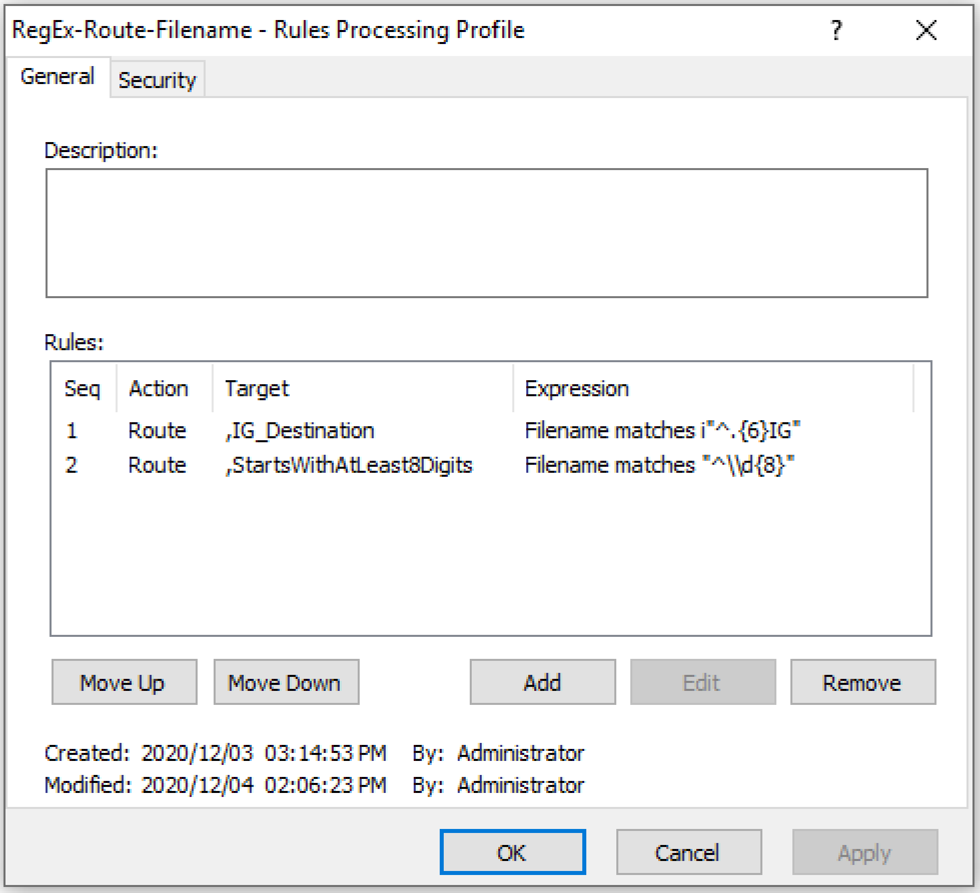
NOTE: To match on a literal character that is also one of the RegEx special characters that follows, two backslash characters (\\) must precede the character in the 'matches' syntax typed into the 'Value' field of the "Expression Builder":

* ? + [( ) { } ^ $ | .

NOTE: To match on a literal backslash (\), a total of four backslash characters (\\\\) must be used in the 'matches' syntax typed into the 'Value' field of the "Expression Builder".

NOTE: After typing consecutive backslashes in the "Expression Builder" and clicking OK, half of the backslashes will be removed from the "Expression Builder" 'Value' field but will still be visible in the 'Expression' window.

RegEx examples with Source of Filename:



RegEx-Route-Filename - Rules Processing Profile

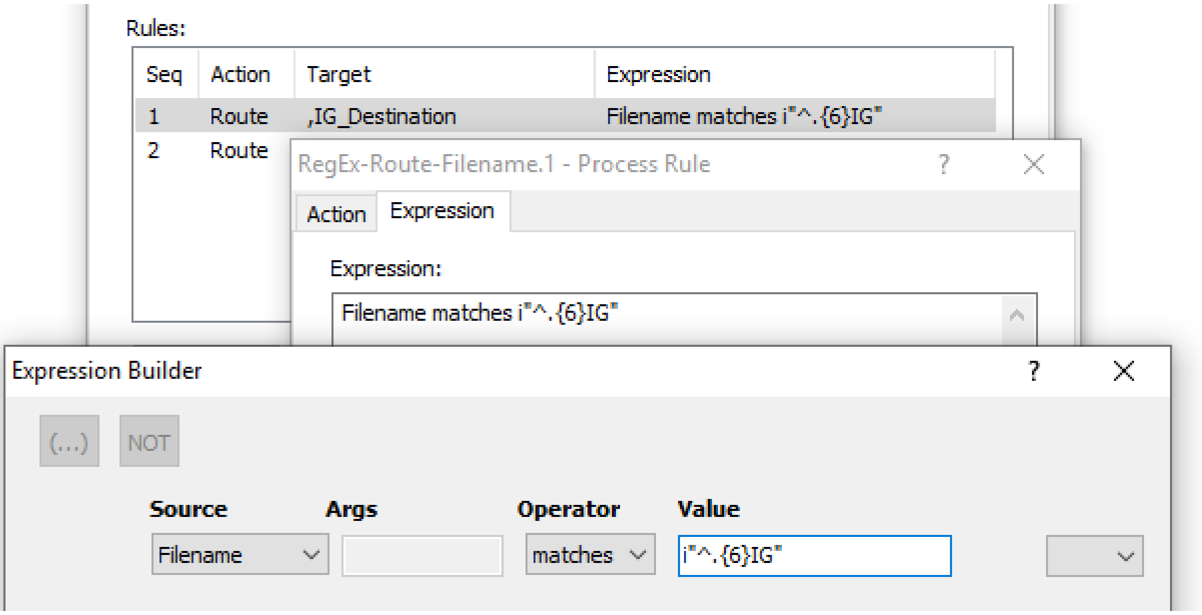
Description:

Rules:

Seq	Action	Target	Expression
1	Route	,IG_Destination	Filename matches i"^.{6}IG"
2	Route	,StartsWithAtLeast8Digits	Filename matches "^\\d{8}"

Created: 2020/12/03 03:14:53 PM By: Administrator
Modified: 2020/12/04 02:06:23 PM By: Administrator

Rules/Seq 1: Routes files where the filename begins with (^) six characters of any type followed by IG, case insensitive (i).



Rules:

Seq	Action	Target	Expression
1	Route	,IG_Destination	Filename matches i"^.{6}IG"
2	Route		

RegEx-Route-Filename.1 - Process Rule

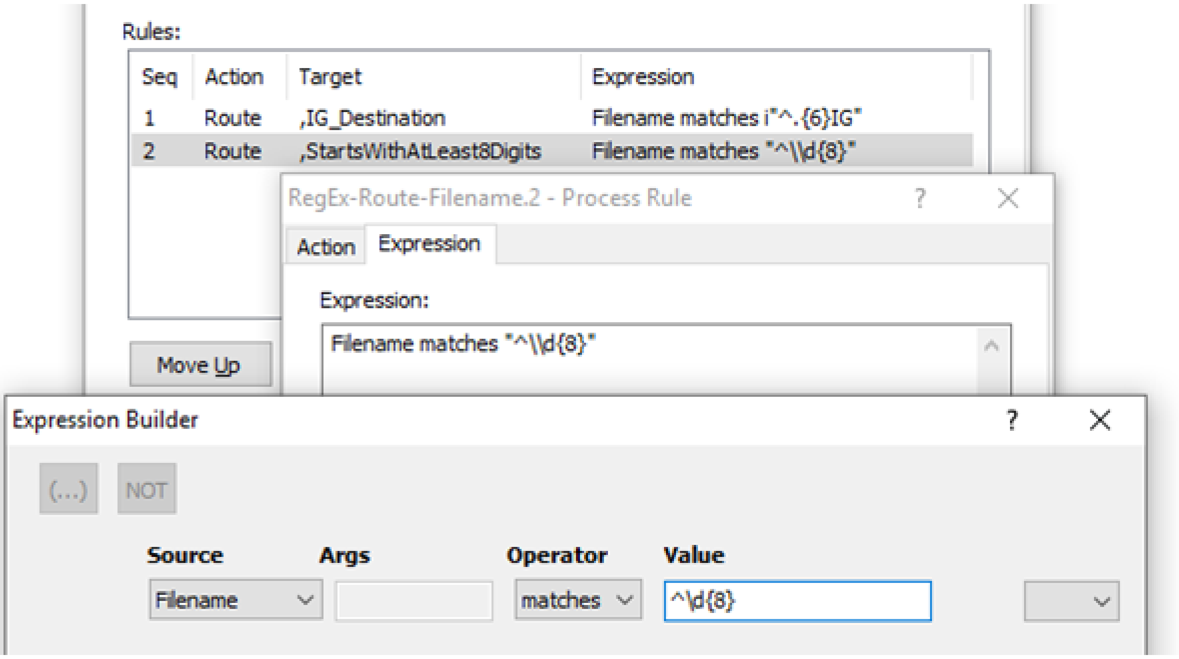
Expression:

```
Filename matches i"^.{6}IG"
```

Expression Builder

Source	Args	Operator	Value
Filename		matches	i"^.{6}IG"

Rules/Seq 2: Routes files where the filename begins with (^) at least eight digits (\d{8}).



Rules:

Seq	Action	Target	Expression
1	Route	,IG_Destination	Filename matches i"^.{6}IG"
2	Route	,StartsWithAtLeast8Digits	Filename matches "^\\d{8}"

RegEx-Route-Filename.2 - Process Rule

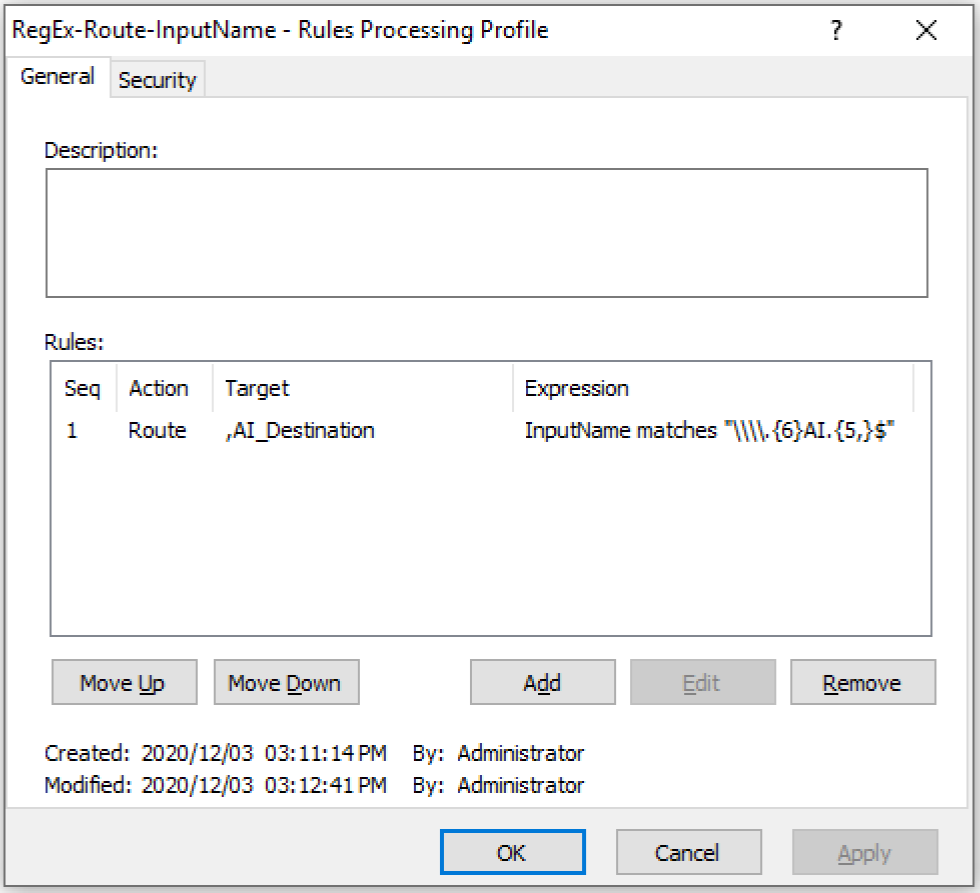
Expression:

```
Filename matches "^\\d{8}"
```

Expression Builder

Source	Args	Operator	Value
Filename		matches	^\d{8}

RegEx example with Source of InputName:



RegEx-Route-InputName - Rules Processing Profile

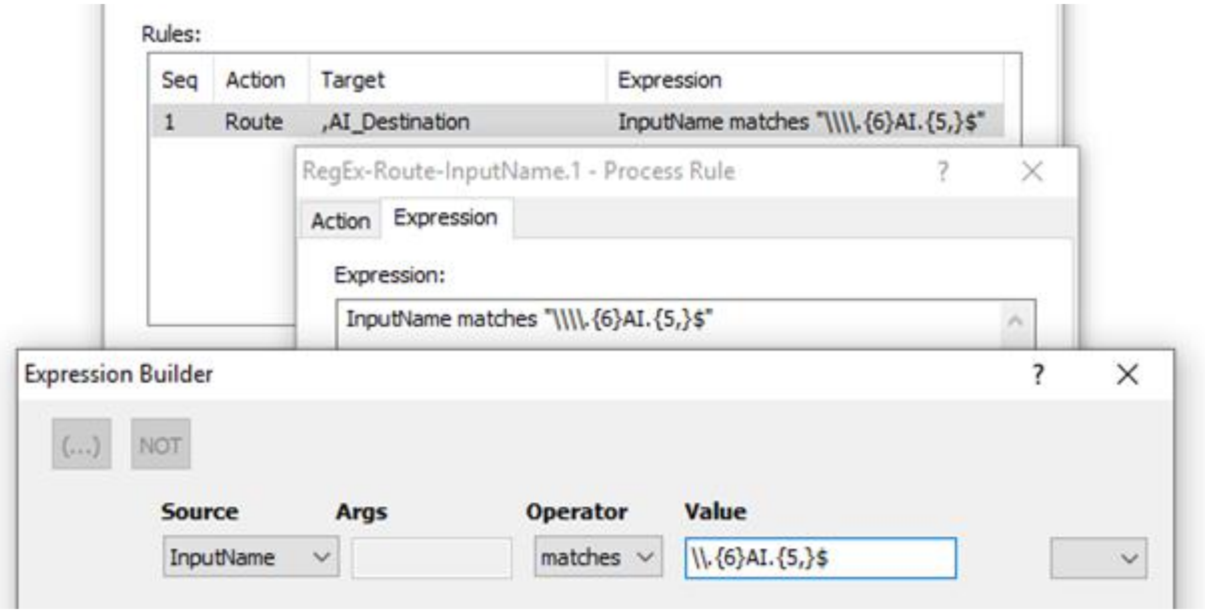
Description:

Rules:

Seq	Action	Target	Expression
1	Route	,AI_Destination	InputName matches "\\\\.{6}AI.{5,}$"

Created: 2020/12/03 03:11:14 PM By: Administrator
Modified: 2020/12/03 03:12:41 PM By: Administrator

Rules/Seq 1: Routes files where the input name ends with ($) a backslash (\\) followed by six characters of any type followed by AI followed by at least five characters of any type.



Rules:

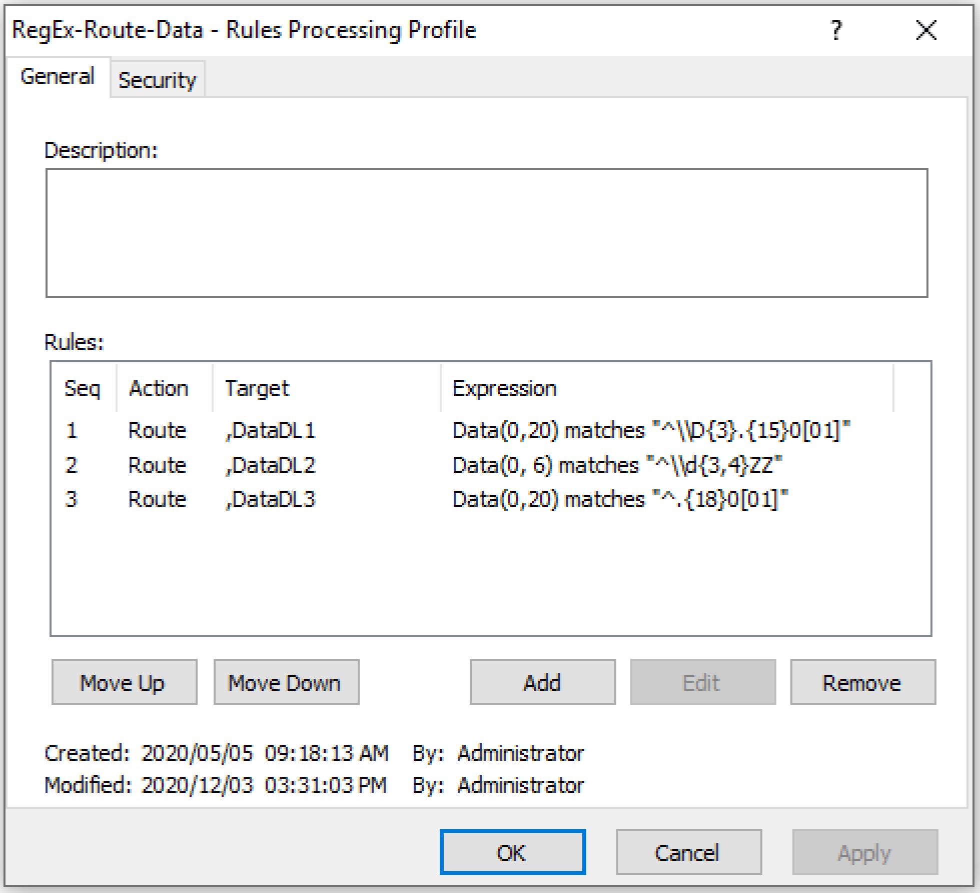
Seq	Action	Target	Expression
1	Route	,AI_Destination	InputName matches "\\\\\.{6}AI.{5,}$"

Expression:

```
InputName matches "\\\\\.{6}AI.{5,}$"
```

Source: InputName
Args:
Operator: matches
Value: \\\.{6}AI.{5,}$

RegEx examples with Source of Data:



RegEx-Route-Data - Rules Processing Profile

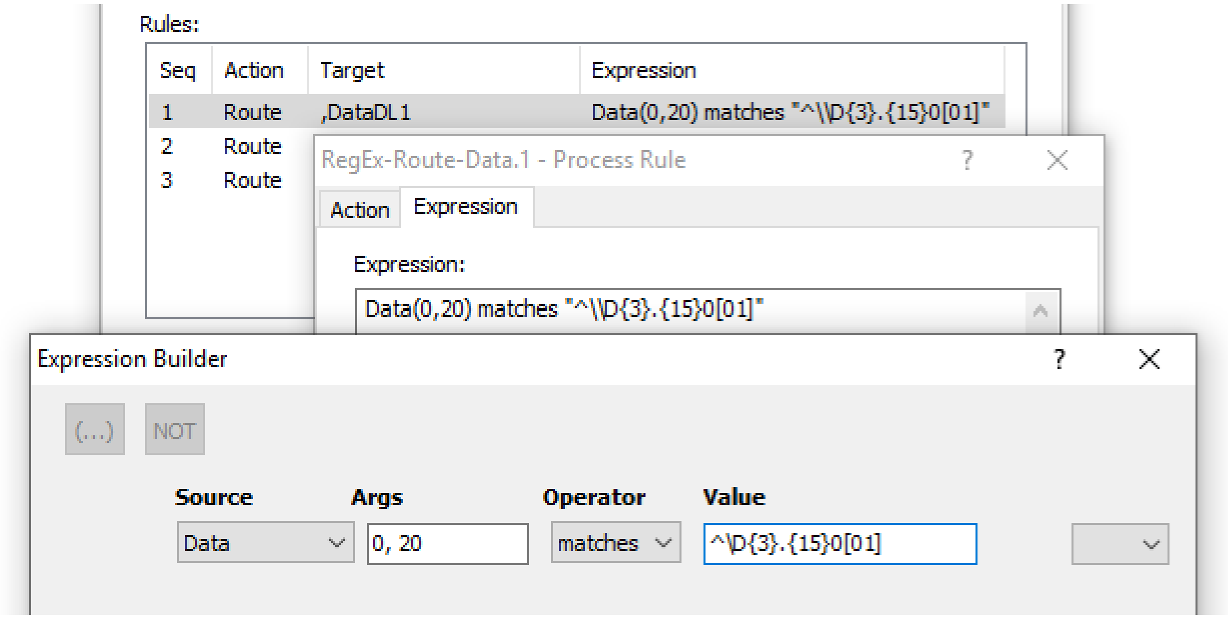
Description:

Rules:

Seq	Action	Target	Expression
1	Route	,DataDL1	Data(0,20) matches "^\\D{3}.{15}0[01]"
2	Route	,DataDL2	Data(0, 6) matches "^\\d{3,4}ZZ"
3	Route	,DataDL3	Data(0,20) matches "^.{18}0[01]"

Created: 2020/05/05 09:18:13 AM By: Administrator
Modified: 2020/12/03 03:31:03 PM By: Administrator

Rules/Seq 1: Routes files containing data where in the selected data range (offset 0 for a length of 20) the first (^) three characters are non-digits (\D{3}) followed by fifteen characters of any kind (.{15}) followed by either 00 or 01 (0[01]).



Rules:

Seq	Action	Target	Expression
1	Route	,DataDL1	Data(0,20) matches "^\\D{3}.{15}0[01]"
2	Route		
3	Route		

RegEx-Route-Data.1 - Process Rule

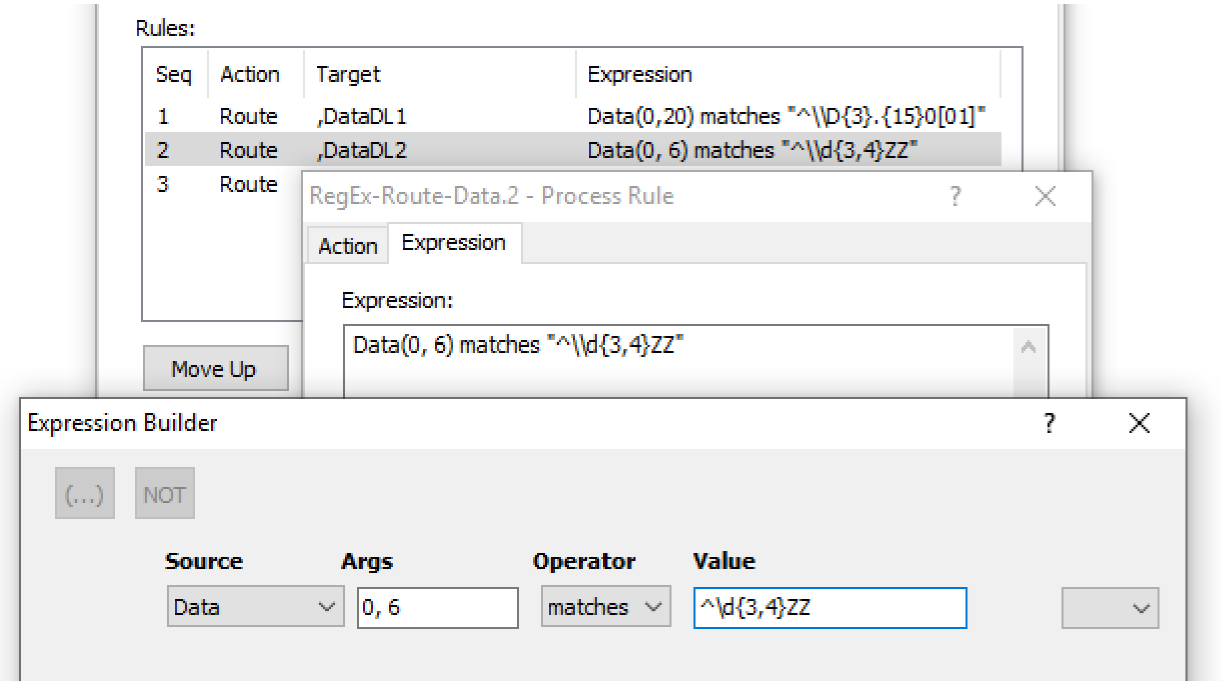
Expression:

Data(0,20) matches "^\\D{3}.{15}0[01]"

Expression Builder

Source	Args	Operator	Value
Data	0, 20	matches	^\D{3}.{15}0[01]

Rules/Seq 2: Routes files containing data where in the selected data range (offset 0 for a length of 6) the first (^) three or four characters are digits (\d{3,4}) followed by ZZ.



Rules:

Seq	Action	Target	Expression
1	Route	,DataDL1	Data(0,20) matches "^\\D{3}.{15}0[01]"
2	Route	,DataDL2	Data(0, 6) matches "^\\d{3,4}ZZ"
3	Route		

RegEx-Route-Data.2 - Process Rule

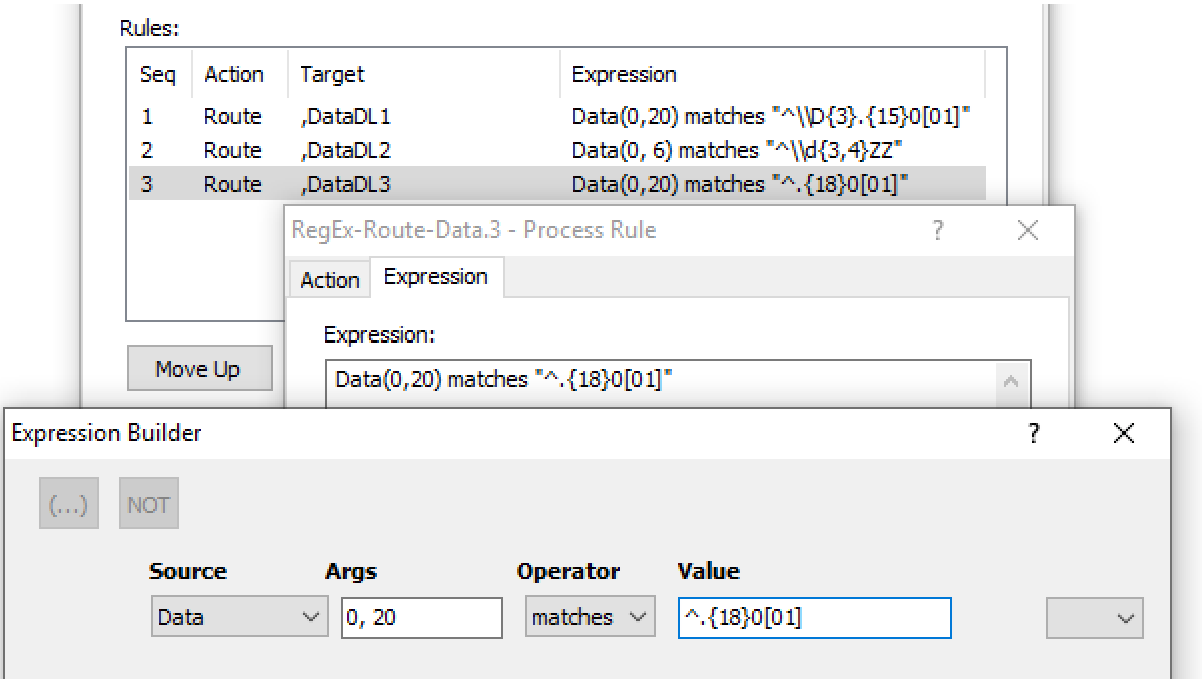
Expression:

Data(0, 6) matches "^\\d{3,4}ZZ"

Expression Builder

Source	Args	Operator	Value
Data	0, 6	matches	^\d{3,4}ZZ

Rules/Seq 3: Routes files containing data where in the selected data range (offset 0 for a length of 20) the first (^) eighteen characters are of any type (.{18}) followed by either 00 or 01 (0[01]).



Rules:

Seq	Action	Target	Expression
1	Route	,DataDL1	Data(0,20) matches "^\\D{3}.{15}0[01]"
2	Route	,DataDL2	Data(0, 6) matches "^\\d{3,4}ZZ"
3	Route	,DataDL3	Data(0,20) matches "^.{18}0[01]"

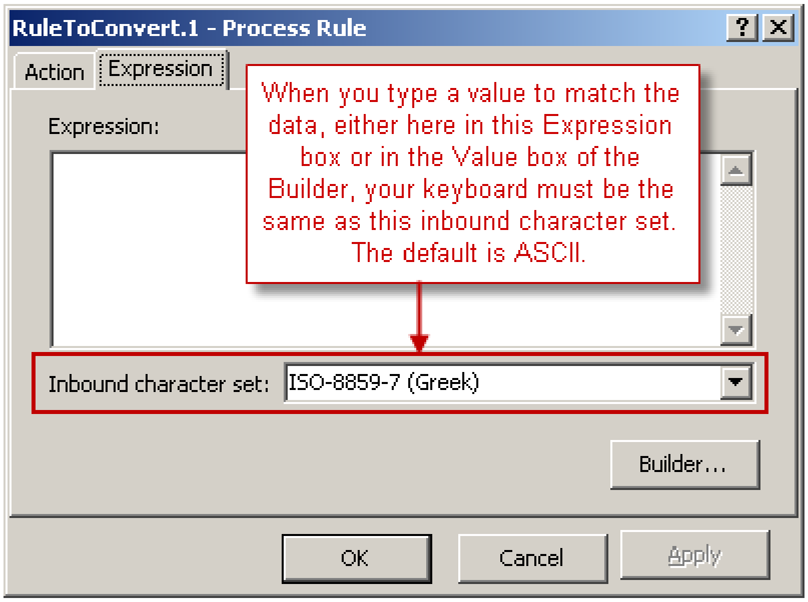
Expression:

Data(0,20) matches "^.{18}0[01]"

Source	Args	Operator	Value
Data	0, 20	matches	^.{18}0[01]

Value

When an inbound character set is specified on the **Expression** tab of the Process Rule window, your keyboard must use the same character set when you type the value either in the **Expression** box directly or in the **Value** box of the Expression Builder. The parameters of the rule must be in ASCII, so it may be easier to use the Expression Builder.



When you type a value to match the data, either here in this Expression box or in the Value box of the Builder, your keyboard must be the same as this inbound character set. The default is ASCII.

Inbound character set: ISO-8859-7 (Greek)

The following table specifies constraints on values based on the source selected:

Source	Constraint
Size	The literal must be a decimal value for the integer comparison.
Not Size	Literal values must be enclosed in double quotation marks for the byte-by-byte comparison. Escape sequences may be used before the opening quotation marks, as specified in the following table.
Filename or InputName	▪ If a "\" is used to fully qualify the filename or inputname, another "\" must be used to escape it. For example: C:\\folder\\subfolder\\filename
Data Type	Select one of the following: ▪ X12 ▪ EDIFACT ▪ XML ▪ ZIP ▪ Unknown ▪ UTF-8 ▪ UTF-16BE ▪ UTF-16LE ▪ UTF-32BE ▪ UTF-32LE

Source	Constraint
Content Type	▪ application/edifact ▪ application/edi-x12 ▪ application/gzip ▪ application/pdf ▪ application/vnd.hp-pcl ▪ application/vnd.lotus-1-2-3 ▪ application/vnd.ms-excel ▪ application/vnd.ms-powerpoint ▪ application/vnd.realmedia ▪ application/x-bzip ▪ application/xml ▪ application/x-shockwave-flash ▪ application/zip ▪ audio/basic ▪ audio/mpeg ▪ audio/vnd.rn-realaudio ▪ audio/x-aiff ▪ audio/x-wav
Content Type (continued)	▪ image/bmp ▪ image/gif ▪ image/jpeg ▪ image/png ▪ image/tiff ▪ image/x-psd ▪ text/plain ▪ video/mpeg ▪ video/quicktime ▪ video/x-msvideo ▪ video/x-ms-wmv

This table shows special character options available for values:

Option	Description
i	Use lower case **i** before the value, which will be in double quotation marks, to indicate that the comparison is not case sensitive. The default is case insensitive.
E	Use upper case **E** before the value, which will be in double quotation marks, to indicate that this is EBCDIC data.

Option	Description
K, M or G	Use upper case K immediately after the numeric value for kilobytes (10*2^10), e.g. *10K*. Use upper case M immediately after the numeric value for megabytes (10*2^20), e.g. *10M*. Use upper case G immediately after the numeric value for gigabytes (10*2^30), e.g. *10G*. **CAUTION:** Any other combination of letters, e.g. MB, or any lower case characters will display an error message, "Size value must be numeric."
\"	Escape sequence to include double quotation mark in the value, which is within quotation marks.
\\	Escape sequence to include back-slash in the value, which is within quotation marks.

And Or

To add another rule to this expression, select **AND OR** from the drop-down list. Another line of options appears. You may add up to eight rules for a single expression.

Parentheses Button

This is a toggle button that places and removes parentheses around expressions to change the associativity of the And and Or operators. To control the order of evaluation of the expressions, move your cursor to the left of one or more rows until you the cursor changes to a hand. Click the mouse to highlight the selected expressions, dragging your cursor down the left side to select as many as required. Then select the parentheses button. Note that the expressions you selected are now surrounded by a pair of parentheses.

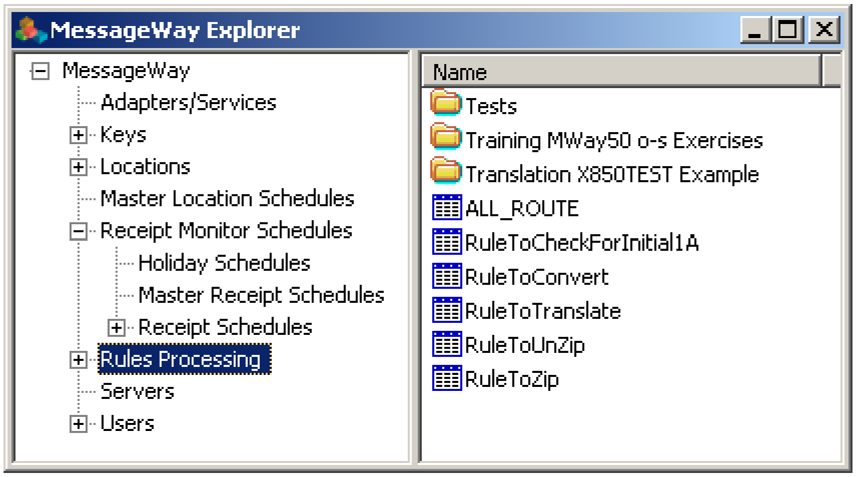
Not Button

This is a toggle button that applies and removes the negative operator, Not, for expressions. To negate expressions, move your cursor to the left of one or more rows until you the cursor changes to a hand. Click the mouse to highlight the selected expressions, dragging your cursor down the left side to select as many as required. Then select the **Not** button. Note that the expressions you selected are now surrounded by a pair of parentheses preceded by Not.

Rules Processing Profile Window

The Rules Processing Profile window allows you to configure rules to route messages based on message properties and message content. You may route messages to a location, link to another rules profile, or you may reject the message. When you associate a location with the Rules Processing Service and specify a rules profile, messages sent to the service location will be processed according to the rules in the profile.

Users access rules processing from the right pane of MessageWay Explorer. Select a rule, and then click the **Properties** button on the toolbar.



Enter New Rules Processing Name

You create a processing rule from MessageWay Explorer using one of three methods:

- In the left pane, right-click the **Rules Processing** or other subfolder, and select **Add Process Rules** from the menu

  - or -

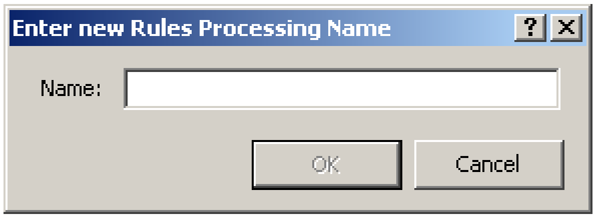
- In the left pane, select **Rules Processing**, and then right-click in a open area of the right pane or on an existing folder and select **Add Process Rules** from the menu

  - or -

- In the right pane, right-click an existing process rule and select **Copy**, then right-click again and select **Paste**

In the last method, a process rule appears with the same name as the original rules processing profile, preceded by the words "Copy of..." To rename the rule, right click and select **Rename** from the pop-up menu.

In the first two methods, the **Enter New Rules Processing Name** dialog box appears. Type a name for the new profile using up to 64 characters.



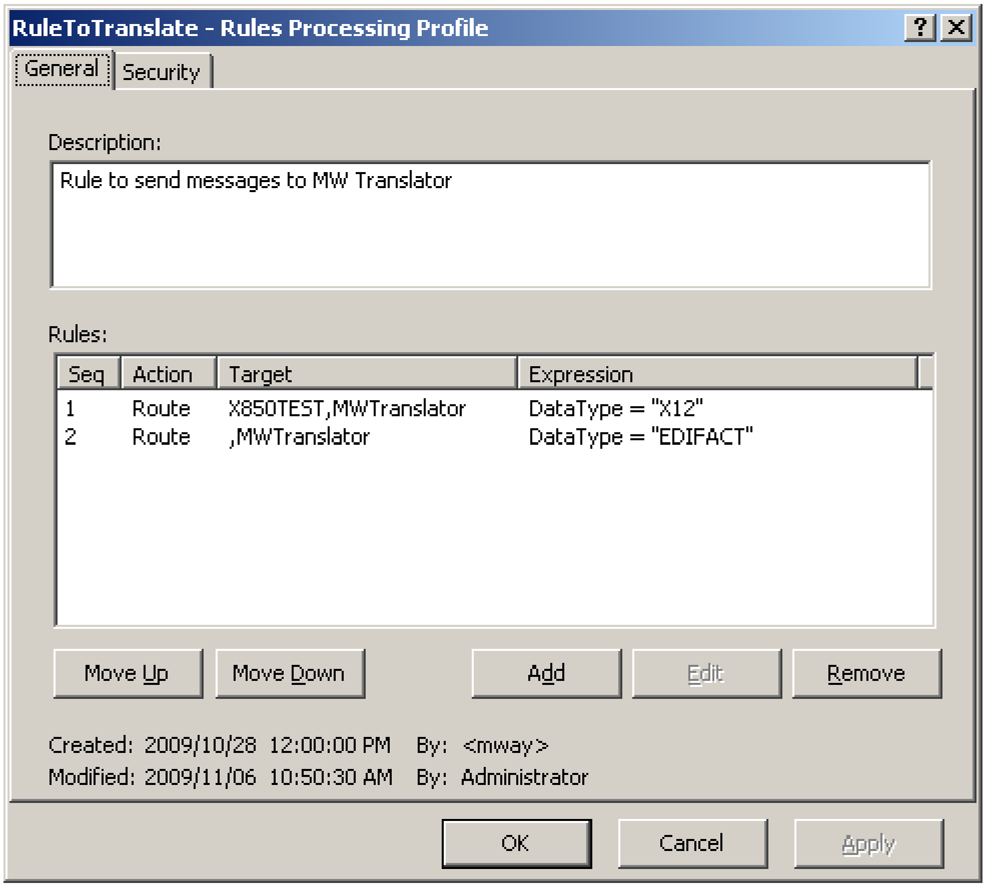
Enter New Rules Processing Name Dialog Box

All profiles must have unique names throughout the system. For management purposes, users may create subfolders. These folders are not used for MessageWay processing, so all profiles, whether they are in folders or not, must have unique names.

(Rules Processing Profile) General Page

The **General** tab of the Rules Processing Profile window shows the name of the rule. The Rules Processing service uses these rules to route the message based on properties of the incoming message or the content of the message.

Process rules are associated with Rules Processing Service locations. When the message arrives in a rules processing service location, the service uses the rules to deliver the message. The service compares the properties of the message header or the content of the message with the rules profile to determine where to send the message.



Description:

Rule to send messages to MW Translator

Rules:

Seq	Action	Target	Expression
1	Route	X850TEST,MWTranslator	DataType = "X12"
2	Route	,MWTranslator	DataType = "EDIFACT"

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/06 10:50:30 AM By: Administrator

General Page (Rules Processing Profile Window)

Description

Enter a description of how you use this profile.

Rules Definitions

Information for the rules definitions list is described in the following table:

Column	Description
Seq	Rules are executed in sequence. This number identifies the location in that sequence, where 1 is the first rule executed. You may change the order using the **Move Up** and **Move Down** buttons.
Action	This is the action performed when the rule applies. The action may be **Route**, **Link** (to another rules profile) or **Reject**.
Target	This is the information required to route the message, such as a location name and priority.

Column	Description
Expression	This expression must evaluate to true for the service to perform the action. If none of the rules evaluate to true, the message will be in error.

Move Up Button

Select a rule, and use the **Move Up** button to move the definition higher in the sequence, so it will be processed before those that follow.

Move Down Button

Select a rule, and use the **Move Down** button to move the definition lower in the sequence, so it will be processed after those that preceed.

Add Button

Use the **Add** button to enter a new rule.

Edit Button

To modify an existing rule, select it from the list and click the **Edit** button.

Remove Button

To delete an existing rule, select it from the list and click the **Remove** button.

Created

Created is the date and time the rules processing profile was created.

By (Created)

This is the MessageWay user that created this profile. When a system service creates an entity, this value identifies the service, which appears in angle brackets, < >, to distinguish it from a MessageWay user. For example, imported definitions will use <mwimp>.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

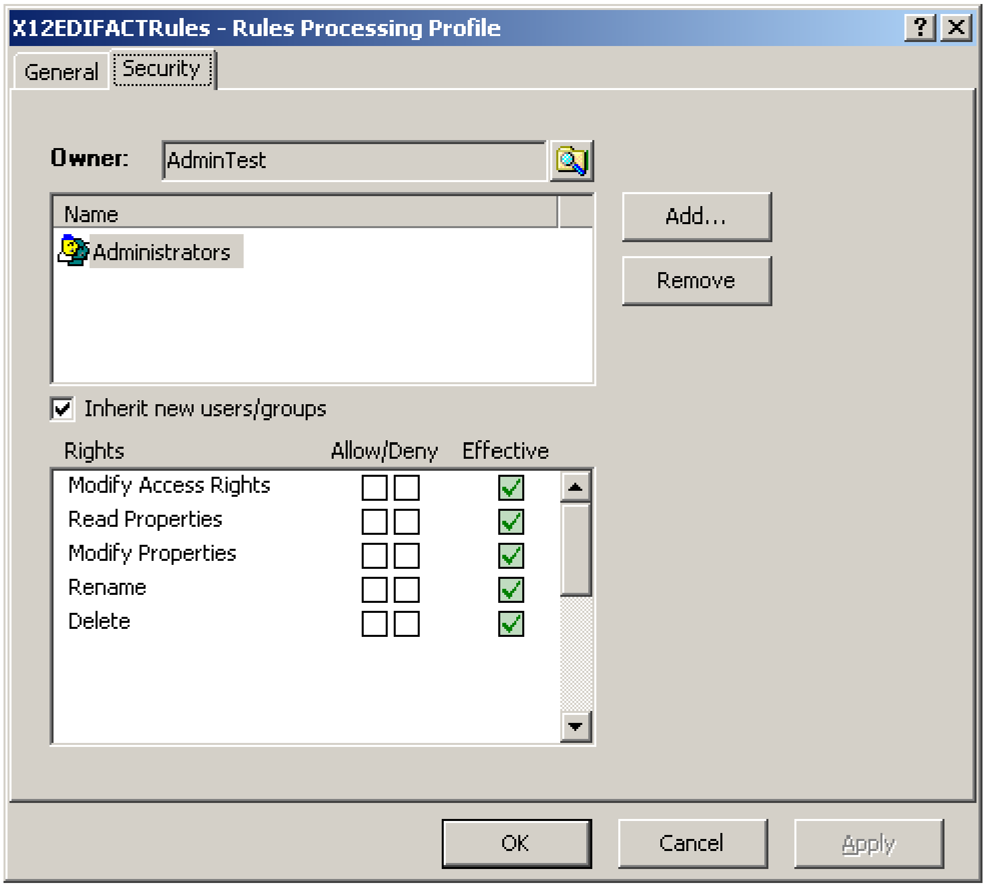
(Rules Processing Profile) Security Page

The **Security** page of the Rules Processing Profile window shows the owner of the profile, which users or user groups are allowed access to the profile and what actions these users or user groups may perform.

Access to a profile is controlled by an access list, which consists of a list of users or user groups and the rights that each one has. The profile may inherit users and user groups and their rights from the **Rules Processing** folder or one of its subfolders. These rights appear in the **Effective** column when you select the user or user group in the **Name** box.

IMPORTANT: When you copy or move this object, the affect on access rights varies. When you copy and paste an existing object (location, rules profile or key), MessageWay will remove all access rights that have been inherited from the object's current parent folder and update all inherited access rights from the object's new parent folder. When you cut and paste/move an existing object (folder, location, rules profile or key), MessageWay will retain all access rights that have been inherited from the object's current parent folder. To update the inherited access rights to those of the object's new parent folder, for each user and group on the list, you must first clear the Inherit new users/groups box and then recheck the box. After moving a folder, the access rights must be correctly updated for the folder itself and for all of its offspring (sub-folders, locations, rules profiles and keys).

IMPORTANT: To perform any functions for a profile, users must also have appropriate rights set on their **Rights** page of the User Properties window.



Owner: AdminTest

Name
Administrators

☑ Inherit new users/groups

Rights	Allow/Deny		Effective
Modify Access Rights	□	□	☑
Read Properties	□	□	☑
Modify Properties	□	□	☑
Rename	□	□	☑
Delete	□	□	☑

Security Page (Rules Processing Profile Window)

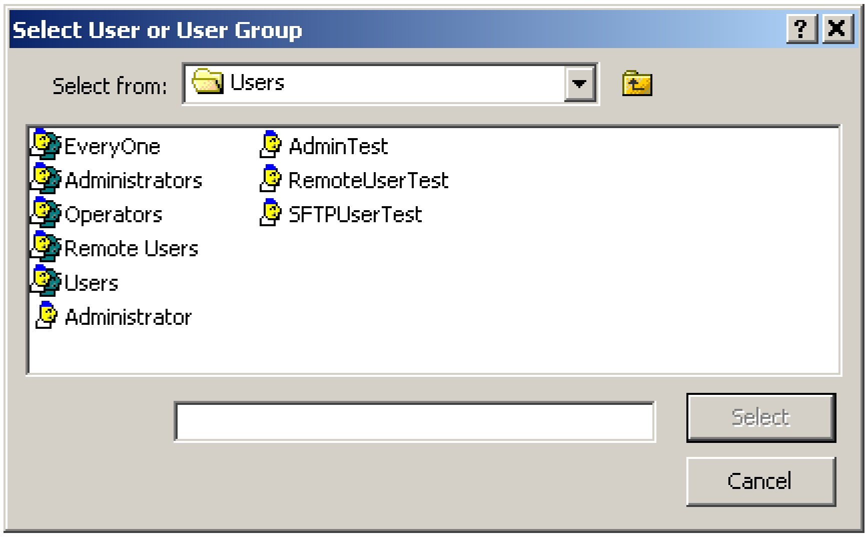
- To add the same users and groups and their rights as listed for the parent folder, check the **Inherit new users/groups** box.
- To override inherited rights, check the appropriate boxes in the **Allow/Deny** columns.
- To give a user or user group access to this rules processing profile:

1. Click **Add**.

   The Select User or User Group window appears.

2. Select a group from the list or type the name of a group in the **Select** box.
3. Click **Select**.

NOTE: The EveryOne group is on the selection list, but not on the list under the Users folder, unless someone has added it manually. This group is only available for access lists. Add this group to the list to grant access rights to all users. All users are implicitly members of the EveryOne user group. As a result, when EveryOne is added to an access list, the associated rights are granted to all users.



Select User or User Group

Owner

Initially, the owner is the user that created the rules profile. The owner may transfer ownership to another user. Owners have complete access rights to the profile, regardless of other configurations. Owners always have the right to change the names on the access list and the right to read and change the properties of the profile.

Browse Button

When you are the owner, click this button to give ownership to another user.

Name

The **Name** list contains users or user groups that are permitted to access this profile. Use the **Add** and **Remove** buttons to maintain this list. The **Name** list and the **Rights** list compose the access list that MessageWay uses to determine who has what rights to this profile.

Add Button

Click this button to add names of users or user groups to the **Name** list.

Remove Button

Click this button to delete names of users or user groups from the **Name** list. To remove names from the list, you must first clear the **Inherit new users or groups** box.

Inherit new users or groups

When this box is selected, any users or user groups that are added to the **Name** list of the parent folder will also be added to the **Name** list of this profile. The parent folder might be the **Rules Processing** folder or one of its subfolders. To remove users or user groups from the list, you must clear this box first.

Rights

The Rights list contains the functions that the users or user groups in the Name list may perform. The Rights list and the Name list compose the access list to determine who has what rights to this profile. Rules profiles may inherit rights from their parent folder. These rights appear in the *Effective* column when you select the user or user group in the Name list.You may override these effective rights by checking the Allow/Deny boxes. To select or clear all rights at once, hold **SHIFT** while you click one of the boxes.

The following table explains the rights for rules processing profiles:

Right	Description
Modify Access Rights	Change values on **Security** page of Rules Processing Profile window. Also requires the right, **Read Properties**.
Read Properties	View properties of a rules profile.
Modify Properties	Change properties of a rules profile Also requires the right, **Read Properties**.
Rename	Rename a rules profile. Also requires the right, **Read Properties**.
Delete	Delete a rules profile. Also requires the right, **Read Properties**.

Schedule Windows (Location, Master Location, Receipt, Master Receipt, Holiday)

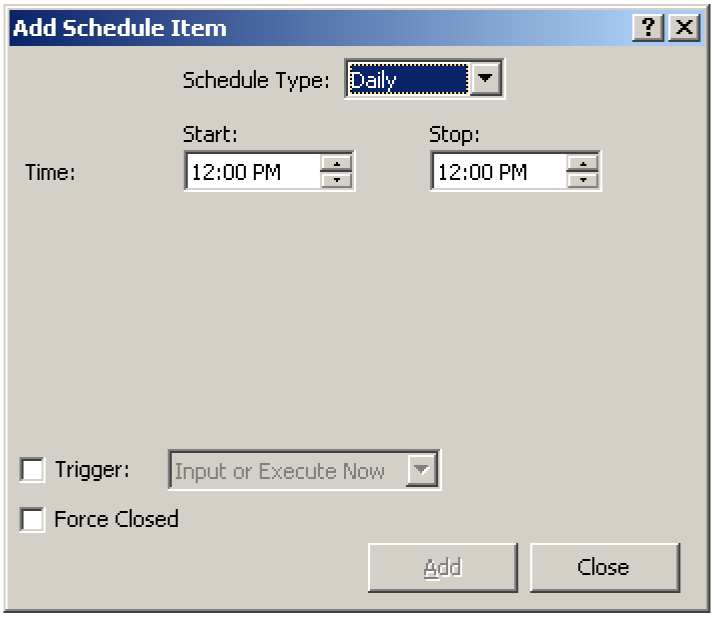
This section contains reference information about the various types of schedule windows. Schedules apply to locations as well as receipt monitor. They include the following:

- Location Schedule
- Master Location Schedule
- Holiday Schedule (Receipt Monitor)
- Master Receipt Schedule (Receipt Monitor)
- Receipt Schedule (Receipt Monitor)

IMPORTANT: Only location or master location schedules will actually affect when locations are open or closed. Receipt Monitor schedules, receipt and master receipt schedules, do not control whether locations are open or closed. They are only used to monitor the number of messages received from a defined address, which may or may not be the same as a MessageWay location.

Add and Edit Schedule Item Windows

For Location, Master Location, Receipt and Master Receipt schedules, the Add Schedule Item and Edit Schedule Item windows allow users to enter recurring or absolute date and time windows. For Receipt Monitor schedules, users may enter notification event parameters. Users access these windows by selecting the **Add** or **Edit** buttons on the **Schedule** page.



Add Schedule Item

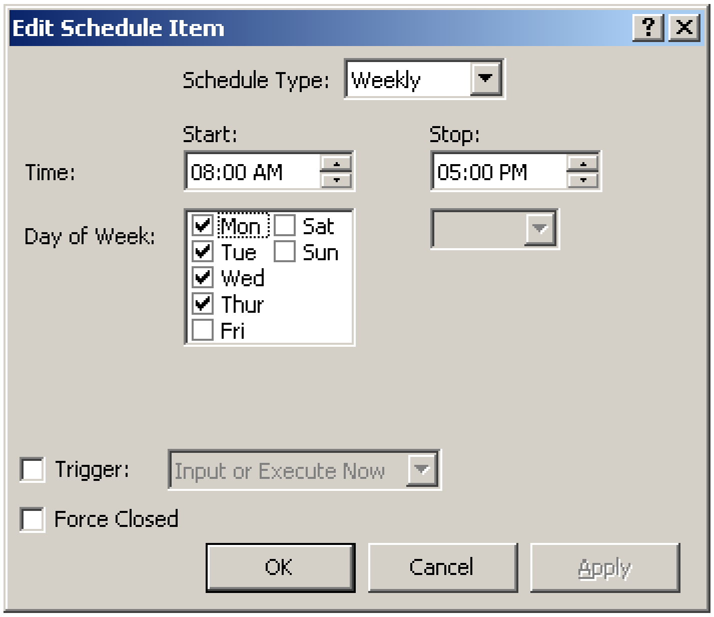
Schedule Type: Daily

Time: Start: 12:00 PM Stop: 12:00 PM

□ Trigger: Input or Execute Now

□ Force Closed

Add Schedule Item Window (Location and Master Location Schedules)



Schedule Type: Weekly

Time: Start: 08:00 AM Stop: 05:00 PM

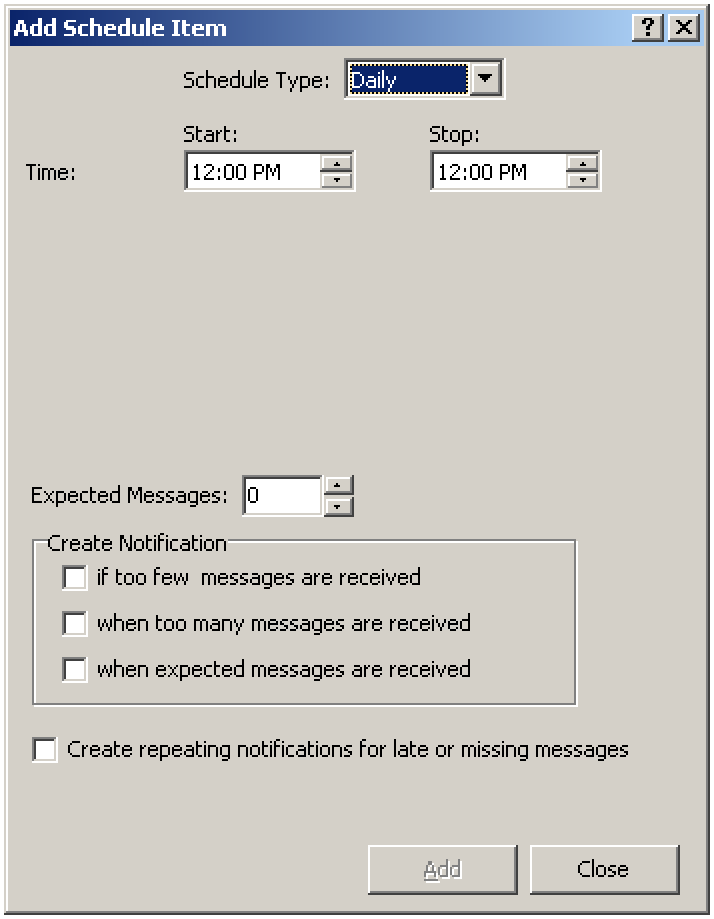
Day of Week:

☑ Mon ☐ Sat
☑ Tue ☐ Sun
☑ Wed
☑ Thur
☐ Fri

☐ Trigger: Input or Execute Now

☐ Force Closed

Edit Schedule Item Window (Location and Master Location Schedules)



Add Schedule Item

Schedule Type: Daily

Time: Start: 12:00 PM Stop: 12:00 PM

Expected Messages: 0

Create Notification

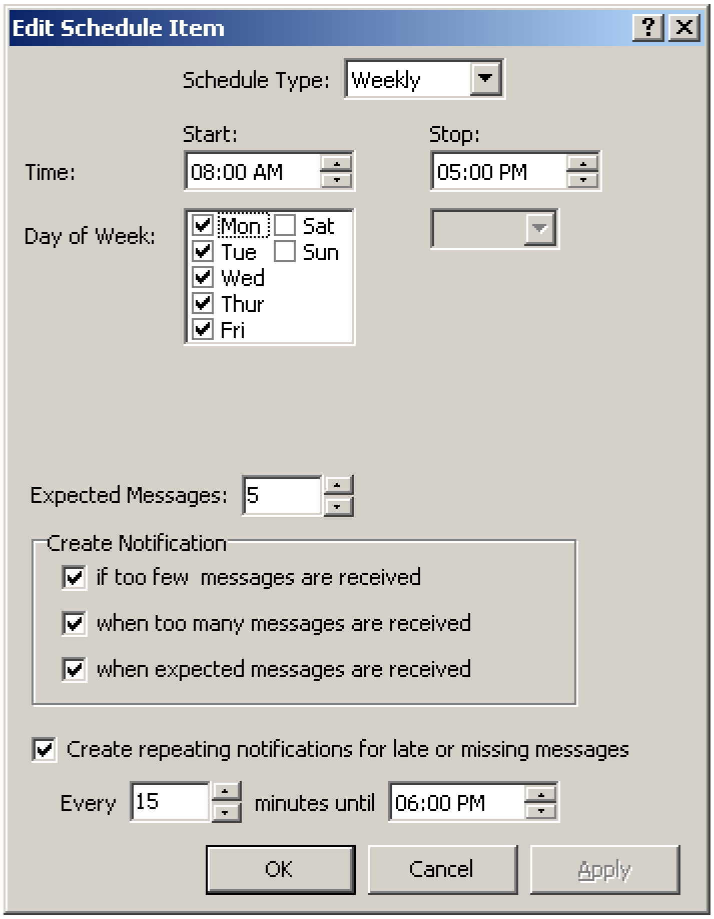
□ if too few messages are received

□ when too many messages are received

□ when expected messages are received

□ Create repeating notifications for late or missing messages

Add Schedule Item Window (Receipt and Master Receipt Schedules)



Edit Schedule Item

Schedule Type: Weekly

Time: Start: 08:00 AM Stop: 05:00 PM

Day of Week: ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri □ Sat □ Sun

Expected Messages: 5

Create Notification

☑ if too few messages are received

☑ when too many messages are received

☑ when expected messages are received

☑ Create repeating notifications for late or missing messages

Every 15 minutes until 06:00 PM

Edit Schedule Item Window (Receipt and Master Receipt Schedules)

Schedule Type

Choose one of the five options: **Daily**, **Weekly**, **Monthly**, **Yearly** or **Absolute**. Daily, weekly, monthly and yearly schedules are recurring. They apply to all years through 2025. Absolute schedules are continuous and only affect the period for the specified year(s).

Time Start

Type or select a time to begin the schedule. If you type military time, the value converts to standard time.

Time Stop

Type or select a time to end the schedule. If you type military time, the value converts to standard time.

Day of Week Start

For a weekly schedule that must start and stop on specific days, check the days to use the schedule. For a weekly schedule that continues for a period of days, check one day to begin the schedule from this list and then choose the day to end the schedule from the list in the next box.

For monthly and yearly schedules, choose the day of the week to start the schedule.

This creates a recurring schedule through all years to 2025. For a non-recurring, absolute schedule, this affects only the period specified.

Day of Week Stop

For a weekly schedule that continues for a period of days, choose the day of the week to end the schedule.

For monthly and yearly schedules, choose the day to end the schedule.

This creates a recurring schedule through all years to 2025. For a non-recurring, absolute schedule, this affects only the period specified.

Week Start

For monthly and yearly schedules, choose the week to start the schedule: **1st**, **2nd**, **3rd**, **4th**, **5th** or **Last**.

This creates a recurring schedule through all years to 2025. For a non-recurring, absolute schedule, this affects only the period specified.

Week Stop

For monthly and yearly schedules, choose the week to end the schedule: **1st**, **2nd**, **3rd**, **4th**, **5th** or **Last**.

This creates a recurring schedule through all years to 2025. For a non-recurring, absolute schedule, this affects only the period specified.

Day of Month Start

For a monthly or yearly schedule that must start on a specific day every month, select the day of the month or **Last** from the list. This creates a recurring schedule through all years to 2025. For a non-recurring, absolute schedule, this affects only the period specified.

Day of Month Stop

For a monthly or yearly schedule that starts on a specific day every month, select the day of the month or **Last** from the list when the schedule stops. This creates a recurring schedule through all years to 2025. For a non-recurring, absolute schedule, this affects only the period specified.

Month Start

For a yearly schedule that must start on a specific month, select the month from the list. This creates a recurring schedule through all years to 2025. For a non-recurring, absolute schedule, this affects only the period specified.

Month Stop

For a yearly schedule that starts on a specific month, select the month from the list when the schedule stops. This creates a recurring schedule through all years to 2025. For a non-recurring, absolute schedule, this affects only the period specified.

Year Start

For an absolute schedule that only affects the year(s) specified, type or select the year to begin the continuous schedule.

Year Stop

For an absolute schedule that only affects the year(s) specified, type or select the year to end the continuous schedule.

Trigger Check Box

Check this box to initiate one of the following actions for a location: Input or execute now, hold location, release location, hold outputs, release outputs.

Trigger

Click the arrow to initiate one of the following actions: input or execute now, hold location, release location, hold outputs, release outputs. The event occurs at the start date and time. When this box is checked, the end date and time is ignored and dimmed. Trigger events appear as vertical lines on the calendar.

The following table describes each of the actions:

Action	Description
Hold Location	Places a location on hold, which prevents all messages queued to that location from being processed.
Release Location	Releases a location from hold, which allows queued messages to be processed or delivered.
Hold Outputs	Places all output messages sent from a service location on hold, which prevents the messages from being delivered.

Action	Description
Release Outputs	Releases all output messages sent from a service location from hold, which allows the messages to be delivered.
Input or Execute Now	This action is only appropriate for input sites and service locations and it specifies a specific time when processing will occur. For input sites, any polling interval configured for the site is ignored. For service locations, it's only appropriate for processing that does not require an input message, such as production of a report or performance of a housekeeping task. The trigger action is not effective if the location's status is *On Hold*.

Force Close

Check this box to close the schedule for the period specified. This overrides any part of an open schedule that may be active for a period. Force closed items appear in red on the calendar.

Expected Messages

Type or select the number of messages that you expect to receive. When the expected messages arrive, an entry appears in the event log and optional notifications may be sent to a recipient.

Create Notification

Check any combination of these boxes to generate optional notifications. Note that an entry is always made in the event log when any of the checked events occur.

The options are as follows:

Notification Option	Description
If too few messages are received	Generate a notification message when fewer messages are received during the window than the number specified in the Expected Messages box.
If too many messages are received	Generate a notification message when more messages are received during the window than the number specified in the Expected Messages box.
When expected messages are received	Generate a notification message when the number of messages specified in the Expected Messages box are received.

Create Repeating Notifications for Late or Missing Messages

Check this box to send notifications periodically within the specified time range when the options selected in the Create Notifications box has occurred: If too few messages are received; If too many messages are received; or When expected messages are received.

Every

Type or select the number of minutes to repeat notification when the expected messages have not arrived by the end of the receipt window.

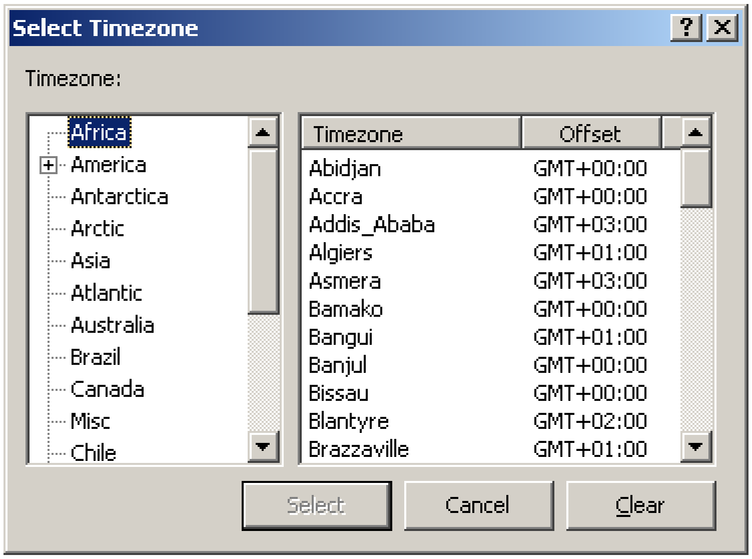
Until

Type or select the time when notifications of late or missing messages will stop.

Select Timezone

You may select a time zone for a location schedule, master location schedule, receipt schedule or master receipt schedule when you click the **Schedule** button, 🔍 the **Schedule** tab.

TIP: To clear the time zone, you must click the **Clear** button on the Select Timezone dialog box.



Timezone	Offset
Abidjan	GMT+00:00
Accra	GMT+00:00
Addis_Ababa	GMT+03:00
Algiers	GMT+01:00
Asmera	GMT+03:00
Bamako	GMT+00:00
Bangui	GMT+01:00
Banjul	GMT+00:00
Bissau	GMT+00:00
Blantyre	GMT+02:00
Brazzaville	GMT+01:00

Select Timezone Dialog Box

Timezone

This informational field displays the time zone that is currently selected. When no zone is selected, it is blank and defaults to the same time zone as the MessageWay server. Schedules are adjusted for Daylight Saving Time (DST) automatically by the Scheduling server between standard and daylight times.

Area of the World

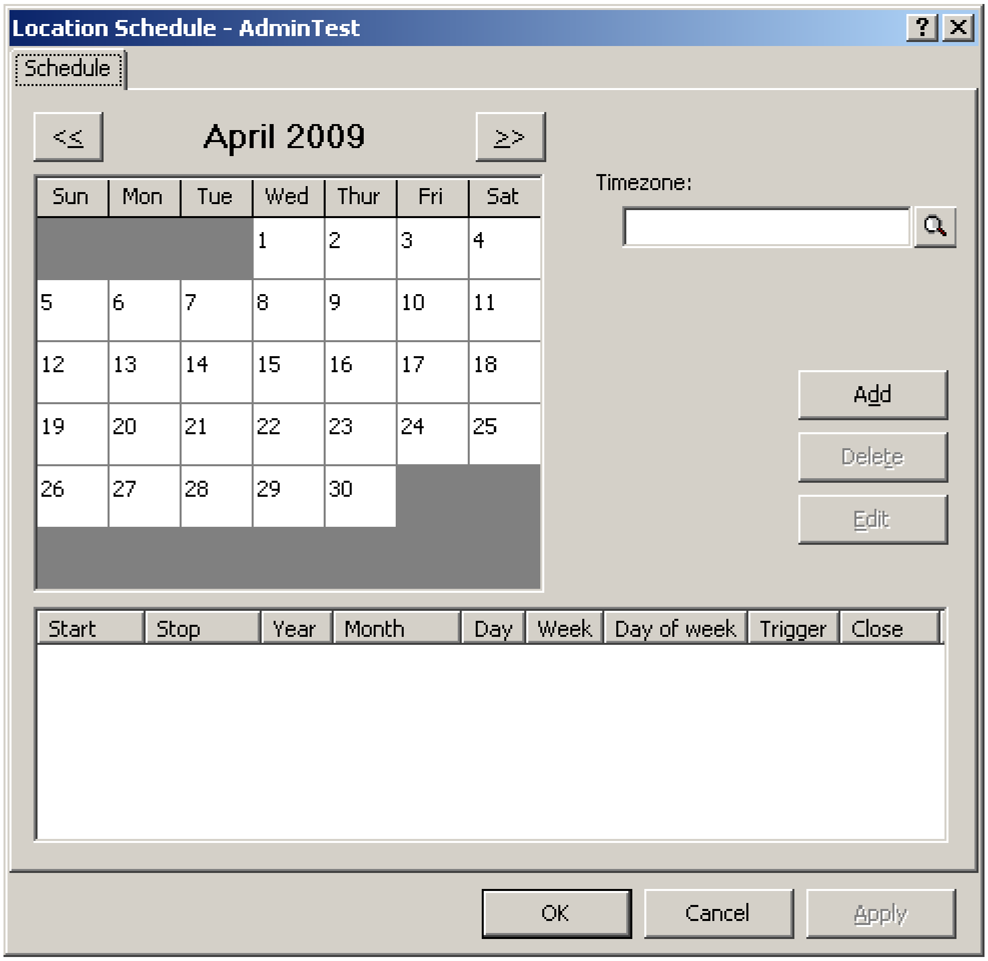
In the left pane, select the area of the world whose time zone you want to specify. Select **Misc** or **Etc** for other options.

Timezone

In the right pane, select the appropriate time zone. These zones show the time relative to Greenwhich Mean Time (GMT). Times will be adjusted automatically for Daylight Saving Time (DST) where appropriate by the Scheduling server. There are additional selections for those areas that do not conform to the time zone of the area where they are included. For example, within the United States (US), Arizona does not generally observe daylight savings, so rather than choose Mountain time, there is a special selection for Arizona. However, the Navajo Nation within Arizona does observe DST, so for that you would choose **Mountain**.

Location Schedule Window

The Location Schedule window appears when users create a local schedule for a location. Users may design a new schedule or use a Master Location Schedule as a template to then modify. The **Schedule** page of the Location Schedule window behaves the same as the **Schedule** page of the Master Location Schedule window. For more information about the fields on this page, refer to the topic, ***Master Location Schedule Window*** (on page 1280).



Sun	Mon	Tue	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

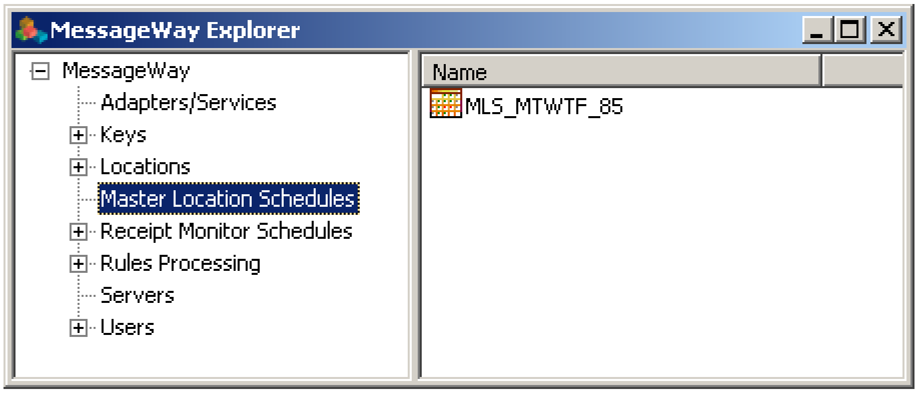
Start	Stop	Year	Month	Day	Week	Day of week	Trigger	Close

Schedule Page (Location Schedule Window)

Master Location Schedule Window

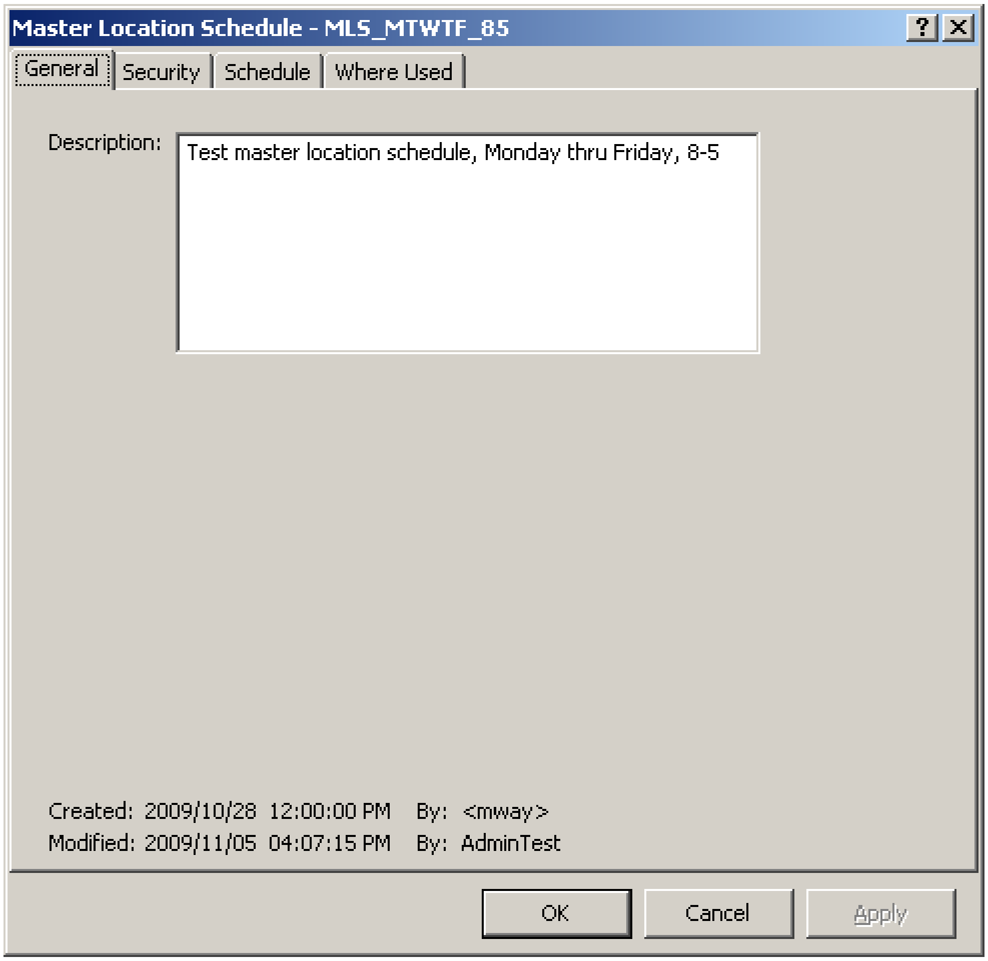
The Master Location Schedule window allows users to enter master schedules that may be shared by many locations. Master location schedules specify date and time windows when the location is open or closed. Users may also use a master location schedule as a beginning template that they then modify for a given location.

Users may view the list of master location schedules in MessageWay Explorer.



(Master Location Schedule) General Page

The **General** page of the Master Location Schedule window allows users to type a brief description of the purpose of this schedule.



Description: Test master location schedule, Monday thru Friday, 8-5

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/05 04:07:15 PM By: AdminTest

General Page (Master Location Schedule)

Description

Type a description for the purpose of this schedule.

Created

Created is the date and time this schedule was created.

By (Created)

This value is the MessageWay user that created the schedule. When a system service creates an entity, this value identifies the service, which appears in angle brackets, < >, to distinguish it from a MessageWay user. For example, imported definitions will use <mwimp>.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

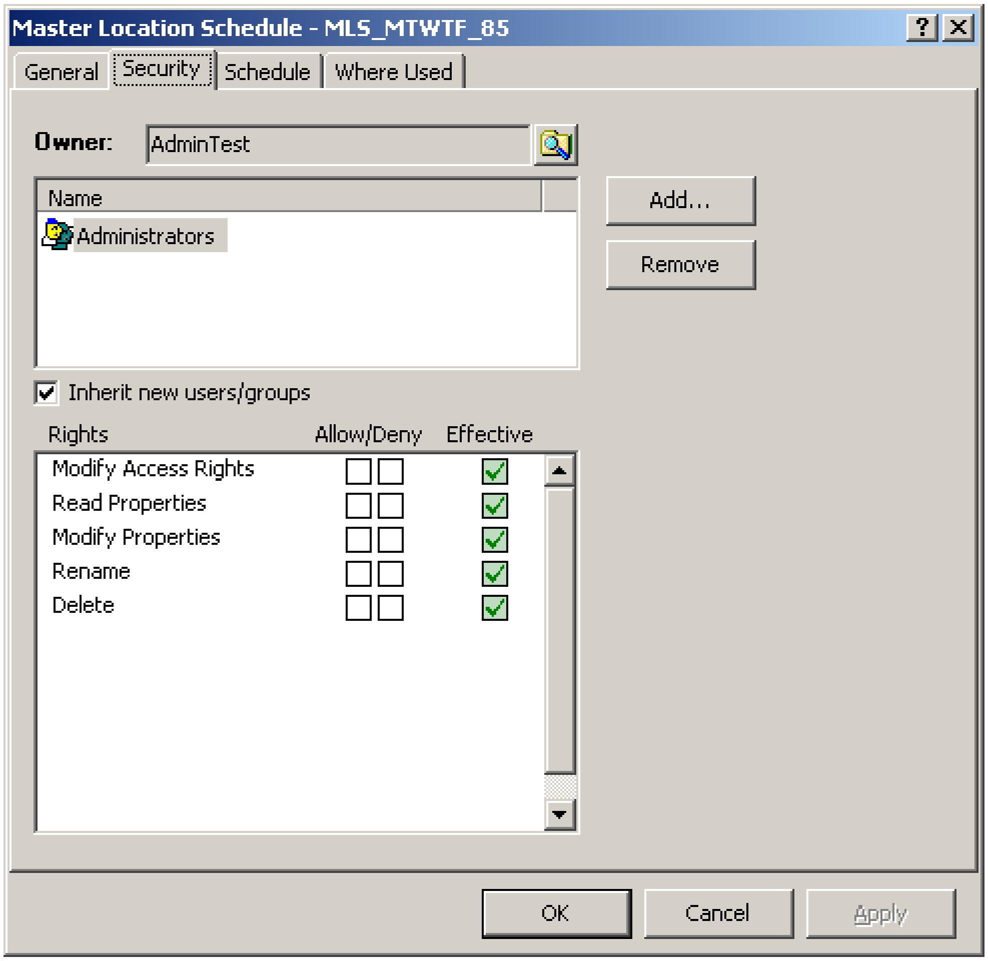
This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

(Master Location Schedule) Security Page

The **Security** page of the Master Location Schedule window shows the owner of schedule, which users or user groups are allowed access to the schedule and what actions these users or user groups may perform.

Access to a schedule is controlled by an access list, which consists of a list of users or user groups and the rights that each one has. The schedule may inherit users and user groups and their rights from the **Master Location Schedules** folder. These rights appear in the Effective rights column when you select the user or user group in the **Name** box.

IMPORTANT: To perform any functions for a schedule, users must also have appropriate rights set on their **Rights** page of the User Properties window.



Master Location Schedule - MLS_MTWTF_85

Owner: AdminTest

Name
Administrators

☑ Inherit new users/groups

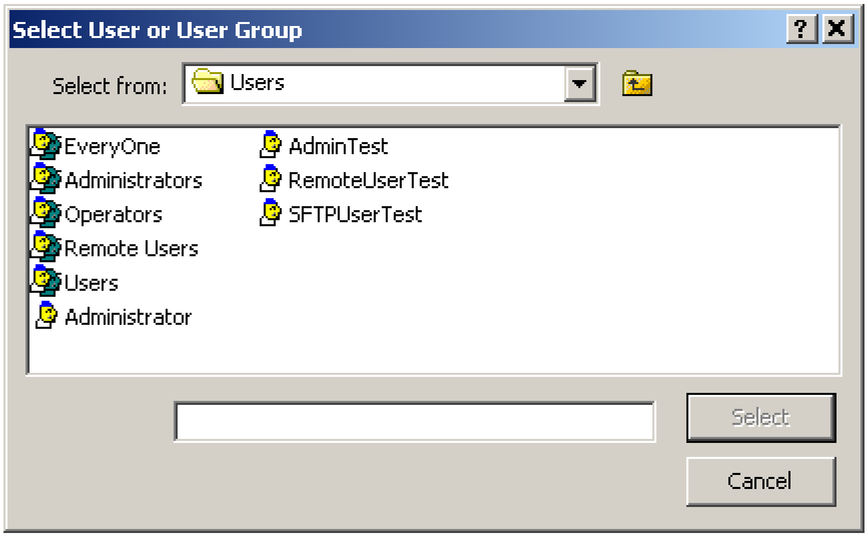
Rights	Allow/Deny		Effective
Modify Access Rights	□	□	☑
Read Properties	□	□	☑
Modify Properties	□	□	☑
Rename	□	□	☑
Delete	□	□	☑

Security Page (Master Location Schedule Window)

Check the **Inherit new users/groups** box to add the same users and groups and their rights as listed for the parent folder. To override inherited rights, check the appropriate boxes in the Allow/Deny columns.

Click the **Add** button to give a user or user group access to this schedule. The Select User or User Group window appears. Select a group from the list or type the name of a group in the Select box, and choose the **Select** button.

NOTE: The EveryOne group is on the selection list, but not on the list under the Users folder, unless someone has added it manually. This group is only available for access lists. Add this group to the list to grant access rights to all users. All users are implicitly members of the EveryOne user group. As a result, when EveryOne is added to an access list, the associated rights are granted to all users.



Select User or User Group Window

Owner

Initially, the owner is the user that created the schedule. The owner may transfer ownership to another user. Owners have complete access rights to the object, regardless of other configurations. Owners always have the right to change the names on the access list and the right to read and change the properties of the schedule.

Browse Button

When you are the owner, you may select this button to give ownership to another user.

Name Schedule

The Name list contains users or user groups that are permitted to access this schedule. The Name list and the Rights list compose the access list used by MessageWay to determine who has what rights to this schedule. The users or groups on the name list may be inherited from a parent folder. Use the **Add** and **Remove** buttons to maintain this list. To remove inherited names from the list, you must first clear the **Inherit new users/groups** box.

Add Button

Select this button to add names of users or user groups to the Name list.

Remove Button

Select this button to delete names of users or user groups from the access list. To delete the name of a user or user group that has been inherited from its parent folder, you must first clear the **Inherit new users/groups** box.

Inherit New Users Or Groups

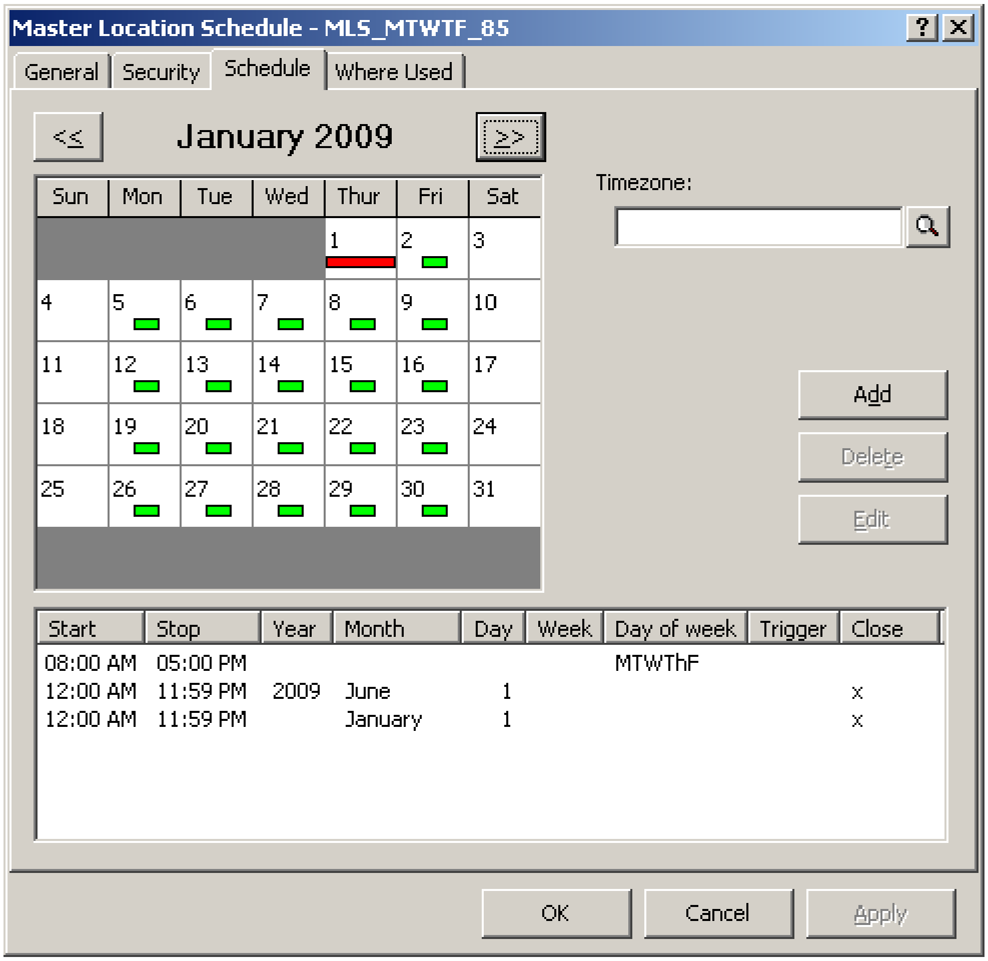
When this box is checked, any users or user groups that are added to the Name list of the parent folder will also be added to the Name list of this schedule. To remove inherited users or user groups from the list, you must clear this box first.

Rights

The Rights list contains the functions that the users or user groups in the Name list may perform. The Rights list and the Name list compose the access list to determine who has what rights to this schedule. Schedules may inherit rights from their parent folder. These rights appear in the Effective column when you select the user or user group in the Name list.You may override these effective rights by selecting the Allow/Deny boxes. To select or clear all rights at once, hold **SHIFT** while you select one of the boxes.

(Master Location Schedule) Schedule Page

The **Schedule** page of the Master Location Schedule window allows users to enter master location schedules.



Sun	Mon	Tue	Wed	Thur	Fri	Sat
				1 🟥	2 🟩	3
4	5 🟩	6 🟩	7 🟩	8 🟩	9 🟩	10
11	12 🟩	13 🟩	14 🟩	15 🟩	16 🟩	17
18	19 🟩	20 🟩	21 🟩	22 🟩	23 🟩	24
25	26 🟩	27 🟩	28 🟩	29 🟩	30 🟩	31

Start	Stop	Year	Month	Day	Week	Day of week	Trigger	Close
08:00 AM	05:00 PM					MTWThF		
12:00 AM	11:59 PM	2009	June	1				x
12:00 AM	11:59 PM		January	1				x

Schedule Page (Master Location Schedule Window)

Monthly Calendar

This calendar displays when you have a schedule item defined. Use the **Previous** and **Next** buttons to view other months and years. To view one or more schedule items in the calendar, select them from the list window at the bottom. Green indicates an open schedule and red a closed schedule item.

Previous Button

Click the **Previous** button to display the calendar for the previous month.

Next Button

Click the **Next** button to display the calendar for the next month.

Timezone

Time zones default to the time of the MessageWay server. Users may need to select a different time zone for a location. For example, the Remote Execution Server, which is an option for MessageWay, provides the ability to schedule and execute user-defined scripts on a remote server. The time zone feature allows users to schedule scripts based on the time zone of the remote server.

Click the **Schedule** button to choose a different time zone. To remove a timezone, click the **Schedule** button, and when the **Select Timezone** dialog box appears, click **Clear**.

Add Button

Click this button to add a schedule item.

Delete Button

Click this button to delete one or more schedules selected from the list.

Edit Button

Click this button to edit a schedule item selected from the list.

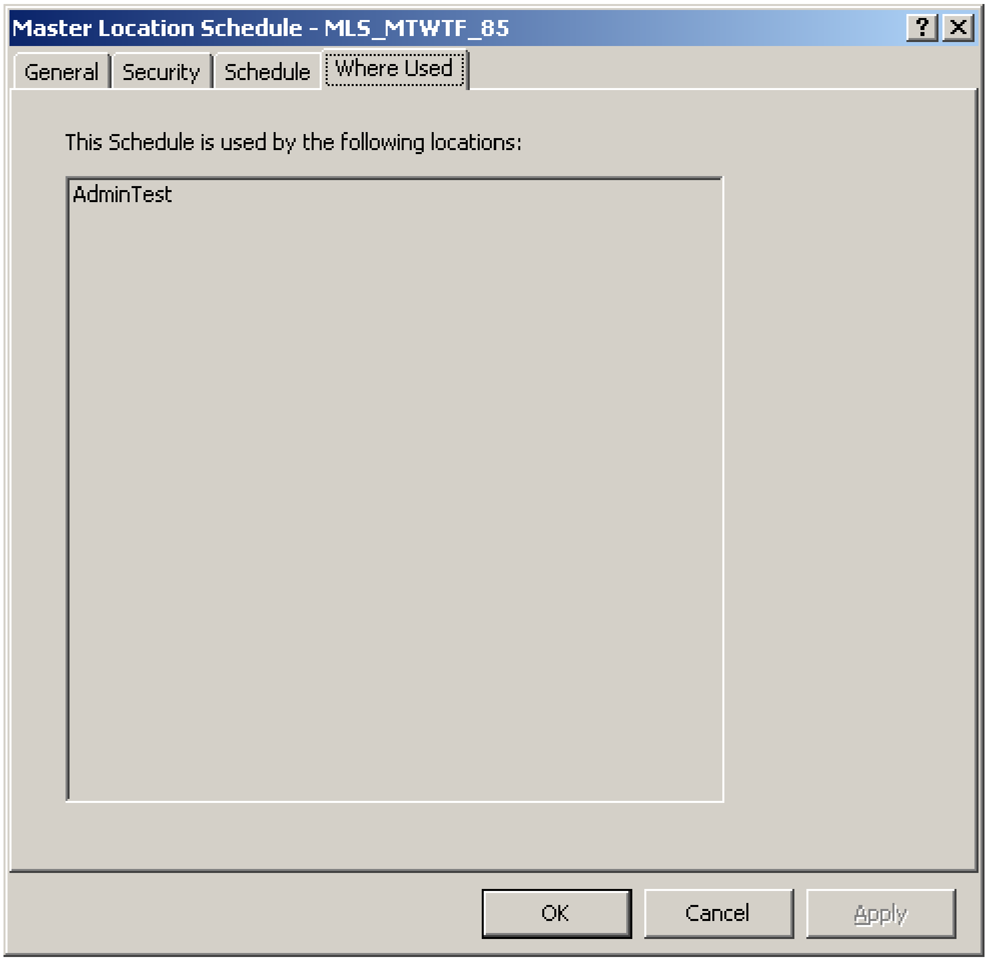
Schedule Items List

This box displays the dates and times of the schedule items. To add, delete or edit items, click the **Add**, **Delete** or **Edit** button.

For more information about what the various columns mean, refer to the topic, ***Add and Edit Schedule Item Windows (Schedules)*** (on page 1271).

Where Used Page

The **Where Used** page of the Master Location Schedule window allows users to view which location schedules use this master schedule. This is useful to determine what definitions would be affected by a change to a master location schedule.



This Schedule is used by the following locations:

AdminTest

Where Used Page (Master Location Schedule Window)

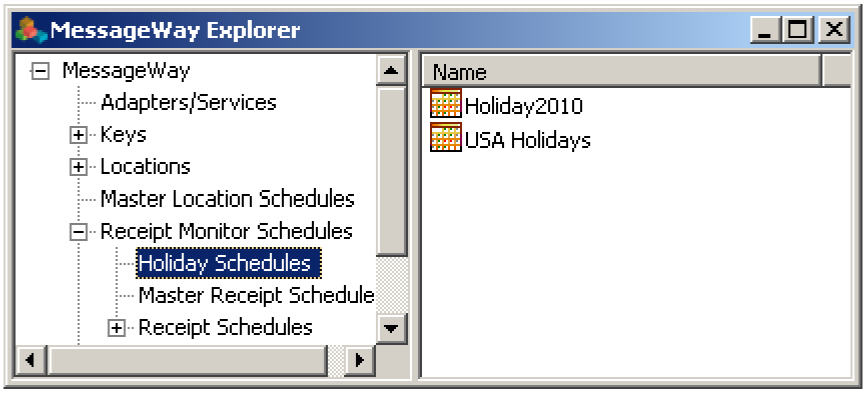
This Schedule Is Used By the Following Locations

This list is maintained by MessageWay and displays the locations that use this master location schedule.

(Receipt Monitor Schedules) Holiday Schedule Window

The Holiday Schedule window of the Receipt Monitor allows users to enter holidays that will be applied to a receipt schedule. Holiday schedules are 24-hour periods and exclude any schedules that *begin* during that day from the notification process. Holidays preempt receipt schedules.

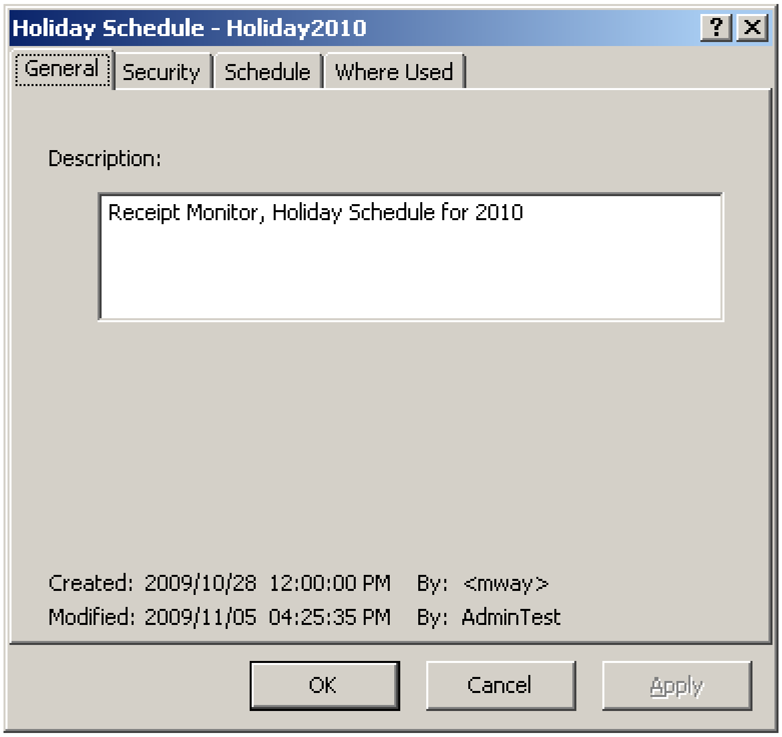
Users may view the list of holiday schedules they have configured in the MessageWay Explorer window.



Holiday Schedules List (MessageWay Explorer Window, Receipt Monitor Schedules)

General Page

The **General** page of the Holiday Schedule window for the Receipt Monitor allows users to describe the schedule.



Description:

Receipt Monitor, Holiday Schedule for 2010

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/05 04:25:35 PM By: AdminTest

General Page (Receipt Monitor, Holiday Schedule Window)

Description

Type text to describe the purpose of this schedule.

Created

Created is the date and time this schedule was created.

By (Created)

This value is the MessageWay user that created the schedule. When a system service creates an entity, this value identifies the service, which appears in angle brackets, < >, to distinguish it from a MessageWay user. For example, imported definitions will use <mwimp>.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

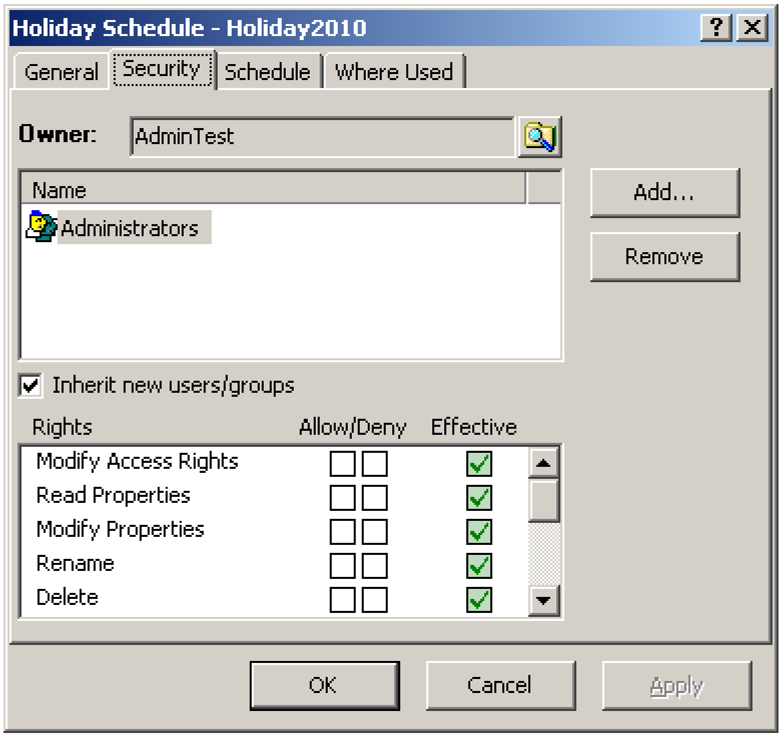
This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

Security Page

The **Security** page of the Holiday Schedule Properties window shows the owner of schedule, which users or user groups are allowed access to the schedule and what actions these users or user groups may perform.

Access to a schedule is controlled by an access list, which consists of a list of users or user groups and the rights that each one has. The schedule may inherit users and user groups and their rights from the Holiday Schedules folder. These rights appear in the Effective rights column when you select the user or user group in the **Name** box.

IMPORTANT: To perform any functions for a schedule, users must also have appropriate rights set on their **Rights** page of the User Properties window.



Holiday Schedule - Holiday2010

Owner: AdminTest

Name: Administrators

☑ Inherit new users/groups

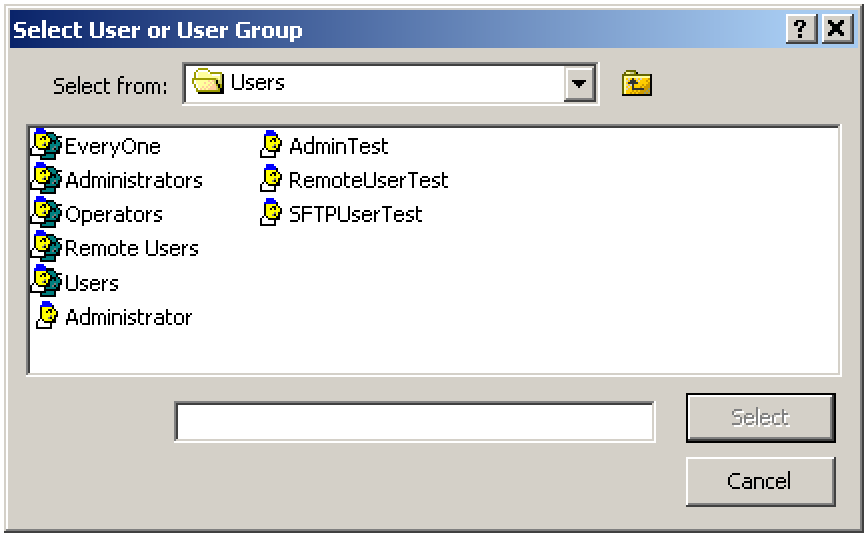
Rights	Allow/Deny		Effective
Modify Access Rights	□	□	☑
Read Properties	□	□	☑
Modify Properties	□	□	☑
Rename	□	□	☑
Delete	□	□	☑

Security Page (Receipt Monitor, Holiday Schedule Window)

Check the **Inherit new users/groups** box to add the same users and groups and their rights as listed for the parent folder. To override inherited rights, check the appropriate boxes in the Allow/Deny columns.

Select the **Add** button to give a user or user group access to this schedule. The Select User or User Group window appears. Select a group from the list or type the name of a group in the Select box, and choose the **Select** button.

NOTE: The EveryOne group is on the selection list, but not on the list under the Users folder, unless someone has added it manually. This group is only available for access lists. Add this group to the list to grant access rights to all users. All users are implicitly members of the EveryOne user group. As a result, when EveryOne is added to an access list, the associated rights are granted to all users.



Select from: Users

Select User or User Group

Owner

Initially, the owner is the user that created the schedule. The owner may transfer ownership to another user. Owners have complete access rights to the object, regardless of other configurations. Owners always have the right to change the names on the access list and the right to read and change the properties of the schedule.

Browse Button

When you are the owner, you may select this button to give ownership to another user.

Name

The Name list contains users or user groups that are permitted to access this schedule. The Name list and the Rights list compose the access list used by MessageWay to determine who has what rights to this schedule. The users or groups on the name list may be inherited from a parent folder. Use the **Add** and **Remove** buttons to maintain this list. To remove inherited names from the list, you must first clear the **Inherit new users/groups** box.

Add Button

Select this button to add names of users or user groups to the Name list.

Remove Button

Select this button to delete names of users or user groups from the access list. To delete the name of a user or user group that has been inherited from its parent folder, you must first clear the **Inherit new users/groups** box.

Inherit new users or groups

When this box is checked, any users or user groups that are added to the Name list of the parent folder will also be added to the Name list of this schedule. To remove inherited users or user groups from the list, you must clear this box first.

Rights

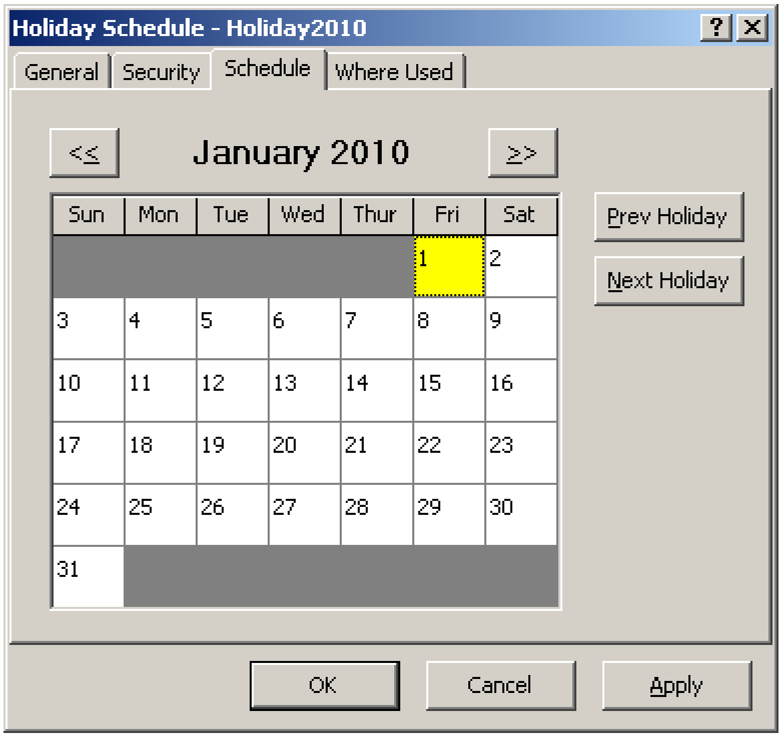
The Rights list contains the functions that the users or user groups in the Name list may perform. The Rights list and the Name list compose the access list to determine who has what rights to this schedule. Schedules may inherit rights from their parent folder. These rights appear in the Effective column when you select the user or user group in the Name list.You may override these effective rights by selecting the Allow/Deny boxes. To select or clear all rights at once, hold **SHIFT** while you select one of the boxes.

The following table describes the rights for holiday schedules:

Right	Description
Modify Access Rights	Change values on **Security** page of Holiday Schedule Properties window. Also requires the right, **Read Properties**.
Read Properties	View properties of a holiday schedule.
Modify Properties	Change properties of a holiday schedule. Also requires the right, **Read Properties**.
Rename	Rename a holiday schedule. Also requires the right, **Read Properties**.
Delete	Delete a holiday schedule. Also requires the right, **Read Properties**.

Schedule Page

The **Schedule** page of the Holiday Schedule window allows user to select dates that compose the schedule. Selecting a day as a holiday excludes any schedule that begins during the 24-hour holiday from notification events. Users may page through the calendar months for any year required.



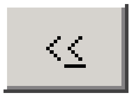
Sun	Mon	Tue	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Schedule Page (Receipt Monitor Schedules, Holiday Schedule Window)

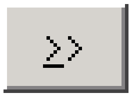
Monthly Calendar

Double-click the left mouse button to select or clear a day as a holiday. Holidays exclude schedules that begin during the 24-hour period from notification events.

Previous Button

Click the Previous button  to display the calendar for the previous month.

Next Button

Click the Next button  to display the calendar for the next month.

Previous Holiday Button

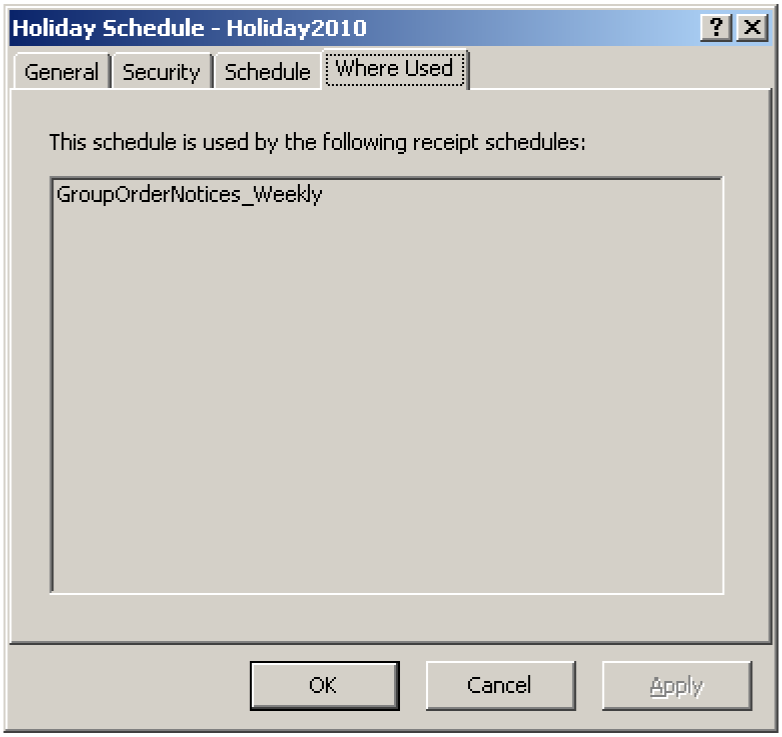
Click the **Previous Holiday** button to move the cursor to the holiday defined prior to the current holiday.

Next Holiday Button

Click the **Next Holiday** button to move the cursor to the next holiday defined after the current holiday.

Where Used Page

The **Where Used** page of the Holiday Schedule window allows users to view which receipt schedules use this holiday schedule. This is useful to determine what definitions would be affected by a change to a holiday schedule.



This schedule is used by the following receipt schedules:

GroupOrderNotices_Weekly

Where Used Page (Receipt Monitor, Holiday Schedule Window)

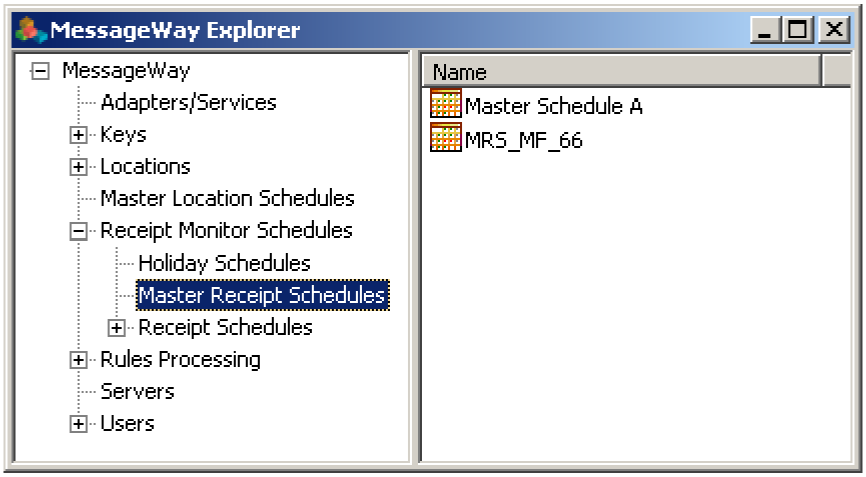
This Schedule Is Used By the Following Receipt Schedules

This list is maintained by MessageWay and displays those receipt schedules that use this holiday schedule.

(Receipt Monitor Schedules) Master Receipt Schedule Window

The Master Receipt Schedule window of the Receipt Monitor allows users to enter master schedules that may be shared by many receipt schedules. Master receipt schedules specify date and time windows when receipt notification is active. These schedules may be excluded by a holiday schedule or modified by a specific receipt schedule.

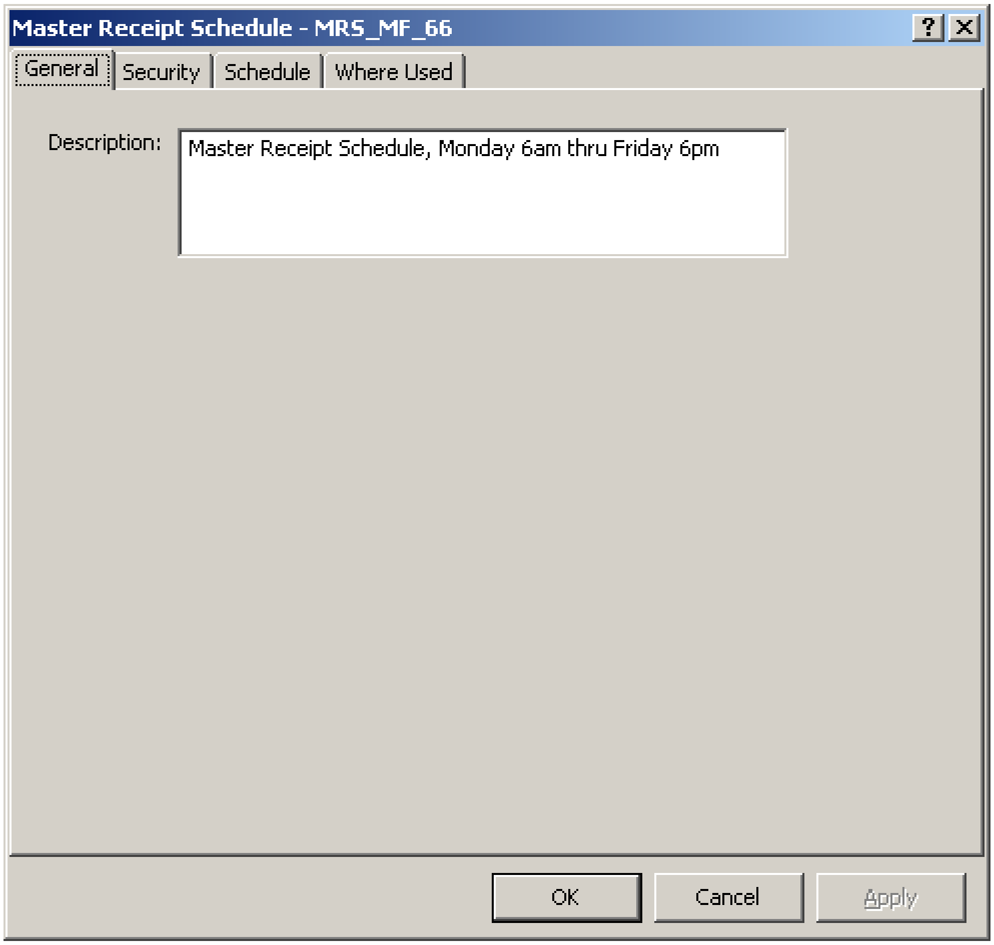
Users may view the list of master receipt schedules in the MessageWay Explorer window.



Master Receipt Schedules List (MessageWay Explorer Window, Receipt Monitor)

General Page

The **General** page of the Master Receipt Schedule window for the Receipt Monitor allows users to type a description for a master schedule.



Description: Master Receipt Schedule, Monday 6am thru Friday 6pm

General Page (Receipt Monitor, Master Receipt Schedule Window)

Description

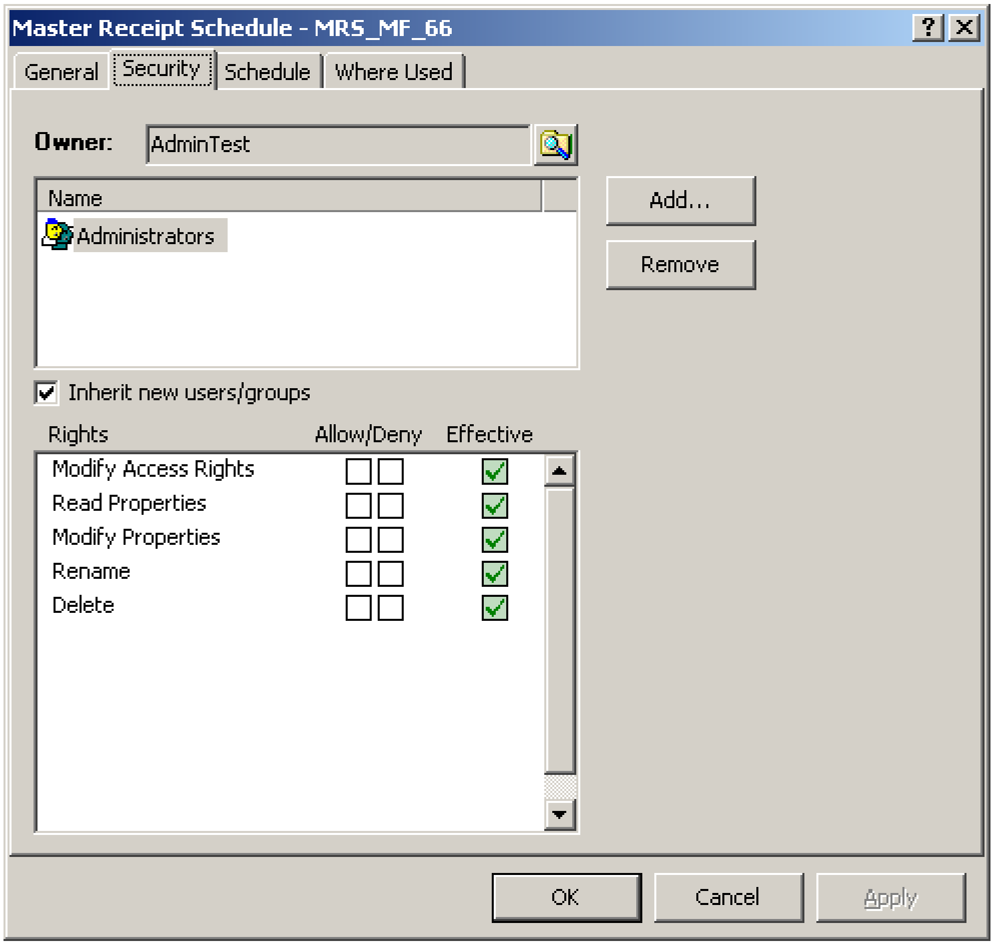
Type a description of the purpose of this schedule.

Security Page

The **Security** page of the Master Receipt Schedule window shows the owner of the schedule, which users or user groups are allowed access to the schedule and what actions these users or user groups may perform.

Access to a schedule is controlled by an access list, which consists of a list of users or user groups and the rights that each one has. The schedule may inherit users and user groups and their rights from the **Master Receipt Schedules** folder. These rights appear in the Effective rights column when you select the user or user group in the **Name** box.

IMPORTANT: To perform any functions for a schedule, users must also have appropriate rights set on their **Rights** page of the User Properties window.



Owner: AdminTest

Name: Administrators

☑ Inherit new users/groups

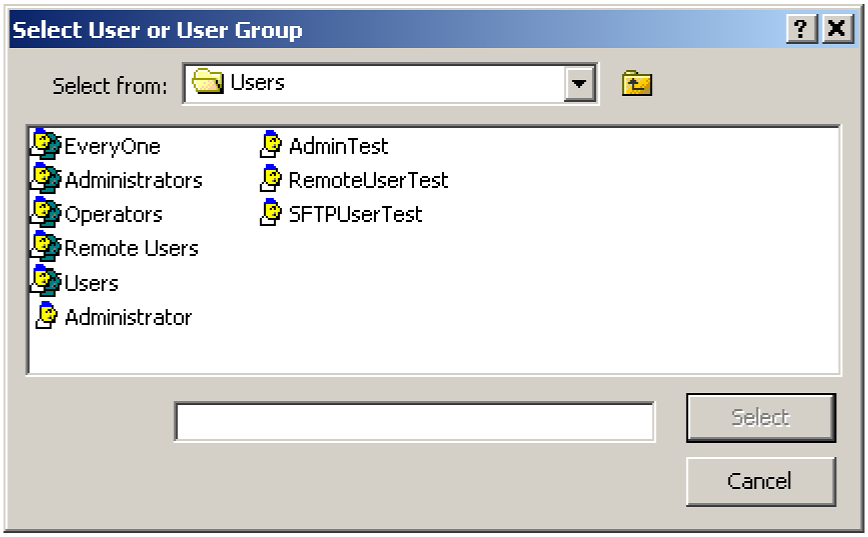
Rights	Allow/Deny		Effective
Modify Access Rights	□	□	☑
Read Properties	□	□	☑
Modify Properties	□	□	☑
Rename	□	□	☑
Delete	□	□	☑

Security Page (Receipt Monitor, Master Receipt Schedule Window)

Check the **Inherit new users/groups** box to add the same users and groups and their rights as listed for the parent folder. To override inherited rights, check the appropriate boxes in the Allow/Deny columns.

Click the **Add** button to give a user or user group access to this schedule. The **Select User or User Group** dialog box appears. Select a group from the list or type the name of a group in the **Select** box, and click the **Select** button.

NOTE: The EveryOne group is on the selection list, but not on the list under the Users folder, unless someone has added it manually. This group is only available for access lists. Add this group to the list to grant access rights to all users. All users are implicitly members of the EveryOne user group. As a result, when EveryOne is added to an access list, the associated rights are granted to all users.



Select User or User Group Window

Owner

Initially, the owner is the user that created the schedule. The owner may transfer ownership to another user. Owners have complete access rights to the object, regardless of other configurations. Owners always have the right to change the names on the access list and the right to read and change the properties of the schedule.

Browse Button

When you are the owner, you may select this button to give ownership to another user.

Name

The Name list contains users or user groups that are permitted to access this schedule. The Name list and the Rights list compose the access list used by MessageWay to determine who has what rights to this schedule. The users or groups on the name list may be inherited from a parent folder. Use the **Add** and **Remove** buttons to maintain this list. To remove inherited names from the list, you must first clear the **Inherit new users/groups** box.

Add Button

Select this button to add names of users or user groups to the Name list.

Remove Button

Select this button to delete names of users or user groups from the access list. To delete the name of a user or user group that has been inherited from its parent folder, you must first clear the **Inherit new users/groups** box.

Inherit new users or groups

When this box is checked, any users or user groups that are added to the Name list of the parent folder will also be added to the Name list of this schedule. To remove inherited users or user groups from the list, you must clear this box first.

Rights

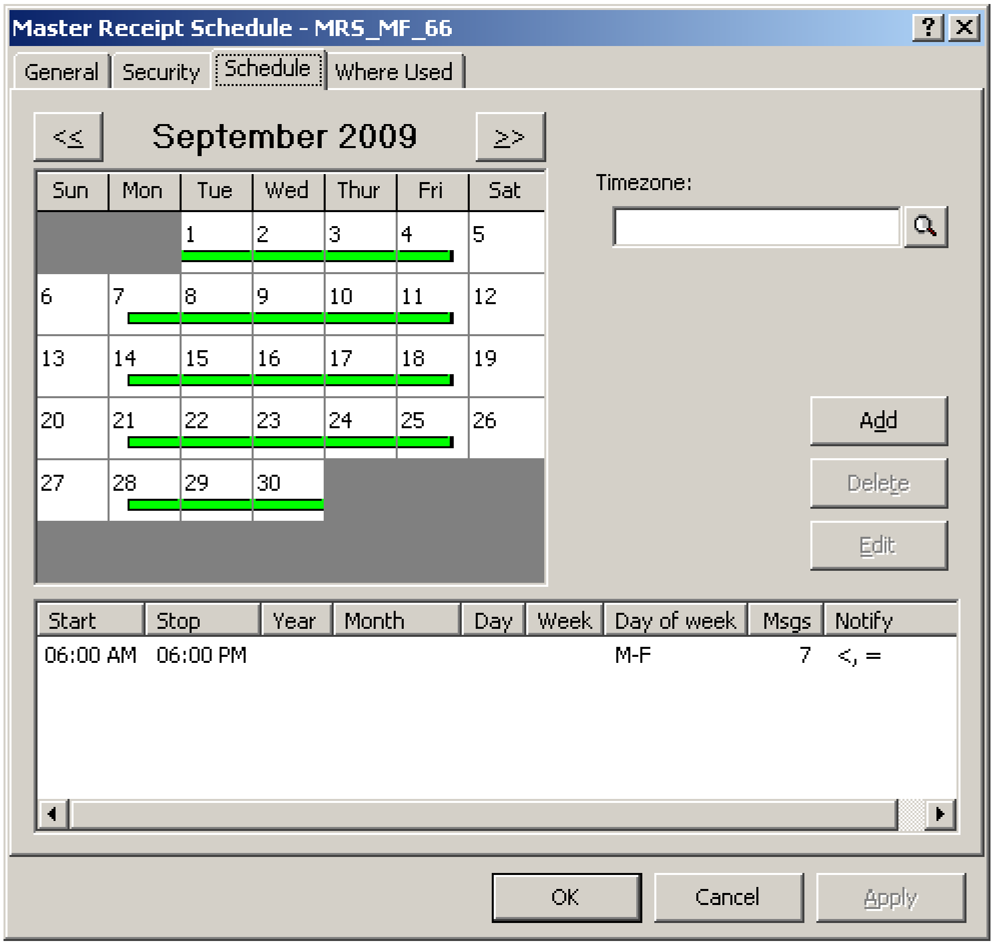
The Rights list contains the functions that the users or user groups in the Name list may perform. The Rights list and the Name list compose the access list to determine who has what rights to this schedule. Schedules may inherit rights from their parent folder. These rights appear in the Effective column when you select the user or user group in the Name list.You may override these effective rights by selecting the Allow/Deny boxes. To select or clear all rights at once, hold **SHIFT** while you select one of the boxes.

The following table describes the rights for master receipt schedules:

Right	Description
Modify Access Rights	Change values on **Security** page of Master Receipt Schedule window. Also requires the right, **Read Properties**.
Read Properties	View properties of a master receipt schedule.
Modify Properties	Change properties of a master receipt schedule. Also requires the right, **Read Properties**.
Rename	Rename a master receipt schedule. Also requires the right, **Read Properties**.
Delete	Delete a master receipt schedule. Also requires the right, **Read Properties**.

Schedule Page

The **Schedule** page of the Master Receipt Schedule window for the Receipt Monitor allows users to enter master receipt schedules.



Master Receipt Schedule - MRS_MF_66

September 2009

Sun	Mon	Tue	Wed	Thur	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

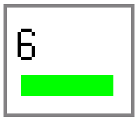
Timezone:

Start	Stop	Year	Month	Day	Week	Day of week	Msgs	Notify
06:00 AM	06:00 PM					M-F	7	<, =

Schedule Page (Receipt Monitor, Master Receipt Schedule Window)

Monthly Calendar

This calendar displays those days of this month for which you have a master receipt schedule defined. Because users may define multiple schedule items for a given day, it helps to understand the use of the visual aids on the calendar.

Visual Aid	Description
	The green bar indicates that there is a schedule for some part of this day. View the schedule date and time in the list box below. Refer to the description for the red bar.

Visual Aid	Description
1 🟨	The yellow square indicates that this day is a holiday and there is no schedule applied to this day.
20 🟥 ▬	The red square and bar indicate that this day is a holiday and there is a schedule for this day that is excluded from notification events. View the schedule in the list box below to determine how long this exclusion persists, because receipt schedules that begin during the 24-hour holiday may span several days. The entire schedule is excluded.

Previous Button

Click the **Previous** button to display the calendar for the previous month.

Next Button

Click the **Next** button to display the calendar for the next month.

Timezone

Time zones default to the time of the MessageWay server. Users may need to select a different time zone for a location. For example, the Remote Execution Server, which is an option for MessageWay, provides the ability to schedule and execute user-defined scripts on a remote server. The time zone feature allows users to schedule scripts based on the time zone of the remote server.

Click the **Schedule** button to choose a different time zone. To remove a timezone, click the **Schedule** button, and when the **Select Timezone** dialog box appears, click **Clear**.

Schedule Items List Box

This box displays the receipt schedule items defined for this schedule.

Add Button

Click this button to add a schedule.

Delete Button (Schedule Item)

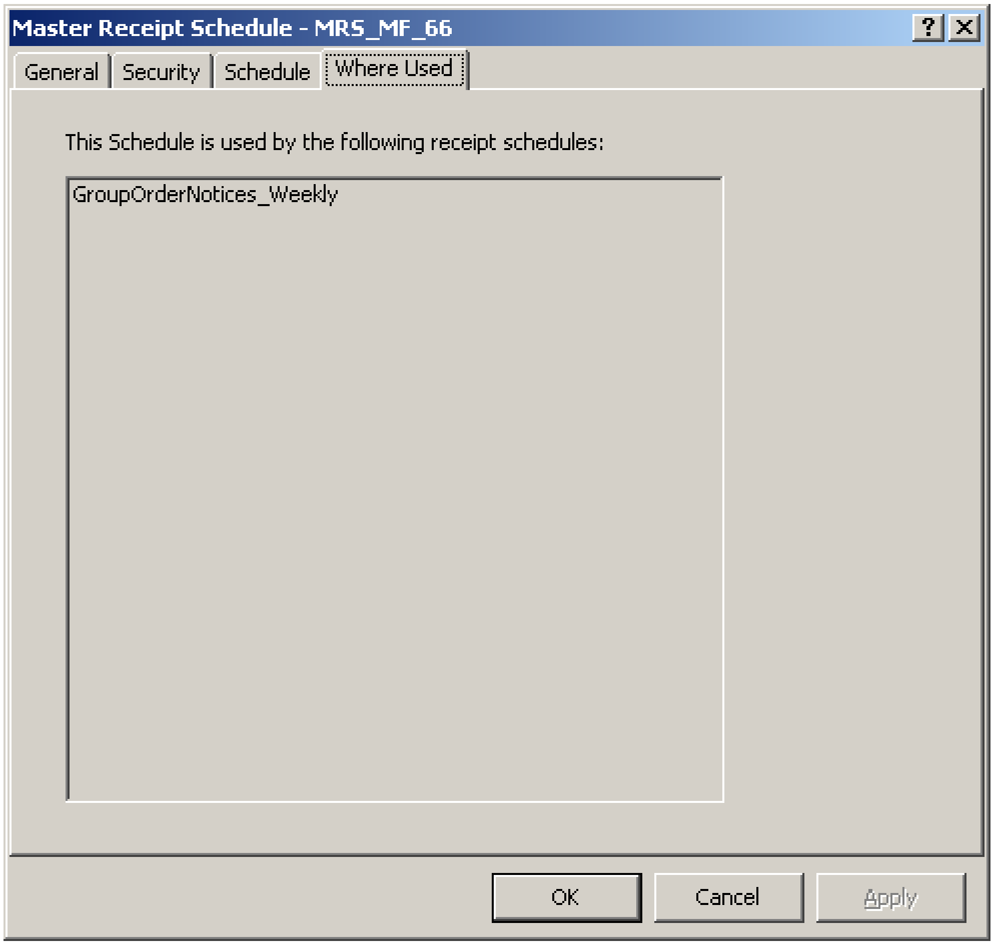
Click this button to delete one or more schedules selected from the list box.

Edit Button

Click this button to edit a schedule selected from the list box.

Where Used Page

The **Where Used** page of the Master Receipt Schedule window allows users to view which receipt schedules use this master receipt schedule. This is useful to determine what definitions would be affected by a change to a master receipt schedule.



Master Receipt Schedule - MRS_MF_66

This Schedule is used by the following receipt schedules:

GroupOrderNotices_Weekly

Where Used Page (Receipt Monitor, Master Receipt Schedule Window)

Receipt Schedule List

This list is maintained by MessageWay and displays those receipt schedules that use this master receipt schedule.

(Receipt Monitor Schedules) Receipt Schedule Window

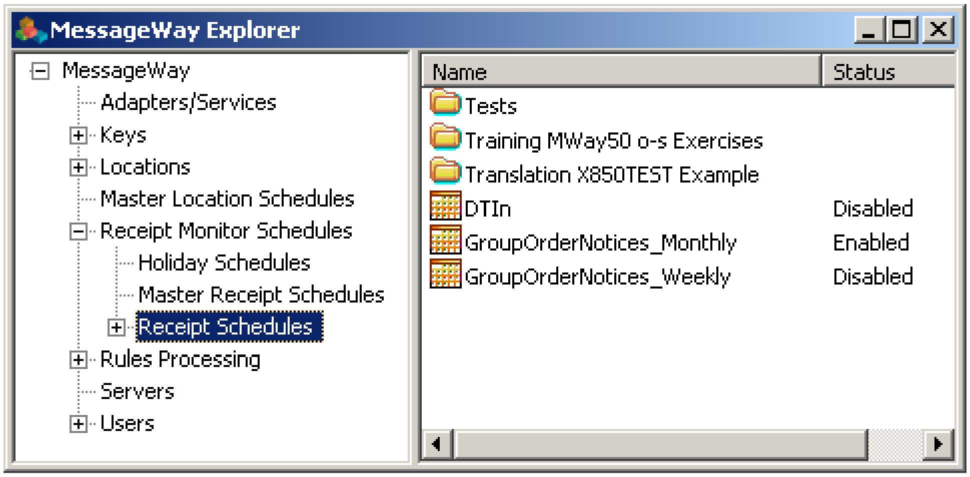
The Receipt Schedule window of the Receipt Monitor allows users to enter schedules for a message sender. Receipt schedules specify date and time windows when receipt notification is active. These schedule windows may be based on a master receipt schedule and a holiday schedule.

When you create a receipt schedule, the receipt schedule name must be the same as the message sender. The message sender is determined by MessageWay as follows:

Source of Message	Message Sender
Disk Transfer, FTP adapters	Input site that retrieves the message.
E-mail adapter	**Reply To** address of an e-mail message or **Sender** address, in that order.
MWTranslator	Sending location as determined by MWTranslator configurations, shown on the Message List and Message Properties windows.

When you use the name of an existing input site, you may access the receipt schedule directly from the site: right-click the site name and selecting **Show receipt schedule** from the menu.

Users may view the list of receipt schedules they have configured in the MessageWay Explorer window.

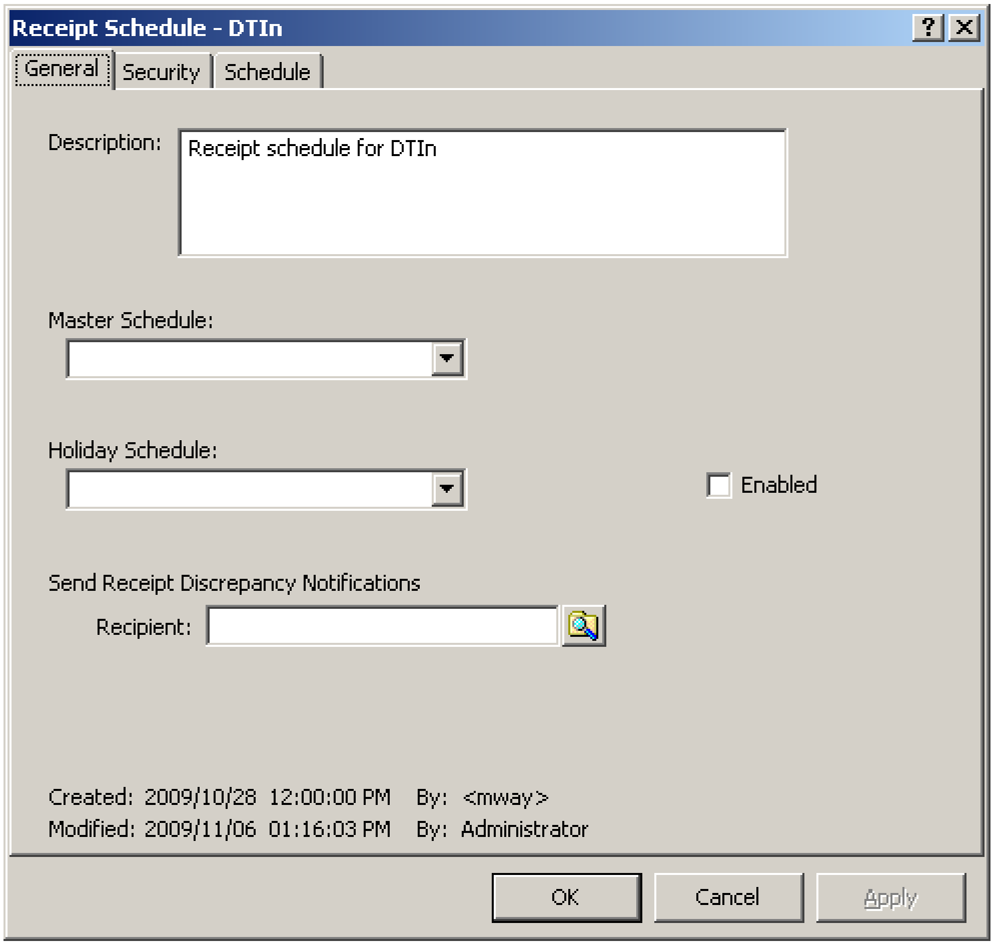


Name	Status
Tests	
Training MWay50 o-s Exercises	
Translation X850TEST Example	
DTIn	Disabled
GroupOrderNotices_Monthly	Enabled
GroupOrderNotices_Weekly	Disabled

Receipt Schedules List (MessageWay Explorer Window, Receipt Monitor)

General Page

The **General** page of the Receipt Schedule window for the Receipt Monitor allows users to describe schedules for an inbound address, associate the schedule with a holiday schedule, and specify a default location to which notification messages will be sent.



Description: Receipt schedule for DTIn

Master Schedule:

Holiday Schedule:

□ Enabled

Send Receipt Discrepancy Notifications

Recipient:

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/06 01:16:03 PM By: Administrator

General Page (Receipt Monitor, Receipt Schedule Window)

Description

Type a description for the purpose of this schedule.

Master Schedule

This field is optional. Select a defined master receipt schedule as a base for receipt schedules for this particular input address. You may then customize particular schedule entries as required.

IMPORTANT: When you customize a receipt schedule that is associated with a master schedule, the receipt schedule is detached from the master to allow you to make changes. Therefore, any subsequent changes made to the master schedule will not be reflected in the receipt schedule. If you decide to add a master schedule to an existing receipt schedule, all schedules will be replaced by those of the master schedule.

Holiday Schedule

This field is optional. Select a defined holiday schedule that exempts periods of time from the days for notification events allowed in the receipt schedule.

Recipient

Type or select one or more addresses to which the receipt discrepancy notifications will be sent.

To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

To enter multiple destinations where the message is piped sequentially to various service locations and where the output of one is the input to the next, press **SHIFT** and select the locations. The locations appear separated by colons.

CAUTION: Do not mix piping and broadcasting syntax, colons and commas, because the order of precedence when mixing is undefined.

When no address is specified here, the notification will be sent to the system mailbox, **{Unknown}**.

Enabled Check Box

Check this box to enable the schedule. Clear the box to disable the schedule without deleting the settings, in case you want to use them later.

Created

Created is the date and time this schedule was created.

By (Created)

This value is the MessageWay user that created the schedule. When a system service creates an entity, this value identifies the service, which appears in angle brackets, < >, to distinguish it from a MessageWay user. For example, imported definitions will use <mwimp>.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

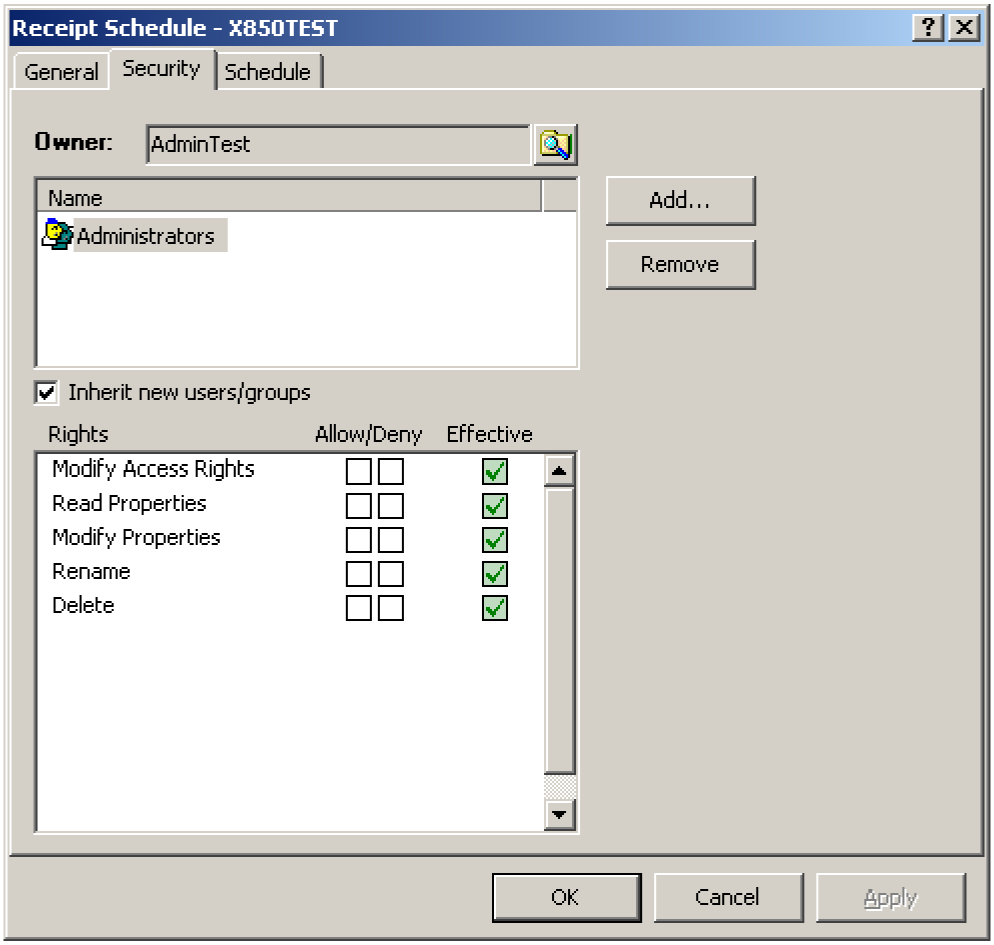
This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

Security Page

The **Security** page of the Receipt Schedule window shows the owner of schedule, which users or user groups are allowed access to the schedule and what actions these users or user groups may perform.

Access to a schedule is controlled by an access list, which consists of a list of users or user groups and the rights that each one has. The schedule may inherit users and user groups and their rights from its parent folder. These rights appear in the Effective rights column when you select the user or user group in the Name box.

IMPORTANT: To perform any functions for a schedule, users must also have appropriate rights set on their **Rights** page of the User Properties window.



Receipt Schedule - X850TEST

General | Security | Schedule

Owner: AdminTest

Name
Administrators

☑ Inherit new users/groups

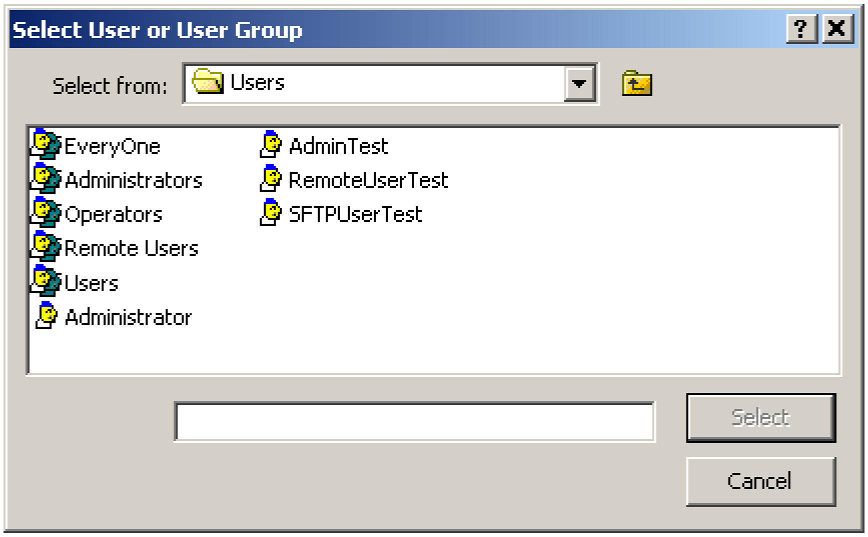
Rights	Allow/Deny	Effective
Modify Access Rights	□ □	☑
Read Properties	□ □	☑
Modify Properties	□ □	☑
Rename	□ □	☑
Delete	□ □	☑

Security Page (Receipt Monitor, Receipt Schedule Window)

Check the **Inherit new users/groups** box to add the same users and groups and their rights as listed for the parent folder. To override inherited rights, check the appropriate boxes in the Allow/Deny columns.

Select the **Add** button to give a user or user group access to this schedule. The Select User or User Group window appears. Select a group from the list or type the name of a group in the Select box, and choose the **Select** button.

NOTE: The EveryOne group is on the selection list, but not on the list under the Users folder, unless someone has added it manually. This group is only available for access lists. Add this group to the list to grant access rights to all users. All users are implicitly members of the EveryOne user group. As a result, when EveryOne is added to an access list, the associated rights are granted to all users.



Select from: Users

Select User or User Group

Owner

Initially, the owner is the user that created the schedule. The owner may transfer ownership to another user. Owners have complete access rights to the object, regardless of other configurations. Owners always have the right to change the names on the access list and the right to read and change the properties of the schedule.

Browse Button

When you are the owner, you may select this button to give ownership to another user.

Name

The Name list contains users or user groups that are permitted to access this schedule. The Name list and the Rights list compose the access list used by MessageWay to determine who has what rights to this schedule. The users or groups on the name list may be inherited from a parent folder. Use the **Add** and **Remove** buttons to maintain this list. To remove inherited names from the list, you must first clear the **Inherit new users/groups** box.

Add Button

Select this button to add names of users or user groups to the Name list.

Remove Button

Select this button to delete names of users or user groups from the access list. To delete the name of a user or user group that has been inherited from its parent folder, you must first clear the **Inherit new users/groups** box.

Inherit new users or groups

When this box is checked, any users or user groups that are added to the Name list of the parent folder will also be added to the Name list of this schedule. To remove inherited users or user groups from the list, you must clear this box first.

Rights

The Rights list contains the functions that the users or user groups in the Name list may perform. The Rights list and the Name list compose the access list to determine who has what rights to this schedule. Schedules may inherit rights from their parent folder. These rights appear in the Effective column when you select the user or user group in the Name list.You may override these effective rights by selecting the Allow/Deny boxes. To select or clear all rights at once, hold **SHIFT** while you select one of the boxes.

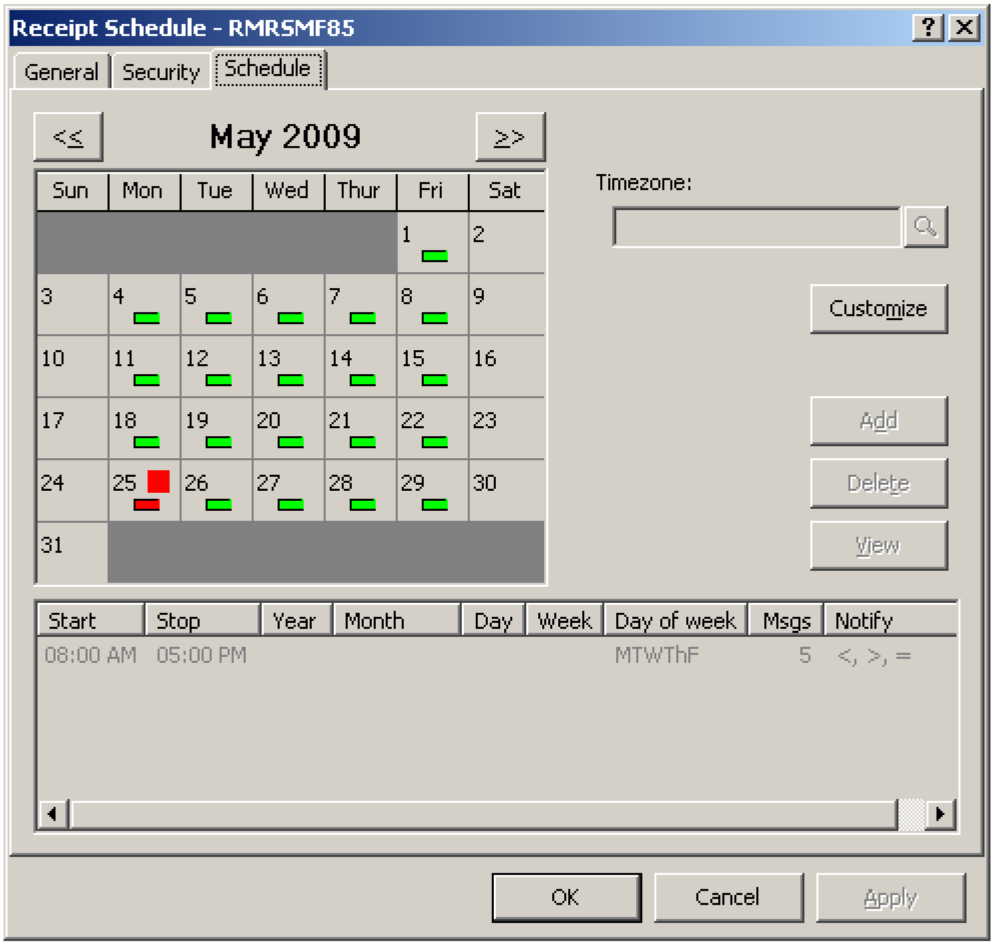
The following table explains the rights for the Receipt Schedule Properties window:

Right	Description
Modify Access Rights	Change values on **Security** page of Receipt Schedule Properties window. Also requires the right, **Read Properties**.
Read Properties	View properties of a receipt schedule.
Modify Properties	Change properties of a receipt schedule. Also requires the right, **Read Properties**.
Rename	Rename a receipt schedule. Also requires the right, **Read Properties**.
Delete	Delete a receipt schedule. Also requires the right, **Read Properties**.

Schedule Page

The **Schedule** page of the Receipt Schedule window for the Receipt Monitor allows users to enter receipt schedules for a particular inbound address, which could also be a configured location. These schedules are subject to exclusion from the optional holiday schedule. The holiday schedule may be specified on the **General** page.

When you specify a master receipt schedule on the **General** page, you must select the **Customize** button to modify the schedule items. Once you modify the receipt schedule, it is no longer associated with the master schedule. The master schedule will be removed from the **General** page. When a schedule uses a master receipt schedule, the entire page appears dimmed.

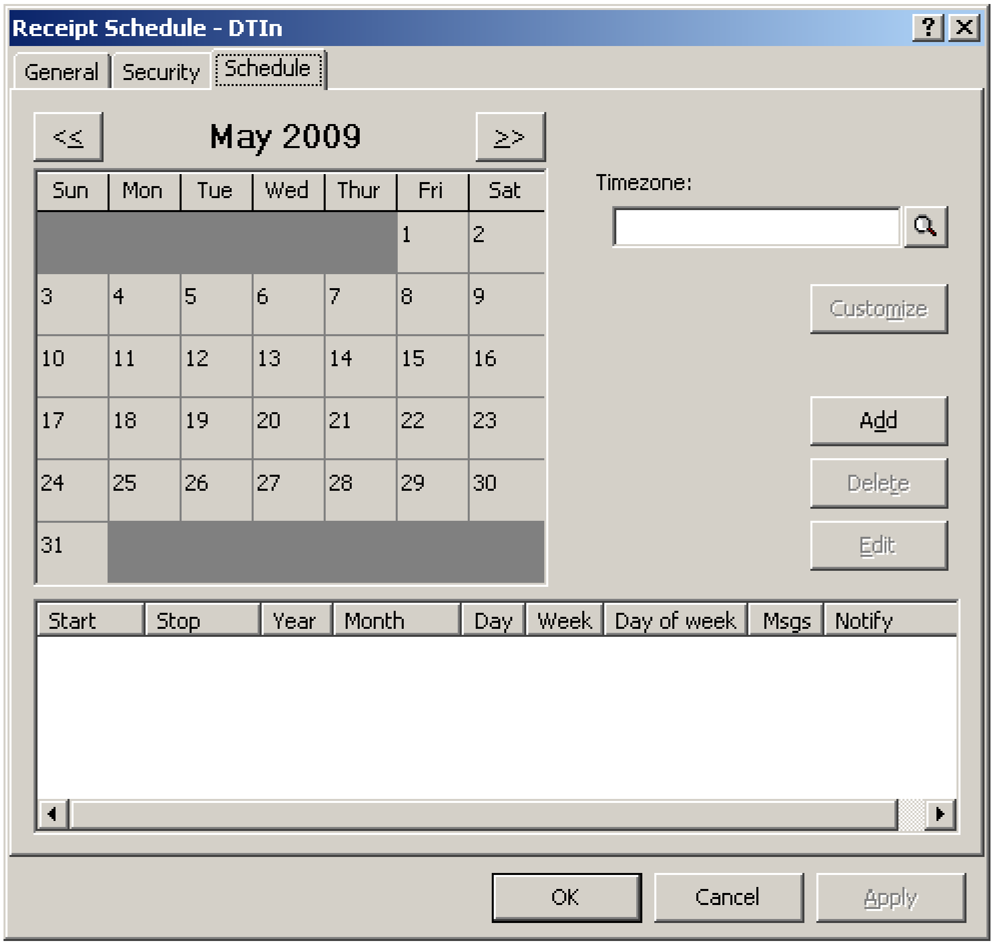


Sun	Mon	Tue	Wed	Thur	Fri	Sat
					1 🟩	2
3	4 🟩	5 🟩	6 🟩	7 🟩	8 🟩	9
10	11 🟩	12 🟩	13 🟩	14 🟩	15 🟩	16
17	18 🟩	19 🟩	20 🟩	21 🟩	22 🟩	23
24	25 🟥	26 🟩	27 🟩	28 🟩	29 🟩	30
31						

Start	Stop	Year	Month	Day	Week	Day of week	Msgs	Notify
08:00 AM	05:00 PM					MTWThF	5	<, >, =

Schedule Page Using Master Receipt Schedule (Receipt Monitor, Receipt Schedule Window)

When you do not specify a master receipt schedule on the **General** page, you simply click the **Add** button to create schedule items.



Sun	Mon	Tue	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Schedule Page Not Using Master Receipt Schedule (Receipt Monitor, Receipt Schedule Window)

Monthly Calendar

This calendar displays those days of this month for which you have a receipt schedule or a holiday defined. Because users may define multiple schedule items for a given day, it helps to understand the use of the visual aids on the calendar.

Visual Aid	Description
6 🟩	The green bar indicates that there is a schedule for some part of this day. View the schedule date and time in the list box below. Refer to the description for the red bar.
1 🟨	The yellow square indicates that this day is a holiday and there is no schedule applied to this day.

Visual Aid	Description
20 🟥 ▬	The red square and bar indicate that this day is a holiday and there is a schedule for this day that is excluded from notification events. View the schedule in the list box below to determine how long this exclusion persists, because receipt schedules that begin during the 24-hour holiday may span several days. The entire schedule is excluded.

Previous Button

Click the **Previous** button to display the calendar for the previous month.

Next Button

Click the **Next** button to display the calendar for the next month.

Timezone

Time zones default to the time of the MessageWay server. Users may need to select a different time zone for a location. For example, the Remote Execution Server, which is an option for MessageWay, provides the ability to schedule and execute user-defined scripts on a remote server. The time zone feature allows users to schedule scripts based on the time zone of the remote server.

Click the **Schedule** button to choose a different time zone. To remove a timezone, click the **Schedule** button, and when the **Select Timezone** dialog box appears, click **Clear**.

Customize Button

When this button is inactive, this receipt schedule is not associated with a master schedule. When this button is active, the schedules displayed are from a master schedule. To modify the schedules that were based on a master schedule, you must first select the **Customize** button. When you select the **Customize** button it becomes inactive, and the master schedule is removed from the General page.

CAUTION: When you customize a receipt schedule, the receipt schedule is detached from the master to allow you to make changes. Therefore, any subsequent changes made to the master schedule will not be reflected in the receipt schedule. If you decide to add a master schedule to an existing receipt schedule, all schedules will be replaced by those of the master schedule.

Add Button

When this button is not active, the schedules displayed are from a master receipt schedule. To activate this button, you must first click the **Customize** button. Click this button to add a schedule.

Delete Button (Schedule Item)

When this button is not active, the schedules displayed are from a master receipt schedule. To activate this button, you must first click the **Customize** button. Click this button to delete one or more schedules selected from the list.

Edit Button

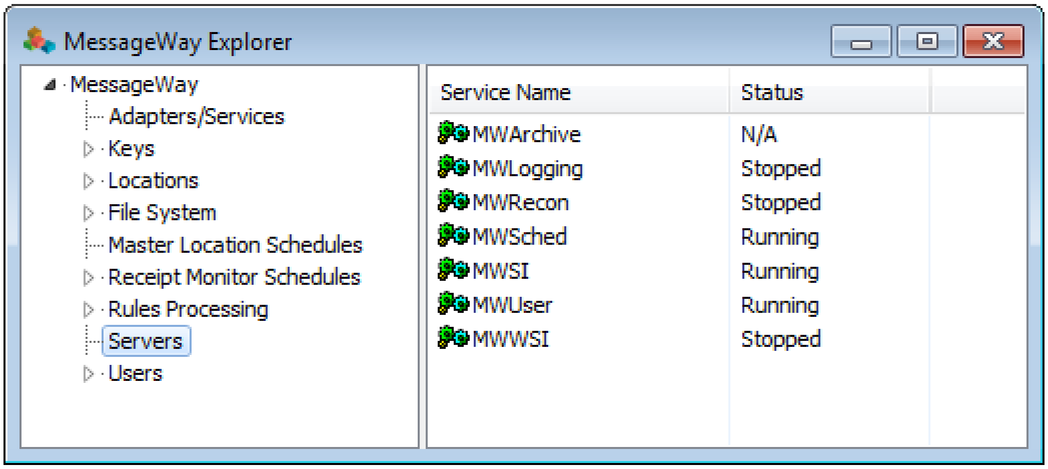
When this button is not active, the schedules displayed are from a master receipt schedule. To activate this button, you must first click the **Customize** button. Click this button to edit a schedule selected from the list.

Receipt Schedule List box

This box displays the dates and times of the receipt schedule items.

Server Properties Window

The servers that may be configured and started and stopped from the Manager are in the Servers folder of MessageWay Explorer. The servers have the same type of information on their **General** and **Security** pages. Some have specific information on an additional page.



Service Name	Status
MWArchive	N/A
MWLogging	Stopped
MWRecon	Stopped
MWSched	Running
MWSI	Running
MWUser	Running
MWWSI	Stopped

Servers Pane (MessageWay Explorer Window)

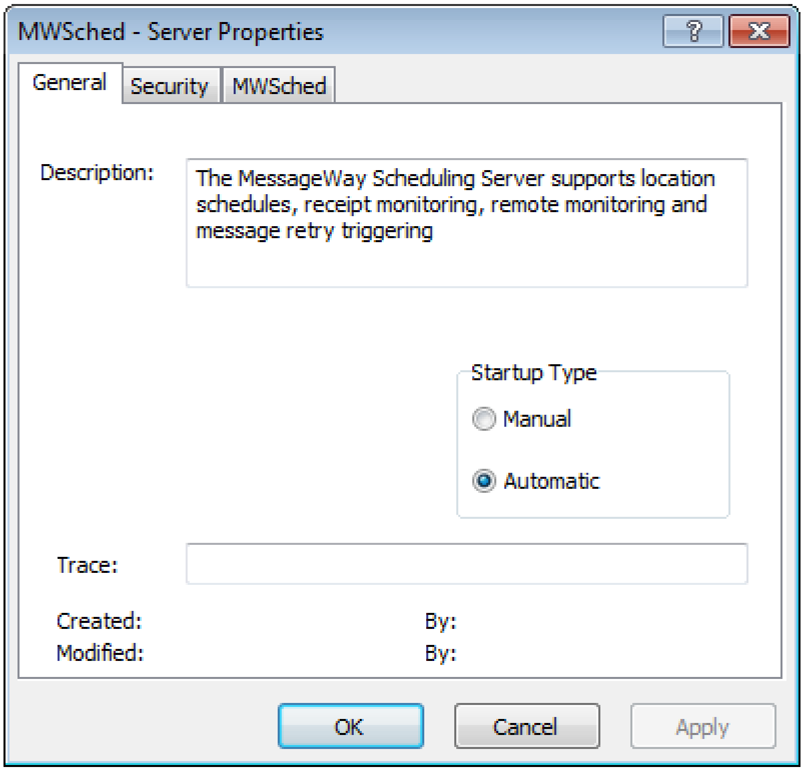
The following table describes the services each server provides:

Server	Description of Services
MWArchive	MessageWay Archive provides system-wide configurations for archiving.
MWLogging	(For MWTranslator) MessageWay Logging Server logs information about output documents created from an input document. Logging is required for reconciliation.

Server	Description of Services
MWRecon	(For MWTranslator) MessageWay Reconciliation Server reconciles output documents sent to trading partners with returned acknowledgments.
MWSched	MessageWay Scheduling Server supports location schedules, receipt monitor schedules, monitoring for the Remote Execution Server, triggers to retry message delivery and removal of inactive sessions.
MWSI	MessageWay Service Interface provides access to MessageWay from outside connections.
MWUser	MessageWay User Server provides security for users that access MessageWay from the MessageWay Manager.

(Server Properties) General Page

The **General** Page provides a description of the server and allows users to select a startup type and, for debugging, configure trace options.



Description: The MessageWay Scheduling Server supports location schedules, receipt monitoring, remote monitoring and message retry triggering

Startup Type
○ Manual
● Automatic

Trace:

Created: By:
Modified: By:

Description

This is the full description of the server.

Startup Type

The startup type can be either Manual or Automatic. Click A**utomatic** to start this server when MessageWay starts. Click Manual to let the user start the server.

Trace

This option specifies the type of activity to log to the MessageWay database for the server. Then you can filter and view the information using the Search Trace Logs feature, or using the trace utility. Enter a list of types, separated by commas, that you want to use to appear in the trace log. The types available vary by server. You may also type an asterisk (*) to trace all activity. You can limit the log information further by location, message ID, user and/or IP address.

The trace utility, mwtrace, allows you to view trace information, online or from a disk file, and to delete trace records from the database. For information about how to use the trace utility, in the Troubleshooting section, refer to the topic, ***Tracing Activity for an Adapter, Service or Server*** (on page 877).

CAUTION: The trace process may have a significant impact on performance, especially when you use the asterisk * to trace everything, and particularly for the MessageWay User Server, mwuser. Except for the MessageWay Messaging Server, tracing starts as soon as you enter your trace options and click **Apply** or **OK**. When you have finished debugging, clear the field of all text to turn off the trace. If there is an asterisk in a trace field of core or other active servers when MessageWay starts, you risk overwhelming your system with trace activity.

The syntax of the trace option is as follows:

trace-type-list [: [*location-list*] [: [*msgid-list*] [: [*user-list*] [: *ip-list*]]]]

Where the following rules apply:

- Trace-type is mandatory
- Each list must be separated from other lists by a colon (**:**)
- Each list may contain one or more items, separated by commas
- Trace-type-list only may use the asterisk (*****) in place of a list of types (not recommended)

Trace Component	Description
trace-type	One of the predefined types in the following table, for example, ftp, queue, pipe, sched
location	Name of a MessageWay location
msgid	MessageWay message ID

Trace Component	Description
trace-type	One of the predefined types in the following table, for example, ftp, queue, pipe, sched
user	Name of a MessageWay user
ip	Source IP address for an mwsi connection

The following table describes some examples. The value under Trace Option would be the value entered in the appropriate Trace field. The results vary depending on where the trace is defined.

Trace Option	Description
`*`	Logs all activity for the entity (not recommended)
`pipe:::AdminTest`	Logs all pipe activity for the entity associated with the user, AdminTest
`pipe:DTIN`	Logs all pipe activity for the location, DTIN

The following table shows which types are useful for MessageWay internal system servers.

Trace Type	messageway	mwsched	mwuser	mwsi
auditlog	OK	OK	OK	OK
connects			OK	
counts	OK			
DST		OK		
enctcp			OK	
heartbeat			OK	
http				OK
httpbody				OK
http-chunk				OK
ldap			OK	OK
pipe	OK	OK	OK	OK
pipe-buffer	OK	OK	OK	OK
queue	OK	OK		
receipt		OK		
receipt-actual		OK		
receipt-detail		OK		

Trace Type	messageway	mwsched	mwuser	mwsi
remote		OK		
remote-detail		OK		
resend	OK			
sched		OK		
sched-detail		OK		
sessions		OK		
si				OK
ssl		OK		OK
tcp			OK	OK

Note the following:

- messageway = MessageWay Messaging Server, MessageWay Server
- mwsched = MessageWay Scheduling Server
- mwuser = MessageWay User Server
- mwsi = MessageWay Service Interface
-

Created

Created is the date and time the server was installed.

By (Created)

The system service itself creates this value. When a system service creates an entity, this value identifies the service, which appears in angle brackets, < >, to distinguish it from a MessageWay user. For example, imported definitions will use <mwimp>.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

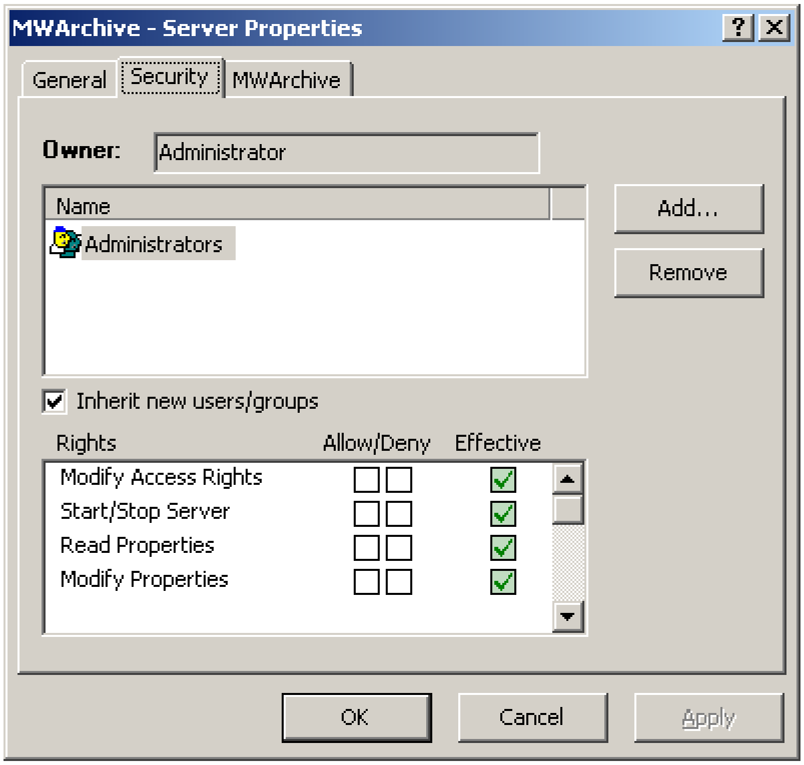
This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

(Server Properties) Security Page

The **Security** page of the Server Properties window shows the owner of server, which users or user groups are allowed access to the server and what actions these users or user groups may perform.

Access to a server is controlled by an access list, which consists of a list of users or user groups and the rights that each one has. The schedule may inherit users and user groups and their rights from the **Servers** folder. These rights appear in the Effective rights column when you select the user or user group in the Name list.

IMPORTANT: To perform any functions for a server, users must also have appropriate rights set on their **Rights** page of the User Properties window.



Owner: Administrator

Name
Administrators

☑ Inherit new users/groups

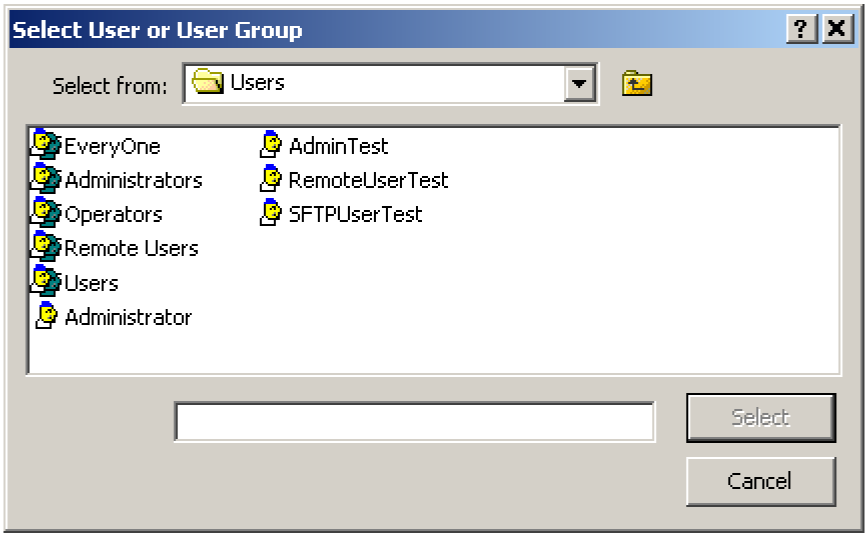
Rights	Allow/Deny	Effective
Modify Access Rights	□ □	☑
Start/Stop Server	□ □	☑
Read Properties	□ □	☑
Modify Properties	□ □	☑

Security Page (Server Properties Window)

Here are some things you can do:

- To add the same users and groups and their rights as listed for the parent folderCheck the **Inherit new users/groups** box.
- To override inherited rights, check the appropriate boxes in the Allow/Deny columns.
- To give a user or user group access to this server, click the **Add** button. When the Select User or User Group window appears, select a group from the list or type the name of a group in the Select box, and choose the **Select** button.

NOTE: The EveryOne group is on the selection list, but not on the list under the Users folder, unless someone has added it manually. This group is only available for access lists. Add this group to the list to grant access rights to all users. All users are implicitly members of the EveryOne user group. As a result, when EveryOne is added to an access list, the associated rights are granted to all users.



Select User or User Group Window

Owner

Initially, the owner is the user that created the server, which is always the original administrator. The owner may transfer ownership to another user. Owners have complete access rights to the server, regardless of other configurations. Owners always have the right to change the names on the access list and the right to read and change the properties of the server.

Browse Button

When you are the owner, you may select this button to give ownership to another user.

Name

The Name list contains users or user groups that are permitted to access this server. Use the **Add** and **Remove** buttons to maintain this list. The Name list and the Rights list comprise the access list used by MessageWay to determine who has what rights to this server.

Add Button

Select this button to add names of users or user groups to the Name list.

Remove Button

Select this button to delete names of users or user groups from the access list.

Inherit New Users or Groups

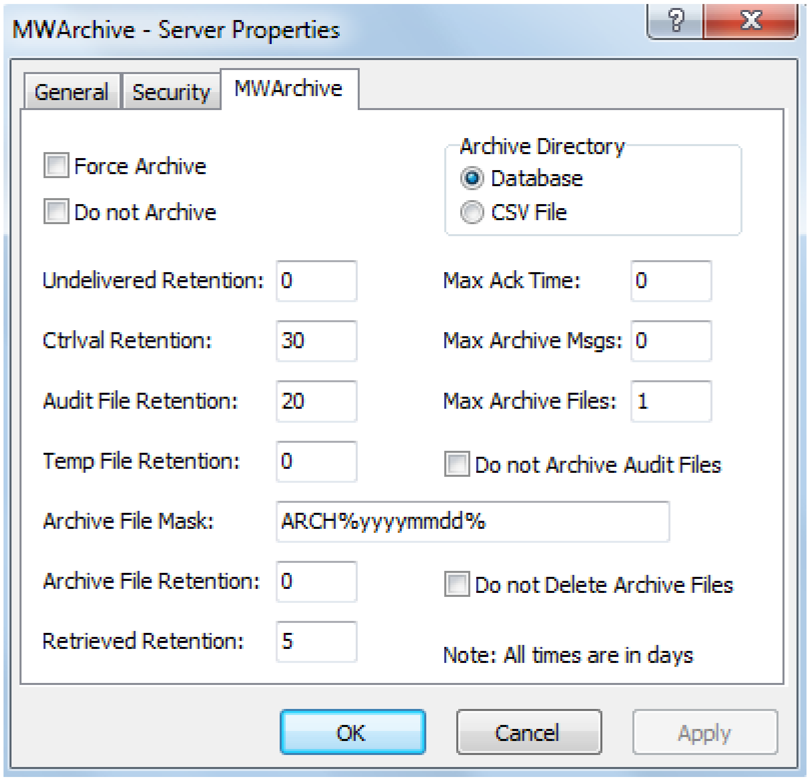
Check this box to add any users or user groups that are on the Name list of of the **Servers** folder to the Name list of this server. To remove users or user groups from the list that have been inherited from the **Servers** folder, you must clear this box first.

Rights

The Rights list contains the functions that the users or user groups in the Name list may perform. The Rights list and the Name list compose the access list to determine who has what rights to this server. A server may inherit rights from the **Servers** folder. These rights appear in the Effective rights column when you select the user or user group in the Name list. Check the Allow/Deny boxes to override these effective rights. To check or clear all rights at once, hold **SHIFT** while you click one of the boxes.

MWArchive Page

The MWArchive page allows users to configure system-wide settings for archiving, some of which override other specific settings.



□ Force Archive

□ Do not Archive

Archive Directory
● Database
○ CSV File

Undelivered Retention: 0

Ctrlval Retention: 30

Audit File Retention: 20

Temp File Retention: 0

Archive File Mask: ARCH%yyyymmdd%

Archive File Retention: 0

Retrieved Retention: 5

Max Ack Time: 0

Max Archive Msgs: 0

Max Archive Files: 1

□ Do not Archive Audit Files

□ Do not Delete Archive Files

Note: All times are in days

MWArchive Page (Server Properties Window)

Force Archive

Check this box to set a system-wide flag that forces all messages to be archived when they are eligible. This overrides the archive flag for individual locations. Clear this box to allow location configurations to control the archive process.

Do Not Archive Check Box

Check this box to set a system-wide flag that deletes all messages when they are eligible without archiving them first. This overrides the archive flag for individual locations. Clear this box to allow location configurations to control the archive process. This option is particularly useful for test systems. Otherwise, users must manually mark each message for delete.

Archive Directory

Choose whether to store the archive directory information in the database or on disk as comma-separated-value (CSV) files.

Header Retention

When the archive directory is stored in the ArchiveMessages table of the database, type the number of days to retain header detail records. Records will be deleted when (Archive program run date > ArchiveTime + Header Retention). A value of *0* (zero) means that these header records with cross-references to the archived message files are retained indefinitely. This value does not affect the archive directory when it is stored on disk in the ArchiveDirectory.csv file, which users must maintain manually.

Undelivered Retention

Normally, only messages with a status of *Complete* and that meet other criteria will be archived or deleted. This option affects messages with a status of *Error, Available* or *Canceled.* The *Undelivered Retention* option is the number of days after the date of the inbound timestamp when the qualifying message will be eligible for archive or delete.

When the value is **0**, messages with a status of *Error*, *Available* or *Canceled* will remain on the system and are not eligible for archive or delete.

When the value is **1** or more, messages will be available for archive or delete that meet the following conditions:

- Have a status of *Error*, *Available* or *Canceled*
  - and -
- When the *later* one of these two events occurs (the later date takes precedence):
  - The message has passed the retention date
    - or -
  - The message has passed the date calculated by adding the Undelivered Retention days to the inbound complete timestamp

Ctrlval Retention

This option is used for the MWTranslator Enhanced Control Reference Processing. CTRLVAL is part of the optional Control Reference Processing in MWTranslator that is used to validate control references in incoming data. Type the number of days after which you want the archive process to delete records from the CTRLVAL file. The default value is 30 days. This setting does not affect deletion of messages.

Audit File Retention

This value controls the retention of the audit and eventlog records stored in the database. Type the number of days after which the audit and eventlog records will be deleted or archived. The default is 20 days. When audit records are also written to disk, they are stored in two types of files: Audit files, names beginning with *audit* that log user activity from the MessageWay Manager; Service Interface audit files, names beginning with *siaudit* that log activity from remote users. These files will also be retained for the number of days set here.

Temp File Retention

Type the number of days to retain any temporary files in the /server/temp, /server/<adapter or service>/temp and /server/<adapter or service>/tmp directories. The default is 30 days. To retain the files indefinitely, type **0** (zero).

For example, temporary files are used by:

- MWTranslator for logging and reconciliation. Normally, these are automatically removed.
- MWCustomIO and MWCustomProc to place scripts for execution that are stored in MessageWay. These scripts are not started from a command line that resides in memory, but from this temporary disk location. In the event of a script failure, these may be left for debugging.

Archive File Mask

Type the mask used to create file names for the compressed and log files created by the archive program. The compressed files contain message content, message detail information and audit files. The log files contain statistics for the execution of the archive program. Use any combination of constants and MessageWay tokens. These files are located in the messageway\archives directory on Windows and in /var/opt/messageway/archives directory on UNIX/Linux.

The valid tokens are:

Token	**Description**
applid	Counting from the left, the first eight characters up to a period (.) that will be displayed in the Filename property of a message.
classid	By default, the classid value is extracted from the input message. Users may also assign a class ID. To do this, simply use literals for the class ID, for example: To assign a class ID to an output message, type: **MyClassID@MyLocationName** To assign a class ID to a mask for a file name, type: **MyClassID%yyyymmdd%.txt**
contenttype	Content type associated with a message. The content type uses the MIME type/subtype notation and values typically used with SMTP, POP3 and HTTP. If a content type is not provided with a new message, MessageWay determines the type from the first 250 bytes of data. An unrecognized content type is set to blank and assumed to be application/octet-stream.
ddd	Julian date to specify numeric day within a year. Padded on the left with zero (0) for a width of 3 (001-366).
dd	Day of month. Padded on the left with zero (0) for a width of 2 (01–31).
d	Day of month without padding (1-31).

Token	Description
filebase	All characters to left of the last decimal mark in a filename. When not found, no value is returned.
fileext	All characters to right of the last decimal mark in a filename. When not found, the filename value will be returned.
filename	Name of file up to 128 characters, which may include a base value, a decimal mark and a file extension.
gmt:	When followed by date/time tokens, this will be the current GMT time.
gmttimei:	When followed by date/time tokens, this will be the Inbound Start Time in GMT.
gmttimec:	When followed by date/time tokens, this will be the current GMT time.
gmttimeo:	When followed by date/time tokens, this will be the current Outbound Start Time in GMT.
hh	Hour of day. Padded on the left with zero (0) for a width of 2 (00-23).
h	Hour of day without padding (0-23).
inputmsgid	Input Message Id of the message.
inputname	Input Name.
location	The MessageWay location where the message resides. Replaces *mailbox*.
msgid	The Message Id of the message. Replaces *msg*.
ms	Milliseconds (000-999). **NOTE:** The Manager shows milliseconds on Message Properties.
mmmm	Full month name (January, February, March)
mmm	Abbreviated month name (Jan,Feb,Mar)
mm	Month number. Padded on the left with zero (0) for width of 2 (01-12).
m	Month number (1-12).
nn	Minutes. Padded on the left with zero (0) for a width of 2 (00-59).
n	Minutes (0-59).
outputname	Output Name
recipient	Message Recipient
sender	Message Sender
ss	Seconds. Padded on the left with zero (0) for a width of 2 (00-59).
s	Seconds (0-59).
timei:	When followed by date/time tokens, this will be the Inbound Start Time.

Token	Description
timec:	When followed by date/time tokens, this will be the current time.
timeo:	When followed by date/time tokens, this will be the Outbound Start Time.
yyyy	Four digit year.
yy	Two digit year.
#!	Non-persistent counter (1-999999999). When the adapter or service is restarted, this number reinitializes to 1.
#	Persistent counter (1-999999999).
#@name	Persistent named counter.
#@classid	Persistent counter specific to classid
#@classloc	Persistent counter specific to classid and location
#@inputname	Persistent counter specific to input name
#@outputname	Persistent counter specific to output name
#@sender	Persistent counter specific to sender name
#@recipient	Persistent counter specific to recipient name
#@location	Persistent counter specific to location

Here are some examples:

```
MW%msgid%.txt

TR%yyyymmddhhnnss#%.txt
```

To pad or truncate values that replace tokens, you can use :n after the token. The following table describes a couple of specialized examples:

Token	Description
%#:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999)

Token	Description
%#!:n%	System generated sequence of fixed width n, where n = 0-9. The number of names are guaranteed to be unique within a one-minute period shown in the following examples: To allow 9 unique names per minute, n=1 (1-9) To allow 99 unique names per minute, n=2 (01-99) To allow 999 unique names per minute, n=3 (001-999) When the MessageWay server is restarted, this number reinitializes to 1.

Here are some examples:

```
%#@classloc:4%
%applid:8%
X%ddhhnn#:3%.xml
```

TIP: On systems that allow file names longer than 8 characters, use the *msgid* token to easily relate the output message with the message in MessageWay. The message ID is unique. Use the *filename* token if you want a persistent name that is applied to the message throughout its life cycle, unless it is changed by a rules profile setting. A filename does not have to be unique in MessageWay.

When MessageWay receives a value for the Filename, it validates it and modifies it as necessary using the following rules:

- All input paths will be removed.
- Maximum of 128 characters in length, left justified. Characters greater than the 128 will be truncated.
- The period character cannot occur consecutively. The second period and all subsequent consecutive occurrences to the right of the first will be deleted.
- The following restricted characters will be replaced with the underscore, _:
  \ / : * ? " < > | ! & ` ' ;

NOTE: In MessageWay 6.1, parentheses were removed from the list and are now stored in the database as parentheses.

- Duplicate Filename values are allowed within the same location within the Locations folder.

Duplicate Filenames are *not* allowed within the same location within the File System folder, unless one has been canceled.

Archive File Retention

Type the number of days to retain archive files and all related MessageWay Archive Messages. Archive files and messages will be deleted when (Archive program run date > Archived Date - Archive File Retention). A value of 0 (zero) means that Archive files and messages will be retained indefinitely.

Retrieved Retention

Type the number of days to retain Archive Message retrieved content. Retrieved content will be deleted when (Archive program run date > Retrieved Date - Retrieved Retention). A value of 0 (zero) means that retrieved content will be deleted along with the Archive file (see Archive File Retention). Note that retrieved content may also be manually deleted from the manager program.

Max Ack Time

This option is used for the MWTranslator Reconciliation processing. When some part of the message is awaiting an acknowledgment, such as an interchange, functional group or document, by default, the message will not be archived until the required acknowledgment is received. This option overrides the requirement.

The *Max Ack Time* specifies a number of days after the outbound timestamp when the message will be eligible for archive or delete. A message whose parts are awaiting an acknowledgment will be eligible for archive or delete when the later one of these two events occurs:

- The message has passed the retention date
  - or -
- The message has passed the date calculated from the outbound timestamp plus the *Max Ack Time* days.

Max Archive Messages

Type the maximum number of messages to be archived to a file before a new file is created. When a very large number of messages will be archived to one file, it is possible to run out of memory. To avoid memory problems, this option archives a specified number of messages to separate files, creating new files until all messages have been archived.

Max Archive Files

When you use Max Archive Messages, type the maximum number of files to be created during a single run of the archive program. This option limits the number of files created, which may not archive all messages during the run, but remaining messages can be archived in subsequent runs.

Do Not Archive Audit Files

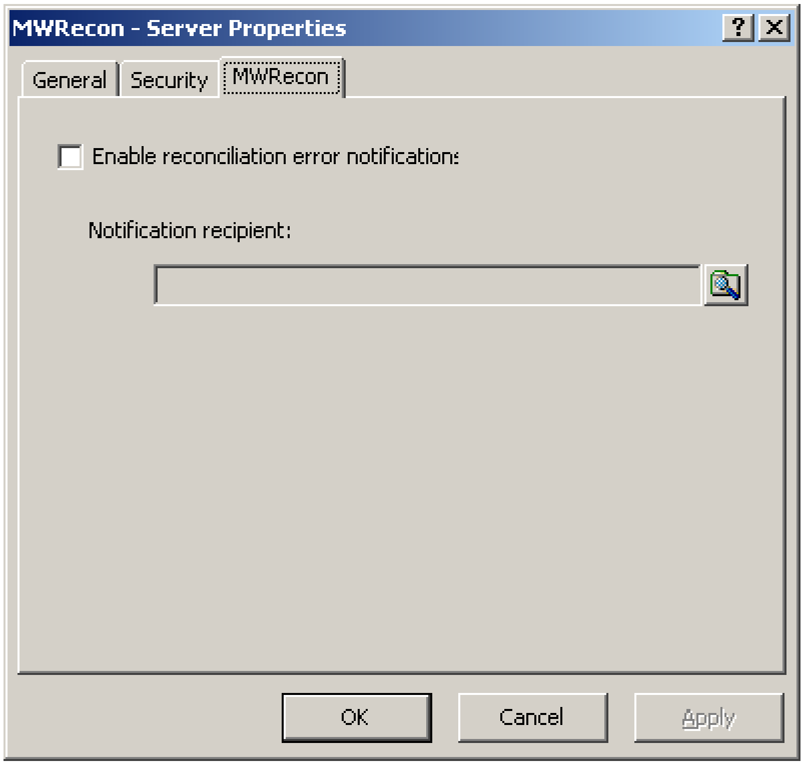
This setting allows users to override the default behavior, to archive audit files. Check this box to delete audit files that have passed the retention date. Clear this box to archive audit files that have passed the retention date.

Do not Delete Archive Files

This setting allows users to disable deletion of archive files. If checked, MessageWay Archive Messages and related data will be deleted but the Archive zip file will be retained. This is intended to allow for 3rd party offline archive of the zip files where the 3rd party process which archives the zip files is also responsible for deleting them.

MWRecon Page

The MessageWay Reconciliation Server provides the reconciliation service for the MessageWay Translator, MWTranslator. For specific information about the reconciliation process, refer to the section, "Using Audit and Reconciliation" in the *MWTranslator Operator Guide and Reference*.



□ Enable reconciliation error notifications

Notification recipient:

MWRecon Page (Server Properties Window)

Enable Reconciliation Error Notifications

Click this box to create error notifications when reconciliation fails. This server provides reconciliation of documents sent to trading partners with acknowledgments that you receive from the trading partners in response to these documents. This process is an additional feature of the MWTranslator service.

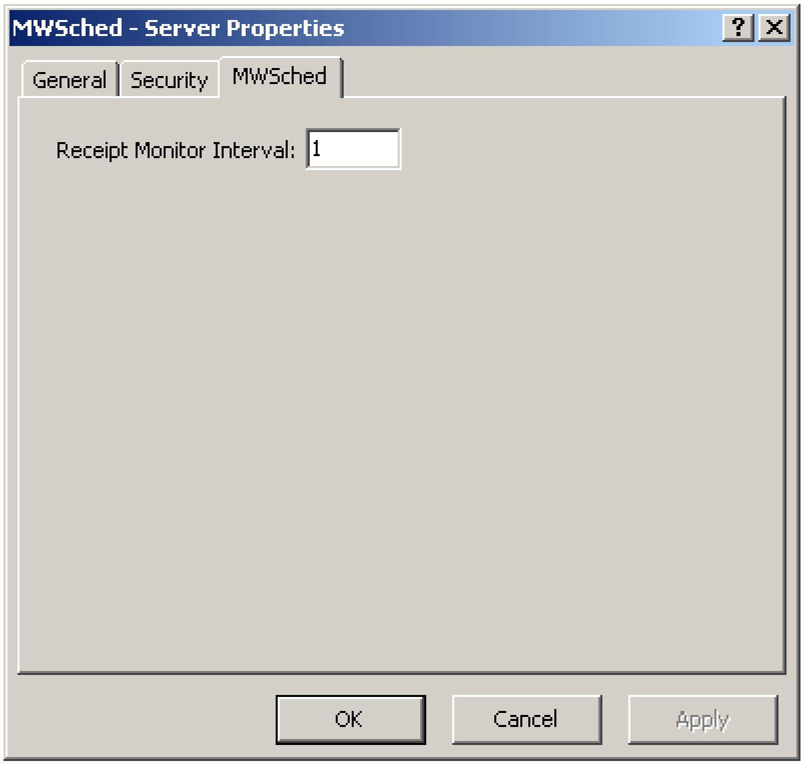
Notification Recipient

Type or select the location name to which the notification report(s) will be sent when reconciliation fails. Select or type one or more locations, separated by commas. To enter a dynamic distribution list, multiple destinations entered on a single line and separated by commas, press **CTRL** and select the locations. The locations appear separated by commas.

MWSched Page

The MessageWay Scheduling Server supports the following:

- Location schedules
- Receipt monitor schedules
- Monitoring for the Remote Execution Server
- Triggers to retry message delivery
- Removal of orphaned sessions



Receipt Monitor Interval: 1

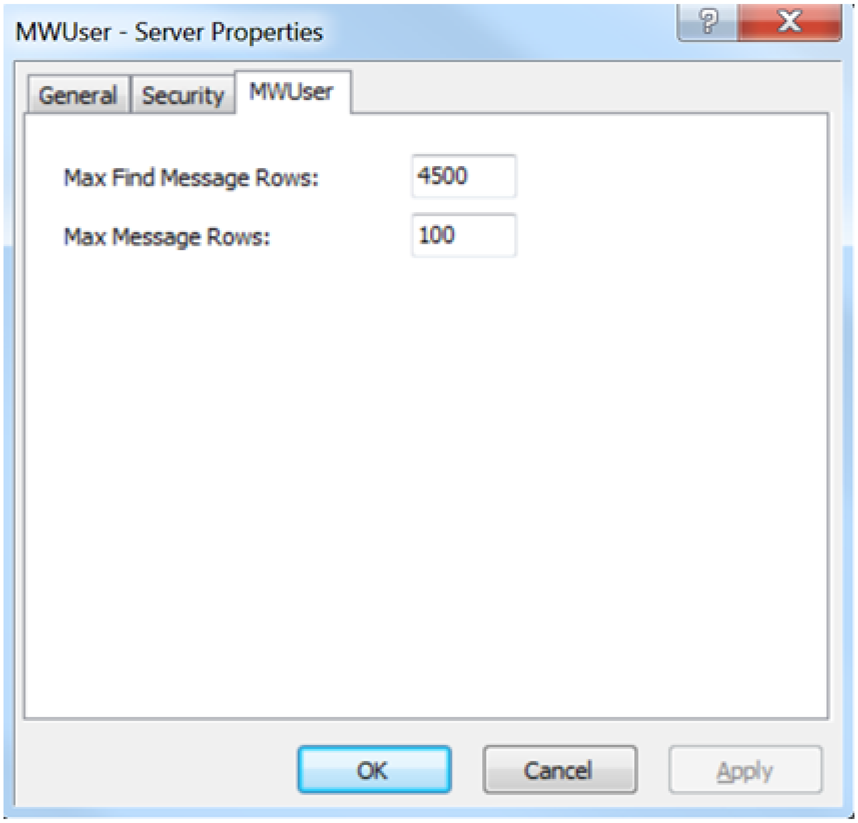
MWSched Page (Server Properties Window)

Receipt Monitor Interval

Type the number of minutes between polling cycles when the receipt monitor will initiate an action. It supports location schedules, receipt monitor schedules, monitoring for the Remote Execution Server, triggers to retry message delivery and removal of inactive sessions. The default value is 1 minute. This server deletes orphaned sessions based on the *Logon Idle Lifetime* value from User Policies. If it determines that an orphaned session exists that surpasses the value for timeout, the scheduling server will delete the session, which forces a user to log on again.

MWUser Page

The MessageWay User Server supports MessageWay access from the MessageWay Manager.



Max Find Message Rows: 4500

Max Message Rows: 100

MWUser Page (Server Properties Window)

Max Find Message Rows

This is the maximum number of messages that will be returned and available to view when using the MessageWay Manager **Find Messages** or **Find Archive Messages** options.   Note that the number of rows returned when using the **Find Locations**, **Find Rules** or **Find Users** options is hard coded to 10,000.

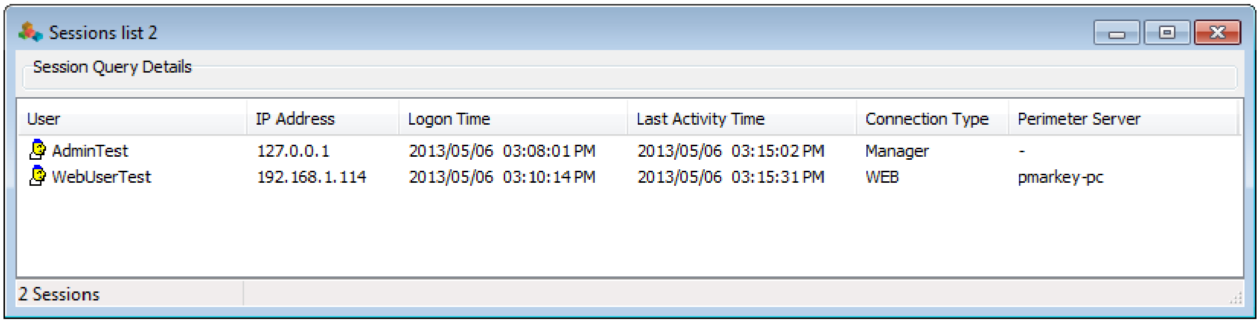
Max Message Rows

This is the maximum number of messages that will be displayed in a message list window at a time, accessible by scrolling, if necessary. When you monitor more than one system, this number is the lowest of all the system configurations. For example, if one system to which you are connected allows a maximum of 1000 and the second system allows 100, you will only see a maximum of 100 messages in a message list window.

Sessions List Window

The Sessions List window appears when you use the **Find Sessions** command to search for current active connections to the MessageWay server through the Manageror one of the perimeter servers, FTP, SFTP, or through AS2 or Web Client. When you search through multi-system environments, a System Name column also appears.

To sort by column content, click the column heading.



User	IP Address	Logon Time	Last Activity Time	Connection Type	Perimeter Server
AdminTest	127.0.0.1	2013/05/06 03:08:01 PM	2013/05/06 03:15:02 PM	Manager	-
WebUserTest	192.168.1.114	2013/05/06 03:10:14 PM	2013/05/06 03:15:31 PM	WEB	pmarkey-pc

User

This is the MessageWay user that is currently connected.

IP Address

This is the IP address of the system connected to MessageWay.

Logon Time

This is the date and time the user logged on to MessageWay.

Last Activity Time

This is the date and time that MessageWay logged activity for this user. MessageWay uses this information to time out the session if the user has been idle for a certain length of time.

A session remains active until the user logs off or the session times out, which is determined by the configurations for the entity that makes the connection. For example, if you are logged on through the MessageWay Manager, the *Logon Idle Lifetime* setting on the **General** tab of the User Policies window determines when a user's session times out. The Scheduling Server cleans out invalid sessions based on its Receipt Monitor Interval setting. If this is blank, it will not clean out invalid sessions. If you change the monitor interval, you must restart the Scheduling Server for the changes to take effect.

Connection Type

Following is a list of current connection types.

Connection Type	Description
AS2	AS2 Interface
FTP	MessageWay FTP Perimeter Server
SFTP	MessageWay SFTP Perimeter Server
Manager	MessageWay Manager (Graphical User Interface)
WEB	Web Client (client connects via Web browser eventually through MWSI)
MWIR	Reporting (client connects via Web browser eventually through MWSI)

Perimeter Server

This is the name of the system of the perimeter server that provides the connection to MessageWay. For connections from MessageWay Manager, this value is blank.

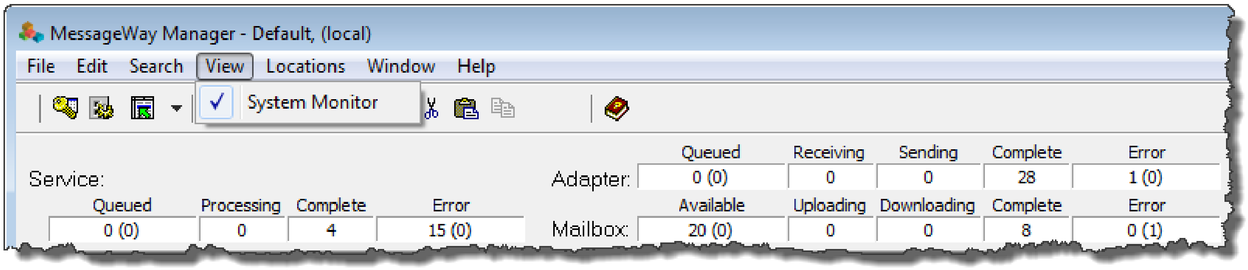
System Name

An additional column will appear if you are currently monitoring multiple systems. The value is the name of the user's system.

System Monitor Bar

The system monitor displays consolidated numbers for the various types of adapters and services. This allows operators to quickly assess the status of message processing. You can toggle the display of the monitor by selecting **View|System Monitor** from the menu bar. The information is updated dynamically. To update the numbers manually, press SHIFT+F5.

By default, these numbers reflect a single-system environment.

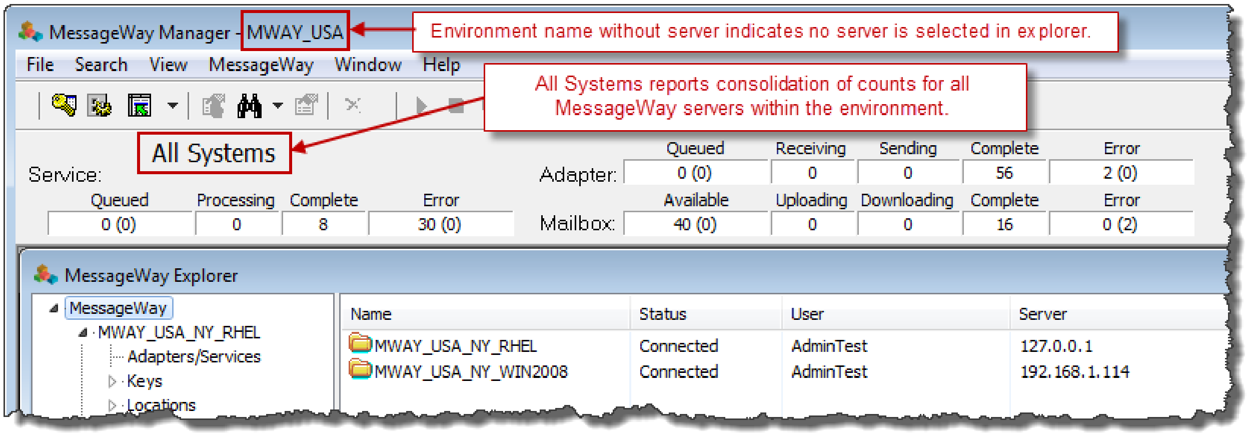


Service:

Queued	Processing	Complete	Error
0 (0)	0	4	15 (0)

	Queued	Receiving	Sending	Complete	Error
Adapter:	0 (0)	0	0	28	1 (0)
	Available	Uploading	Downloading	Complete	Error
Mailbox:	20 (0)	0	0	8	0 (1)

However, an environment may include more than one MessageWay Server system with a limit of 4, which is called a multi-system environment. Users can choose which of the systems they want to monitor in the group. If they choose to monitor all of the systems, these numbers reflect the consolidated statuses and statistics of all the systems.



Environment name without server indicates no server is selected in explorer.

All Systems reports consolidation of counts for all MessageWay servers within the environment.

Service:

Queued	Processing	Complete	Error
0 (0)	0	8	30 (0)

	Queued	Receiving	Sending	Complete	Error
Adapter:	0 (0)	0	0	56	2 (0)
	Available	Uploading	Downloading	Complete	Error
Mailbox:	40 (0)	0	0	16	0 (2)

Name	Status	User	Server
MWAY_USA_NY_RHEL	Connected	AdminTest	127.0.0.1
MWAY_USA_NY_WIN2008	Connected	AdminTest	192.168.1.114

Services Statuses

The following consolidated message status information appears on the **System Monitor** bar for all services. Each column identifies messages as they pass through their various states. Users can view the state of a message on the **General** page of the Message Properties window. This information is updated dynamically. To update the numbers manually, press **SHIFT+F5**.

Category	Description
Queued ( )	Displays the total number of messages awaiting processing. Numbers in parentheses show the total number of messages awaiting processing that are currently on hold, which includes the message states of *Hold*, *Hold Output* and *Schedule Wait*.
Processing	Displays the total number of messages currently being processed.
Complete	Displays the total number of messages that have been delivered.

Category	Description
Error ( )	Displays the total number of messages that have an error status. Numbers in parentheses show the total number of messages that have been canceled. Operators may cancel any messages that do not have the state of *Receiving*, *Complete* or *Error*.

Adapters Statuses

The following consolidated message status information appears on the **System Monitor** bar for all adapters. Each column identifies messages as they pass through their various states. Users may view the state of a message on the **General** page of the Message Properties window. This information is updated dynamically. To update the numbers manually, press **SHIFT+F5**.

Category	Description
Queued ( )	Displays the total number of messages that are awaiting delivery. Numbers in parentheses show the total number of messages awaiting delivery that are currently on hold, which includes the message states of *Hold*, *Hold Output* and *Schedule Wait*.
Receiving	Displays the total number of messages currently being received into MessageWay.
Sending	Displays the total number of messages currently being sent to their destination.
Complete	Displays the total number of messages that have been sent to their destination.
Error ( )	Displays the total number of messages that have an error status and are not yet delivered. Numbers in parentheses show the total number of messages that have been canceled. Operators may cancel any messages that do not have the status of *Receiving*, *Complete* or *Error*.

Mailbox Statuses (System Monitor)

The following consolidated message status information appears on the **System Monitor** bar for all other types of messages not associated with adapters or services. Each column identifies messages as they pass through their various states. Users can view the state of a message on the **General** page of the Message Properties window. These counts include messages sent to pickup mailboxes and messages sent to the system mailbox, {Unknown}. This information is updated dynamically. To update the numbers manually, press **SHIFT+F5**.

Category	Description
Available ( )	Displays the total number of messages that are awaiting pickup from a pickup type mailbox. Numbers in parentheses indicate the total number of messages awaiting pickup that are currently on hold, which includes the message states of *Hold*, *Hold Output* and *Schedule Wait*.

Category	Description
Uploading	Displays the total number of messages currently being received into MessageWay.
Downloading	Displays the total number of messages currently being sent to their destination.
Complete	Displays the total number of messages that have been sent to their destination.
Error ( )	Displays the total number of messages that have an error status and are not yet delivered or that have not yet been picked up. Numbers in parentheses show the total number of messages that have been canceled. Operators may cancel any messages that do not have the status of *Receiving*, *Complete* or *Error*.

User Group Properties Window

The User Group Properties window allows you to configure rights for user groups. Rights for users may be inherited from a group to which they belong. For this reason, it is easier to add users to groups and allow the members to inherit the rights rather than set the rights for each user.

To access a user group configuration:

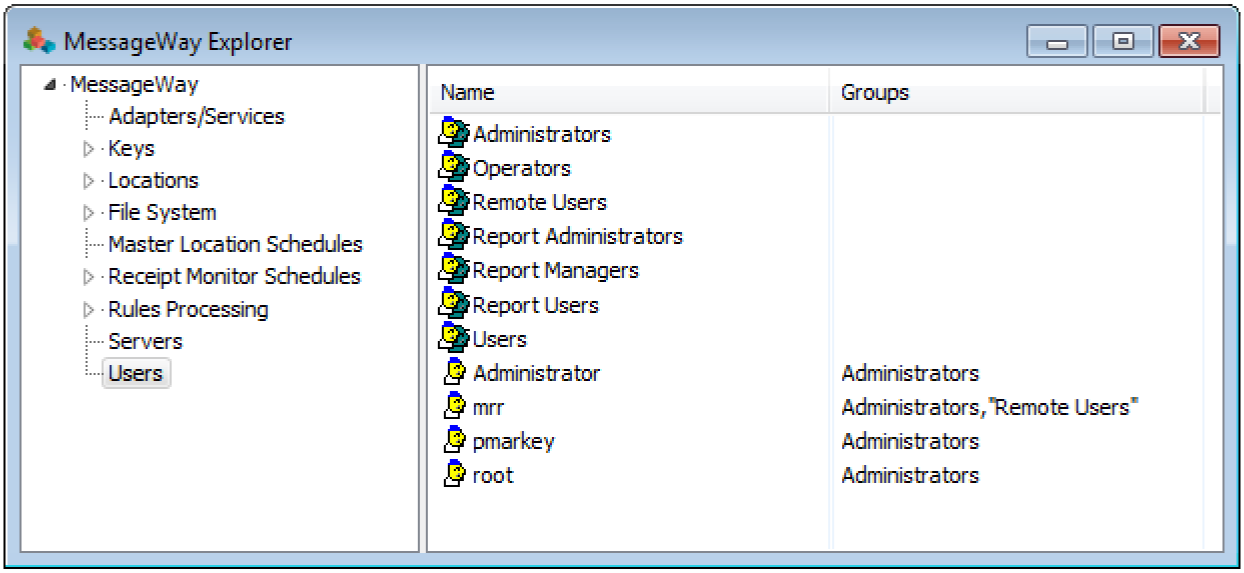
1 From the right pane of MessageWay Explorer, select a user group.

2 Click the **Properties** icon on the task bar.

The User Group Properties window appears

The icons distinguish between single users and groups, as follows:

Icon	Description
👤	Security properties for a single user
👥	Security properties for a group of users



Name	Groups
Administrators	
Operators	
Remote Users	
Report Administrators	
Report Managers	
Report Users	
Users	
Administrator	Administrators
mrr	Administrators,"Remote Users"
pmarkey	Administrators
root	Administrators

Name

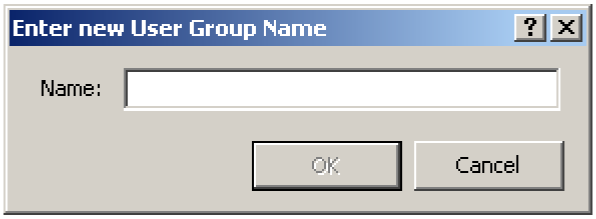
You create a user group from MessageWay Explorer as follows:

1 In the left pane, select the **Users** folder, and then from the **Users** menu, click **Add User Group.**

- or -

Right-click an existing folder, or in an open area of the right pane, and click **Add User Group** from the pop-up menu.

The **Enter New User Group Name** dialog box appears.

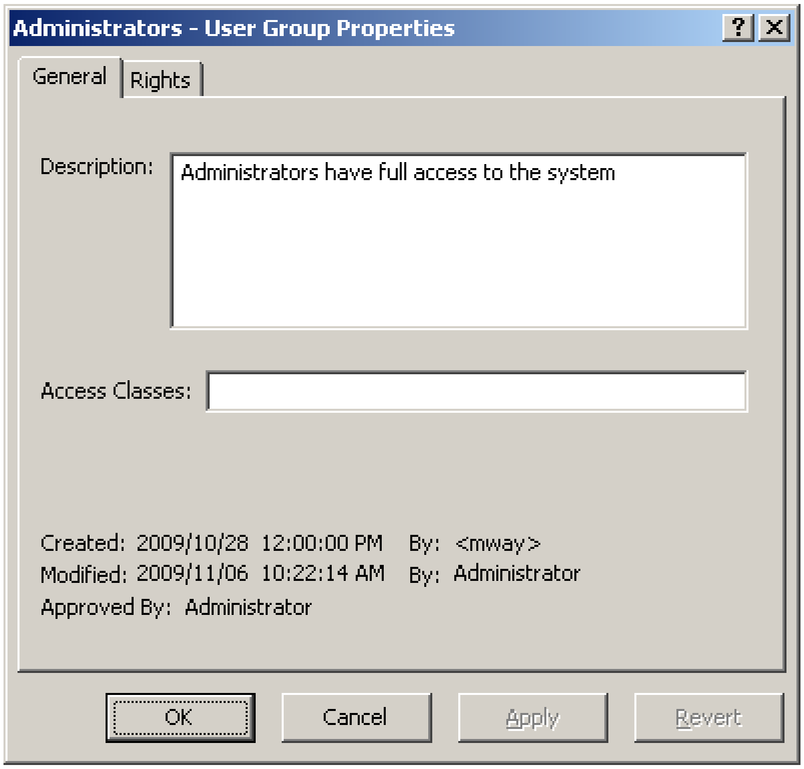


2 Type a name with up to 32 displayable characters.

(User Group Properties) General Page

The **General** page of the User Group Properties window provides a description of the group and the ability to control access to MessageWay through the optional Web Client, FTP Server, the SFTP Server or the AS2 Interface.

IMPORTANT: Changes made to user or user group properties will take effect when the user logs on in a subsequent session.



Description: Administrators have full access to the system

Access Classes:

Created: 2009/10/28 12:00:00 PM By: <mway>
Modified: 2009/11/06 10:22:14 AM By: Administrator
Approved By: Administrator

General Page (User Group Properties Window)

Description

Enter text to describe this user group. User groups provide a convenient way to endow users with rights, because the users inherit rights from the groups to which they belong.

You should configure user groups to suit your needs, for example by product line. For your convenience, there are four preconfigured user groups:

- **Administrators** is a group intended for a few users who will administer the system. They have all rights.
- **Operators** is a group intended for users who monitor the system, but do not need to view messages or add and delete users.
- **Remote Users** is a group intended for customers who send and retrieve their messages, but have no access to the MessageWay Manager.
- **Users** is a group that typically provides support to customers using the Manager.

Access Class

Access classes control access by external users to MessageWay through the optional products: FTP Server, SFTP Server, and the AS2 Interface. Enter one or more access classes, separated by commas. Access class names are case sensitive. They must match the access class names configured in the configuration files for the FTP Server (mwftpd.conf), the SFTP Server (mwsftpd.conf), and the AS2 Interface (mwas2.conf). When no access class is assigned to a user, that is, when there is no entry on the list, and when there is no access class configured for the server, the user has full access.

When you assign access classes to a user group, all members of the group are controlled by the access class. You may override the access for a specific user on the User Properties window. Unless a user is assigned one or more access classes to override group settings, the effective access class list is the combination or union of all access classes defined for all groups to which the user belongs.

Created

Created is the date and time the user group was created.

By (Created)

For pre-defined user groups, Administrators, Operators, Remote Users and Users, the system service itself creates this value, which appears in angle brackets, < >, to distinguish it from a MessageWay user. For other user groups, this is the MessageWay user that created this group. When a system service creates an entity, this value identifies the service, which appears in angle brackets, < >, to distinguish it from a MessageWay user. For example, imported definitions will use <mwimp>.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

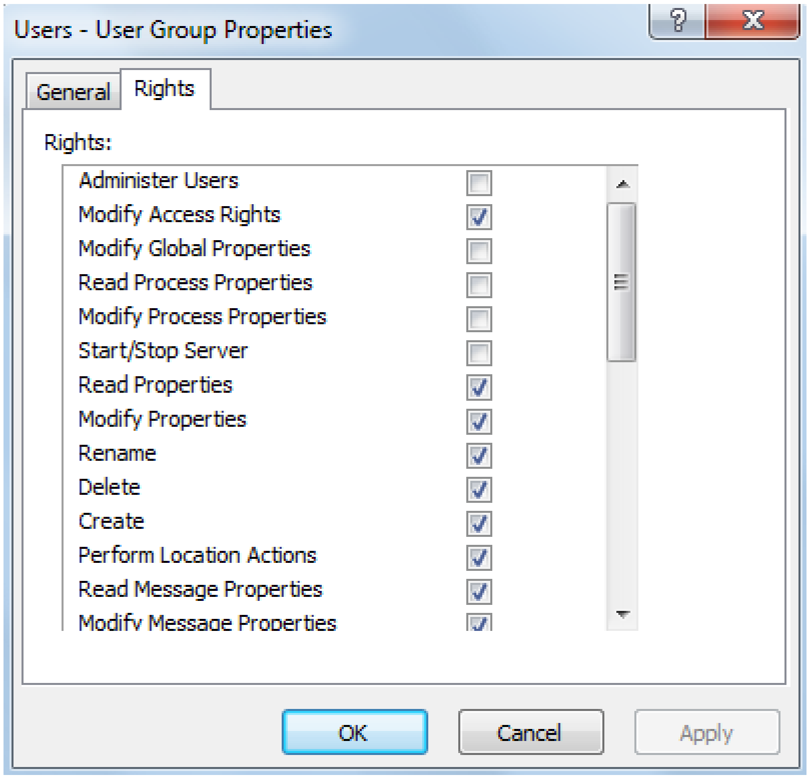
(Maker/Checker Option) Approved By

Approved By is the MessageWay user that has approved this change. This field appears only when you use the optional Maker/Checker feature.

(User Group Properties) Rights Page

The **Rights** page of the User Group Properties window allows you to control the type of access users have who belong to this group and the tasks these users may perform. The boxes checked here will display in the Effective column on the **Rights** page of the User Properties window for each member of the group.When a user belongs to more than one group, the Effective column shows the combined rights granted by those groups.

IMPORTANT: Changes made to user or user group properties will take effect when the user logs on in a subsequent session.



Rights:

- Administer Users ☐
- Modify Access Rights ☑
- Modify Global Properties ☐
- Read Process Properties ☐
- Modify Process Properties ☐
- Start/Stop Server ☐
- Read Properties ☑
- Modify Properties ☑
- Rename ☑
- Delete ☑
- Create ☑
- Perform Location Actions ☑
- Read Message Properties ☑
- Modify Message Properties ☑

Rights Page (User Group Properties Window)

The following table describes the default settings applied to each pre-defined group, Administrators, Operators, Remote Users and Users. Asterisks indicate those rights assigned to the group.

Right	Admin.	Oper.	Rem. Users	Users	Description
Administer Users	*				Add and remove MessageWay user accounts and modify global user configurations. When this is clear, the **Users** folder is not visible in the Manager.
Modify Access Rights	*	*		*	Change values on **Security** page of folders and objects, which controls who can perform which tasks on specific objects. Also requires the right **Read Properties**.

Right	Admin.	Oper.	Rem. Users	Users	Description
Administer Users	*				Add and remove MessageWay user accounts and modify global user configurations. When this is clear, the **Users** folder is not visible in the Manager.
Modify Global Properties	*	*			Change properties for the MessageWay Server to modify database access, location of directories or settings to automatically start related servers. When this is clear, users cannot access the MessageWay Server Properties window.
Read Process Properties	*	*	*		View the statuses of the adapters or services. Also requires the rights **Read Properties** and **View Adapters/Services**. When this is unchecked, users cannot access the Adapter or Service Properties window.
Modify Process Properties	*	*			Change properties for the adapters or services, such as thread distribution, startup options and security. Also requires the rights **Read Process Properties**, **Read Properties**, **Modify Properties**, and **View Adapters/Services**. When this is clear, users may still be able to access the Adapter or Service Properties window, but the properties are dimmed.
Start/Stop Server	*	*			Start, stop, suspend or resume an adapter or service. Also requires the rights **Read Process Properties**, **Read Properties** and **View Adapters/Services**.
Read Properties	*	*	*	*	View properties of folders and objects other than adapters or services, such as locations.
Modify Properties	*	*		*	Change properties of folders and objects other than adapters or services, such as locations. Also requires the right **Read Properties**.
Rename	*	*		*	Change the name of user-defined folders and locations. Also requires the right **Read Properties**.
Delete	*	*		*	Delete user-defined folders and locations. Also requires the right **Read Properties**.
Create	*	*		*	Create folders and locations. Also requires the right **Read Properties**.

Right	Admin.	Oper.	Rem. Users	Users	Description
Administer Users	*				Add and remove MessageWay user accounts and modify global user configurations. When this is clear, the **Users** folder is not visible in the Manager.
Perform Location Actions	*	*		*	Controls user ability to hold messages, release messages, hold outputs or release outputs. Also requires the right **Read Properties**.
Resubmit Messages	*	*	*	*	Controls user ability to resubmit messages. Also requires the rights **Read Properties** and **Modify Message Properties**.
Redirect Messages	*	*	*	*	Controls user ability to redirect messages. Also requires the rights **Read Properties** and **Modify Message Properties.**
Release Messages	*	*	*	*	Controls user ability to release messages. Also requires the rights **Read Properties** and **Modify Message Properties**.
Restart Receive	*	*	*	*	Controls user ability to restart transfer of messages only partially received. Also requires the rights **Read Properties** and **Modify Message Properties**.
Cancel Messages	*	*	*	*	Controls user ability to cancel messages. Also requires the rights **Read Properties** and **Modify Message Properties**.
Retrieve Archive Messages	*	*	*	*	Controls user ability to retrieve messages from archive. Also requires the rights **Read Properties** and **Modify Message Properties**.
Resubmit Archive Messages	*	*	*	*	Controls user ability to resubmit messages retrieved from archive. Also requires the rights **Read Properties** and **Modify Message Properties**.
Delete Archive Message Content	*	*	*	*	Controls user ability to delete messages retrieved from archive. Also requires the rights **Read Properties** and **Modify Message Properties**.
Read Message Properties	*	*	*	*	View the properties of messages. Also requires the right **Read Properties**.

Right	Admin.	Oper.	Rem. Users	Users	Description
Administer Users	*				Add and remove MessageWay user accounts and modify global user configurations. When this is clear, the **Users** folder is not visible in the Manager.
Modify Message Properties	*	*		*	Controls user ability to: modify retention date and change priority; mark for archive and mark for deletion. Also requires the rights **Read Properties** and **Read Message Properties**.
View Messages	*			*	Read message content. Also requires the rights **Read Properties** and **Read Message Properties**.
Upload Messages	*		*		Send messages to MessageWay. Required for the user or user group when they are the sender of messages only. Also requires the rights **Read Properties** and **Read Message Properties**.
Download Messages	*		*		Retrieve messages from MessageWay. Required for the user or user group when they are the sender or recipient of messages. Also requires the rights **Read Properties** and **Read Message Properties**.
View System Counts	*	*		*	View statistics in the System Monitor.
View Adapters/ Services	*	*		*	View the **Adapters/Services** folder and the list of adapters and services. When denied, also denies **Start/Stop Server** and **Modify Process Properties**. When this is clear, the **Adapters/Services** folder is not visible in the Manager.
View Logs	*				Controls user ability to view audit logs, event logs and trace logs. Also requires the rights **Read Properties** and **Modify Message Properties**.
Maker (Maker/ Checker option)	*				Change the properties of user groups.
Checker (Maker/ Checker option)	*				Validate changes made to the properties of user groups.

Right	Admin.	Oper.	Rem. Users	Users	Description
Administer Users	*				Add and remove MessageWay user accounts and modify global user configurations. When this is clear, the **Users** folder is not visible in the Manager.
Generate Reports (reporting option)	*				Controls user ability to logon to reporting application. Also requires the rights **View Reports**.
View Reports (reporting option)	*				Controls user ability to logon to reporting application. Also requires the rights **Generate Reports**.

Pre-defined user groups for reporting include Report Administrators, Report Developers, Report Managers, and Report Users. Asterisks indicate those rights assigned to the group.

Right	Report Admin.	Report Dev.	Report Mgr.	Report Users	Description
Administer Users	*				Add and remove MessageWay user accounts and modify global user configurations. When this is clear, the **Users** folder is not visible in the Manager.
Modify Access Rights	*	*	*		Change values on **Security** page of folders and objects, which controls who can perform which tasks on specific objects. Also requires the right **Read Properties**.
Modify Global Properties					Change properties for the MessageWay Server to modify database access, location of directories or settings to automatically start related servers. When this is clear, users cannot access the MessageWay Server Properties window.
Read Process Properties	*	*	*	*	View the statuses of the adapters or services. Also requires the rights **Read Properties** and **View Adapters/Services**. When this is clear, users cannot access the Adapter or Service Properties window.

Right	Report Admin.	Report Dev.	Report Mgr.	Report Users	Description
Administer Users	*				Add and remove MessageWay user accounts and modify global user configurations. When this is clear, the **Users** folder is not visible in the Manager.
Modify Process Properties		*			Change properties for the adapters or services, such as thread distribution, startup options and security. Also requires the rights **Read Process Properties**, **Read Properties**, **Modify Properties**, and **View Adapters/Services**. When this is clear, users may still be able to access the Adapter or Service Properties window, but the properties are dimmed.
Start/Stop Server					Start, stop, suspend or resume an adapter or service. Also requires the rights **Read Process Properties**, **Read Properties** and **View Adapters/Services**.
Read Properties	*	*	*	*	View properties of folders and objects other than adapters or services, such as locations.
Modify Properties	*	*	*		Change properties of folders and objects other than adapters or services, such as locations. Also requires the right **Read Properties**.
Rename	*	*	*		Change the name of user-defined folders and locations. Also requires the right **Read Properties**.
Delete	*	*	*		Delete user-defined folders and locations. Also requires the right **Read Properties**.
Create	*	*	*		Create folders and locations. Also requires the right **Read Properties**.
Perform Location Actions					Controls user ability to hold messages, release messages, hold outputs or release outputs. Also requires the right **Read Properties**.
Resubmit Messages					Controls user ability to resubmit messages. Also requires the rights **Read Properties** and **Modify Message Properties**.
Redirect Messages					Controls user ability to redirect messages. Also requires the rights **Read Properties** and **Modify Message Properties**.

Right	Report Admin.	Report Dev.	Report Mgr.	Report Users	Description
Administer Users	*				Add and remove MessageWay user accounts and modify global user configurations. When this is clear, the **Users** folder is not visible in the Manager.
Release Messages					Controls user ability to release messages. Also requires the rights Read Properties and Modify Message Properties.
Restart Receive					Controls user ability to restart transfer of messages only partially received. Also requires the rights **Read Properties** and **Modify Message Properties**.
Cancel Messages					Controls user ability to cancel messages. Also requires the rights **Read Properties** and **Modify Message Properties.**
Retrieve Archive Messages					Controls user ability to retrieve messages from archive. Also requires the rights **Read Properties** and **Modify Message Properties**.
Resubmit Archive Messages					Controls user ability to resubmit messages retrieved from archive. Also requires the rights **Read Properties** and **Modify Message Properties**.
Delete Archive Message Content					Controls user ability to delete messages retrieved from archive. Also requires the rights **Read Properties** and **Modify Message Properties**.
Read Message Properties	*	*	*	*	View the properties of messages. Also requires the right **Read Properties**.
Modify Message Properties					Controls user ability to: modify retention date and change priority; mark for archive and mark for deletion. Also requires the rights **Read Properties** and **Read Message Properties**.
View Messages		*			Read message content. Also requires the rights **Read Properties** and **Read Message Properties**.
Upload Messages	*	*			Send messages to MessageWay. Required for the user or user group when they are the sender of messages only. Also requires the rights **Read Properties** and **Read Message Properties**.

Right	Report Admin.	Report Dev.	Report Mgr.	Report Users	Description
Administer Users	*				Add and remove MessageWay user accounts and modify global user configurations. When this is clear, the **Users** folder is not visible in the Manager.
Download Messages	*	*	*	*	Retrieve messages from MessageWay. Required for the user or user group when they are the sender or recipient of messages. Also requires the rights **Read Properties** and **Read Message Properties**.
View System Counts		*			View statistics in the System Monitor.
View Adapters/ Services		*			View the **Adapters/Services** folder and the list of adapters and services. When denied, also denies **Start/Stop Server** and **Modify Process Properties**. When this is clear, the **Adapters/Services** folder is not visible in the Manager.
View Logs	*	*	*	*	Controls user ability to view audit logs, event logs and trace logs. Also requires the rights **Read Properties** and **Modify Message Properties**.
Maker (Maker/ Checker option)					Change the properties of user groups.
Checker (Maker/ Checker option)					Validate changes made to the properties of user groups.
Generate Reports (reporting option)	*	*	*	*	Controls user ability to logon to reporting application. Also requires the rights **View Reports**.
View Reports (reporting option)	*	*	*	*	Controls user ability to logon to reporting application. Also requires the rights **Generate Reports**.

Rights

This is a list of all possible rights that a user group might have. These rights are inherited by the users who belong to this group and appear in the Effective column of the **Rights** page on the User Properties window. When a user belongs to multiple groups, the user's rights are the combined rights of all the groups. These rights may be overridden for a specific user by checking boxes in the Allow and Deny columns on the **Rights** page for that user.

User Policies Window

The **User Policies** window allows users to set policies for passwords and logon/lockout, which apply to the entire MessageWay system. MessageWay enforces password policies when a user logs on or creates or modifies a password. The lockout policies are to mitigate a brute force attack from unknown sources trying to gain access to MessageWay.

IMPORTANT: You must restart MessageWay for changes to User Policies to take effect.

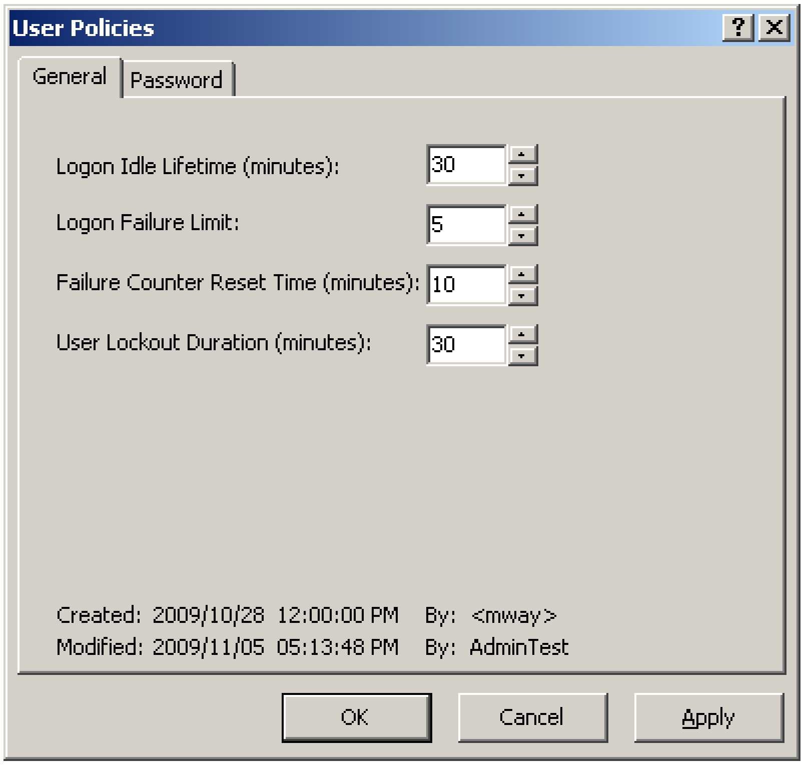
To access the User Policies window, from the task bar, click the **Edit User Policies** button, .

(User Policies) General Page

The **General** page of the User Policies window allows users to set policies for logon and lockout, which apply to the entire MessageWay system. The lockout policies are to mitigate a brute force attack from unknown sources trying to gain access to MessageWay.

Note that there are two types of automatic reset:

- *Failure Counter Reset Time* resets the count after the specified number of minutes when users stop trying after they have reached the *Logon Failure Limit*
- *User Lockout Duration* resets the count after the specified number of minutes when users have exceeded the number specified in *Logon Failure Limit*



Logon Idle Lifetime (minutes): 30

Logon Failure Limit: 5

Failure Counter Reset Time (minutes): 10

User Lockout Duration (minutes): 30

Created: 2009/10/28 12:00:00 PM By: <mway>

Modified: 2009/11/05 05:13:48 PM By: AdminTest

General Page (User Policies Window)

Logon Idle Lifetime (minutes)

Type or select the number of minutes, from 0 to 999, the user may remain logged on without any activity. When this time expires, the connection terminates and the user must log on again. A value of zero retains the session indefinitely and never logs a user off because of inactivity. You must restart the User Server, mwuser, the Service Interface, mwsi, and the Scheduling Server, mwsched, to make changes take effect as expected.

The Scheduling Server, mwsched, should also be restarted because mwsched uses the Logon Idle Lifetime to determine that a session record is orphaned, typically because the physical connection is not maintained, before deleting it. After the timeout passes, mwsched deletes the session record, which forces users to log on again to access the system.

Logon Failure Limit

Type or select the number of times users may attempt to log on before they are locked out of the system. If users stop attempting to log on when they *reach* this limit, they must wait the number of minutes specified in *Failure Counter Reset Time* before they can attempt to log on again. If users *exceed* this limit, they must wait the number of minutes specified in *User Lockout Duration* before they can attempt to log on again. This policy is to mitigate brute force logon attempts, when unknown sources might try to access the MessageWay system.

Users who have been locked out may attempt to log on again when:

- The number of minutes shown in the Failure Counter Reset Time has passed

  - or -

- The number of minutes shown in the User Lockout Duration has passed

Failure Counter Reset Time (minutes)

Type or select the number of minutes users must wait after consecutive failed logon attempts, when the failed logon counter resets to zero. The number of attempts must be no more than the number in **Logon Failure Limit**. This applies to users who have not been locked out. For example, when the *Logon Failure Limit* is three, users who stop after three consecutive invalid logon attempts may wait this number of minutes before they try to log on again.

User Lockout Duration (minutes)

Type or select the number of minutes users must wait after being locked out before the system resets their status to allow further logon attempts. When users are locked out, the status appears on the **General** page of the User Properties window in the lower right corner. To unlock the user, select the **Unlock User** button.

Created

Created is the date and time the policy was created.

By (Created)

The system service itself creates this value, which appears in angle brackets, < >, to distinguish it from a MessageWay user.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

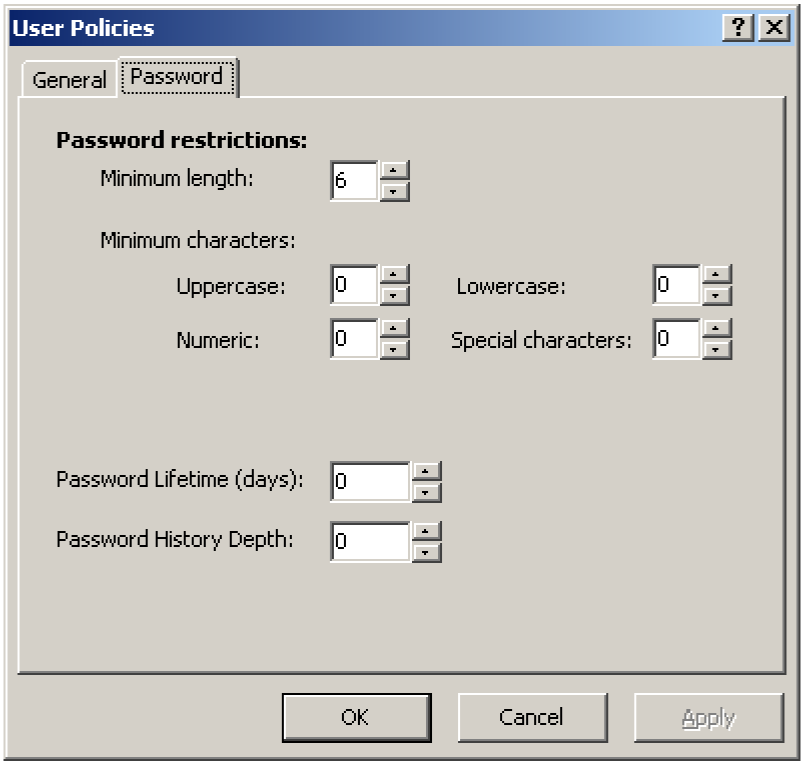
By (Modified)

This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

(User Policies) Password Page

The **Password** page of the User Policies window allows users to control how they create passwords.

IMPORTANT: User Policies for user passwords count Unicode characters as special characters only. If users require upper, lower, or numeric characters, they must be ASCII.



User Policies

General | Password

Password restrictions:

Minimum length: 6

Minimum characters:

Uppercase: 0
Lowercase: 0
Numeric: 0
Special characters: 0

Password Lifetime (days): 0

Password History Depth: 0

Password Page (User Policies Window)

Minimum Length

This is the minimum number of characters that a user must enter to create a password. It must be equal to or greater than the sum of all characters specified for each of the character types under *Minimum characters*.

Uppercase

This is the minimum number of uppercase characters the user must enter to create a password.

Lowercase

This is the minimum number of lowercase characters the user must enter to create a password.

Numeric

This is the minimum number of numeric characters the user must enter to create a password.

Special Characters

This is the minimum number of special characters the user must enter to create a password.

Password Lifetime (days)

Enter the number of days that a password may be used before it must be changed. When a user logs on and the password has expired, the user must change the password before the logon process finishes. A value of zero means users will never have to change their passwords. To override this setting for a specific user, you can check the box *Password never expires* on the User Properties window.

Password History Depth

Enter the number of prior passwords that are saved in a history list. When a user creates a password, the new password must be different from the current or any previous passwords on the list. A value of zero means users will never have to change their passwords. To override this setting for a specific user, you can check the box *Password never expires* on the User Properties window.

User Properties Window

The User Properties window allows you to configure rights for users. Rights for users may be inherited from a group to which they belong. For this reason, it is easier to add users to groups and allow the members to inherit the rights rather than set the rights for each user.

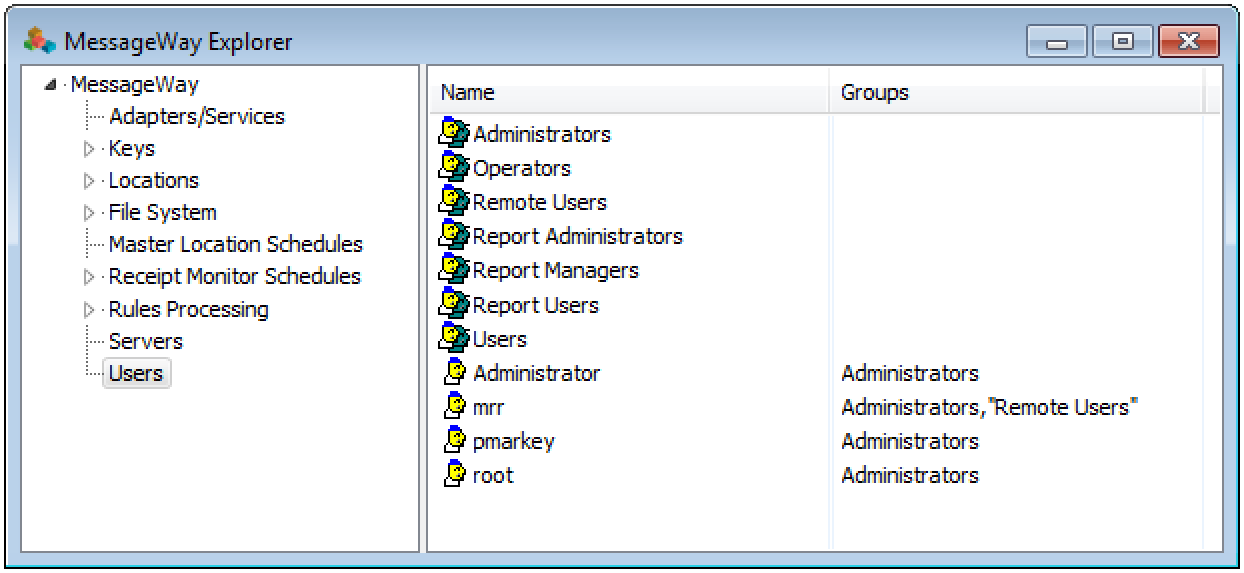
To access user configurations:

1 From the right pane of MessageWay Explorer, select a user

2 Click the **Properties** button on the task bar.
The User Properties window appears.

The icons distinguish between single users and groups, as follows:

Icon	Description
👤	Security properties for a single user
👥	Security properties for a group of users



Name	Groups
Administrators	
Operators	
Remote Users	
Report Administrators	
Report Managers	
Report Users	
Users	
Administrator	Administrators
mrr	Administrators,"Remote Users"
pmarkey	Administrators
root	Administrators

Name

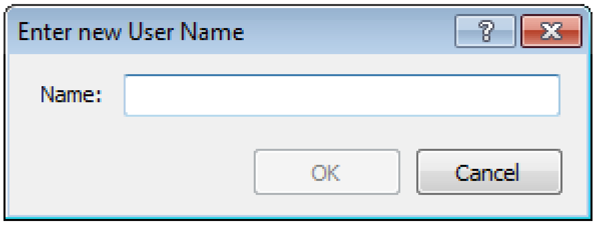
You create a user by adding a new one or copying an existing one as follows:

1 Right-click an existing group, or in a open area of the right pane, and select **Add User** from the menu

- or -

Right-click an existing user and select **Copy**, then right-click again, and select **Paste**

The **Enter New User Name** dialog box appears.

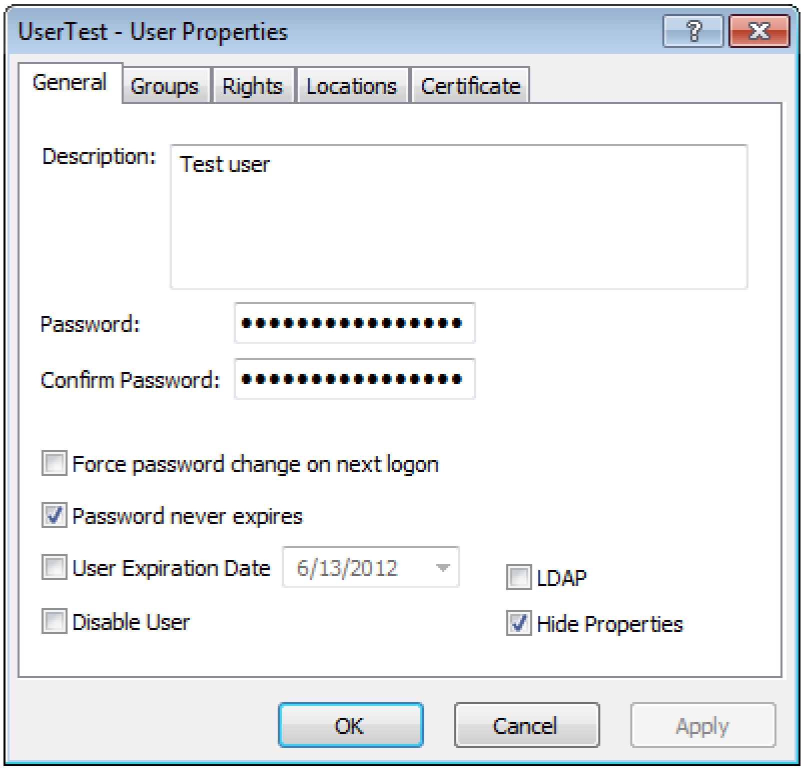


2 Type a name with up to 128 displayable characters, excluding the colon (:).

(User Properties) General Page

The **General** page of the User Properties window provides methods to control passwords and access to the system for the user.

IMPORTANT: Changes made to user or user group properties will take effect when the user logs on in a subsequent session.



Description: Test user

Password: ●●●●●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●●●●●

□ Force password change on next logon

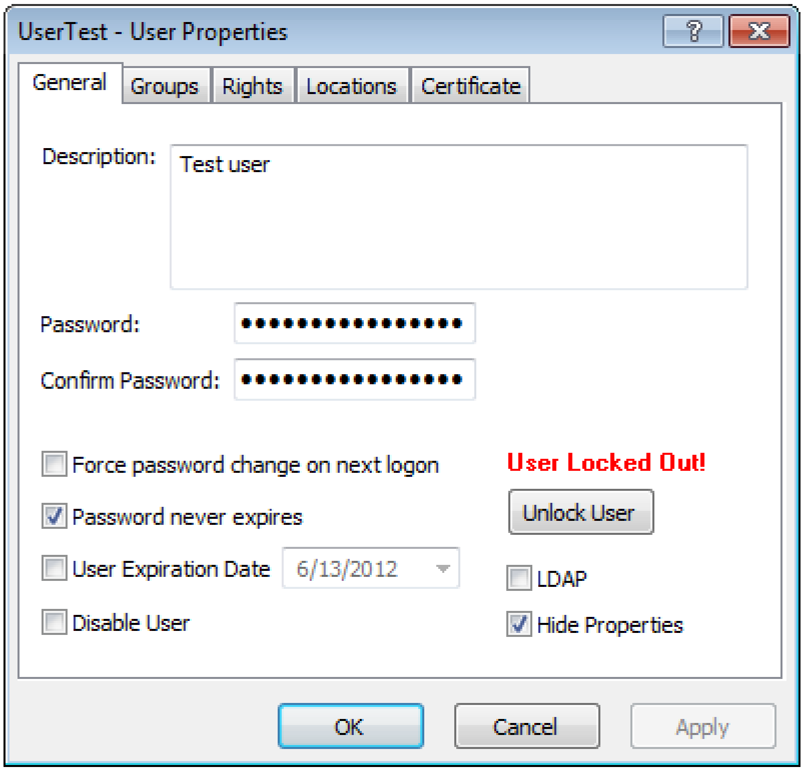
☑ Password never expires

□ User Expiration Date 6/13/2012

□ LDAP

□ Disable User

☑ Hide Properties



Description: Test user

Password: ●●●●●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●●●●●

□ Force password change on next logon

User Locked Out!

☑ Password never expires

□ User Expiration Date 6/13/2012

□ LDAP

□ Disable User

☑ Hide Properties

Description

Type text to describe this user.

Password

Type a valid password. The minimum length is specified on the **Password** page of the **User Policies** window. This field is unavailable for LDAP users.

Confirm Password

Re-enter the password you typed in the **Password** field to confirm that you did not make an error. This field is unavailable for LDAP users.

Force Password Change on Next Logon

Check this box to force the user to change the password during the next logon session. This field is unavailable for LDAP users. Note that if the user logs onto via an MWFTPD perimeter server, the user will not see the change password prompt, but instead will see a "logon failed" message. In this case, an Administrator will need to reset the password or turn off the *force password change* option.

Password never expires

Check this box so that the current password never expires for the user. This check box overrides the password expiration timing identified on the **Password** page of the Users Policies window that applies to all users. This field is unavailable for LDAP users.

User Expiration Date check box

Check this box to set an expiration date for the user. Any logon attempts from this date forward will be denied, with an error "Logon failed: Invalid User or Password." To reinstate the user, clear this box or change the date in the **User Expiration Date** field to a future date. When this box is not checked, the user will not expire.

User Expiration Date

Click the arrow to display a calendar from which you may choose a date when this user will expire. Attempts to log on to the MessageWay Manager on or after this date will be denied. To reinstate this user, clear the **User Expiration Date** box or change this date to a future date.

Disable User

Check this box to prohibit the user from logging on in subsequent sessions.

Unlock User Button

This button appears when a user has been locked out because of successive logon failures. Click this button to unlock the user and reset the logon failures to zero.

LDAP

Check this box to use Lightweight Directory Access Protocol (LDAP), such as with Open LDAP or Microsoft Active Directory, to authenticate MessageWay users, either external or internal. External users are those that access MessageWay through the FTP, SFTP connections, for example. Internal users access MessageWay from the MessageWay Manager. The user must be defined in MessageWay, but the password is controlled by LDAP.

Hide Properties

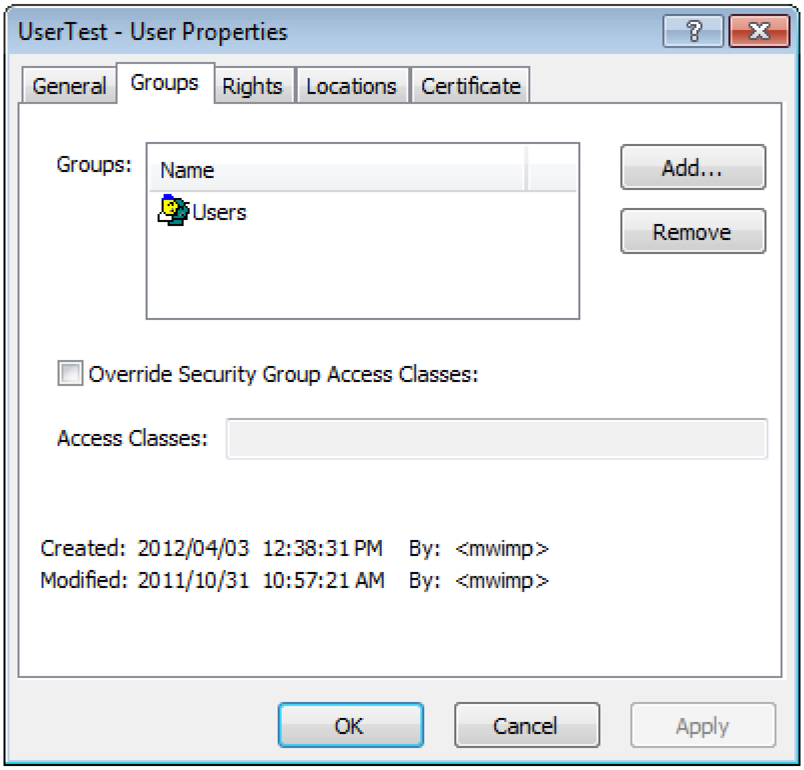
Check this box to hide objects on the MessageWay Manager or make them inaccessible.

When this box is checked, a user will experience the following:

- MessageWay Server option will not appear
- Within the Schedules folder, Receipt Schedule and Master Receipt Schedule folders will not appear
- Rules Processing folder will not appear
- No property windows will be accessible or visible, even if the user has explicit access to view properties

(User Properties) Groups Page

The **Groups** page of the User Properties window allows you to maintain the groups to which this user belongs.



Groups: Name: Users

□ Override Security Group Access Classes:

Access Classes:

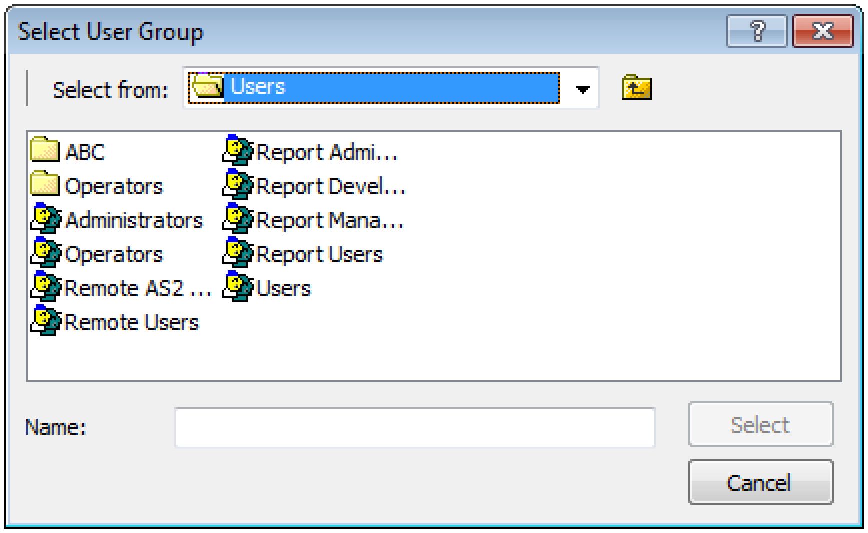
Created: 2012/04/03 12:38:31 PM By: <mwimp>
Modified: 2011/10/31 10:57:21 AM By: <mwimp>

To add this user to a group:

1 Click the **Add** button.

The Select User Group window appears.

2 Select a group from the list or type the name of a group in the **Select** box, and click the **Select** button.



Select User Group Window (User Properties)

Groups

This is a list of groups to which this user belongs. Use the **Add** and **Remove** buttons to add or remove this user from groups.

Add Button

Select this button to add this user to a group. You may add users to more than one group. The user inherits the combined rights from all the groups to which it belongs.

Select from

From the Select User Group window, click the down arrow. Select a folder from the list that contains the user groups you want to show in the list box.

Group Listbox

Choose from among the user groups on the list to which you want to add this user. To show a list of user groups, you must select a folder from the Select From list where the groups are defined.

Select

To add this user to a group, either choose a group from the list box and it will display in the box beneath it or type a group name in the box. Click the **Select** button to complete the process.

Remove Button

Choose this button to delete this user from the selected group.

Override Security Group Access Classes

Check this box to override the access classes inherited from the user groups to which this user belongs, or, when there are no inherited access classes, to add classes as required.

Access Classes

Access classes control access by external users to MessageWay through the optional products: FTP Server, SFTP Server, and the AS2 Interface. Enter one or more access classes, separated by commas. Access class names are case sensitive. They must match the access class names configured in the configuration files for the FTP Server (mwftpd.conf), the SFTP Server (mwsftpd.conf), and the AS2 Interface (mwas2.conf). When no access class is assigned to a user, that is, when there is no entry on the list, and when there is no access class configured for the server, the user has full access.

Users may inherit access classes from user groups to which they belong. In this case, the list of access classes applied to the user is the combination or union of the classes for all groups to which the user belongs. When you assign access classes to a user, you override the inherited access class list. If the user has no inherited access class list, you can assign a list to the user here.

Created

Created is the date and time the user was created.

By (Created)

For Administrator, the system service itself creates this value, which appears in angle brackets, < >, to distinguish it from a MessageWay user. For most users, this is the MessageWay user that created this user.

Modified

Modified is the last date and time the properties were changed. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

By (Modified)

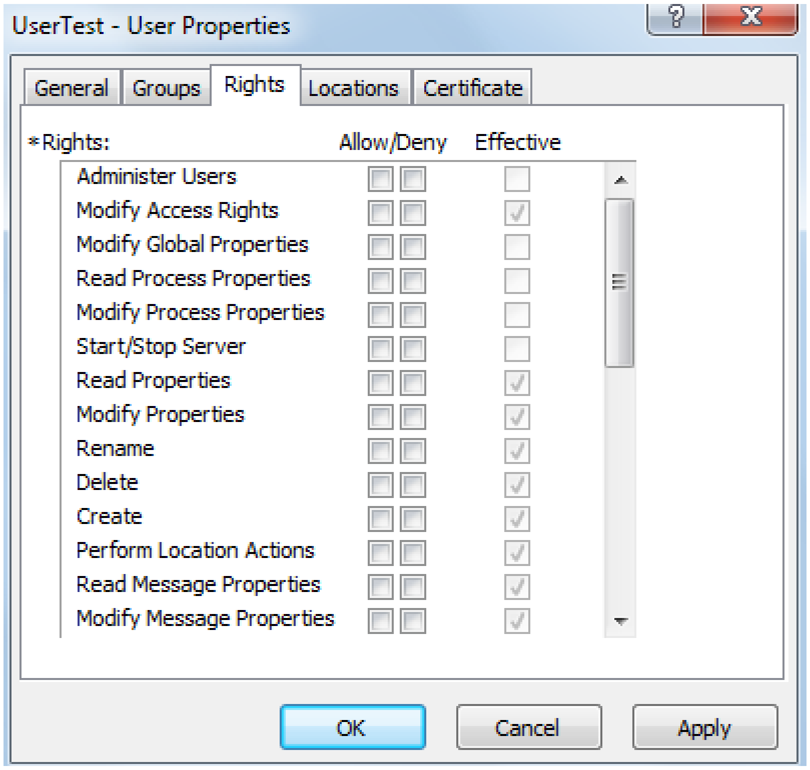
This is the last MessageWay user to change the properties. For existing systems that have been upgraded to version 5.0, this value is set initially by the installation process.

Approved By

Approved By is the MessageWay user that has approved this change. This field appears only when you use the optional Maker/Checker feature.

(User Properties) Rights Page

The **Rights** page of the User Properties window controls the type of access this user has and the tasks this user may perform. The Effective column shows any rights that have been inherited from groups to which the user belongs. They may be overridden by selecting any of the check boxes in the Allow/Deny columns.



*Rights:	Allow/Deny		Effective
Administer Users	□	□	□
Modify Access Rights	□	□	☑
Modify Global Properties	□	□	□
Read Process Properties	□	□	□
Modify Process Properties	□	□	□
Start/Stop Server	□	□	□
Read Properties	□	□	☑
Modify Properties	□	□	☑
Rename	□	□	☑
Delete	□	□	☑
Create	□	□	☑
Perform Location Actions	□	□	☑
Read Message Properties	□	□	☑
Modify Message Properties	□	□	☑

The following table describes what each right means to the user.

Right	Description
Administer Users	Add and remove MessageWay user accounts and modify global user configurations. When this is clear, the **Users** folder is not visible in the Manager.
Modify Access Rights	Change values on **Security** page of folders and objects, which controls who can perform which tasks on specific objects. Also requires the right **Read Properties**.
Modify Global Properties	Change properties for the MessageWay Server to modify database access, location of directories or settings to automatically start related servers. When this is clear, users cannot access the MessageWay Server Properties window.
Read Process Properties	View the statuses of the adapters or services. Also requires the rights **Read Properties** and **View Adapters/Services**. When this is clear, users cannot access the Adapter or Service Properties window.
Modify Process Properties	Change properties for the adapters or services, such as thread distribution, startup options and security. Also requires the rights **Read Process Properties**, **Read Properties**, **Modify Properties**, and **View Adapters/Services**. When this is clear, users may still be able to access the Adapter or Service Properties window, but the properties are dimmed.

Right	Description
Start/Stop Server	Start, stop, suspend or resume an adapter or service. Also requires the rights **Read Process Properties**, **Read Properties** and **View Adapters/Services**.
Read Properties	View properties of folders and objects other than adapters or services, such as locations.
Modify Properties	Change properties of folders and objects other than adapters or services, such as locations. Also requires the right **Read Properties**.
Rename	Change the name of user-defined folders and locations. Also requires the right **Read Properties**.
Delete	Delete user-defined folders and locations. Also requires the right **Read Properties**.
Create	Create folders and locations. Also requires the right **Read Properties**.
Perform Location Actions	Controls user ability to hold messages, release messages, hold outputs or release outputs. Also requires the right **Read Properties**.
Resubmit Messages	Controls user ability to resubmit messages. Also requires the rights **Read Properties** and **Modify Message Properties**.
Redirect Messages	Controls user ability to redirect messages. Also requires the rights **Read Properties** and **Modify Message Properties**.
Release Messages	Controls user ability to release messages. Also requires the rights **Read Properties** and **Modify Message Properties**.
Restart Receive	Controls user ability to restart transfer of messages only partially received. Also requires the rights **Read Properties** and **Modify Message Properties**.
Cancel Messages	Controls user ability to cancel messages. Also requires the rights **Read Properties** and **Modify Message Properties**.
Retrieve Archive Messages	Controls user ability to retrieve messages from archive. Also requires the rights **Read Properties** and **Modify Message Properties**.
Resubmit Archive Messages	Controls user ability to resubmit messages retrieved from archive. Also requires the rights **Read Properties** and **Modify Message Properties**.
Delete Archive Message Content	Controls user ability to delete messages retrieved from archive. Also requires the rights **Read Properties** and **Modify Message Properties**.
Read Message Properties	View the properties of messages. Also requires the right **Read Properties**.
Modify Message Properties	Controls user ability to: modify retention date and change priority; mark for archive and mark for deletion. Also requires the rights **Read Properties** and **Read Message Properties**.
View Messages	Read message content. Also requires the rights **Read Properties** and **Read Message Properties**.

Right	Description
Upload Messages	Send messages to MessageWay. Required for the user or user group when they are the sender of messages only. Also requires the rights **Read Properties** and **Read Message Properties**.
Download Messages	Retrieve messages from MessageWay. Required for the user or user group when they are the sender or recipient of messages. Also requires the rights **Read Properties** and **Read Message Properties**.
View System Counts	View the System Monitor, which shows counts for all adapters and services, and view counts in the adapters/services monitor. When this is clear, the System Monitor is not visible in the Manager.
View Adapters/Services	View the **Adapters/Services** folder and the list of adapters and services. When denied, also denies **Start/Stop Server** and **Modify Process Properties**. When this is clear, the **Adapters/Services** folder is not visible in the Manager.
View Logs	Controls user ability to view audit logs, event logs and trace logs. Also requires the rights **Read Properties** and **Modify Message Properties**.
Maker (Maker/Checker option)	Change the properties of users.
Checker (Maker/Checker option)	Validate changes made to the properties of users.
Generate Reports (reporting option)	Controls user ability to logon to reporting application. Also requires the rights **View Reports**.
View Reports (reporting option)	Controls user ability to logon to reporting application. Also requires the rights **Generate Reports**.

Rights

The Rights column is a list of all possible rights that a user might have to manipulate adapters or services, locations, receipt monitor schedules, rules and user definitions. When a user tries to perform a task, the rights on the specific object, such as a location, must allow the user access and these rights must permit the user to perform the task. Some of the rights are specific to optional MessageWay features, such as Maker/Checker.

Allow

Check any boxes in the Allow column to override the settings in the Effective column and permit this user those rights. To check or clear all boxes in the column, press **SHIFT** and click any box in the column. Some rights have dependencies. When you check a right that has dependencies, those check boxes will also be checked. Remote users must have the rights to upload and download messages.

Deny

Check any boxes in the Deny column to override the settings in the Effective column and deny this user those rights. To check or clear all boxes in the column, press **SHIFT** and click any box in the column. Some rights have dependencies. When you check a right that has dependencies, those check boxes will also be checked.

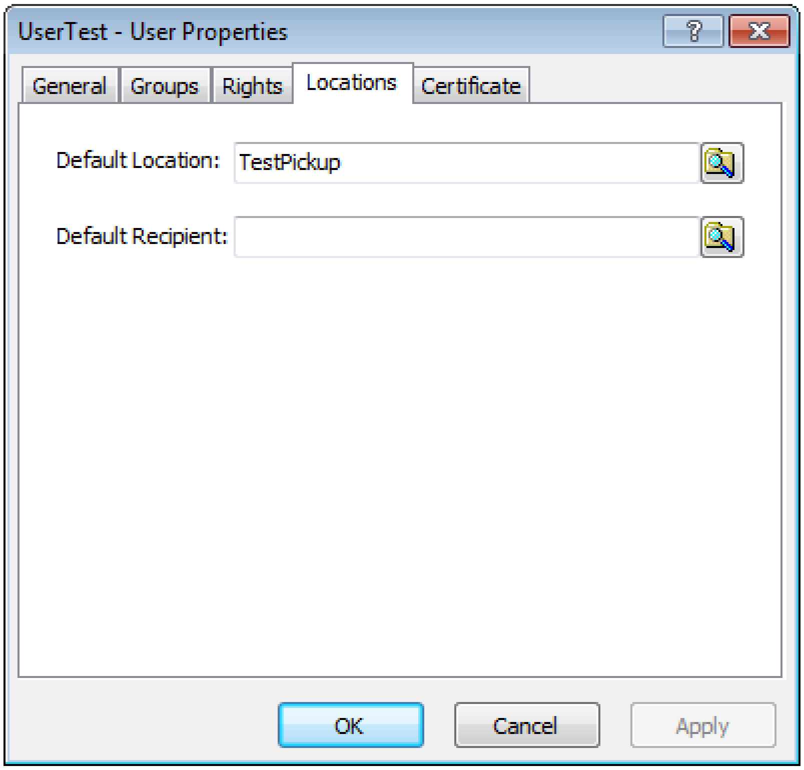
Effective (display only)

The check boxes in the Effective column show which rights the user currently has. These may be inherited from groups to which it belongs, if any. When a user is part of one or more user groups, the effective rights represent the combined rights of the groups. Check any boxes in the Allow and Deny columns to override the settings in the Effective column. To check or uncheck all boxes in one of the columns, press **SHIFT** and click any box in the column.

Remote users must have the rights to upload and download messages.

Locations Page

The **Locations** page of the User Properties window provides default locations for remote users who use an optional service to collect their messages from MessageWay. The Default Location value must be entered for any remote user to be able to log on. It provides the source mailbox for uploaded messages. The Default Recipient provides the default destination location where this user will be directed to collect messages from MessageWay.



Default Location: TestPickup

Default Recipient:

Default Location

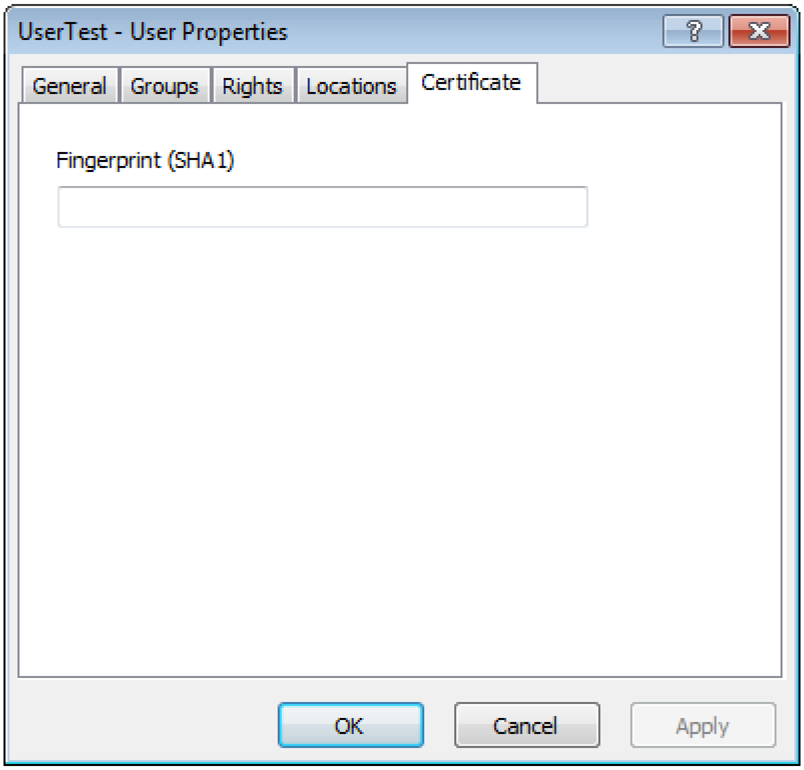
This value provides the source location for uploaded messages and the default pickup location where users can collect messages from MessageWay. Type a valid location name or select a name from the list using the **Browse** button. A default location is required for remote users to be able to access MessageWay. To download messages from this location, this user must have the download right set for the location. When there is no value in Default Recipient, this is the default location where messages will be uploaded. The remote client may override these settings and specify some other location in a **PUT** command or override the sender for the session using a **SITE SENDER** command. To upload to this location, this user must have the upload right set for the location. For more information about the use of these commands, refer to the section to configure the appropriate perimeter server.

Default Recipient

This value provides a default recipient for messages that are uploaded to MessageWay. Otherwise, the default recipient is the Default Location. It is useful when users access MessageWay with client software, such as WS_FTP Pro, and do not always want to specify a MessageWay location to send uploaded files. Type a valid location name or select a name from the list using the **Browse** button. To upload files to this location, this user must have upload rights set for the location.

Certificate Page

Reserved for future use.



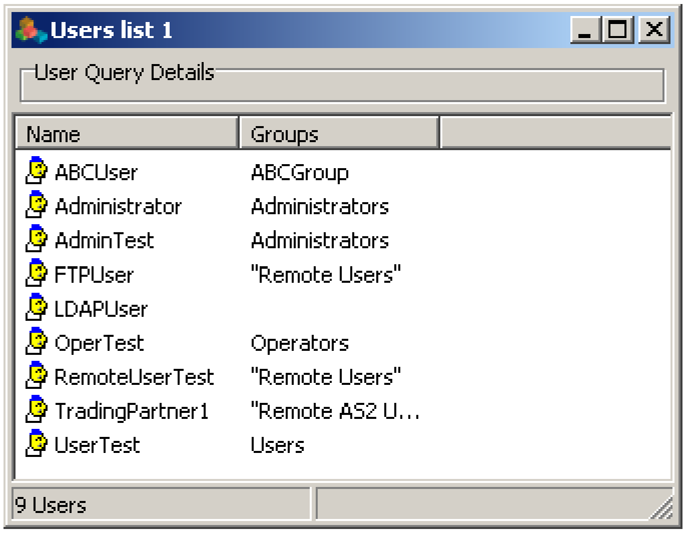
Fingerprint (SHA1)

Reserved for future use.

Users List Window

The Users List window appears when you use the **Find Users** command. When you search through multi-system environments, a System Name column also appears.

To sort by column content, click the column heading. For more information about the columns, refer to the topic, ***User Properties Window*** (on page 1351).



Name	Groups
ABCUser	ABCGroup
Administrator	Administrators
AdminTest	Administrators
FTPUser	"Remote Users"
LDAPUser	
OperTest	Operators
RemoteUserTest	"Remote Users"
TradingPartner1	"Remote AS2 U...
UserTest	Users

9 Users

This page intentionally blank.

Appendix Licenses

This section provides additional legal notices and information.

Cyrus SASL

Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact

Office of Technology Transfer
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3890
(412) 268-4387, fax: (412) 268-7395
tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Computing Services
at Carnegie Mellon University (http://www.cmu.edu/computing/)."

Expat

ICU

This includes information for both the software and the unicode data.

ICU License 1.8.1 and Later

Copyright (c) 1995-2009 International Business Machines Corporation and others

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Unicode

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991-2009 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the

Libssh

Two licenses cover the library modules used: LPGL and BSD.

Libssh LGPL License

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of,this License, whose permissions for other licensees extend to the,entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.

Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete

machine-readable "work that uses the Library", as
object code and/or source code, so that the user
can modify the Library and then relink to produce
a modified executable containing the modified
Library. (It is understood that the user who
changes the contents of definitions files in the
Library will not necessarily be able to recompile
the application to use the modified definitions.)

b) Use a suitable shared library mechanism for
linking with the Library. A suitable mechanism is
one that (1) uses at run time a copy of the
library already present on the user's computer
system, rather than copying library functions into
the executable, and (2) will operate properly with
a modified version of the library, if the user
installs one, as long as the modified version is
interface-compatible with the version that the
work was made with.

c) Accompany the work with a written offer, valid
for at least three years, to give the same user
the materials specified in Subsection 6a, above,
for a charge no more than the cost of performing
this distribution.

d) If distribution of the work is made by offering
access to copy from a designated place, offer
equivalent access to copy the above specified
materials from the same place.

e) Verify that the user has already received a
copy of these materials or that you have already
sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an

explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,

INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Linking with OpenSSL

17. In addition, as a special exception, we give permission to link the code of its release of libssh with the OpenSSL project's "OpenSSL" library (or with modified versions of it that use the same license as the "OpenSSL" library), and distribute the linked executables. You must obey the GNU Lesser General Public License in all respects for all of the code used other than "OpenSSL". If you modify this file, you may extend this exception to your version of the file, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

END OF TERMS AND CONDITIONS

Libssh BSD License

Some parts are under the BSDv2 License:

Copyright (c) 2000 Markus Friedl. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF

OpenLDAP

This includes information for both the OpenLDAP license and notice.

OpenLDAP License

BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

OpenLDAP Notice

Copyright 1998-2007 The OpenLDAP Foundation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by other parties and/or subject to additional restrictions.

OpenSSH

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)

[Tatu continues]

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

2)

The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Ariel Futoransky <futo@core-sdi.com>

<http://www.core-sdi.com>

3)

ssh-keyscan was contributed by David Mazieres under a BSD-style license.

4)

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

6)

Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl

Theo de Raadt

Niels Provos

Dug Song

Aaron Campbell

Damien Miller

Kevin Steves

Daniel Kouril

Wesley Griffin

Per Allansson

Nils Nordman

Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom

Tim Rice

Andre Lucas

Chris Adams

Corinna Vinschen

Cray Inc.

Denis Parker

Gert Doering

Jakob Schlyter

Jason Downs

Juha Yrjölä

Michael Stone

Networks Associates Technology, Inc.

Solar Designer

Todd C. Miller

Wayne Schroeder

William Jones

Darren Tucker

Sun Microsystems

The SCO Group

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

8) Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

b) snprintf replacement

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller

Theo de Raadt

Damien Miller

Eric P. Allman

The Regents of the University of California

Constantin S. Svintsoff

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium.

Todd C. Miller

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

*

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

OpenSSL

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==

*

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

Xerces

This information includes both the Apache license and an Apache Xerces notice.

Apache License

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

1. You must give any other recipients of the Work or Derivative Works a copy of this License; and

2. You must cause any modified files to carry prominent notices stating that You changed the files; and

3. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

4. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding

those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by

applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Apache Xerces Notice

NOTICE file corresponding to section 4(d) of the Apache License, Version 2.0, in this case for the Apache Xerces distribution.

This product includes software developed by

The Apache Software Foundation (http://www.apache.org/).

Portions of this software were originally based on the following:

- software copyright (c) 1999, IBM Corporation., http://www.ibm.com.

Zlib

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

This page intentionally blank.

Index