Version 8.1

MOVEit Central User's Guide

IPSWITCH
FILE TRANSFER

Copyright

The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc., also assumes no liability for damages resulting from the use of the information contained in this document.

This document was published on Friday, June 05, 2015 at 10:25.

Contents

Introduction 1

Overview 1

Key Features 3

Getting Started 9

First: Install the Software 9

Second: Define a Host 9

Third: Configure a Task 10

Fourth: Monitor a Task 11

Central Service 13

Overview 13

Starting and Stopping 13

Firewall Considerations 14

Running As... 14

Recommended Configuration: Running As a Service Under a Specific Windows Administrator15

Converting From MOVEit Central as a LocalSystem Service 15

Running MOVEit Central in the Foreground, Not As a Service 16

Additional Considerations 17

Central Config Utility 17

General Tab 18

License Tab 20

Database Tab 21

Errors Tab....23

Failover Tab (Enterprise Only) 24

Virus Tab 27

Tamper Tab....28

SSL Tab 29

Selecting SSL Encryption Methods....30

Selecting SSL Versions....31

How to Test SSL Changes 31

About Tab....35

Proxy Servers....35

No Proxy Server 36

Proxy Server, No Authentication Required....36

Proxy Server with "Windows Integrated" NTLM Authentication 36

Proxy Server Settings on Non-MOVEit Hosts....37

Backup....38

Disaster Recovery 38

Automated Configuration Replication....39

Failover (Enterprise Only) 42

Overview 42

Installation 47

Admin Failover Tab 51

Common Procedures 52

FTP Failover....54

Admin Console 79

Overview 79
Requirements 80
Installation 81
Remote MOVEit Central Admin Users 81
Remote MOVEit Central Admin Upgrades 82
Connecting... 82
Access Control 84
Domain Authentication 84
"MOVEit-User" Groups 85
Managing Members 90
Admin-specific Options 94
Command Menu 95
Settings Menu 96
Options Menu 97
Tasks Menu 98
View Menu 99
Help Menu 100

Configuring Tasks 101

Overview 101
Traditional vs. Synchronization Tasks 101
Traditional vs. Advanced Tasks 102
Icon Legend 102

Task Information 104

Task Information 105

Global Task Parameters 108

Tasks Tab 109

Task Schedule Status 112

Manipulating Tasks 112

Task Permissions 113

Task Groups 113

Viewing Task History 113

Editing Task Transfer Exceptions 114

Editing Source Timestamps 116

Task Groups 116

Edit Task Groups Dialog 117

Adding and Removing Task Groups 117

Editing Task Groups 118

Task Elements 120

Source 120

Destination 126

Schedule 130

Process 132

Next Action 136

Macro 137

Date List 144

AS1, AS2, AS3 (Enterprise Only) 148

Hosts..148

Overview 148

Hosts Tab 149

Host Operations...159

File Notifications 160

AS1, AS2, AS3 (Enterprise Only)..162

Processes/Scripts 163

Overview 163

Scripts Tab..164

Syntax (Enterprise Only) 165

Sample Scripts (Enterprise Only) 171

Built-in..173

Keys and Certs..211

Key/Cert Manager..212

Importing SSH Client Keys..216

SSL Client Certificates 217

Managing PGP Keys 219

Monitoring Tasks 229

Overview 229

Related Settings 229

"Central Config" Settings 229

System Settings..229

Troubleshooting 236

...With Admin 237

Status Tab 238

Debug Log Tab 240

Reports Window 241

Task Filter 258

...Without Admin 262

Event Log 262

Email Notification 264

Direct Access 264

Common Applications 265

Trigger Files 265

"Last Day Of Month" Schedules 270

Converting Unisys Print Backup Files to Text 274

Converting EBCDIC Text to ASCII Text 275

HTTP Uploads and Downloads 276

MessageWay Translation 277

Basic Instructions 277

Sample Task 278

Synchronization 283

Overview 283

Advanced Synchronization Architecture 285

Synchronization Icons 287

Options 288

Sync Direction 288

Sync Deletes 288

Best Option Scenarios 288

Hosts 292

Folders 292

Folder Permissions and Settings 293

Folder A 293

Folder B 294

Next Actions 294

Preview 295

Preview Columns 296

Preview Controls 296

Sync Preview Example 297

Task Actions 300

Adding a New Synchronization Task 300

"Add New Task" Dialog 301

"Synchronization Options" Dialog 302

Folder A Dialogs 302

Folder B Dialogs 303

"Initial Run Options" Dialog 304

"Preview" Dialog 305

Advanced Tasks (Enterprise Only) 307

Overview 307

Getting Started..308

File Loop...309

If Block..312

Task Elements 315

File Loop...315

If Block..316

Run Task...317

Email 318

Delete/Rename Original 318

Move Commands...319

Adding a New Advanced Task 320

Converting a Traditional Task 322

PGP Encryption 325

Overview 325

Encrypting 326

Configuring the Process 326

Configuring the Destination...329

Using Global Parameters for Keys 330

Decrypting 330

S/MIME Email 333

Overview 333

Configuring Certificates 334

Sending and Receiving 335

AS1, AS2, AS3 (Enterprise Only) 337

Overview 337

AS1, AS2 and AS3 339

Identifying My Organization and a Partner 342

Optional Elements 343

Limitations of the ASx Protocols 343

The AS1 Protocol 344

How an AS1 File Transfer Works 345

MOVEit Implementation of AS1 347

Advantages/Disadvantages of AS1 (Compared to AS2 and AS3) 349

The AS2 Protocol 350

How an AS2 File Transfer Works 351

MOVEit Implementation of AS2 356

Advantages/Disadvantages of AS2 (Compared to AS1 and AS3) 360

The AS3 Protocol 361

How an AS3 File Transfer Works 362

MOVEit Implementation of AS3 364

Advantages/Disadvantages of AS3 (Compared to AS1 and AS2) 367

MOVEit Implementation 368

Drummond "eBusinessReady" Certification 369

Why MOVEit DMZ is best choice for AS3....369

Advantages of MOVEit's Implementation 370

Limitations of MOVEit's Implementation 370

Certificates 370

What Are "Certificates"?....371

Where Do You Get a Certificate?....371

Where Might You Configure AS Certificates in MOVEit Central....372

Hosts....373

Overview 373

AS1 376

AS2 379

AS3 387

Tasks....389

AS1 389

AS2 391

AS3 394

Advanced Topics 399

FTP Source Integrity 399

Custom Directory Parsing....400

Column-based Custom Parsing 401

Directory Parsing Script 402

SysLog and SNMP 407

Syslog Utilities 407

SNMP 409

Antivirus 409

POP3 Sources 411

GetMICConfig Utility 412

Port Numbers 413

System Internals 415

Local Mail Relay 421

Instructions 422

Troubleshooting 430

MessageWay CLI 431

Program Arguments 431

Input File 432

Output File 435

Return Code 438

Database 438

Schema 438

MySQL 444

MSSQL 448

Converter 458

Tamper Detection 466

Trimming 466

Troubleshooting 467

Legal Information 469

Software License 469

Legal Information - Americans with Disabilities Act (ADA) Compliance 478

Legal Information - Export Restrictions 479

About Ipswitch 481

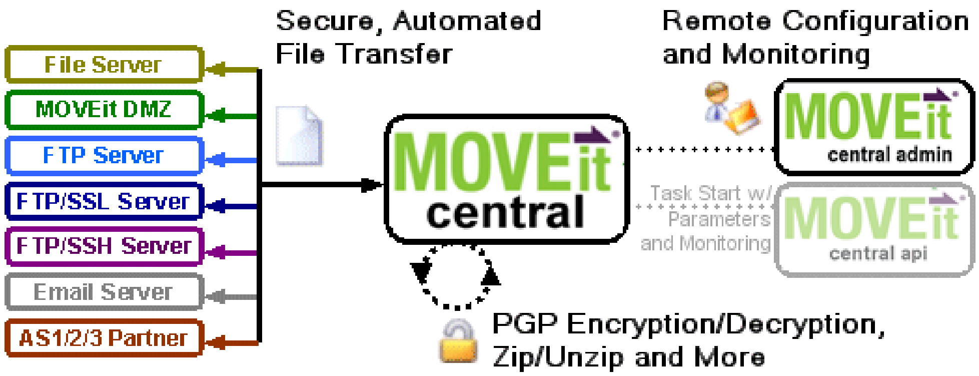
Contact... 481

Index 483

Introduction

Overview

MOVEit Central is an enterprise-level, Windows-based, automated managed file transfer (MFT) workflow engine that pulls, processes and pushes files on a scheduled, event-driven or on-demand basis between internal and external systems, including MOVEit DMZ servers. MOVEit Central does this using easily created tasks (no programming required) that can exchange files between multiple systems using multiple protocols, and process files with many built-in functions (including OpenPGP encryption) and custom VBScript scripts.


Secure, Automated File Transfer
Remote Configuration and Monitoring
File Server
MOVEit DMZ
FTP Server
FTP/SSL Server
FTP/SSH Server
Email Server
AS1/2/3 Partner
MOVEit central
MOVEit central admin
Task Start w/ Parameters and Monitoring
MOVEit central api
PGP Encryption/Decryption, Zip/Unzip and More

Supported Servers and Protocols

MOVEit Central Corporate and Enterprise editions securely and automatically transfer files to and from:

- FTP servers
- FTP over SSL (FTPS) servers
- FTP over SSH (SFTP) servers
- the local filesystem
- network folders
- email servers
- MOVEit DMZ servers
- AS1, AS2 or AS3 servers (Enterprise only)

Supported File Processing

File and folder synchronization/replication is available between any two selected folders on these servers.

PGP encryption/decryption, zip operations, rename, find and replace, command-line applications and anti-virus integration are also built in and require no additional software. *(Native PGP must be enabled in your MOVEit Central license code.)*

Automated server-to-server file transfers require no knowledge of any script language because MOVEit Central provides an operator-friendly user interface to schedule tasks and monitor their progress.

In cases where custom scripts are necessary, MOVEit Central Enterprise fully supports VBScript, with many custom functions to make integration with MOVEit Central tasks seamless. External applications and schedulers may also be used to start tasks, pass task parameters, monitor running tasks, and retrieve transfer and audit logs through **MOVEit Central API**, available in component and command-line versions for Windows and Java.

Security

Based on a robust scheduling facility, MOVEit Central also takes care not to become a security target itself by protecting sensitive access information with powerful encryption, local files with NIST 800-88-compliant data erasure and configuration channels with SSL.

Remote access to MOVEit Central is restricted to specific Windows users in local or domain groups. With MOVEit Central Enterprise, group access to transfer tasks and related elements can be fine tuned to delegate management in a number of commonly requested configurations. For example, group permissions can grant full administrative access, grant "just run and/or report" access to specific tasks, grant a limited ability to transfer anything between two designated servers or create a private "slice" of MOVEit Central that other groups cannot access.

All transactions are logged to a tamper-evident ODBC database usable not only by MOVEit Central's built-in reporting, but also by custom billing and tracking systems. Local or remote configuration, control and monitoring of the MOVEit Central service is performed through the **MOVEit Central Admin** application. Unlimited copies of this management client may be run at any given time, and different permissions to different task groups may be allocated to different users.

Notice: The new Web-based Admin program is now available for preview. It requires a separate installation process, described in the MOVEit Central Installation Guide.

FIPS VALIDATED 140-2 ™

MOVEit crypto

NIST National Institute of Standards and Technology

Communications Security Establishment

Centre de la sécurité des télécommunications

Canada

Cryptographic services, including complete encryption of all configuration files, are provided by **MOVEit Crypto**. Also available as a separately licensed commercial product for Windows or Linux developers, MOVEit Crypto is only the tenth product to have been validated under FIPS-140-2 by the United States and Canadian governments.

Key Features

Exchange Files with:

- **FTP servers**
  - Insecure FTP
  - FTP over SSL (Explicit and Implicit Connect Modes, plus "CCC" support)
  - Client Certificates
  - Active and Passive Data Transfer Modes
  - Supports Custom "Quote" Commands (Upon Connection and Per-File)
  - Supports Unusual Directory Listings (e.g., IBM)
  - Supports Synchronization/Replication
  - Automatic Retry of Failed Transfers
  - "Partial File" Protection (Avoids Pulling Files in Use, Rename After Upload)
  - Client NAT
  - Download Integrity Verification (MD5)
- **SSH Servers**
  - Password and Public Key Authentication
  - Supports Unusual Directory Listings
  - Supports Synchronization/Replication
  - Automatic Retry of Failed Transfers
  - "Partial File" Protection (Avoids Pulling Files in Use, Rename After Upload)
  - Download Integrity Verification (MD5)
- **MOVEit DMZ servers** (HTTPS interface)
  - Event-Driven ("Transfer Immediately Upon Complete Receipt")
  - Complete Guaranteed Delivery
    - Cryptographic-Quality Integrity Check (SHA1)
    - Automatic Restart of Partial Transfers
    - Automatic Retry of Failed Transfers

  - "Partial File" Protection (Avoids Pulling Files in Use, Rename After Upload)
  - Session Reuse (For Performance)
  - Supports Synchronization/Replication
- **Windows servers**
  - Local Filesystem
    - Event-Driven ("Transfer Immediately Upon Complete Receipt")
  - Windows-based network shares (Including "Mapped Drive Letters")
    - Event-Driven ("Transfer Immediately Upon Complete Receipt")
  - Novell and other NAS resources
  - (All)
    - Automatic Retry of Failed Transfers
    - "Partial File" Protection (Avoids Pulling Files in Use, Rename After Upload)
  - Supports Synchronization/Replication
- **Email servers**
  - Outbound Protocol: SMTP
  - Inbound Protocol: POP3
  - Password Authentication
  - SMIME Encrypt/Decrypt/Sign Scripts Included
  - Automatic Retry of Failed Transfers
- **AS1, AS2 and AS3 Partners** (Enterprise only)
  - Drummond "eBusiness" certified software
  - AS1: POP3/S and SMTP/S with email MDN support
  - AS2: HTTP/S with asynchronous, synchronous and email asynchronous MDN support
  - AS3: FTP/S with MDN support
- **HTTP (web) servers**
  - HTTP or HTTPS protocol
  - HTTP authentication
  - Upload via PUT or POST
  - Download via GET
  - Special support for Microsoft SharePoint Server

Schedule Tasks to run:

- AS SOON AS TARGET FILE IS COMPLETE (*MOVEit DMZ and FileSystem only*)
- Once at a specific time (e.g., "at 5pm")
- Several times in a specified time range (e.g., "from 1pm to 3pm")
- Only on specific days of the month or weekdays (e.g., "Mondays, 3rd")
- Until certain files are transmitted successfully
- In response to other successful or failed transfers
- When certain files are found on disk (e.g., "trigger files")
- When commanded to do so by an external application through MOVEit Central's API interface (Enterprise only)

Configure Tasks to:

- Zip/unzip files
- Only retrieve new files (e.g., "newer than 1 days" or simply "since the last time MOVEit Central looked")
- Only retrieve old files (e.g., "older than 7 days")
- Only retrieve small or large files
- Transfer available files in batches (up to X files or just more than Y bytes per task run)
- Never overwrite existing files
- Append to existing files
- Create outbound folders if they do not already exist
- Run simultaneously with many other tasks, even to different hosts
- Ignore specified files or folders
- Delete, rename or move source files after a successful transfer
- Run command-line applications against files
- Use macros (e.g. "[mm][yyyy]") to rename outbound files or select source files
- Use macros to look for inbound files
- Kick off other tasks or send email notifications in response to responses and failures
- React to and/or parse "trigger files"
- PGP Encrypt/Decrypt Files (Using native PGP and license)
- SMIME Encrypt/Decrypt Files (Using Included SMIME Control)
- Handle massive (>10GB) files
- Synchronize/replicate files and folders between two selected folders
- Record the path, size and date of source and destination files, the speed of the transfer, and any errors encountered or processes run in a tamper-evident transfer database
- Execute custom VBScript against any file (Enterprise only)

- Use Advanced Tasks to apply conditional processing and consolidate "chained" tasks (Enterprise only)

Configure Integrated Antivirus to:

- Work with Symantec AntiVirus, McAfee VirusScan, and Trend Micro OfficeScan
- Either ignore infected source files or actively delete them.

Configure Logs and Events to:

- Write to a text file
- Write to the Windows Application Event Log or a Windows "MOVEit" Event Log (either of these sources may be sent to SysLog or SNMP servers)
- Send email notifications if tasks succeed, fail or do nothing

Monitor Tasks through:

- Running "debug log" with extensive debugging information (e.g. FTP "200" messages)
- Display of active and inactive tasks
- "Reports" dialog with historical task run and audit events
- Drill-down views of specific task runs and file transfers
- Your own custom log display using MOVEit Central API (or ODBC) access to real-time log database (Enterprise only)

Ensure Security with:

- Encrypted file transport using FTP over SSL, FTP over SSH and HTTPS
- Encrypted Admin/Central communications (requires installation of valid SSL certificate on MOVEit Central platform)
- Encrypted configuration files (256-bit AES)
- Encryption of individual files with PGP or SMIME
- AS2 and the other ASx protocols (AS1 and AS3) (Enterprise only)
- Auditing of administrator actions, task runs, and file transfers
- Tamper detection of audit and activity logs, via cryptographic hashing
- Overwrites of temporary cache files with cryptographic-quality random data (NIST 800-88-compliant data erasure)
- NIST-validated cryptography

Run as:

- A **service** on Windows 2008 and 2012.
- A desktop application with the scheduler disabled and/or a special test configuration file in test and development situations.

Delegate to Operators the Ability to: (Enterprise only)

- Monitor, run, make minor or major changes to, add and delete certain tasks
- Monitor/reference or make changes to, add and delete certain hosts, SSL certs, SSH certs, PGP keys, and scripts
- Start/restart/stop certain tasks

Licensing:

Enterprise version:

- Unlimited number of remote hosts (i.e., sources, destinations)
- Unlimited number of scheduled tasks plus
- Unlimited number of advanced tasks, which allow conditional processing
- Unlimited number of SSH keys, SSL certificates and PGP keys
- Unlimited number of administrators
- Ability to create custom processes (scripts)
- Support for alternate hosts to provide rollover to another host during processing of a task
- Delegation of permissions via access control lists (hosts/tasks, groups/users)
- OPTIONAL: Automatic Failover
- OPTIONAL: Native OpenPGP Support
- OPTIONAL: AS1, AS2 and AS3 Support
- OPTIONAL: API Interface module

Corporate version:

- Up to 10 remote hosts (i.e., sources, destinations); excludes "local" hosts
- Up to 50 scheduled tasks
- Unlimited number of SSH keys, SSL certificates
- Up to 10 PGP keys
- Unlimited number of administrators
- OPTIONAL: Native OpenPGP support

Getting Started

First: Install the Software

Basic MOVEit Central uses two installation programs: MOVEit Central on a server and MOVEit Central Admin that provides access to MOVEit Central.

Your first task is to install MOVEit Central on a supported platform. Refer to the MOVEit Central Installation Guide for more information.

Next, you should install MOVEit Central Admin either on the same server as MOVEit Central or on a remote system.

If you just want to take a tour of MOVEit Central, take the defaults for all installation options. You will, however, be required to point to a license file.

To administer MOVEit Central remotely, you can also use the standalone MOVEit Central Admin installation program to set up the client on each of your remote desktops.

After both MOVEit Central and MOVEit Central Admin have been installed, run MOVEit Central Admin and connect to "localhost" (no username/password is required). If you cannot connect, refer to the ***Troubleshooting*** (on page 236) guide.

Second: Define a Host

After MOVEit Central Admin connects to MOVEit Central, click over to the ***"Hosts" tab*** (see "***Hosts Tab***" on page 149). This tab displays a complete list of all the servers MOVEit Central can connect and exchange files with. By default, the only Host MOVEit Central knows about is the local filesystem, so our first task here is to define a new, remote host so we can begin to experiment with real file transfers.

1 **Click the "Add Host..." button**. on the right side of the Hosts tab. A "Define New Host" dialog will pop up with three fields.

2 **Select the type of host you wish to access** from the drop-down in the "Define New Host" dialog. For this exercise, please select an "SSH", "FTP" or "MOVEit DMZ" server.

3 **Enter the IP address or hostname of your remote host** in the middle text box. You can change this value later if necessary.

4 **Enter a "friendly name"** like "My Test FTP Server" in the bottom text box. You can also change this value later.

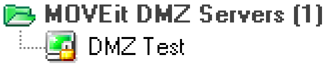
5 **Press the "OK" button** to move on to more details about your host.

The following "host definition" dialog comes in several unique flavors depending on the type of host you selected. There are several constants here however. (See the ***"Hosts"*** (see "***Hosts Tab***" on page 149) sections in the "Configuring Tasks" section of the manual for a complete description of all options.)

- **Username and Password**: Username and password used to authenticate to the remote server. Please fill this in.
- **Port**: TCP port number used by the remote service. Typical values are 22 for SSH, 443 for MOVEit DMZ and 21 or 990 for FTP. Generally the default value will do, but you may have to change it depending on your remote host.
- **Retry**: Allows transfers to automatically be retried if they encounter transient problems. You may want to set this to "0" for now so any errors you encounter will immediately end your task.

Before you save this host, use the "Test" button to make sure the IP/hostname, credentials and other information you provided about this host will grant your tasks the access they need.

After you press "OK" on this dialog, you will see a new blue (FTP/S), green (MOVEit DMZ) or purple (SFTP) host entry in your list of available hosts.



MOVEit DMZ Servers (1)
DMZ Test

You can make adjustments to this host definition at any time by double-clicking on your host. (A right-click pop-up menu also offers this and other options.)

Third: Configure a Task

Now that MOVEit Central can access TWO hosts (the one you just defined plus the local filesystem), it is time to build a task to exchange files between them. Click over to the ***"Tasks" tab*** (see "***Tasks Tab***" on page 109) and perform the following steps.

1 Click the "Add Task..." button - In response to your click a new dialog will appear. Select "traditional" task here rather than "synchronization" task.

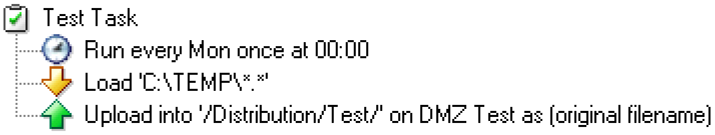
2 Enter and Task Name and Select Your Task Elements using the first dialog. You should make sure the default values of "Source", "Destination" and "Schedule" are checked. Click "OK" to continue.

3 Define a Source using the next dialog. First, select the type of host you wish to access. Please select "Load from local folder..." for this example; the second drop-down will be grayed out at this point. Click "OK" to continue.

4 Define ***Source Details*** (see "***Source***" on page 120) using the next dialog which appears. Like the host details dialog you encountered earlier, the exact appearance of this dialog will be determined by the type of host you are accessing, and there are many options. For this example, simply use the "Browse..." button to select a local folder that contains a few small files, and click "OK".

5. Define a Destination using the next dialog. You will again be prompted to select the type of host you wish to transfer to. For this example, select the type of host you just added and then make sure the specific host you just added is selected in the second drop-down box. Click "OK" to continue.
6. Define ***Destination Details*** (see "***Destination***" on page 126) using the next dialog. Again, the exact appearance of this dialog will vary depending on the destination type, but for our example we can take most of the defaults presented. One critical change we will want to make, however, is the file path. Use the "Browse..." button to select an appropriate path on the remote host and press "OK" when done. (If you encounter problems connecting to the remote host with the browse button, double-check your username/password credentials and the IP address/hostname on your host definition.)
7. Define a ***Schedule*** (on page 130) using the next dialog. First select a day of the week and press the related "Add" button. Then select a single time and press its related "Add" button. Notice your changes are displayed in red text in the "result" panel. When you have provided information to constitute a legal schedule, the "OK" button will be activated. Press it to continue.
8. Do NOT Run Task Now using the next dialog. We want to step back and take a quick look at our new task before proceeding. (We will run and monitor it in the next section.)

Your new task should look similar to the following example.



Test Task
- Run every Mon once at 00:00
- Load 'C:\TEMP\*.*'
- Upload into '/Distribution/Test/' on DMZ Test as (original filename)

Notice the yellow down arrow indicates a "download from filesystem host" step, the green up arrow indicates an "upload into MOVEit DMZ" step and the stopwatch icon represents a schedule. Also note that this task has a green checkmark on it, indicating that it is "ready and scheduled" and will be run by the MOVEit Central at the scheduled time. (Tasks with "pause icons" will not be run by MOVEit Central at scheduled times, but may sometimes be run manually.)

Fourth: Monitor a Task

Now it is time to run and monitor your task.

1. Left-click a task, and select the "Set Filter to This Task" item.
2. Left-click the task again and select the "Run Now" item.
3. Switch first to the ***Debug Log tab*** (on page 240). Detailed information about your task run will be displayed here. (When you opted to "Set Filter...", the task-level debug level was automatically elevated to "More Debug".)
4. Now switch to the ***Status tab*** (on page 238) where you can see a quick, "what happened during my last run" view of the task.

5 Then switch over to the ***Reports window*** (on page 241) (if it is not already selected, make sure to set the Display option to Task Runs). Your task run (and more like it if you rerun the task) should be listed at the top of the "Task Runs" view. If you are fast enough, you will see your task listed with a yellow "working" icon in the Status column. Otherwise, your task may be listed with a red exclamation point or green checkmark icon. (If you see a red icon, your task failed.)

6 If you flip over to the "File Activity" view you should also see any files your task moved at the top.

7 Finally, if you flip over to the "Audit" view you should see your manual task start action ("task_run") logged at the top.

At this point you have the skills to configure and monitor file transfers tasks on MOVEit Central using MOVEit Central Admin. The rest of this manual discusses the many options and configurations which affect how these tasks operate.

Central Service

Overview

The MOVEit Central installation program installs these components:

- MOVEit Central service

  MOVEit Central is normally installed as a service. This is the program that maintains the configuration files and runs configured tasks.
- MOVEit Central Config Utility

  Most MOVEit Central settings, such as hostnames, directories, schedules, and logging, are managed by MOVEit Central Admin. However, a few settings are managed by a separate program, MOVEit Central Config. These are ordinarily set once at installation; there is rarely a need to change them.

The MOVEit Central Admin program, installed separately, is used to configure and control file transfer and manipulation tasks, but the MOVEit Central service is the program which actually maintains the configuration file and runs configured tasks.

NOTICE: The new Web-based Admin program is now available for preview. It requires a separate installation process, described in the *MOVEit Central Installation Guid*e.

Starting and Stopping

The MOVEit Central service normally starts automatically when the computer boots. However the service and/or the underlying service application may also be started manually through the Windows command-line console or the Windows Service control panel if the MOVEit Central service is not currently running. (The "***Service - Running As...*** (see "***Running As...***" on page 14)" documentation has more information about this.)

The MOVEit Central service can also be stopped through the Windows command-line console or the Windows Service control panel, but a cleaner way to stop the service (and avoid killing running tasks) is to use MOVEit Central Admin's "***Shut Down Service*** (on page 95)" command.

Firewall Considerations

The type of "outbound" access MOVEit Central requires through a firewall depends on what remote hosts you wish to access. For example, if you wish to access a remote MOVEit DMZ server, you will need to allow Central to connect to that server using HTTPS.

It is not normally necessary for firewall rules to be configured to allow "inbound" access to a MOVEit Central. Two exceptions:

- If MOVEit Central Admin needs to be allowed to connect from a remote IP addresses through a firewall. (In this case, MOVEit Central should be configured to force SSL encryption when communicating with MOVEit Central Admin). Ports 3471, 3472, and 3473 are used.
- If an additional server (e.g., Microsoft IIS FTP) has been installed on the same platform as MOVEit Central. (Strictly speaking, inbound firewall rules are still not required to access MOVEit Central in this situation. However most firewall administrators take a "rules for machine" view rather than "rules for application" view, so it is best to be up front with your firewall administrators if you plan on installing any "helper" services on the MOVEit Central platform.)

For more information, see ***Port Numbers*** (on page 413).

Running As...

MOVEit Central normally runs as a service. It can be stopped and started from the Services control panel or from the command line, but the cleanest way to stop the service if tasks may be running is with the "***Shut Down Service*** (on page 95)" command in MOVEit Central Admin's "Command" menu. MOVEit Central is usually installed to run under a specific, local Windows administrator account.

Recommended Configuration: Running As a Service Under a Specific Windows Administrator

If you are running MOVEit Central as a service, you must run that service as a specific Windows administrator rather than as "LocalSystem" if you want to access remote (or mapped) Windows file systems. Fortunately, this is how new installations of MOVEit Central are configured.

Note: Early installations of MOVEit Central set up the MOVEit Central service to run as "LocalSystem". See the "***Converting From MOVEit Central as a LocalSystem Service*** (on page 15)" topic for instructions how how to convert from LocalSystem to a specific account.

If you wish to authenticate MOVEit Central Admin (and MOVEit Central API) users to a Windows domain (or Active Directory), you may need to run MOVEit Central under a domain user account that is also an administrator on the local MOVEit Central machine. (If you do not, you may see "RPC Server is unavailable" errors when your domain users attempt to authenticate to MOVEit Central.) It is rarely a good idea to run MOVEit Central as a full domain administrator; running as a domain user with local administrative permissions is preferred.

Converting From MOVEit Central as a LocalSystem Service

If you are running the MOVEit Central service as LocalSystem and you want to switch this to a specific administrator account, please follow the following procedure.

1. Go to Administrative Tools / Services.
2. Right-click **MOVEit Central**, and choose **Properties**.
3. Choose the **Log On** tab.

   You will see that the Local System account is selected.
4. Choose **This account** and select a local administrator account (for which you know the password).
5. Then choose **OK** to change the user under which MOVEit Central runs.

   This step is necessary because Windows will not allow services to access network shares if they are running under the local system account.
6. The account you choose must have the *Act as part of the operating system* right. To configure this:

   a) Go to Administrative Tools / Local Security Policy.

   b) Expand the Local Policies tree, and choose **User Rights Assignment**.

   c) Double-click **Act as part of the operating system**.

   d) Click **Add** on the dialog that appears, and add the user under which the service will be running.
7. Make sure the account you choose has full file/folder permission rights to the MOVEit Central "Program Files\MOVEit" folder and cache folder.

Running MOVEit Central in the Foreground, Not As a Service

There are two ways to run MOVEit Central in the foreground as a "normal" application instead of as a service. Doing so is normally useful in only two situations: you are attempting to replicate and diagnose unusual problems caused by permissions or policies recently applied to the administrative user under which MOVEit Central runs; or, you want to bring MOVEit Central up with the scheduler disabled so you can examine an imported configuration without running any tasks.

To just run MOVEit Central as a normal foreground application, select the "Run MOVEit Central Service in Foreground" option from the Start menu "MOVEit Central" program group.

To take advantage of other run options, you must start MOVEit Central from the command line. Some of these options can harm your existing MOVEit Central implementation, so please read the entire description of each option before using it. The following options are currently available:

- -? - Causes MOVEit Central to display a very short help dialog and exit.
- -manual - Causes MOVEit Central to run as a normal foreground application. (Using this option and this option only will achieve the same result as selecting the "Run MOVEit Central Service in Foreground" option from the Start menu "MOVEit Central" program group.)
- -config [config_file] - Causes MOVEit Central to launch using a config file other than "miccfg.xml". When this option is used, "-manual" is also almost always used as well.
- -k - Causes MOVEit Central to launch with the scheduler disabled. When this option is used, "-manual" is also almost always used as well.
- -remove - Causes MOVEit Central to uninstall its Windows service entry. (This is much different than uninstalling the entire application.) Using this option could break your MOVEit Central implementation.
- -install - Causes MOVEit Central to install its Windows service entry. (This is much different than installing the entire application.) Using this option could break your MOVEit Central implementation.

Ipswitch technicians use the following batch file (saved in the "/Program Files/MOVEit" folder) to safely launch customer configurations in the foreground for troubleshooting purposes. This batch file disables the scheduler and requires technicians to type in the explicit name of an alternate configuration.

```
@echo off SET CUSTOMERCONFIG=%1 if R%CUSTOMERCONFIG%R==RR GOTO NOCONFIG
"c:\program files\moveit\micentral.exe" -k -manual -config %1 GOTO THEEND
:NOCONFIG echo *** You MUST provide the path of a custom config file! :THEEND
```

Additional Considerations

- If you would like to be able to manage task permission groups from MOVEit Central Admin, be sure the user under which MOVEit Central runs is an administrator.
- The user under which MOVEit Central runs should have FULL permissions to the local folder in which the MOVEit Central program and configuration files are stored. The same user must also have FULL permissions to the MOVEit Central cache folder.
- The user under which MOVEit Central runs need NOT have permission to all Windows file shares you would like to access. Specific Windows file share credentials will be configured for each file share.

Note: If the Windows user (for MOVEit Central Service) does not have permissions to the MOVEit folder where its configuration and other important elements are stored, no changes or additions to Central's configuration would be permanent. They would be gone the next time the service starts. To help prevent this from happening, during start-up, MOVEit Central checks permissions to the folder. If permissions are insufficient, an alert is sent to the Email Address set in the Config Utility - Errors tab with instructions for resolving the issue, and MOVEit Central terminates the current session.

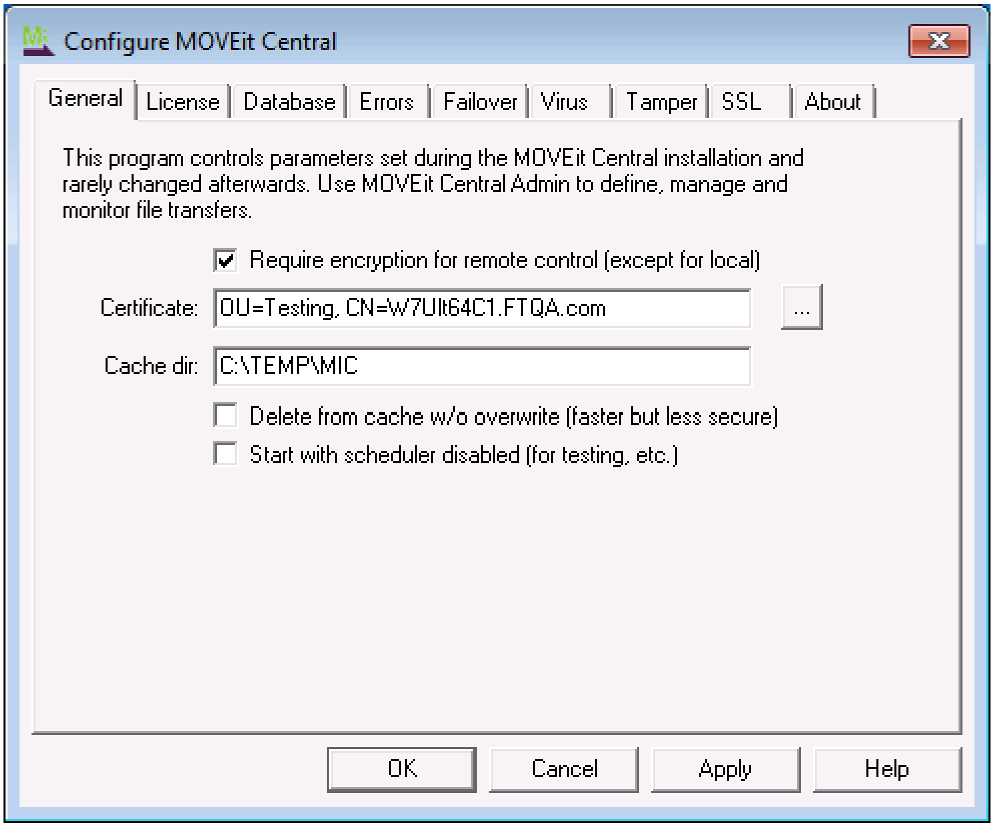
Central Config Utility

Most MOVEit Central settings, such as hostnames, directories, schedules, and logging, are managed by MOVEit Central Admin. However, a few settings are managed by a separate program, MOVEit Central Config. These are ordinarily set once at installation; there is rarely a need to change them.

To run the configuration program, use the Start menu shortcut **MOVEit Central Config**.

The configuration program displays a dialog with several tabs.

General Tab



This program controls parameters set during the MOVEit Central installation and rarely changed afterwards. Use MOVEit Central Admin to define, manage and monitor file transfers.

☑ Require encryption for remote control (except for local)

Certificate: OU=Testing, CN=W7Ult64C1.FTQA.com

Cache dir: C:\TEMP\MIC

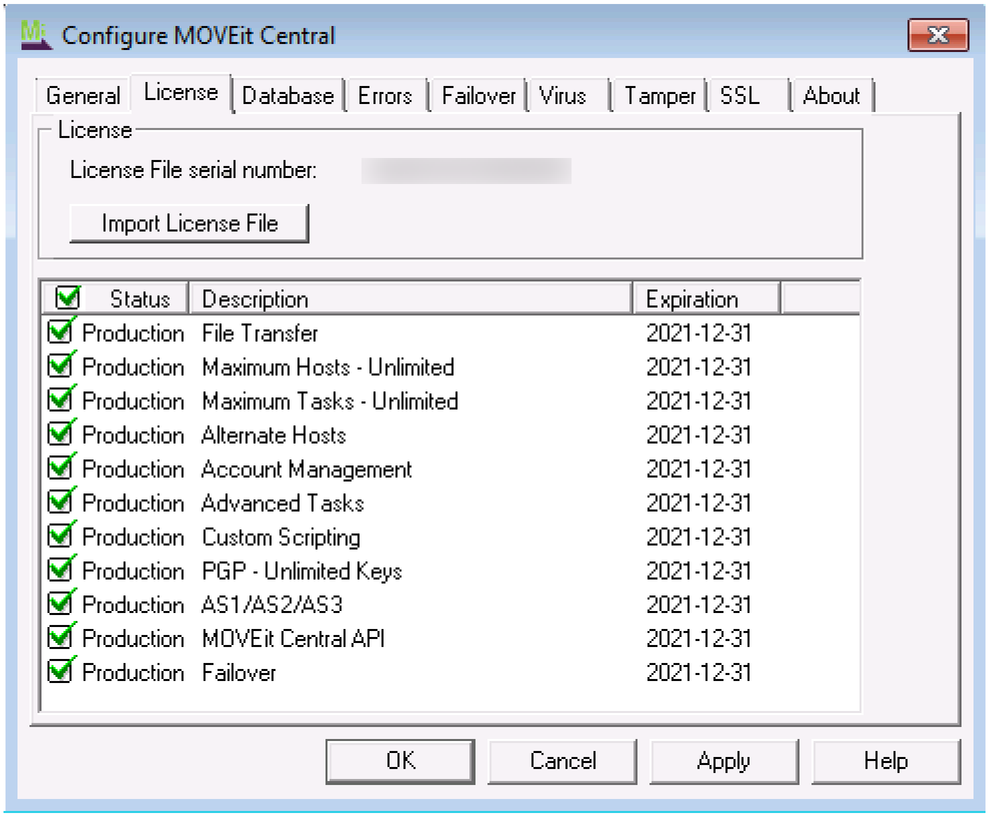
□ Delete from cache w/o overwrite (faster but less secure)

□ Start with scheduler disabled (for testing, etc.)

The settings on this tab are:

- **Whether connections from MOVEit Central Admin or API should be encrypted**. Normally, you should enable encryption, for best security. However, you can disable encryption if, for instance, you have not obtained a certificate. Note: encryption is always disabled when MOVEit Central Admin or API is connecting from the same computer (localhost).
- **Encryption certificate**. This is used only for encrypted links from MOVEit Central Admin or MOVEit Central API. The installation program will by default install a "test" (self-signed) certificate for this purpose. If you have an existing SSL certificate on the MOVEit Central system, you may select it here. Providing a secure connection for MOVEit Central Admin is not necessary, but it is recommended if MOVEit Central Admin sessions will be accessing the Central server from outside your private network. You can use MOVEit Central's ***SSL Certificate Manager*** (see "***Key/Cert Manager***" on page 212) to create a certificate suitable for use here.
- **Cache dir**. This is the directory that will be used to store files while they are being processed by a task; files will automatically be deleted from here (with NIST 800-88-compliant cryptographic overwrite) when related tasks complete. Normally this directory should be on your largest available hard drive. WARNING: You must create any alternate folder specified by this location by hand; MOVEit Central will not create this folder if it is missing. Also, the user under which the MOVEit Central service runs must have read/write/delete/subdirectory access to this folder.
- **Delete from cache w/o overwrite**. MOVEit Central normally takes care to delete and then overwrite its cache files with cryptographic-quality random data. If this option is enabled, file transfers may be faster (especially large, filesystem-to-filesystem transfers).
- **Start with scheduler disabled**. Normally, MOVEit Central starts running tasks right after starting. Check this box if, for testing or operational purposes, you don't want MOVEit Central's scheduler active when MOVEit Central starts. MOVEit Central will still able to start tasks explicitly via MOVEit Central Admin or MOVEit Central API. If this option is selected, you can enable the scheduler after startup via MOVEit Central Admin; however, the next time MOVEit Central starts, the scheduler will again be disabled until this option is unselected in the configuration program.

License Tab



License File serial number: [redacted]

☑ Status	Description	Expiration
☑ Production	File Transfer	2021-12-31
☑ Production	Maximum Hosts - Unlimited	2021-12-31
☑ Production	Maximum Tasks - Unlimited	2021-12-31
☑ Production	Alternate Hosts	2021-12-31
☑ Production	Account Management	2021-12-31
☑ Production	Advanced Tasks	2021-12-31
☑ Production	Custom Scripting	2021-12-31
☑ Production	PGP - Unlimited Keys	2021-12-31
☑ Production	AS1/AS2/AS3	2021-12-31
☑ Production	MOVEit Central API	2021-12-31
☑ Production	Failover	2021-12-31

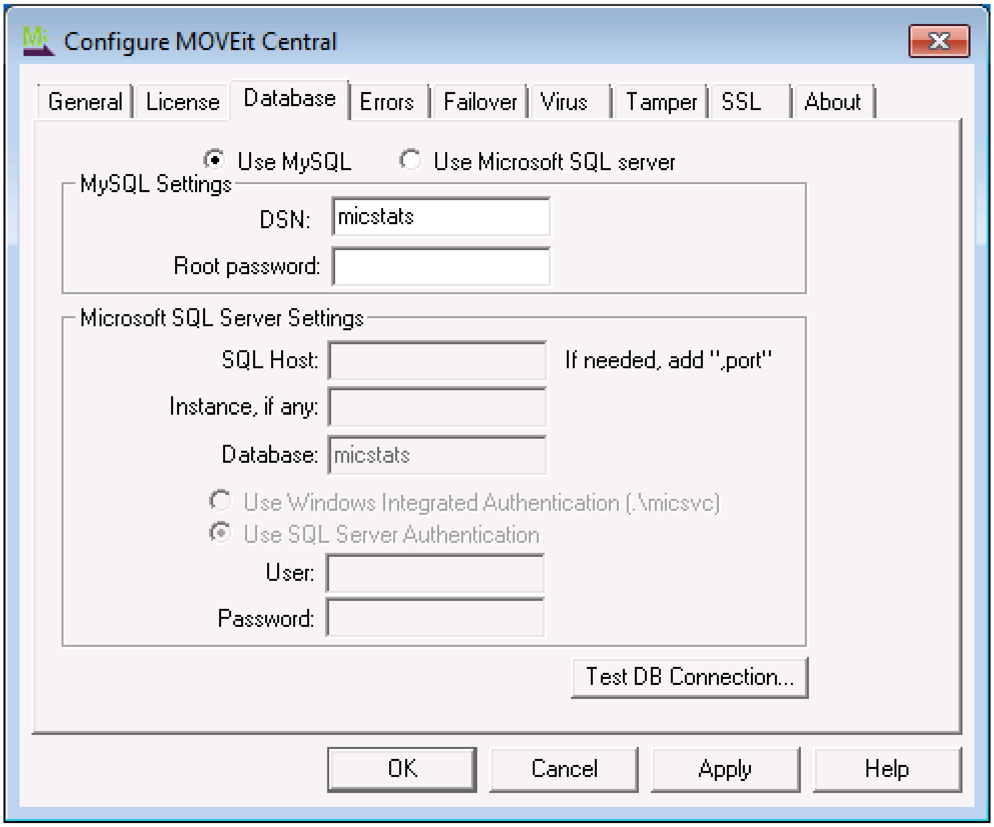
This tab shows the license file serial number and the features enabled by the license. A license file is required to activate the program. The file is provided to you when you evaluate or license the program. In addition to enabling the basic operation of MOVEit Central, a license file can also activate optional features of the program. Each license file expires on a certain date; some license files have different features that expire on different dates.

The settings on this tab are:

- **License File serial number**. The serial number of the file you supplied during the install process.
- **Import License File**. To switch to a different license file, browse for your license file, and select to change it.

The license file is activated when you click **Apply** or **OK**.

Database Tab



Configure MOVEit Central

General | License | Database | Errors | Failover | Virus | Tamper | SSL | About

● Use MySQL ○ Use Microsoft SQL server

MySQL Settings

DSN: micstats

Root password:

Microsoft SQL Server Settings

SQL Host: If needed, add ",port"

Instance, if any:

Database: micstats

○ Use Windows Integrated Authentication (.\micsvc)

● Use SQL Server Authentication

User:

Password:

This tab allows you to choose which database engine to use, and to select options specific to that database engine:

If you choose *Use MySQL*, you can change these settings:

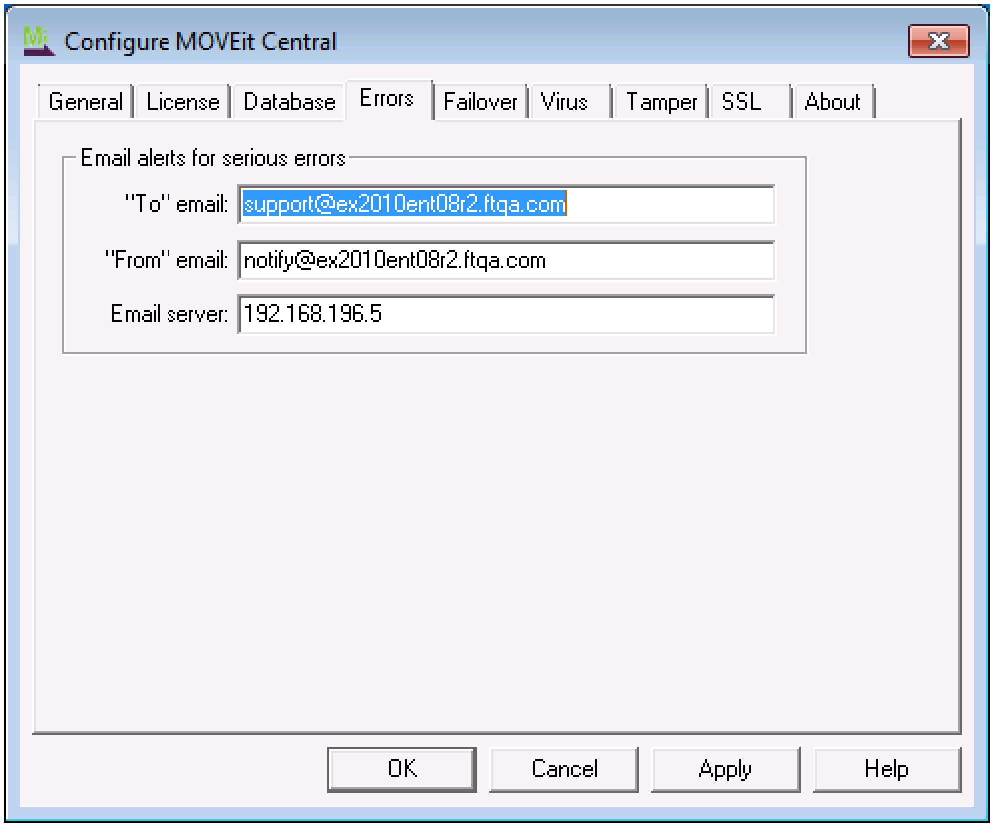
- **DSN**. The ODBC Data Source Name of the database. There is rarely a need to change this from the default of "micstats".
- **MySQL root password**. The password of the "root" user in the MySQL database. This is stored encrypted in the registry, and is used only by the install program. The previous value is not displayed in the dialog box when the program starts--not even masked by *'s--for security reasons.

If you choose *Use Microsoft SQL Server*, you can change these settings:

- **Host**: The hostname of the SQL Server.
- **Instance**: The name of the SQL Server "instance". This is usually empty, meaning the default instance.
- **Database**: The name of the database. This is nearly always "micstats".
- **Use Windows Integrated Authentication**. This causes MOVEit Central to authenticate to SQL Server using the credentials associated with the MOVEit Central service. These credentials are shown on the radio button; for instance, "(.\micsvc)" means the local Windows user micsvc (as opposed to a domain user). The SQL Server must have a login with the same name, associated with a Windows username of the same name.
- **Use SQL Server Authentication**. This causes MOVEit Central to authenticate to SQL Server using the specified SQL login and password. The password is stored encrypted in the local registry. These credentials must exist on the SQL Server, and there must be a corresponding user in the micstats database on that server. Typically these are created during creation of the database, and usually do not need to be changed.

Test DB Connection. Click this button to test whether you can connect to the database using the specified credentials.

Errors Tab



Email alerts for serious errors

"To" email: support@ex2010ent08r2.ftqa.com

"From" email: notify@ex2010ent08r2.ftqa.com

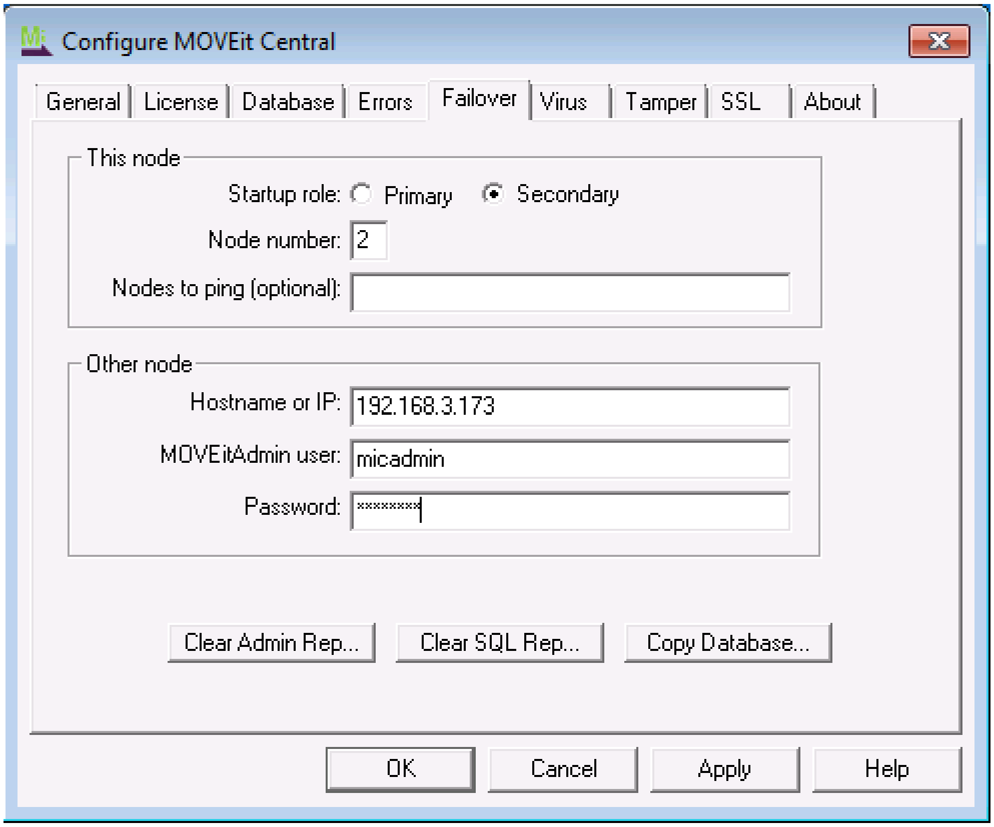
Email server: 192.168.196.5

The Errors tab is used to configure email messages that are sent when a serious error occurs. MOVEit Central sends these emails primarily when in failover mode. These settings are independent of the Host and Task email settings that are used in normal running of tasks.

The settings on this tab are:

- **"To" error email**. This is an optional comma-separated list of email addresses to which a message should be sent when a serious error occurs. Some of the situations in which MOVEit Central will send messages to this/these address(es) include pending and actual failover and tamper detection instances. If this value is left empty, no email is sent.
- **"From" email**. This is the address that MOVEit Central should place in the "From:" line of emails it sends as a result of a serious error.
- **Email server**. This is the hostname or IP address of the email server to use for these messages.

Failover Tab (Enterprise Only)



This node

Startup role: ○ Primary ● Secondary

Node number: 2

Nodes to ping (optional):

Other node

Hostname or IP: 192.168.3.173

MOVEitAdmin user: micadmin

Password: ********

The Failover tab is used to configure the ***Failover*** (on page 42) capability of MOVEit Central. This tab is grayed out unless you have entered a license key that enables failover. Sites which have not licensed failover can ignore this tab.

The settings on this tab are:

This node

- **Startup role**. This is the role that this node will assume when MOVEit Central starts. When installing failover for the first time, you should set one node to be Primary and the other node to be Secondary. Subsequently, MOVEit Central itself will manage this value on the two nodes when a failover occurs.
- **Node number**. This is 0, 1, or 2. 0 disables the failover feature even if you have a license for failover. To enable failover, assign the number 1 to one node, and 2 to the other node. The numbers 1 and 2 have no special significance; however, by convention, the value 1 is typically given to the node that is initially assigned the primary role, and the value 2 is given to the node initially assigned the secondary role.
- **Nodes to ping**. This is an optional comma-separated list of nodes that MOVEit Central should "ping" before assuming the primary role. If this list is empty, no ping test is done. If the list is not empty, at least one of the nodes must respond to a ping before MOVEit Central will start running tasks. The purpose of this feature is to prevent two copies of MOVEit Central from each thinking the other is down because the network between them is down. To take best advantage of this feature, you should enter the hostname of one or more computers that reside on the same network as the other node.
- It is recommended that the value of a "nearby" and trusted router be configured in this field. If you do not have a dedicated network device which fits the bill, it is probably best to leave this value blank.

Other node

- **Hostname or IP**. The hostname or IP address of the other node.
- **MOVEit Admin user**. The Windows user on the other node which MOVEit Central should use to login to the other node. You must create this user on the other node, and make it a member of the "MOVEit Admin" group. It need not belong to the "Users" group. You may wish to follow the convention of using the username "micfailover" on both nodes.
- **Password**. The password of the above user. This password is stored in the registry, using 256-bit AES encryption.

The buttons on this tab are typically used only during a ***resynchronization*** (on page 54) operation after MOVEit Central has been stopped:

- **Clear Admin Rep...** This erases any MOVEit Central Admin commands that are scheduled to be replicated from this node to the other node. It does this by deleting the MICMisc.blg file. (A new blank file will be created automatically when MOVEit Central is next started.)
- **Clear SQL Rep...** This erases any SQL statements that are scheduled to be replicated from this node to the other node. It does this by deleting the MICSQL.blg file. (A new blank file will be created automatically when MOVEit Central is next started.)

- **Copy Database...** This allows you to copy the MICStats database from the other node to this node. This process overwrites the current node's statistics database with the contents of the other node's database. This operation should ordinarily be performed only on the secondary node.

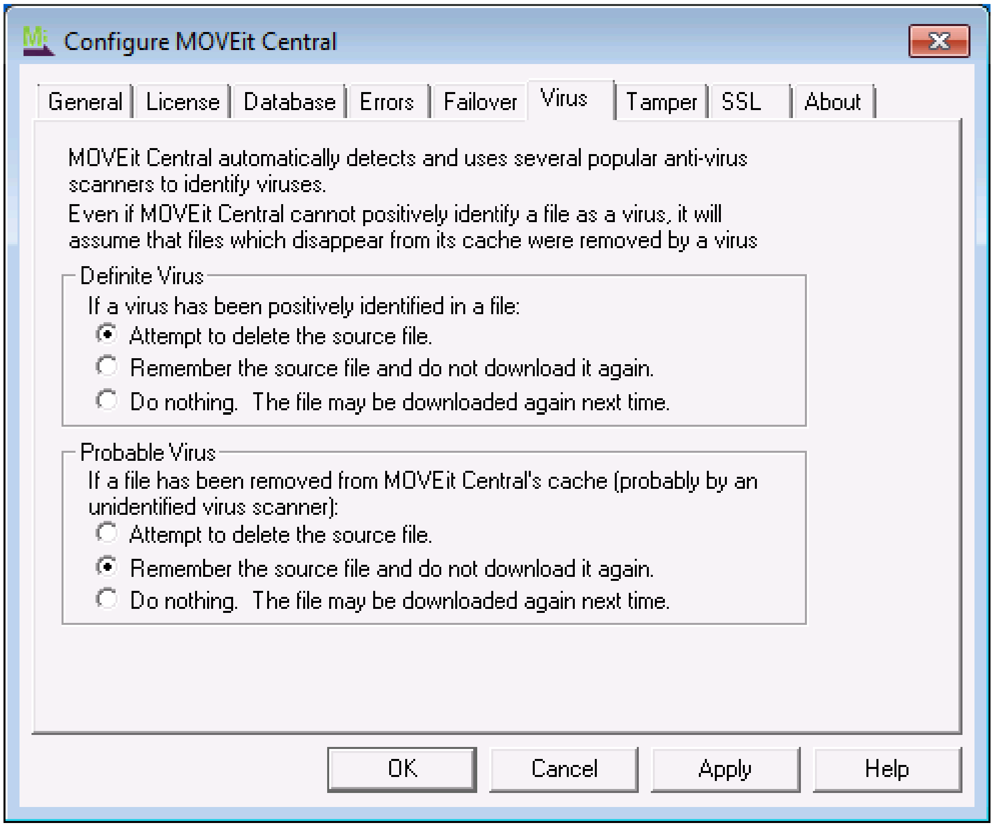
  You need to do a Copy Database on the secondary node when you first install the secondary node. You may also perform this operation subsequently if the database on the current node has gotten out-of-sync with the one on the other node.

  When you choose Copy Database, you will be prompted for the remote directory from which to copy the database files, and the local directory to which you should copy them. The program's initial defaults assume that you have installed MySQL on C: and that you are using the default database name. Check the suggested paths and, if necessary, correct them for your installation before choosing OK to start the copy. The configuration program will remember the changed values the next time you choose Copy Database.

  The Copy Database command requires that there be a Windows user on the remote node with the same username and password as the session under which you are running the configuration program. This user must have read access to the files in the MySQL\Data\micstats directory.

  Please note that if you change the IP address of the other MOVEit Central node in this dialog, the Copy Database parameters will not automatically pick up on the change. If, however, you are using hostnames to define your other host, you may not need to make a change here.

Virus Tab



MOVEit Central automatically detects and uses several popular anti-virus scanners to identify viruses.
Even if MOVEit Central cannot positively identify a file as a virus, it will assume that files which disappear from its cache were removed by a virus

Definite Virus
If a virus has been positively identified in a file:
● Attempt to delete the source file.
○ Remember the source file and do not download it again.
○ Do nothing. The file may be downloaded again next time.

Probable Virus
If a file has been removed from MOVEit Central's cache (probably by an unidentified virus scanner):
○ Attempt to delete the source file.
● Remember the source file and do not download it again.
○ Do nothing. The file may be downloaded again next time.

The Virus tab is used to configure how MOVEit Central interacts with third-party real-time antivirus programs.

- **Definite Virus**. This setting configures what MOVEit Central should do if it determines that a specific antivirus scanner has identified a file as having a specific virus.
- **Probable Virus**. This setting configures what MOVEit Central should do if a file it is processing is suddenly deleted, but either:
  - MOVEit Central cannot determine for certain that the deletion was done by an antivirus program, or
  - MOVEit Central cannot determine from the antivirus program which virus was detected.

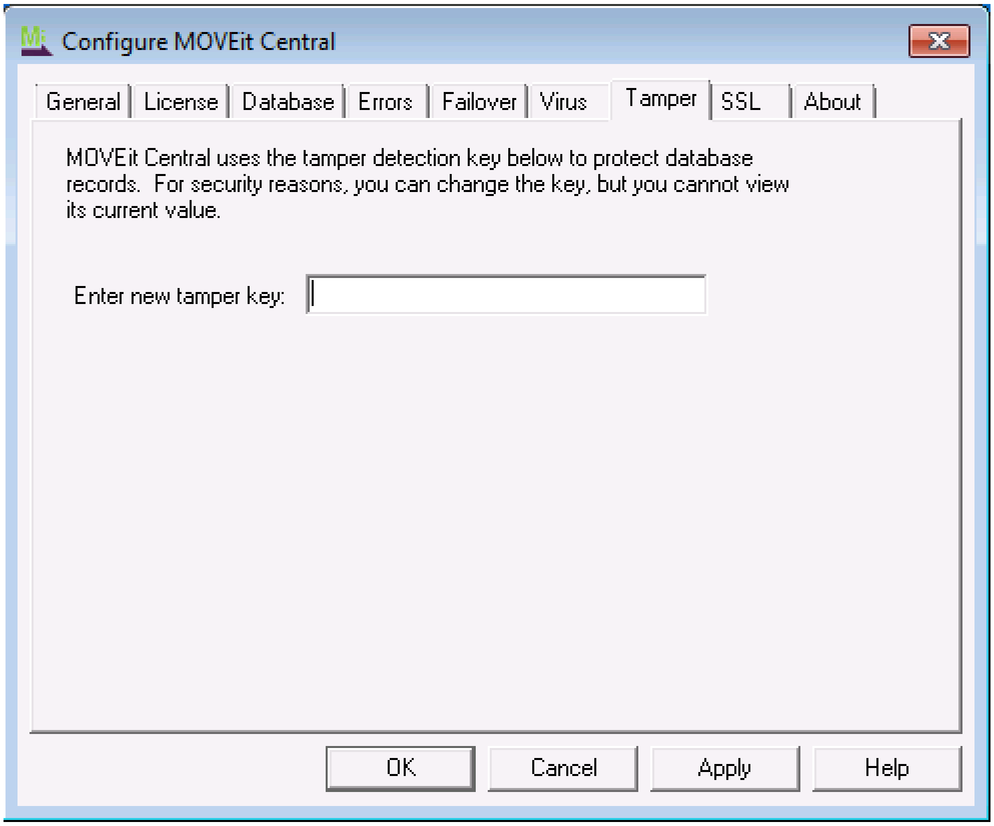
  Typically, this situation arises when an antivirus program that is not supported by MOVEit Central is running.

For each case, there are three actions that can be taken by MOVEit Central (in addition to marking the individual file transfer as failed and task as partially failed):

- **Attempt to delete the source file**. If the source file cannot be deleted from the host (perhaps due to insufficient permissions), MOVEit Central will "remember" the source file, as below.
- **Remember the source file and do not download it again**. MOVEit Central will make an entry in the "Task Transfer Exceptions" list for this task, which will cause future runs of this task to not download the file. If you want MOVEit Central to download the apparently infected file again, remove these entries using MOVEit Central Admin's "Edit Task Transfer Exceptions" right-click menu option.
- **Do nothing**. The file may be downloaded again next time. This option is rarely useful because the antivirus scanner will likely intercept the file again, causing the same situation to occur again.

See also ***Advanced Topics - Antivirus*** (see "***Antivirus***" on page 409).

Tamper Tab



MOVEit Central uses the tamper detection key below to protect database records. For security reasons, you can change the key, but you cannot view its current value.

Enter new tamper key:

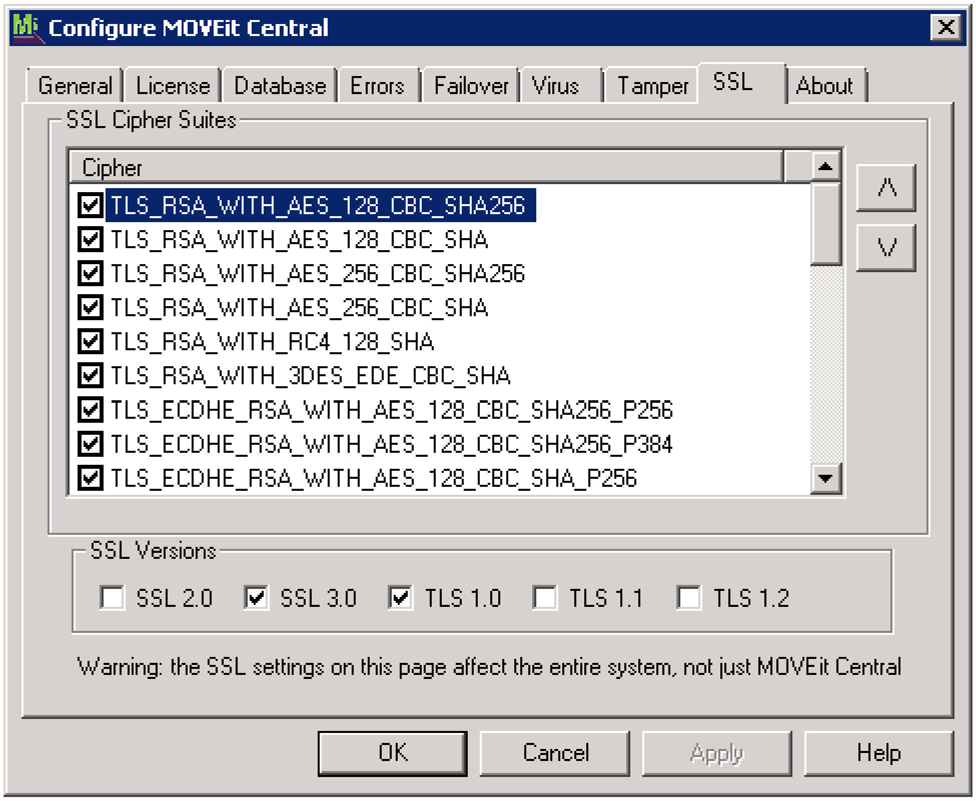
The Tamper tab is used to reset the tamper detection key used to protect database records. Any value typed here will be encrypted and then stored in the registry. (Do not copy the "HashKey" value from the registry into this field; instead copy "HashKey" registry values from one registry to another.) The derived tamper key is used to maintain a cryptographic "hash chain" of database records. For security reasons, the current tamper detection key is not shown; you can use this tab only to set a new tamper detection key. Because the tamper detection key is set during installation and should not be changed once set, there is rarely a need to use this tab.

SSL Tab

MOVEit uses Microsoft's built-in TLS/SSL security support provider (Schannel.dll). In all supported versions of Windows, there are several available protocols and cipher suite options enabled by default. Not all of them will meet your security and compliance needs. For example, the much older SSLv2 protocol is enabled by default on the server but is not allowed for PCI-compliant web applications. Be careful to choose the right mix of strong encryption methods and acceptable client support.

Warning: Changing the cipher suites or TLS/SSL versions can affect any applications that use TLS/SSL. Be sure you are aware of the requirements of other applications before making a change. For example, if you select SSL 2.0 only, MOVEit will not be able to connect to the Microsoft SQL database. The intent of this dialog is to allow you to avoid using a weak cipher where not allowed by PCI, FIPS, or other standards.

You can use the SSL tab to select the cipher suites and SSL versions that can be used when establishing an SSL session.



SSL Cipher Suites

Cipher

☑ TLS_RSA_WITH_AES_128_CBC_SHA256
☑ TLS_RSA_WITH_AES_128_CBC_SHA
☑ TLS_RSA_WITH_AES_256_CBC_SHA256
☑ TLS_RSA_WITH_AES_256_CBC_SHA
☑ TLS_RSA_WITH_RC4_128_SHA
☑ TLS_RSA_WITH_3DES_EDE_CBC_SHA
☑ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
☑ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
☑ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

SSL Versions

□ SSL 2.0 ☑ SSL 3.0 ☑ TLS 1.0 □ TLS 1.1 □ TLS 1.2

Warning: the SSL settings on this page affect the entire system, not just MOVEit Central

Selecting SSL Encryption Methods

The SSL Cipher Suites section allows you to choose which cipher suites are permissible, and their order of preference. A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings. By default, all ciphers suites enabled in the base Windows OS are enabled.

Note: Both the client's and the server's preferences are taken into consideration when choosing the actual cipher for a given session. Though the server's first choice won't always be chosen, the cipher that ends up being chosen will always be in the set of allowed algorithms on both sides.

Select the **Enabled** check box to disable a selected entry or to enable an unselected entry.

Entries closer to the top of the list are given preference over entries lower down. Use the arrow buttons to move entries up or down in the list. Even if you must permit weaker cipher suites, you should always put the stronger ones at the top of the list.

Selecting SSL Versions

SSL Versions are shown at the bottom of the SSL Tab. The default selections include SSL 2.0, SSL 3.0, and TLS 1.0. The versions selected determine the cipher suites that are available.

Select a check box to disable a selected version, or to enable an unselected version.

Note: After any SSL Version change, you need to reboot the system before the change takes affect.

Note: Be aware that the security policy setting **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** will restrict the available cipher suites and protocols. For example, TLS 1.0 will always be enforced.

Note: Be aware that the setting SSL cipher suite order via Group Policy will override any changes made to cipher suite order on this tab.

How to Test SSL Changes

To test SSL changes, first obtain a copy of OpenSSL. You can get OpenSSL.exe from the ***OpenSSL Project*** (***http://www.openssl.org***). Consult the following examples which show how to use this client and understand the information it provides.

(You need to type the commands in purple. Look for the results in red.)

Using OpenSSL to verify TLS1 is running on a remote server

This test was performed against our moveit.ipswitch.com support server. It shows that a connection using TLS1.

```
openssl s_client -connect WIN-TRL4JLD99D8:3471 -tls1
```

```
Loading 'screen' into random state - done

CONNECTED(000000FC)

depth=0 CN = WIN-TRL4JLD99D8, OU = Testing

verify error:num=18:self signed certificate

verify return:1

depth=0 CN = WIN-TRL4JLD99D8, OU = Testing

verify return:1

---

Certificate chain

 0 s:/CN=WIN-TRL4JLD99D8/OU=Testing
```

```
   i:/CN=WIN-TRL4JLD99D8/OU=Testing
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIC0TCCAbmgAwIBAgIBADANBgkqhkiG9w0BAQUFADAsMRgwFgYDVQQDEw9XSU4t
VFJMNEpMRDk5RDgxEDAOBgNVBAsTB1Rlc3RpbmcwHhcNMTQxMjA1MjE0MjUxWhcN
MjMwNDA1MjE0MjUxWjAsMRgwFgYDVQQDEw9XSU4tVFJMNEpMRDk5RDgxEDAOBgNV
BAsTB1Rlc3RpbmcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+Alcm
qM+OpzRA1Sk+qr8Ofsvnt52sVg/B+J9b5UsRWabrNAulXMmh6gHLOXGzZMR4ouha
IXRT91aOoJa4NBnoT/oymRnv4tSIDc77jG/fiXTvX5R+XXvpo83npfuuRIu+9S1S
F1C3elO/c6B2imeblee16HN+x6GNgRaLCX5fFKsdZaM9LEAxCTGcq2bBjOEQiAXH
uZ+S5yu7BUZcIJCoJh5WRDYS1GSlIonMBGgOHCgXOLHjh7mqQvMvugkF8ldz5piZ
mEnHdKnbxXqGhhh/kU7E6OuELc9E+Iscm2ZY2zJt9gylyoLmmm+l102G5bvzHEDT
3Trceu6GHj2mnd+dAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAC+wCLSVwfR8tkWH
tVh0Nd9pyMdMuyDNmR9M1041FBf94F+6SXXSL/R6pcfOVgYqGdzhZqEg/xATD4RW
wnAEg+pSTW0WrJBiSLRIzbV3ykESjHdk5s53wJfCRaOYAgqeWjxy2AHpFTEd7K4Y
OQ98z5sdWQ2ZERttlcTZi1PwTyEgOqpGJqGJ1Bi4sMUPqX8+Ob95zESW5A2dzaB0
F6SUZosCkC8+00QTOhnnGW/MJk02ox5AwOUeVs1HJk/U9IydDy3Knka2gDed9W04
b4f5EAeoGzihBWI3GEKW44Tbmtm17nQTILmtyaBOPJPaRzl5LdG86tDc1SOAcOPz
lHnv2mg=
-----END CERTIFICATE-----
subject=/CN=WIN-TRL4JLD99D8/OU=Testing
issuer=/CN=WIN-TRL4JLD99D8/OU=Testing
---
No client certificate CA names sent
---
SSL handshake has read 1215 bytes and written 349 bytes
```

```
---

New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-SHA

Server public key is 2048 bit

Secure Renegotiation IS supported

Compression: NONE

Expansion: NONE

SSL-Session:

    Protocol  : TLSv1

  Cipher    : ECDHE-RSA-AES256-SHA

    Session-ID:
3F2700008883D23306B46F8A63A138348A412268F08E35B9E016401FD4C98854



    Session-ID-ctx:

    Master-Key:
D54E13EE42BFF28224222EB489758CAA37A1F24D1073F98414EF0A379EE9249F

D4647C1BEC129F306714A5CD17780980

    Key-Arg   : None

    PSK identity: None

    PSK identity hint: None

    SRP username: None

    Start Time: 1418072824

    Timeout   : 7200 (sec)

    Verify return code: 18 (self signed certificate)
```

Using OpenSSL to verify SSL 3 is NOT running on a remote server

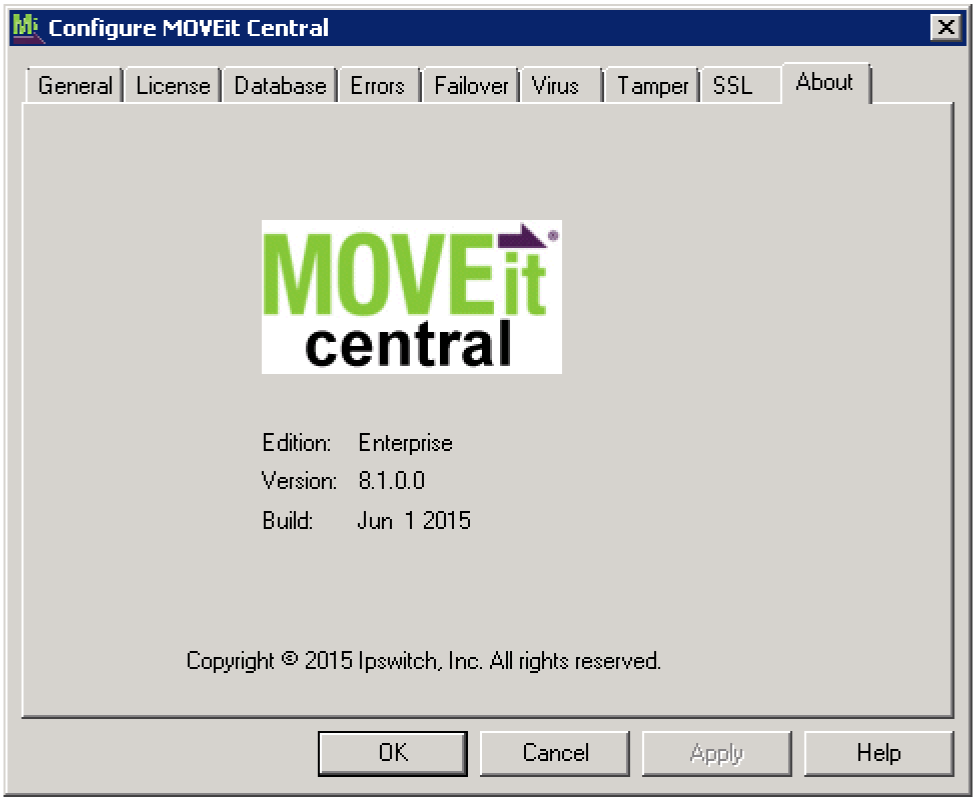
(This test was performed against an internal IIS server after SSL3 was manually disabled.)

```
openssl s_client -connect WIN-TRL4JLD99D8:3471 -ssl3
```

```
Loading 'screen' into random state - done

CONNECTED(0000012C)
```

```
2980:error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number:.\ssl\s3_pkt.c:338:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 5 bytes and written 7 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : SSLv3
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1418074464
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
```

About Tab



Edition: Enterprise
Version: 8.1.0.0
Build: Jun 1 2015

Copyright © 2015 Ipswitch, Inc. All rights reserved.

The About tab shows the MOVEit Central edition you have, the version number, and the software build date.

Proxy Servers

MOVEit Central supports the following HTTP/S proxy server configurations when communicating with any MOVEit DMZ server:

- No Proxy Server
- Proxy Server, No Authentication Required
- Proxy Server with "Windows Integrated" NTLM Authentication

MOVEit Central draws information about whether or not it should use a proxy server at all and what host and port to connect to to access the proxy server from the Internet Explorer settings of the user under which MOVEit Central runs as a service. In other words, MOVEit Central cannot make use of proxy servers to connect to MOVEit DMZ when it is running as "LocalSystem".

No Proxy Server

MOVEit Central uses the hostname/IP address and port number configured in its service user's Internet Explorer settings for its proxy settings. If these values are empty, MOVEit Central knows that no proxy server is in use.

Proxy Server, No Authentication Required

MOVEit Central uses the hostname/IP address and port number configured in its service user's Internet Explorer settings for its proxy settings. If these values are filled in, MOVEit Central knows that a proxy server is in use and will attempt to connect through it.

Proxy Server with "Windows Integrated" NTLM Authentication

MOVEit Central uses the hostname/IP address and port number configured in its service user's Internet Explorer settings for its proxy settings. If these values are filled in, MOVEit Central knows that a proxy server is in use and will attempt to connect through it.

If the proxy server requires "Windows Integrated" NTLM authentication, MOVEit Central will automatically present the proxy server with the same username and password credentials the MOVEit Central service already provides to sign on the Windows server.

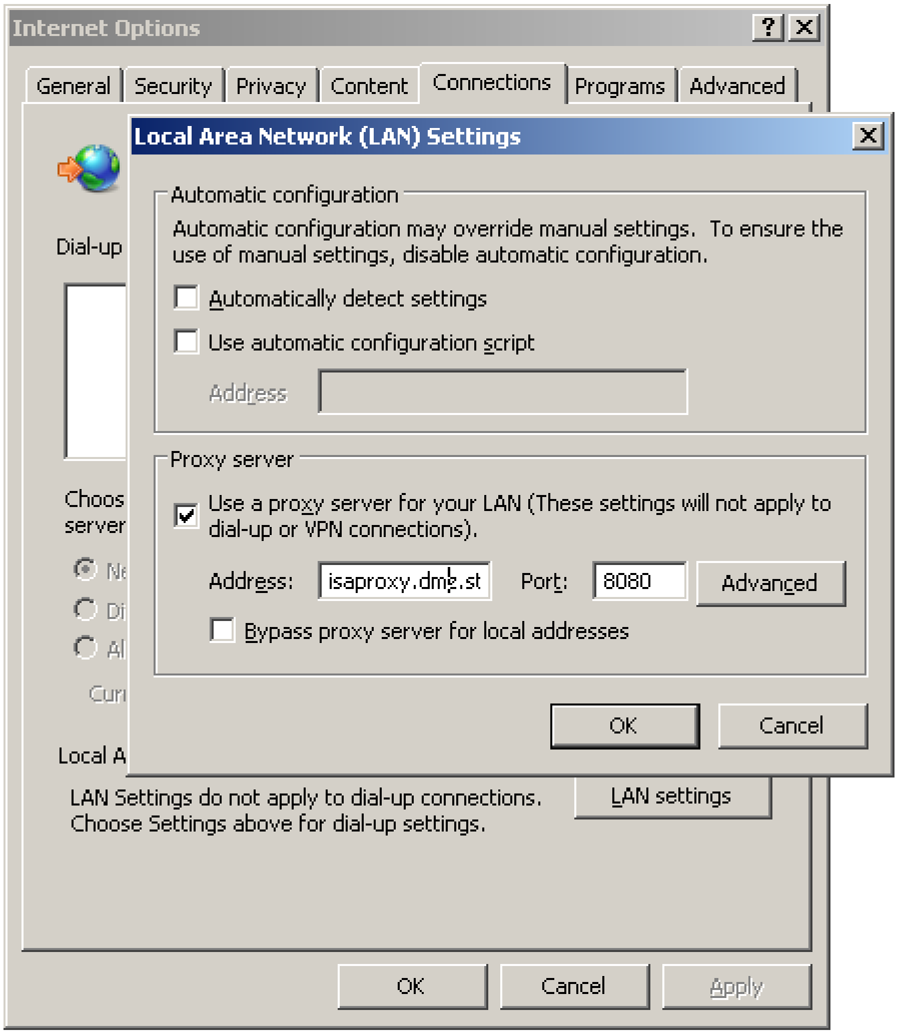
Internet Explorer's Proxy Settings

To access and change MOVEit Central's proxy values, you will likely need to sign on interactively as MOVEit Central's service user and launch Internet Explorer as that user.

To get to Internet Explorer's proxy settings:

1. Open Internet Explorer's multi-tab "Options" panel.
2. Go to the "Connections" tab.

3 Click the "LAN Settings" button.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: isaproxy.dmz.st Port: 8080 Advanced

☐ Bypass proxy server for local addresses

OK Cancel

LAN Settings do not apply to dial-up connections.
Choose Settings above for dial-up settings.

Proxy Server Settings on Non-MOVEit Hosts

When MOVEit Central is not connecting to a MOVEit DMZ server, proxy settings may be configurable items in related host entries. For example, ***AS2 hosts*** (see "***AS2***" on page 379) have their own proxy settings.

Backup

Information required to back up MOVEit Central includes:

- List and description of critical files for disaster recovery
- Steps to use replication for a hot standby server

Disaster Recovery

There are several critical files on MOVEit Central which should be backed up regularly. (Many installations actually use MOVEit Central to copy these files to a remote server for backup to tape or to configure a hot standby on a regular basis.) These files are in the Program Files\MOVEit directory:

- miccfg.xml - MOVEit Central configuration file. Contains a complete list of tasks, hosts, certificates and other information.
- michash.xml - MOVEit Central "hash" file. Contains tamper detection information.
- PGPPath\secring.pgp and PGPPath\pubring.pgp - PGP keyrings. Contains the PGP keys used by MOVEit Central, if the optional PGP capability has been licensed. (These files are found in the PGPPath subdirectory of the MOVEit directory.)

Additionally, the following critical folders should be backed up, contents included. These folders are also in the Program Files\MOVEit directory:

- StateFiles – Contains MOVEit Central "state" files for individual hosts/tasks. These files contain important information such as date/timestamps for folders and files, saved directory listings for synchronization tasks, and more.

Please note that the configuration file and state files are encrypted. In order to make changes to them, you must use MOVEit Central Admin to authenticate to MOVEit Central first.

The Statistics database should also be backed up regularly. This information is stored in a database. If you are using MySQL as your database engine, the database server is usually installed in the "C:\mysql\" or "D:\mysql\" directory. All files in the "..\mysql\data\MICStats" directory should be backed up to protect the statistics database. If you are using Microsoft SQL Server, contact your database administrator for information on backing up the database.

The Microsoft Windows certificate store contains the SSL server certificate used to secure communications with MOVEit Central's clients. If you are using client certificates , S/MIME or AS1/AS2/AS3, the Windows store also contains the related certificates. The client certificates in particular should be backed up. You can create a backup of the client certificates by running a MOVEit Central task that utilizes the "***Certs Backup*** (on page 175)" script. It is less important to back up the MOVEit Central SSL server certificate used to protect MOVEit Central Admin and MOVEit Central API connections because since a new server certificate can be created by doing a fresh install.

Additionally, portions of the registry should be backed up:

- The registry key HKEY_LOCAL_MACHINE\Software\Standard Networks\MOVEitCentral contains values such as:
  - A pointer to the SSL server certificate used to secure communications between MOVEit Central and MOVEit Central Admin/API
  - The ODBC DSN used for the statistics database
  - The temporary cache directory
  - The license key that enables MOVEit Central
- The Windows user database. If you have created Windows users and/or groups for use by MOVEit Central Admin users, the Windows user authentication database should also be backed up. This database is part of the Windows registry.

The registry is typically not changed often, so occasional backups should be sufficient.

Configuration Aging

Each time MOVEit Central successfully saves a copy of its XML-based configuration files (miccfg.xml, etc.), it also ages up to four older versions in a simple grandfather scheme. For example, the "three saves ago" file is titled "miccfg.OL3".

If one of these files gets corrupted (often by an over-zealous anti-virus or backup utility), it is often possible to restore MOVEit Central to a close-to-current state by copying one of the aged copies over the appropriate configuration file. (Contact ***MOVEit support*** (***http://www.ipswitchft.com/company/contactsupport.aspx***) for more information.)

Automated Configuration Replication

To maintain a hot standby Central system, Central itself can be used to replicate its own configuration files to a standby Central server. The process involves setting up a locked-down FTP server on the standby server, and configuring the primary Central to upload its configuration files to the standby server using the FTP server.

NOTE: In order for replication of the configuration files to work properly, both systems must be running the same version of MOVEit Central. Also, there must obviously be a network connection between the two servers.

Please also see the ***MOVEit Central Failover*** (on page 42) documentation.

Setting Up Replication

Follow these steps to set up configuration replication between a production Central (primary) and a hot standby Central (secondary).

1. Install MOVEit Central on the secondary server. Stop the MOVEit Central service and set the start method to MANUAL.
2. Install IIS FTP services on the secondary server. Configure IIS FTP in the following way:

a) Add a new Windows user:

1. Right-click the "My Computer" shortcut on your desktop, and select "Manage" from the right-click pop-up menu.
2. Open the "Configuration \ Local Users and Groups \ Users" tree.
3. Select "New User..." from the right-click pop-up menu.
4. Type in a username of "micftp", any password, UNCHECK the "User must change password at next login" box and CHECK the "user cannot change password" and "password never expires" boxes.
5. Click the "Create" button.

b) Assign permissions to the new Windows user:

1. Browse to the "\Program Files" or "\Program Files (x86)" folder, depending on your system architecture.
2. Select the "MOVEit" folder and select "Properties" from the right-click pop-up menu.
3. Click over to the "Security" tab, click the "Edit…" button, then click the "Add…" button, then select the local computer list of users and select the new "micftp" user. Click the "Add" button and then the "OK" button.
4. Back on the "Security" tab, select the "micftp" user and turn on the FULL CONTROL option.
5. Close this dialog.

c) Install the IIS FTP service if required.

1. If the IIS FTP service is not installed, launch the "Server Manager" dialog by right-clicking "My Computer" and selecting "Manage" from the right-click pop-up menu.
2. Click the "Roles" section. In the resulting display, under the "Role Services" section, click the "Add Role Services" option.
3. Find and select the "FTP Server" option (may be called "FTP Publishing Service" on some machines) from the list of available Role services and click the "Next" button. Click the "Install" button to complete the installation.

d) Configure the IIS FTP service.

1. Open the Internet Information Services manager console.
2. Right click the "Sites" subsection and select the "Add FTP Site…" option from the right-click pop-up menu.
3. Give the FTP site a name and select the "\Program Files\MOVEit" directory as the physical path for the content directory. Click the "Next" button.
4. Enter the desired IP Address, Port, and SSL settings and click the "Next" button
5. Select "Basic" for the authentication type and under "Allow access to:" select "Specified users" and type in "micftp" and select both the "Read" and "Write" options. Click the "Finish" button to complete adding the FTP site.
6. Verify the FTP site is started and test the connection from the other MOVEit Central node.

3 Create a "Certs Backup" task on the primary Central to backup client certificates.

a) Create a new task with a process, destination and schedule (no source).

b) Add a PER-TASK process which runs the "Certs Backup" built-in script. Allow the process to default to the two output filenames CertsPersonal.pfx and CertsOtherPeople.pfx. Specify a password for the output PFX files.

c) Add a destination which copies the file to \Program Files\MOVEit.

d) Add a schedule to run the task periodically every day.

4 Create a "Certs Restore" task on the primary Central to restore client certificates.

a) Create a new task with a source, process and destination (no schedule).

b) Add a source which loads Certs*.pfx from \Program Files\MOVEit.

c) Add a PER-FILE process which runs the "Certs Restore" built-in script. Specify the same password used by the above task.

d) DO NOT schedule the task. This task will not be run under normal circumstances; it will be run manually by operator after a failover, on the newly-promoted primary node.

5 Start broadcasting the Central configuration from the primary server to the secondary server.

a) Add a new FTP host that points to the secondary Central's IIS FTP.

b) Create a new "Backup Central" task:

1. Source: Local File "\Program Files\MOVEit\miccfg.xml"
2. Source: Local File "\Program Files\MOVEit\michash.xml"
3. Source: Local File "\Program Files\MOVEit\CertsPersonal.pfx"
4. Source: Local File "\Program Files\MOVEit\CertsOtherPeople.pfx"
5. Source: All Local Files/Folders under "\Program Files\MOVEit\StateFiles
6. Destination: FTP Host (secondary server); directory /; enable the Overwrite Files option

c) Schedule the task to run every X minutes (5 minutes, 30 minutes?).

d) Test the movement of the configuration files.

e) Create a second "Backup Central 2" task to handle the PGP keyrings.

1. Source: Local Files "\Program Files\MOVEit\PGPPath\*.pgp"
2. Destination: FTP Host (secondary server); directory PGPPath; enable the Overwrite Files option

f) Schedule the task to run every X minutes (5 minutes, 30 minutes?).

g) Test the movement of the PGP keyrings.

6 Test the entire procedure:

a) Stop the MOVEit Central service on the primary server (using MOVEit Central Admin's "***Shut Down Service*** (on page 95)" command if tasks could be running).

b) Start the MOVEit Central service on the secondary server.

c) After you have started the MOVEit Central service on the secondary server, run the "Certs Restore" task on the secondary server.

d) Confirm that the secondary server's configuration is identical to the primary server's configuration.

Failover (Enterprise Only)

MOVEit Central has the capability of running in "failover mode", in which one server automatically stands in for another if the first one fails.

NOTE: This information describes the Legacy Failover system, which eventually will be replaced by the Ipswitch Failover Manager. The Ipswitch Failover Manager will be available in the second half of 2015. Ipswitch will continue to support Legacy Failover installations for MOVEit Central release 8.1. The Legacy Failover system is built into MOVEit Central whereas the new Ipswitch Failover system is installed separately and managed externally. The Legacy Failover system is still in the MOVEit Central documentation. The new Ipswitch Failover system is documented separately.

Overview

This overview describes:

- Requirements
- How failover works
- What failover replicates
- Database replication
- What happens after a failover
- Failover alerts
- Resynchronization
- MOVEit Central Admin considerations
- How to make two Central systems appear as one

Requirements

MOVEit Central Failover requires:

- Two computers running Windows Server 2008 or Windows Server 2012 and using the same type of database server(for supported operating systems and databases, see Requirements). Note: If you need to migrate MOVEit Central to a new server, these Knowledge Base articles can help:
  - ***How do I migrate my MOVEit Central to another server?*** (***http://ipswitchft.force.com/kb/articles/FAQ/How-do-I-migrate-my-MOVEit-Central-to-another-server-1307565958579***)

  - ***How do I get MOVEit Central to work with Microsoft SQL Server?*** (***http://ipswitchft.force.com/kb/articles/FAQ/How-do-I-get-MOVEit-Central-to-work-with-Microsoft-SQL-Server-1307565983335***)
- MOVEit Central. The failover capability is built into all versions of MOVEit Central; however, it must be enabled by a special license.
- A license that enables the failover capability. The same license key can be used on both computers.
- A TCP connection between the two computers that allows access to ports 3472 and 3473. Also, if you use the MySQL database, NetBIOS over TCP must be enabled between the two machines to allow the very useful "Copy Database From" action to occur.

See ***Failover Installation*** (see "***Installation***" on page 47) for how to install failover.

How Failover Works

In a failover configuration, there are two computers running MOVEit Central. At any given time, one of them is the "primary node" and the other is the "secondary node". The primary node is responsible for running all tasks, and for accepting all connections from MOVEit Central Admin users. The secondary node is passive: its only responsibility is to maintain an up-to-date copy of the primary node's settings, and to promote itself to the primary node if the other node fails. The secondary node does not run tasks or allow MOVEit Central Admin to make changes to its configuration.

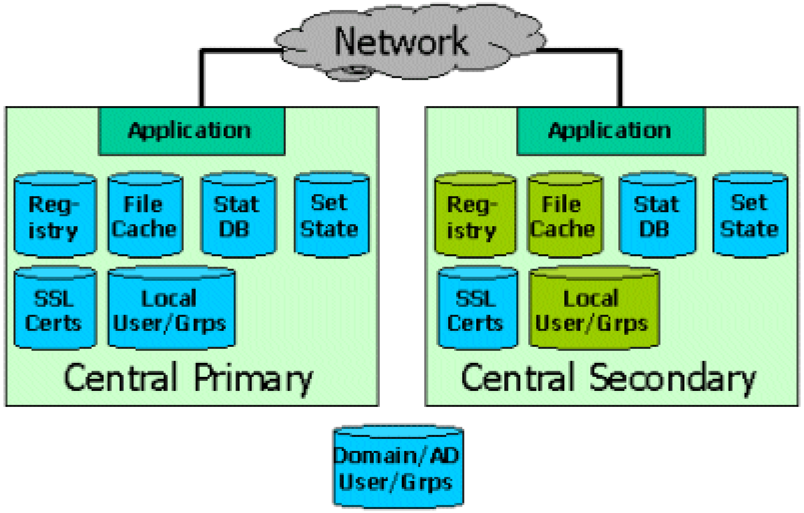
The secondary node connects to the primary node via the same TCP interface that is used by MOVEit Central Admin. It uses this interface to determine the health of the primary node: if it cannot connect for a few minutes, it will assume that the primary is dead and will become the primary itself. The secondary node also uses this TCP interface to replicate changes on-the-fly from the primary node. Also, both nodes use this interface to ensure that there is exactly one primary node at all times. This prevents a situation in which both nodes are primary, and potentially transferring files twice.

Status information on the failover aspects of the system is available on the Failover tab of MOVEit Central Admin.

What Failover Replicates

The following settings are automatically replicated from the primary node to the secondary node:

- The configuration file miccfg.xml, which contains most MOVEit Central settings, including definitions of tasks, hosts, scripts, SSH keys, date lists, and so on.
- The StateFiles folder, which contains various XML configuration files specific to individual hosts/tasks. Each "state" file contains information such as date/timestamps for determining file newness, saved directory listings for synchronization tasks, and more.
- The tamper detection file michash.xml, which contains information used to detect tampering of the database.
- The PGP keyrings, PGPPath\secring.pgp and PGPPath\pubring.pgp. These files contain the PGP keys used by MOVEit Central, if the optional PGP capability has been licensed.
- The MICSTATS database, a database which contains a record of tasks that were run, files that were transferred, and administrator actions that were performed.
- Creation, deletion, and other manipulation of local Windows users and groups used to access MOVEit Central. (Domain users and groups don't need to be replicated as long as both failover nodes are members of the same domain.)
- SSL certificates, in the Microsoft Windows certificate store. This includes:
- Client certificates, with private keys, optionally used to identify MOVEit Central when connecting to secure FTP and MOVEit DMZ servers.
- Server certificates, with private keys, used to secure communications with MOVEit Central Admin.
- Other people's certificates, without private keys, used for sending S/MIME email (a rarely used capability).



The following are **not** replicated:

- The registry key, which can be found in one of the following locations:
  - HKEY_LOCAL_MACHINE\Software\Standard Networks\MOVEitCentral
  - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Standard Networks\MOVEitCentral

  This key contains infrequently-changed settings such as the license key, the directory used for temporary files, and so on. These settings are maintained by the *Configure MOVEit Central* program. If you run this configuration program and make changes on one node, you should make those same changes to the other node.
- The temporary "cache" directory. Any files stored temporarily by a running task are not replicated to the secondary node. The state of any tasks which were running will be lost. Those tasks will be run at the next normally scheduled interval on the secondary node after it takes over.

Database Replication

Note: If you use Microsoft SQL Server, a single database is shared by Node 1 and Node 2 (and generally installed on a third node), so database replication is unnecessary.

If you use the MySQL database, the database is replicated by the primary node sending SQL statements to the secondary node, which runs them itself on its own copy of the database. (Replication features built in to the database are not used.) During the usually short time between the original update of the primary database and the corresponding update of the secondary database, the SQL statements are stored in an encrypted file named MICSQL.blg. This buffering of SQL statements allows the replication to be done at a later time if the secondary node is down.

After a Failover

When the secondary node becomes a primary node, it enables the task scheduler, allowing tasks to be run. It also begins accepting connections from MOVEit Central Admin. Because the other node is dead, the new primary node will initially not be able to replicate changes to it.

When the dead node comes back to life, it checks with the other running node before deciding whether to be the primary or secondary node. Assuming that the other node is still running in primary node, the formerly dead node will become secondary and will catch up on any changes made while it was down.

Failover Alerts

If a MOVEit Central failover occurs, you should expect to see the following message from the following MOVEit Central node sent to the email address configured on the "Errors" tab of the MOVEit Central Configuration utility.

- From the SECONDARY NODE: "I cannot contact the other MOVEit Central node. I was the secondary node, but I'm becoming primary." Upon receipt of this message, an administrator should take whatever steps necessary to restore the MOVEit Central service on the old primary node.

When the MOVEit Central service is restored on the old primary node, the following messages from the following nodes are to be expected:

- From the PRIMARY (old secondary) NODE: "I was finally able to login to the remote MOVEit Central."
- From the SECONDARY (old primary) NODE: "Other node is running as primary. Even though we were primary last time, we'll be secondary now."

Resynchronizing

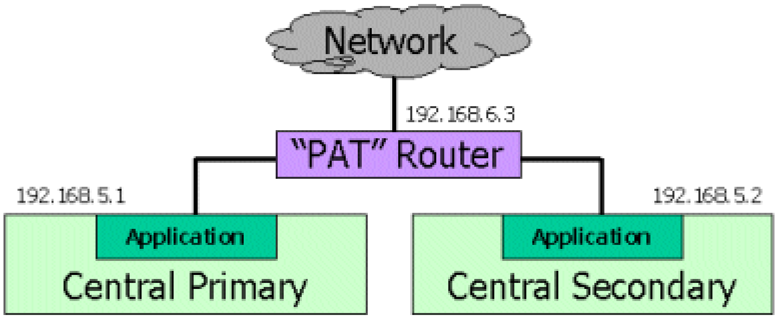
See the "***Failover - Common Procedures - Resynchronization*** (see "***Resynchronization***" on page 53)" documentation for this procedure. Also, see "***Central Service - Failover - Common Procedures - Node Swap*** (see "***Node Swap***" on page 53)" for instructions on switching the primary / secondary roles of two nodes.

MOVEit Central Admin Considerations

The ***Failover Tab*** (on page 51) allows you to monitor failover status. Additionally, if you connect to a failover-enabled node that is not running in primary mode, all tabs other than Log and Failover will be empty.

How to Make Two Central Systems Appear As One

Firewalls and internal servers may only be configured to accept connections from a single IP address. In this case installers may wish to set their network up in such a way that any non-MOVEit Central machine sees the MOVEit Central cluster as a single IP address. The best way to do this is to use a router that does network address translation and overloading of a single address with multiple sessions. (Cisco calls this "PAT" or "NAT overloading").



For example, if Central node #1 has IP address 192.168.5.1 and node #2 has IP address 192.168.5.2, a router can be configured to overload IP address 192.168.6.3. 192.168.6.3 would be the only IP address the rest of the world would know about; neither of the 192.168.5.* addresses would need to be configured in any IP-specific firewall or configuration.

Installation

Initial installation of a failover-capable MOVEit Central node is the same as any MOVEit Central install or upgrade, since the failover capabilities are built into all copies of MOVEit Central 3.2 or later. However, to make a MOVEit Central system failover-capable, some additional steps need to be taken on each of the two nodes after the software have been installed on both nodes.

See also ***Failover Overview*** (on page 42).

Assumptions and Requirements

These instructions assume that:

- The same version of MOVEit Central has been installed on both Node 1 and Node 2. The two nodes need to use the same database type (MySQL or Microsoft SQL Server).

  Note: If you use the MySQL database, MOVEit Central maintains the databases on Node 1 and Node 2. If you use Microsoft SQL Server, a single database is shared by Node 1 and Node 2 (and generally installed on a third node).

- The same tamper detection key has been entered during installation on both nodes. If this is not the case, use RegEdit to manually copy the registry value for HashKey from Node 1 to Node 2. This registry value, which can be found in one of the following locations:
  - HKEY_LOCAL_MACHINE\Software\Standard Networks\MOVEitCentral\HashKey
  - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Standard Networks\MOVEitCentral\HashKey

  (Do not use the "Tamper" tab of the MOVEit Central Config utility.)
- Node 1 is where the current MOVEit Central configuration and database can be found. (If using Microsoft SQL Server, the database can be on a third node.)
- Node 1 can connect to Node 2 (and visa versa) with Windows connectivity.
- Any Windows users and groups used by MOVEit Central are already present on both nodes. (Note: Once failover is installed and running, any changes made to Windows users and groups used by MOVEit Central will automatically be replicated.)
- If using Microsoft SQL Server as the database, make sure the SQL Server Utilities are installed on both nodes. MOVEit Central will use these utilities to access the database on a daily basis to read and write the transaction records. When you install MOVEit Central and select to use a SQL Server database, or if you ***convert a MySQL installation*** (see "***Converter***" on page 458) to SQL Server, MOVEit Central installs the SQL Server Utilities. You can can also download the utilities from Microsoft's web site.

Step-by-Step Instructions

You should not proceed unless the previous assumptions are in fact true.

1. **Nodes 1 and 2**: Using the "Permissions" dialog in MOVEit Central Admin, create a Windows user (either a local or domain user) named "centralfailover" into the "MOVEit Admin" Windows group on both nodes. Use the same password on both nodes.

   The "centralfailover" user will be used by the other node for replication. You may use an alternate username, but make sure it is the same username on both machines.
2. **Nodes 1 and 2**: Stop the MOVEit Central service on both nodes. Use MOVEit Central Admin's "***Shut Down Service*** (on page 95)" command on Node 1 if tasks could be running. You may issue the command "net stop moveitcentral" or use the Windows control panel to stop the service on Node 2.
3. **Nodes 1 and 2**: If the ***MOVEit Central Config*** (see "***Central Config Utility***" on page 17) program is not already running, start it via the shortcut located in "Start | Programs | MOVEit Central" on both nodes.
4. **Nodes 1 and 2**: Enter the same failover-capable license key in the ***License tab*** (on page 20) on both nodes.
5. Nodes 1 and 2: Configure the email addresses of an administrator in the ***Errors tab*** (on page 23) on both nodes. If you do not enter these values, you will not be emailed when serious errors or failover events are encountered.

6 **Node 1 ONLY**: Go to the ***Failover tab*** (on page 24) and configure the following information:

- This Node - **Startup Role**: Primary
- This Node - **Node Number**: 1
- This Node - **Nodes to ping**: (*Optional: usually the IP address of trusted router, leave blank if unsure*)
- Other Node - **Hostname or IP**: [IP Address of Node #2]
- Other Node - **MOVEit Admin user**: centralfailover
- Other Node - **Password**: [centralfailover's Password]
- Click **Apply**.

7 **Node 2 ONLY**: Go to the ***Failover tab*** (on page 24) and configure the following information:

- This Node - **Startup Role**: Secondary
- This Node - **Node Number**: 2
- This Node - **Nodes to ping**: (*Optional: usually the IP address of trusted router, leave blank if unsure*)
- Other Node - **Hostname or IP**: [IP Address of Node #1]
- Other Node - **MOVEit Admin user**: centralfailover
- Other Node - **Password**: [centralfailover's Password]
- Click **Apply**.

8 **Nodes 1 and 2**: If you are using MySQL as your database, click the "Clear SQL Rep..." button on the ***Failover tab*** (on page 24) on both nodes.

Note: The first time that you click "Clear SQL Rep...", you may see error messages that state that there is nothing to replicate. You can ignore these errors.

9 **Node 2 ONLY**: If you are using MySQL as your database: On node 2 only, click the "Copy Database" button on the ***Failover tab*** (on page 24) to do a one-time replication of the database from the primary node to the secondary node. This may take several minutes if your existing database is large.

You may also need to change the "Copy from" value on the "Copy statistics database" dialog which will appear. If you encounter "'From' directory does not exist or cannot be accessed" errors, use the following command-line sequence to confirm this MOVEit Central can connect to the other MOVEit Central via Windows File Sharing, that the "centralfailover" user may be authenticated to the other MOVEit Central, and that "centralfailover" enjoys read access to the file share listed in the "Copy from" field.

```
C:\>net use H: \\192.168.3.172\micstats /user:centralfailover
The password or user name is invalid for \\192.168.3.172\micstats.
Enter the password for 'centralfailover' to connect to
'192.168.3.172': *******
The command completed successfully.
C:\>H:
H:\>dir stats.myi
09/22/2005 02:28 AM           53,248 stats.MYI
H:\>copy stats.myi c:\
1 file(s) copied.
```

10 **Node 1 and 2**: If you are using Microsoft SQL Server as your database: On both nodes, make sure that you set the registry entry DWORD named SuppressDBRep to a value of 1. This registry entry is found in one of these locations (you may need to add the registry entry):

- HKEY_LOCAL_MACHINE\Software\Standard Networks\MOVEitCentral\Resil
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Standard Networks\MOVEitCentral\Resil

You do not want the SQL Server database to be replicated because Node 1 and Node 2 share the same SQL Server database.

11 **Node 1 ONLY**: Start the MOVEit Central service. (From a command line, you may issue the command "net start moveitcentral".)

12 **Node 2 ONLY**: Start the MOVEit Central service. (From a command line, you may issue the command "net start moveitcentral".)

13 **Node 1 ONLY**: Open MOVEit Central Admin and connect to "localhost". Within about three minutes, ***MOVEit Central Admin's Failover tab*** (on page 51) should show that Node 1 is the primary MOVEit Central node and Node 2 is the secondary MOVEit Central node.

14 **Node 1 ONLY**: Use MOVEit Central Admin's Command | Reset Tamper Detection menu item to reset tamper detection for the failover system.

Securing Connections Between Nodes

It is also recommended that, on both nodes, you assign an SSL certificate and choose "Require encryption for remote control" in the MOVEit Central configuration program's ***General tab*** (on page 18), if you have not already done so. This will allow MOVEit Central to use SSL-encrypted TCP connections to replicate settings.

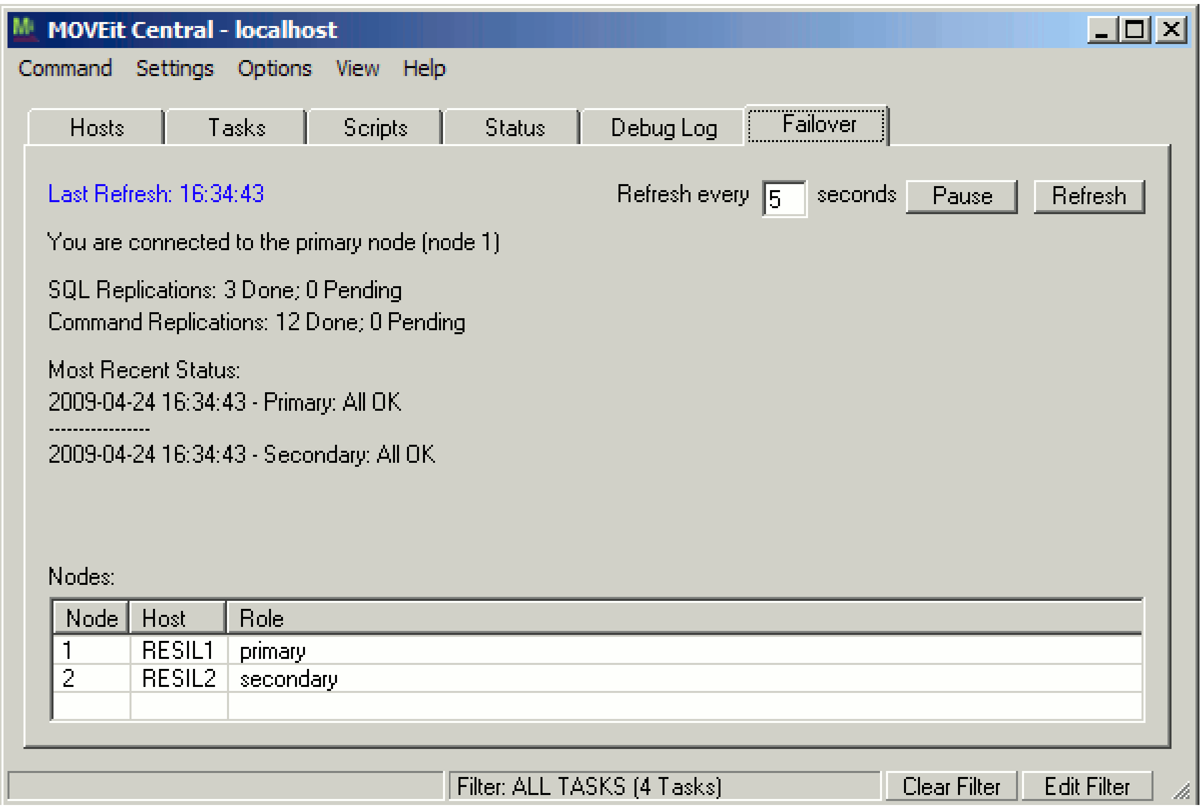
Upgrades

See the "***Failover - Common Procedures - Software Upgrade*** (see "***Software Upgrade***" on page 52)" documentation for information about upgrading MOVEit Central when deployed in a Failover configuration.

Admin Failover Tab

MOVEit Central Admin's Failover tab is used to monitor the failover status of MOVEit Central. The Failover tab appears only when the failover feature is enabled. (MOVEit Central must be licensed for failover, and its node number must be greater than 0.)

(See ***MOVEit Central Config - Failover Tab documentation*** (on page 24) for information about the "Failover" tab in the MOVEit Central Config utility.)



Last Refresh: 16:34:43

Refresh every 5 seconds

You are connected to the primary node (node 1)

SQL Replications: 3 Done; 0 Pending
Command Replications: 12 Done; 0 Pending

Most Recent Status:
2009-04-24 16:34:43 - Primary: All OK

2009-04-24 16:34:43 - Secondary: All OK

Nodes:

Node	Host	Role
1	RESIL1	primary
2	RESIL2	secondary

Filter: ALL TASKS (4 Tasks)

If you are connected to a primary node, the following information is displayed:

- The node number to which you are connected (1 or 2).
- The number of SQL statements that have successfully been replicated to the secondary node since MOVEit Central has started.
- The number of pending SQL statements; that is, the number that are waiting to be replicated.

  If the number of pending statements is greater than zero, and the number of statements that have been replicated hasn't changed in 20 seconds, there is probably a problem.
- The failover status of MOVEit Central, and its timestamp.
- A list of the nodes, with these items for each node:
  - The node number
  - The hostname

- That node's current role

If the node you are connected to is not a primary, only the failover status is shown.

If the node changes roles, then the next time you are on the Failover tab, you will be asked to exit MOVEit Central Admin and reconnect. This will allow MOVEit Central Admin to reset its displays to correctly reflect the new role of the node.

See also ***Failover Overview*** (on page 42).

Common Procedures

You may perform some common procedures, such as:

- Backups
- Software upgrades
- Node swaps
- Resynchronization

Backup

Use normal backup procedures to back up your MOVEit Central Failover primary node. Backup files created through these procedures can be restored on either standalone or failover MOVEit Central systems. See the "***Central Service - Backup*** (on page 38)" documentation for more details about recommended backup procedures.

Software Upgrade

Before upgrading make sure both nodes have been ***synchronized*** (see "***Resynchronization***" on page 53). Then stop the MOVEit Central service on both nodes (using MOVEit Central Admin's "***Shut Down Service*** (on page 95)" command on the primary node). Once the services have been stopped on both nodes run the upgrade on the primary node first and make sure the MOVEit Central service is started on this node before upgrading the secondary node. (By upgrading the primary node first no unnecessary failover will occur.)

After the upgrade, you may receive an email from one or both MOVEit Centrals reporting that they could not contact the other Central node. This is a result of having the service running on one node and not the other during the upgrade process. This message can safely be ignored.

Windows Updates

Windows updates can normally be applied without shutting the MOVEit Central services down. However, if a reboot is required by a Windows update package, plan to take down the MOVEit Central service on the secondary node, then boot the primary node and let it come back up before rebooting the secondary node. (Make sure the secondary node also brings its MOVEit Central service up after its reboot.)

Node Swap

You may wish to switch the roles of a primary and secondary node back after a failover. For instance, if you have computers named CENTRALA and CENTRALB, you may find it convenient to have the CENTRALA computer normally be the primary node. Thus, after a failover from CENTRALA to CENTRALB, you may wish to force CENTRALA to be the primary node again.

To accomplish this:

1. Ensure that the new primary (CENTRALB in this example) actually does have the current task configuration.
2. Run briefly with both nodes up in the reversed role scenario, to allow any changed settings to replicate from recently-promoted CENTRALB to the recently-demoted CENTRALA.

   Important: Both nodes must be running to allow MOVEit Central to sync the state file.
3. Follow the instructions for ***resyncing the database*** (see "***Resynchronization***" on page 53), but do not start the MOVEit Central services. (Remember to always invoke the copy function from the current secondary node.)
4. Use the MOVEit Central Configuration utility to set the appropriate values for "Startup Role" on each of the two nodes. (One will be set to "Primary" and the other will be set to "Secondary".)
5. Start the new primary MOVEit Central, followed by the new secondary.

Resynchronization

You may need to resynchronize the two nodes under certain conditions. For instance, after a failover, if the former secondary has become primary, you may wish to force the original primary to be primary again. Follow these instructions to resynchronize the nodes:

1. Stop MOVEit Central service on the current secondary node.
2. Stop MOVEit Central service on the current primary node (using MOVEit Central Admin's "***Shut Down Service*** (on page 95)" command if tasks could be running).
3. Stop MySQL service on both nodes.
4. On the desired new primary node, run the ***MOVEit Central configuration utility*** (on page 24) and:
   a) Set the startup role to primary.
   b) Choose the "Clear Admin Rep" button.
   c) Choose the "Clear SQL Rep" button.
5. On the desired new secondary node, run the MOVEit Central configuration utility and:
   a) Set the startup role to secondary.
   b) Choose the "Clear Admin Rep" button.
   c) Choose the "Clear SQL Rep" button.

6 Determine which of the two nodes has the most current database. Generally, this is the last machine to have served as the primary node. Go to the OTHER node (the one with the less current database) and choose the "Copy Database" button to request a complete copy of the most current database. Wait for the copy procedure to complete.

7 Start MySQL service on both nodes.

8 Start MOVEit Central service on the new primary node.

9 Start MOVEit Central service on the new secondary node.

FTP Failover

This section discusses some additional failover-related configuration that can be done on a MOVEit Central server that is also running an FTP server.

Overview

Some sites run an FTP server on the same computer as MOVEit Central. Remote servers or mainframes send files to MOVEit Central via FTP, and MOVEit Central tasks process the files. (Typically, for better performance and reliability, the local FTP directory is configured as a filesystem source rather than an FTP source.)

In a failover scenario, this presents two types of problems:

- If MOVEit Central server A fails after some files have been sent to MOVEit Central but before the related task runs, those files will not be transferred when the secondary B takes over, because they are on the failed computer. (Admittedly, if MOVEit Central has been set to use filesystem notifications, this time window will be very short.) Furthermore, if the new primary B fails days, weeks, or months later, the old, unprocessed files on server A may be processed when it becomes the primary. Depending on how tasks are configured, this may cause obsolete files to be sent, confusing the recipient.
- Remote processes which have been programmed to send files to FTP server A may not be smart enough to send them to FTP server B if A is down.

These problems can be addressed with features built into Microsoft Windows which allow you to create a single system image from two FTP servers:

- Distributed File System can be used to create a single storage area into which files FTPed to either MOVEit Central computer will be stored. See ***FTP Replication - DFS*** (see "***With DFS***" on page 55).
- Network Load Balancing can be used to assign a single IP address which can be used by remote computers to access either FTP server as if the two were a single computer. See ***FTP Replication - NLB*** (see "***With NLB***" on page 66).

See also ***Failover Overview*** (on page 42).

With DFS

Microsoft Distributed File System (DFS) can be used to essentially create a single storage area into which files FTPed to either MOVEit Central computer will be stored. Files received by the FTP server on either computer will be automatically copied to the corresponding directory on the other computer. The copying is done quickly, so the file appears on both computers nearly simultaneously (depending on the size of the file and other factors).

DFS is available on Windows Server. You must be a member of a domain to use DFS.

Overview

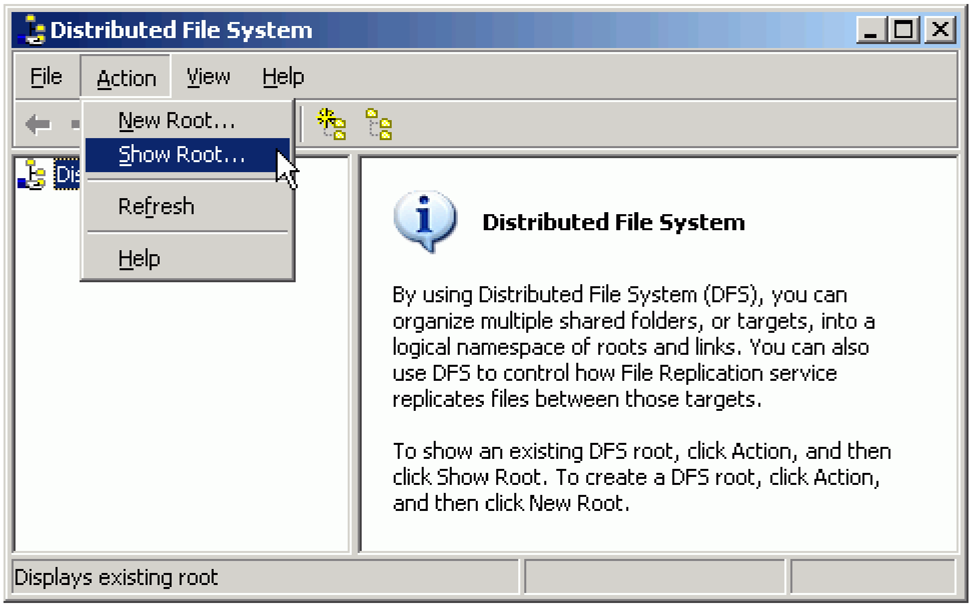
In brief, to use DFS, you take the following steps:

- Create a "DFS root" on your domain if none already exists
- On each FTP server, create a network share for the root FTP directory on that computer
- For each of these shares, add a link to that share to the DFS root
- Use the Replication Wizard to set up replication between these two links

Details

1 Check to see whether a DFS root already exists on your domain:

a) Run Administrative Tools | Distributed File System and choose Action | Show Root...

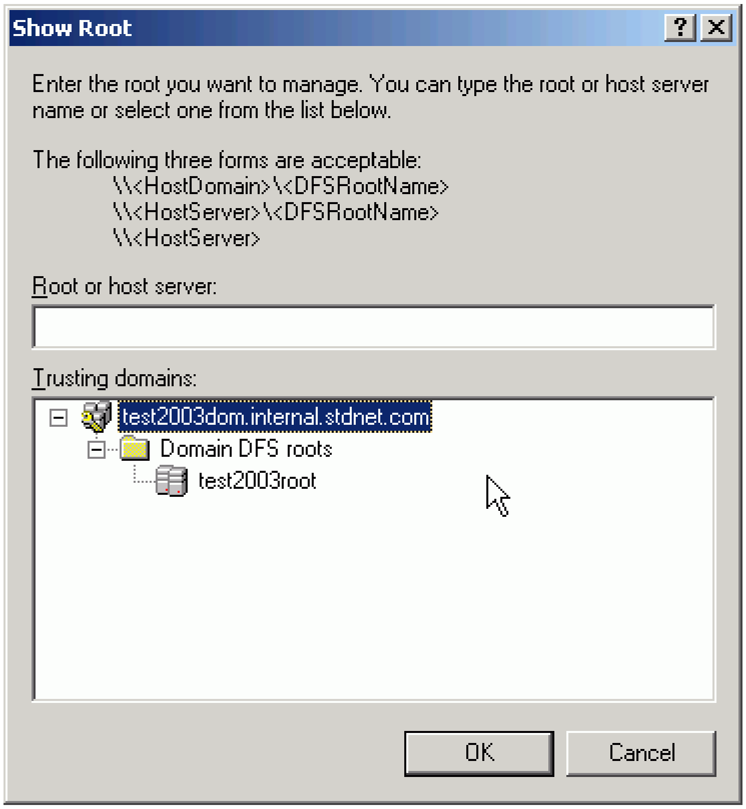


Distributed File System

By using Distributed File System (DFS), you can organize multiple shared folders, or targets, into a logical namespace of roots and links. You can also use DFS to control how File Replication service replicates files between those targets.

To show an existing DFS root, click Action, and then click Show Root. To create a DFS root, click Action, and then click New Root.

b) Expand "Domain DFS roots" and look to see if there are any entries beneath it. In this example, there is already a root named test2003root.



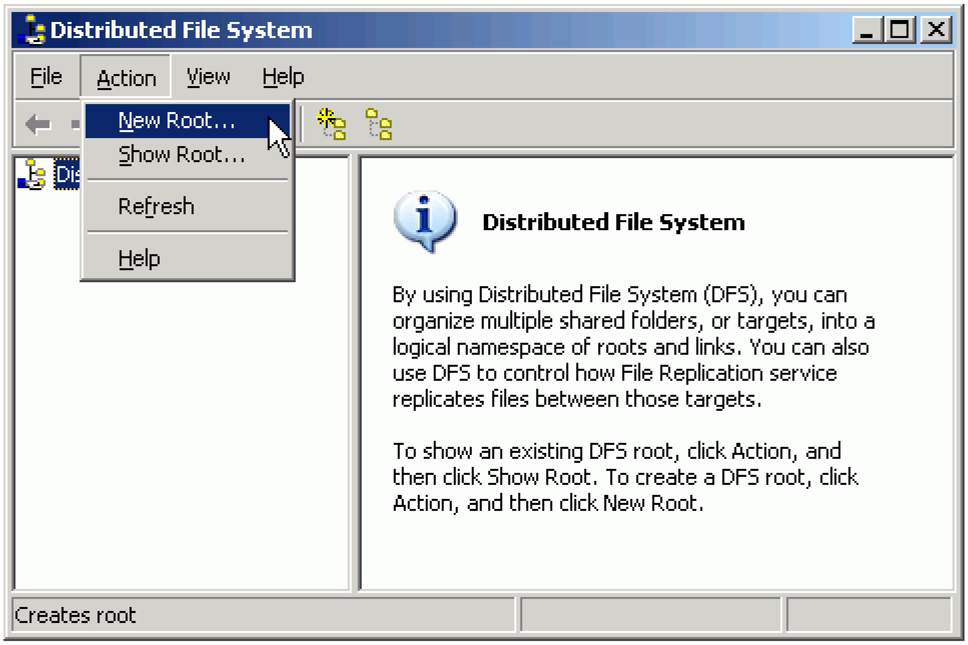
Enter the root you want to manage. You can type the root or host server name or select one from the list below.

The following three forms are acceptable:
\\<HostDomain>\<DFSRootName>
\\<HostServer>\<DFSRootName>
\\<HostServer>

Trusting domains:
- test2003dom.internal.stdnet.com
  - Domain DFS roots
    - test2003root

2 If there is not already a root, create one:

a) Choose Action | New Root...

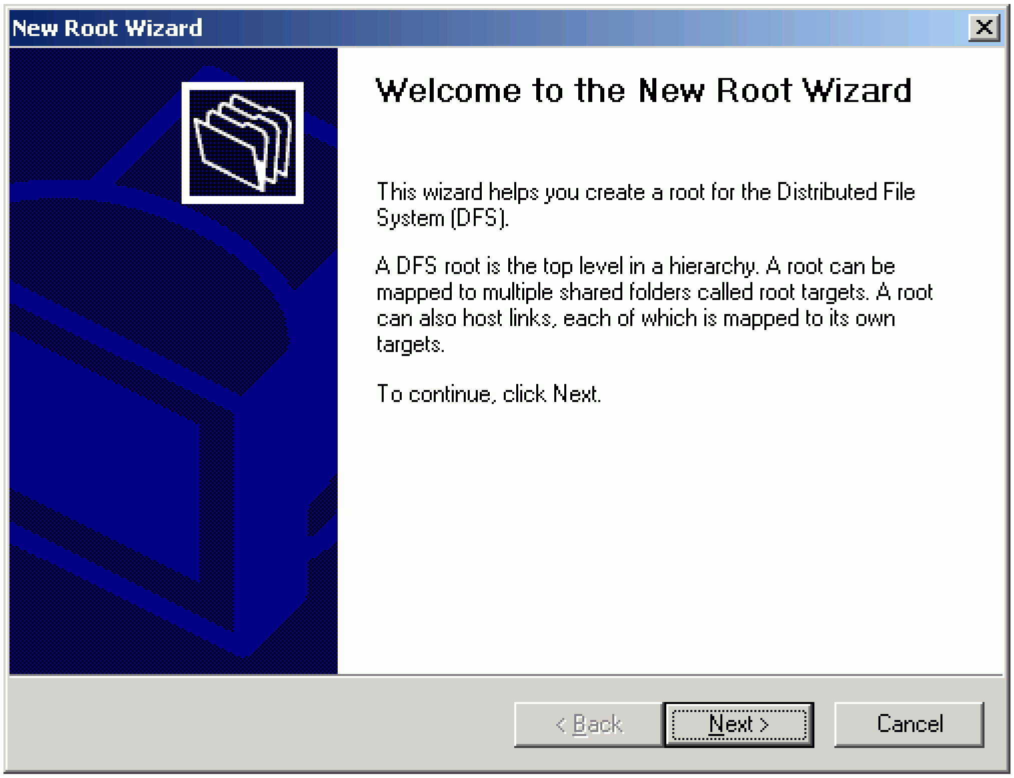


Distributed File System

By using Distributed File System (DFS), you can organize multiple shared folders, or targets, into a logical namespace of roots and links. You can also use DFS to control how File Replication service replicates files between those targets.

To show an existing DFS root, click Action, and then click Show Root. To create a DFS root, click Action, and then click New Root.

b) In the New Root Wizard, choose Next.



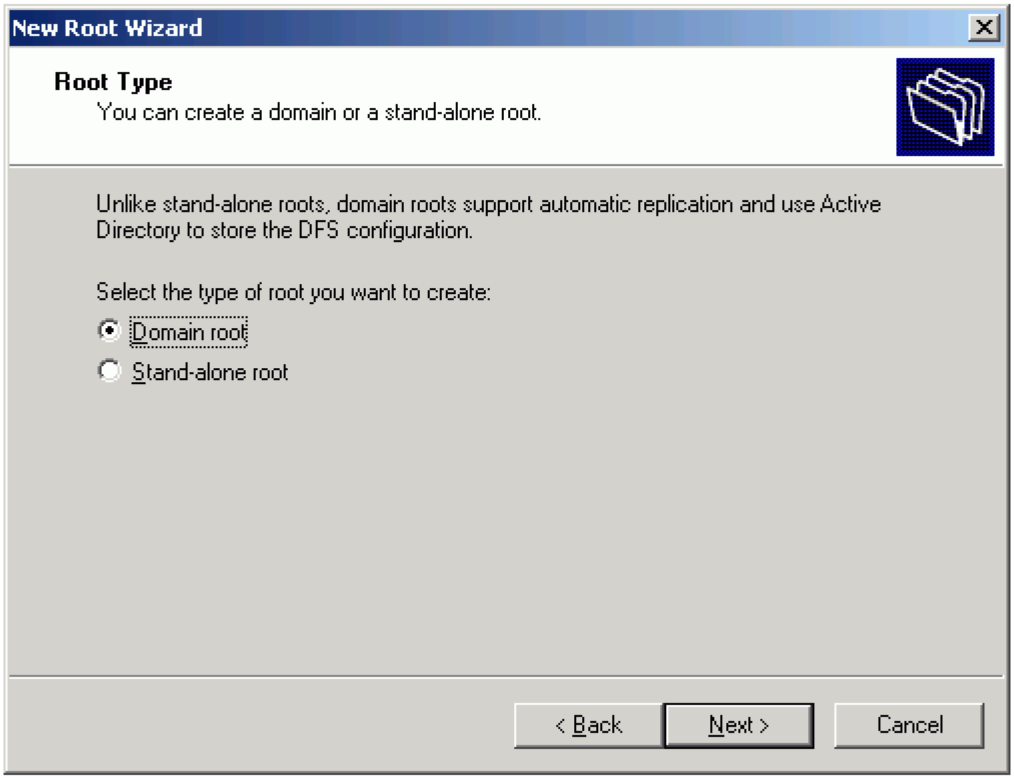
Welcome to the New Root Wizard

This wizard helps you create a root for the Distributed File System (DFS).

A DFS root is the top level in a hierarchy. A root can be mapped to multiple shared folders called root targets. A root can also host links, each of which is mapped to its own targets.

To continue, click Next.

c) For Root Type, choose "Domain root" and then Next. Replication requires the root to be of type Domain.



New Root Wizard

Root Type

You can create a domain or a stand-alone root.

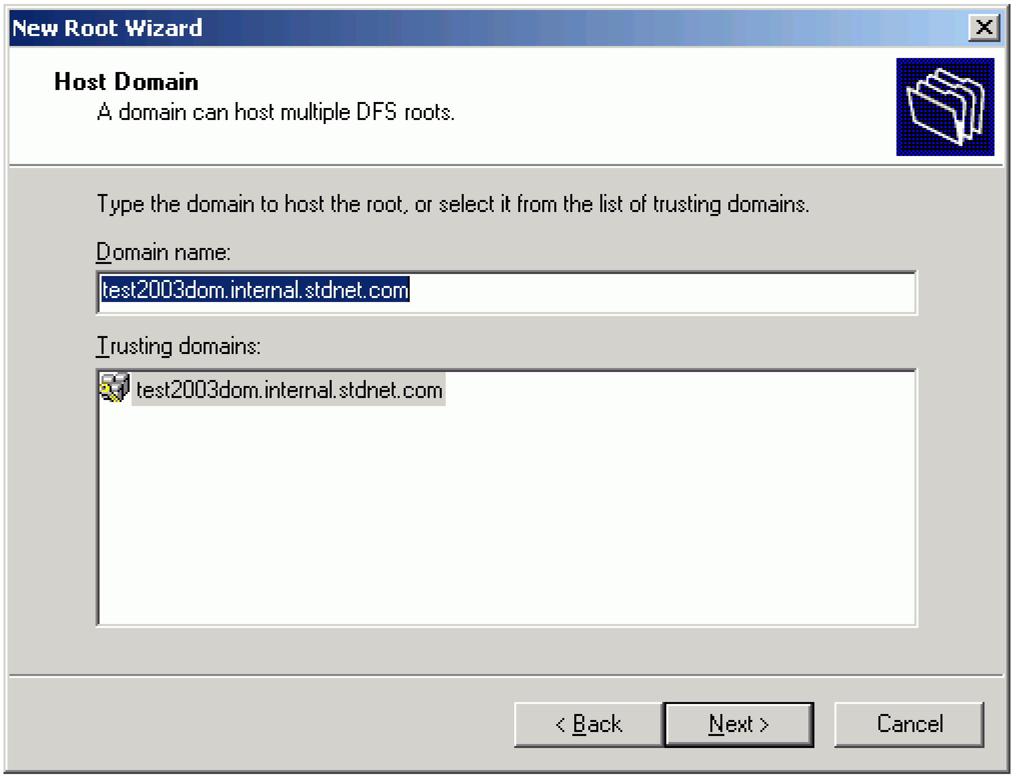
Unlike stand-alone roots, domain roots support automatic replication and use Active Directory to store the DFS configuration.

Select the type of root you want to create:

● Domain root

○ Stand-alone root

d) For Domain, choose the domain and then Next.



Host Domain

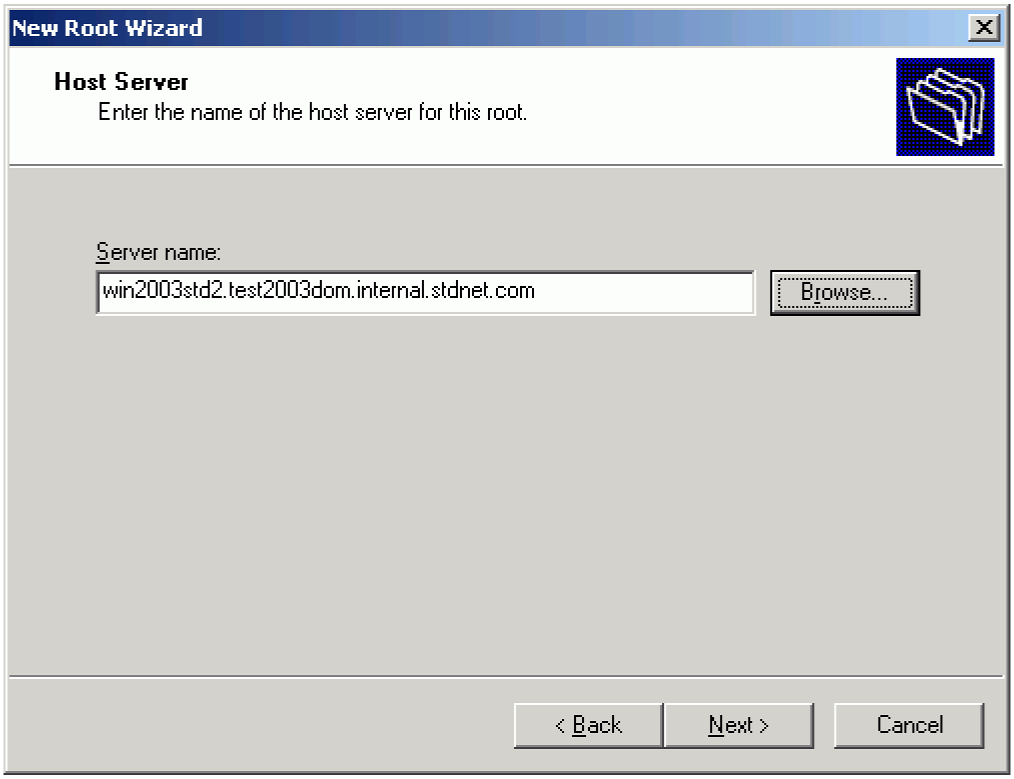
A domain can host multiple DFS roots.

Type the domain to host the root, or select it from the list of trusting domains.

Domain name: test2003dom.internal.stdnet.com

Trusting domains: test2003dom.internal.stdnet.com

e) For Host Server, choose Browse to get the Find Computers dialog and choose the name of a MOVEit Central server from the list. (It does not matter which one you choose.) Then choose OK to dismiss the dialog, and choose Next in the Wizard.



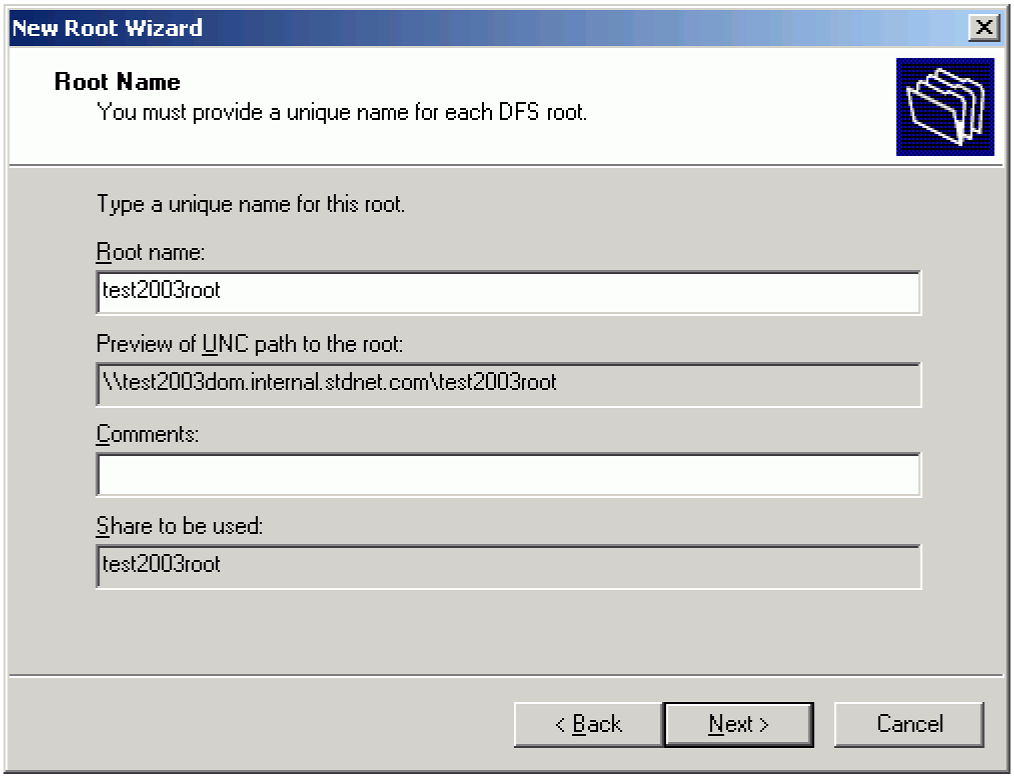
New Root Wizard

Host Server

Enter the name of the host server for this root.

Server name: win2003std2.test2003dom.internal.stdnet.com

f) For Root Name, type in a name of your choosing and choose Next.



Root Name

You must provide a unique name for each DFS root.

Type a unique name for this root.

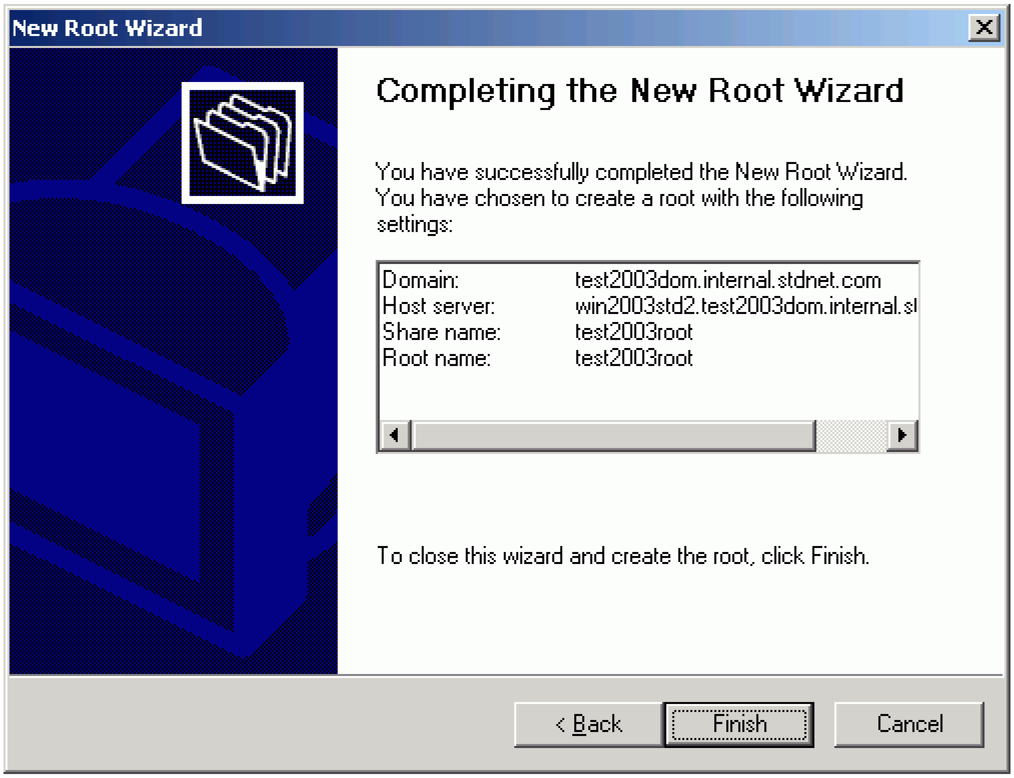
Root name: test2003root

Preview of UNC path to the root: \\test2003dom.internal.stdnet.com\test2003root

Comments:

Share to be used: test2003root

g) Choose Finish at the final dialog.



Completing the New Root Wizard

You have successfully completed the New Root Wizard. You have chosen to create a root with the following settings:

```
Domain:         test2003dom.internal.stdnet.com
Host server:    win2003std2.test2003dom.internal.st
Share name:     test2003root
Root name:      test2003root
```

To close this wizard and create the root, click Finish.

3 Create filesystem shares on each of the MOVEit Central computers, each pointing to the local root FTP directory. For instance, if your two servers are named win2003srv1 and win2003srv2, and each has its IIS FTP root at c:\inetpub\ftproot, then you might create the shares:

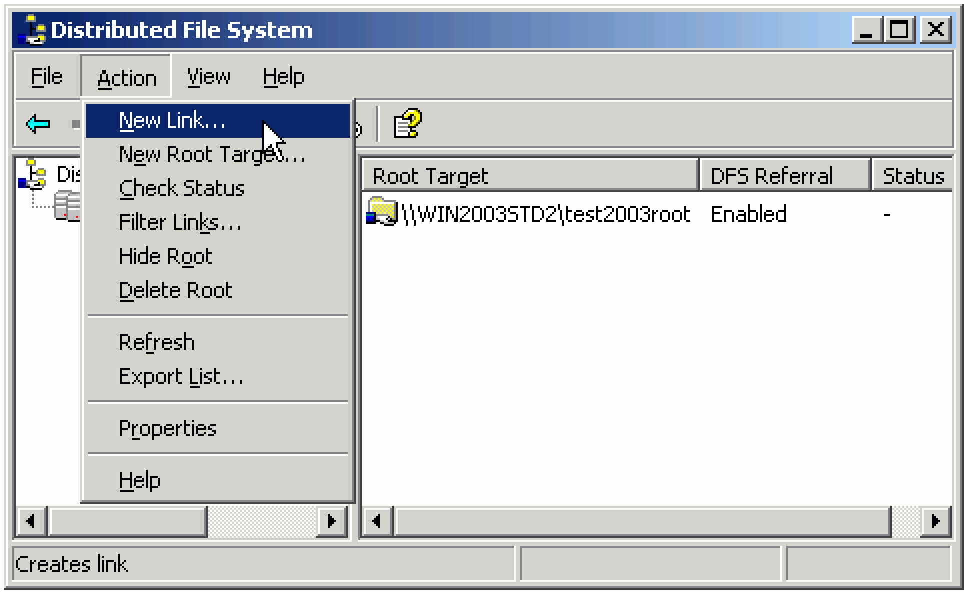
Sharename	**Local directory pointed to**
\\win2003srv1\ftpshare	c:\inetpub\ftproot
\\win2003srv2\ftpshare	c:\inetpub\ftproot

4 On one of the servers (it doesn't matter which), create a link to the local ftpshare:

a) Run Administrative Tools | Distributed File System if it is not already running.

b) Select the DFS root you created. If the root is not visible in the tree, use Action | Show Root... as described above.

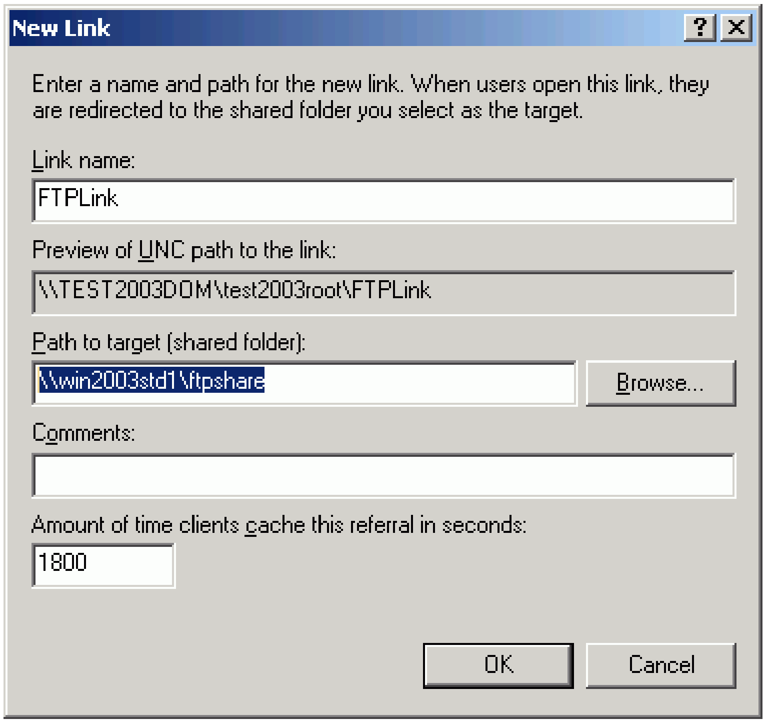
c) Use Action | New Link... to open the New Link dialog.



Root Target	DFS Referral	Status
\\WIN2003STD2\test2003root	Enabled	-

Creates link

d) In the New Link dialog, type a link name of your choice (for example, FTPLink) and type the full path to the share (for example, \\win2003std1\ftpshare) and choose OK.



Enter a name and path for the new link. When users open this link, they are redirected to the shared folder you select as the target.

Link name: FTPLink

Preview of UNC path to the link: \\TEST2003DOM\test2003root\FTPLink

Path to target (shared folder): \\win2003std1\ftpshare

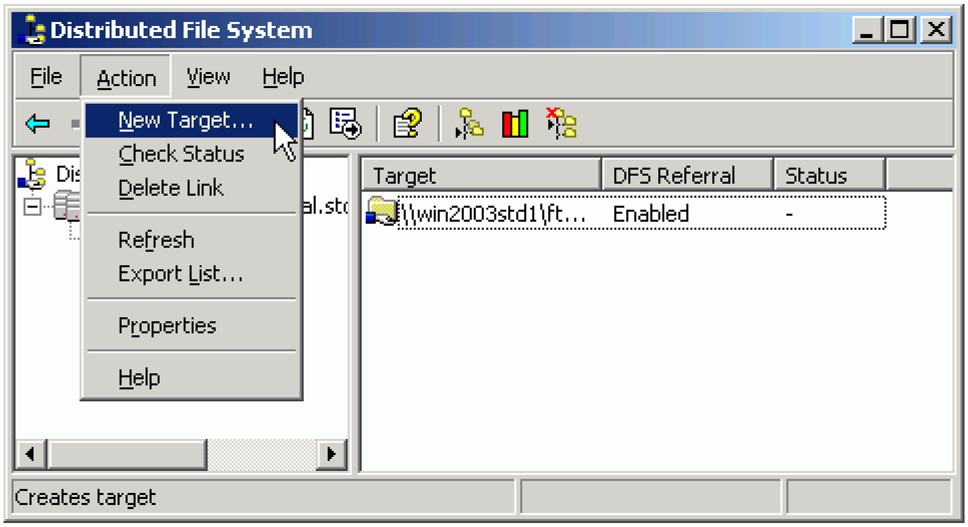
Comments:

Amount of time clients cache this referral in seconds: 1800

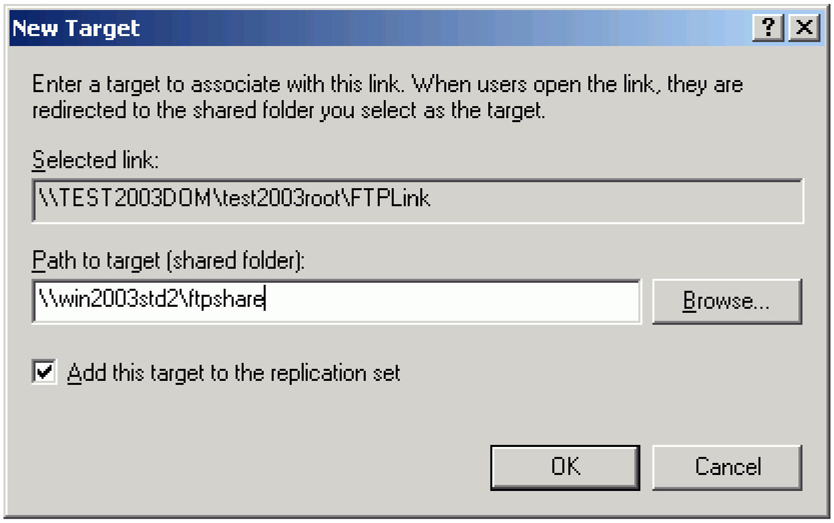
5 Create a second target to that link and enable replication:

a) On either server (but it's more convenient to use the server you just used above) run Administrative Tools | Distributed File System if it is not already running.

b) Select the newly-created link and choose Action | New Target...



c) In the New Target dialog, enter the name of the other FTP share created above. Leave the "Add this target to the replication set" box checked.


New Target

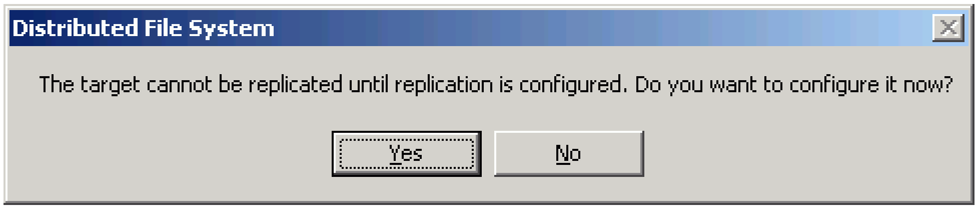
Enter a target to associate with this link. When users open the link, they are redirected to the shared folder you select as the target.

Selected link: \\TEST2003DOM\test2003root\FTPLink

Path to target (shared folder): \\win2003std2\ftpshare

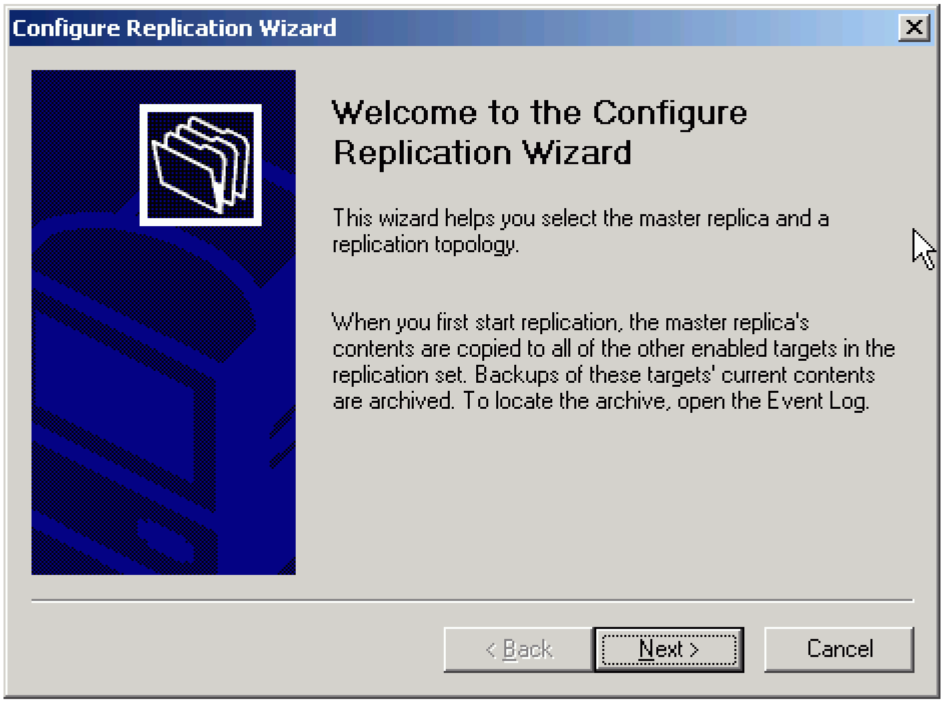
☑ Add this target to the replication set

d) You will be prompted "The target cannot be replicated until replication is configured. Do you want to configure it now?" Choose Yes.


Distributed File System

The target cannot be replicated until replication is configured. Do you want to configure it now?

e) At the Configure Replication Wizard welcome page, choose Next.



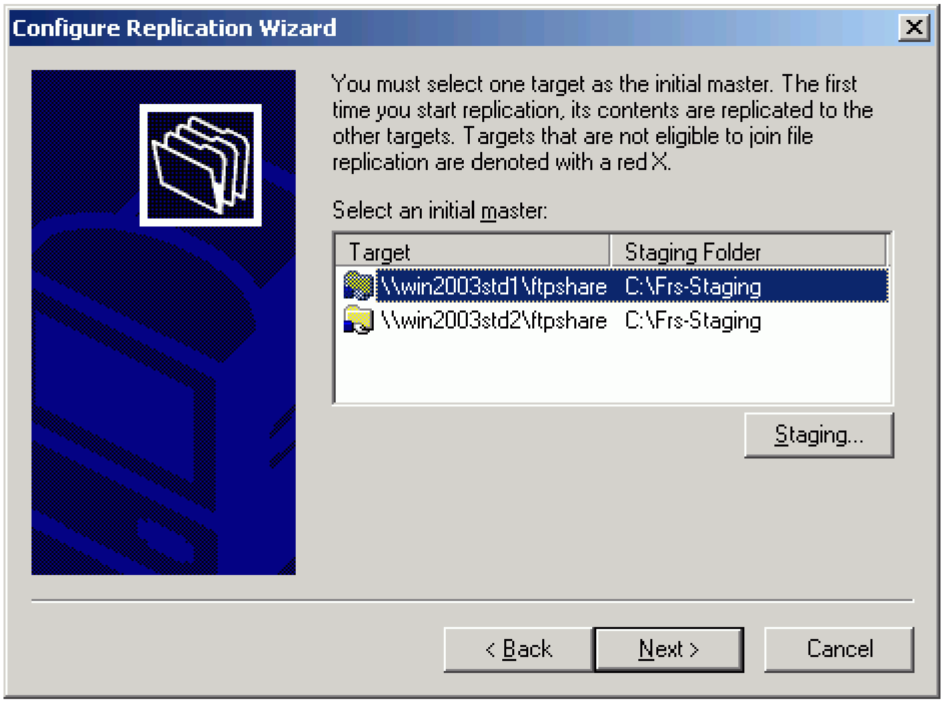
Configure Replication Wizard

Welcome to the Configure Replication Wizard

This wizard helps you select the master replica and a replication topology.

When you first start replication, the master replica's contents are copied to all of the other enabled targets in the replication set. Backups of these targets' current contents are archived. To locate the archive, open the Event Log.

f) You will be asked to choose the initial master. If neither FTP server has received any files yet, it doesn't matter which you choose. Otherwise, choose the FTP server which is more current. Then choose Next.



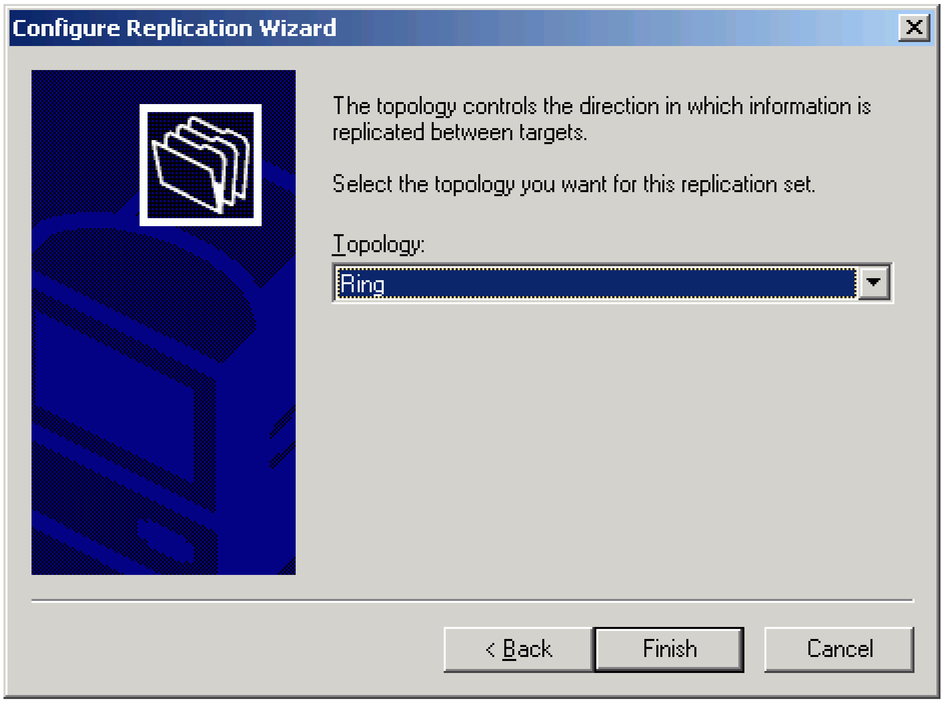
Configure Replication Wizard

You must select one target as the initial master. The first time you start replication, its contents are replicated to the other targets. Targets that are not eligible to join file replication are denoted with a red X.

Select an initial master:

Target	Staging Folder
\\win2003std1\ftpshare	C:\Frs-Staging
\\win2003std2\ftpshare	C:\Frs-Staging

g) For the replication topology, accept the default of Ring, and choose Finish.



The topology controls the direction in which information is replicated between targets.

Select the topology you want for this replication set.

Topology:
Ring

6 Test file replication by sending a short file to one of the FTP servers. It should appear on the other server within seconds. You may have to stop and start the File Replication service on both computers to enable file replication.

After an outage, Windows may take a substantial amount of time--sometimes more than 10 minutes--to re-enable file replication.

You will probably also want to set up ***Network Load Balancing*** (see "***With NLB***" on page 66). See also ***Failover Overview*** (on page 42).

With NLB

Microsoft Network Load Balancing (NLB) can be used to share a single IP address between two servers. This allows incoming FTP sessions to connect to either of the two MOVEit Central computers. If both are running, NLB assigns the incoming session to one of the computers, typically the one with higher priority. If one computer is down, NLB assigns the incoming session to the working computer.

Overview

NLB does not allow outbound connections from both computers to use the same IP address. Thus, you should ensure that either:

- Firewalls protecting hosts accessed by MOVEit Central have rules allow incoming connections from either computer running MOVEit Central

  – or –

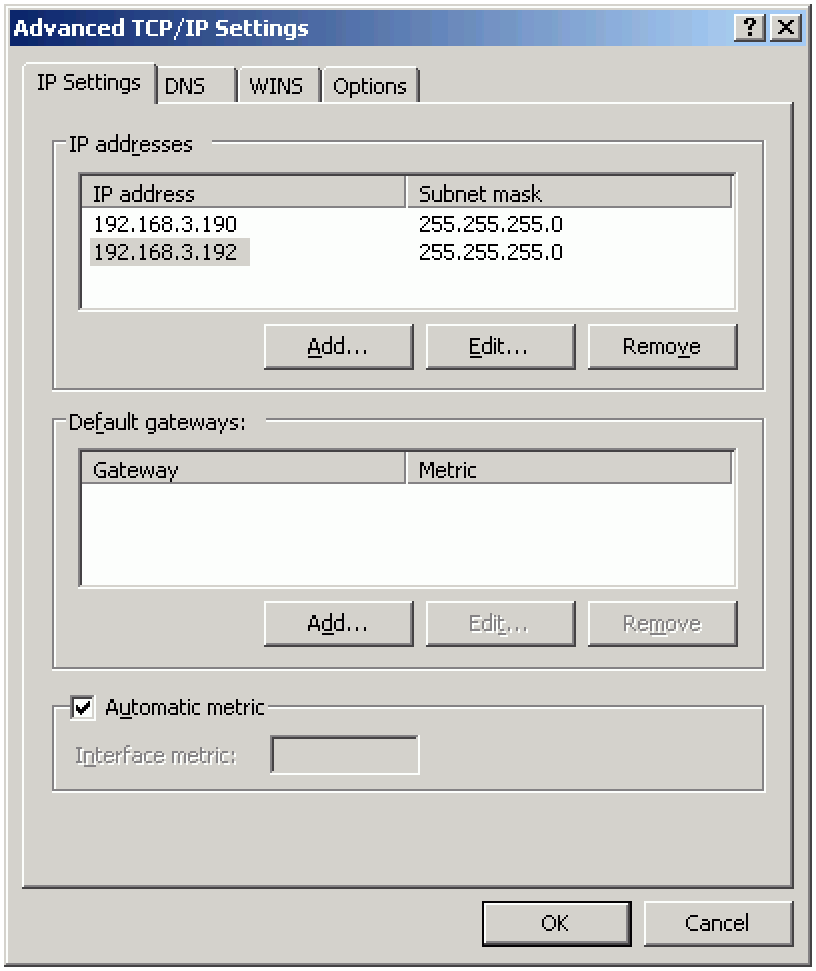
- The firewall protecting MOVEit Central uses Network Address Translation to make both computers look as if they have the same IP address

NLB is available on all editions of Windows 2008 and 2012.

Details

To use NLB, you take the following steps:

1. Decide on an IP address by which the cluster will be known. This should be different from the IP addresses of the individual MOVEit Central computers in the cluster.
2. On one MOVEit Central node, configure Windows Network Load Balancing as follows:
   a) Use Network Connections | (connection name) | Properties | Internet Protocol (TCP/IP) | Properties | Advanced | Add... to add the cluster IP address to the list of addresses for your network adapter. If you have multiple adapters, use the one which will face the systems which you will be accessing.



Advanced TCP/IP Settings

IP addresses

IP address	Subnet mask
192.168.3.190	255.255.255.0
192.168.3.192	255.255.255.0

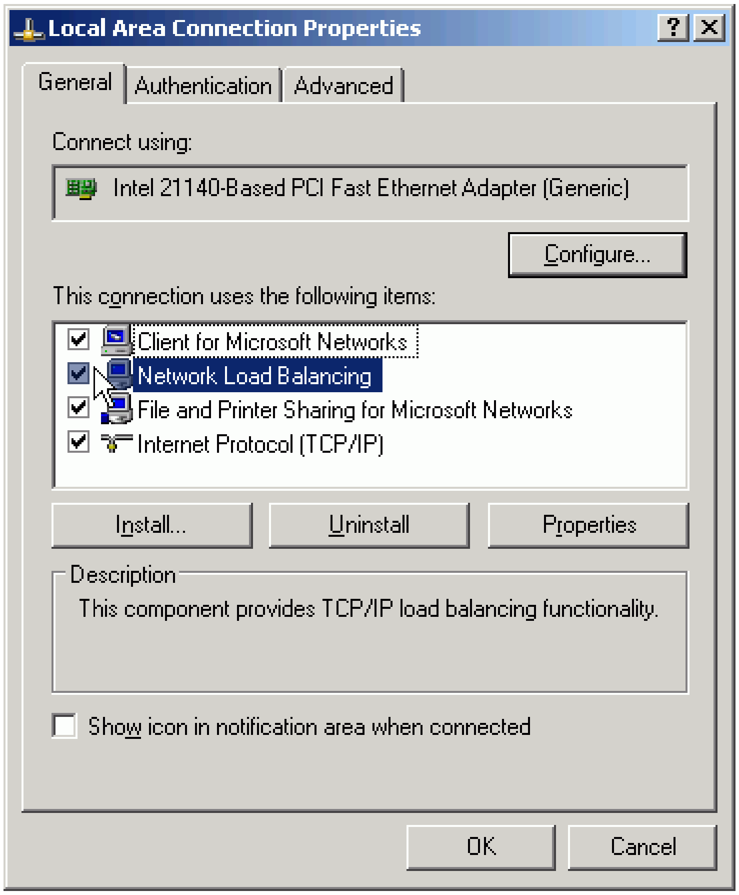
Default gateways:

Gateway	Metric

☑ Automatic metric

Interface metric:

b) Enable Windows Network Load Balancing on each server from the Network Connections | Properties dialog.



Local Area Connection Properties

Connect using:

Intel 21140-Based PCI Fast Ethernet Adapter (Generic)

This connection uses the following items:

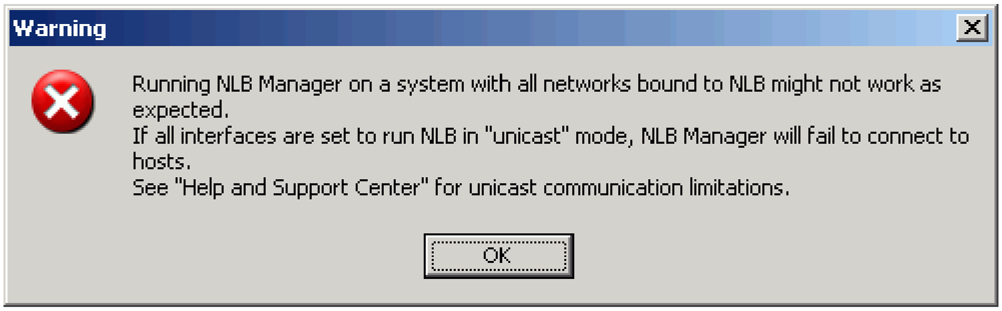
☑ Client for Microsoft Networks
☑ Network Load Balancing
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

This component provides TCP/IP load balancing functionality.

□ Show icon in notification area when connected

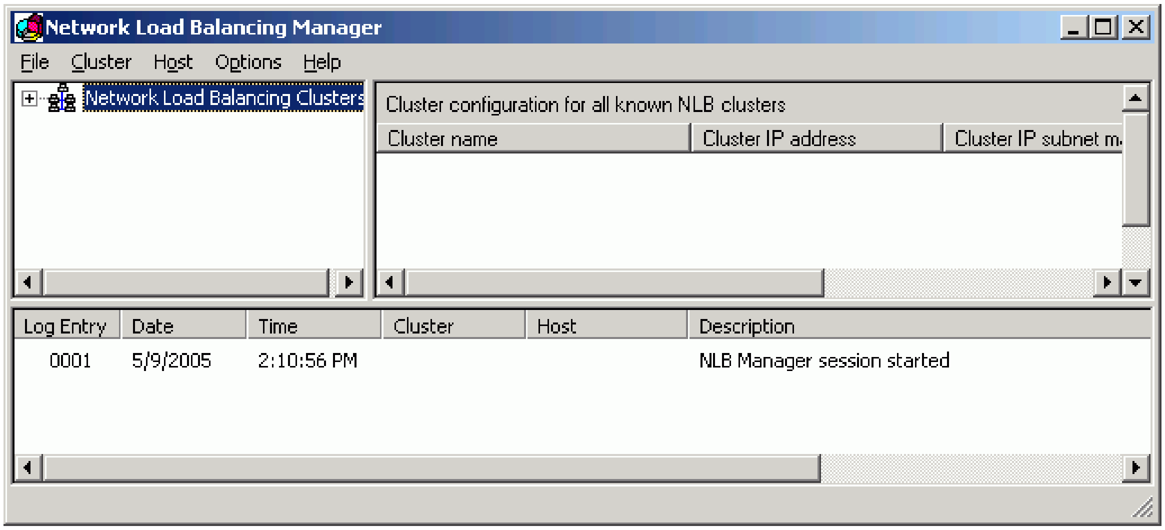
c) Run the Network Load Balancing Manager from Administrative Tools. You can ignore the warning:



Warning

Running NLB Manager on a system with all networks bound to NLB might not work as expected.
If all interfaces are set to run NLB in "unicast" mode, NLB Manager will fail to connect to hosts.
See "Help and Support Center" for unicast communication limitations.

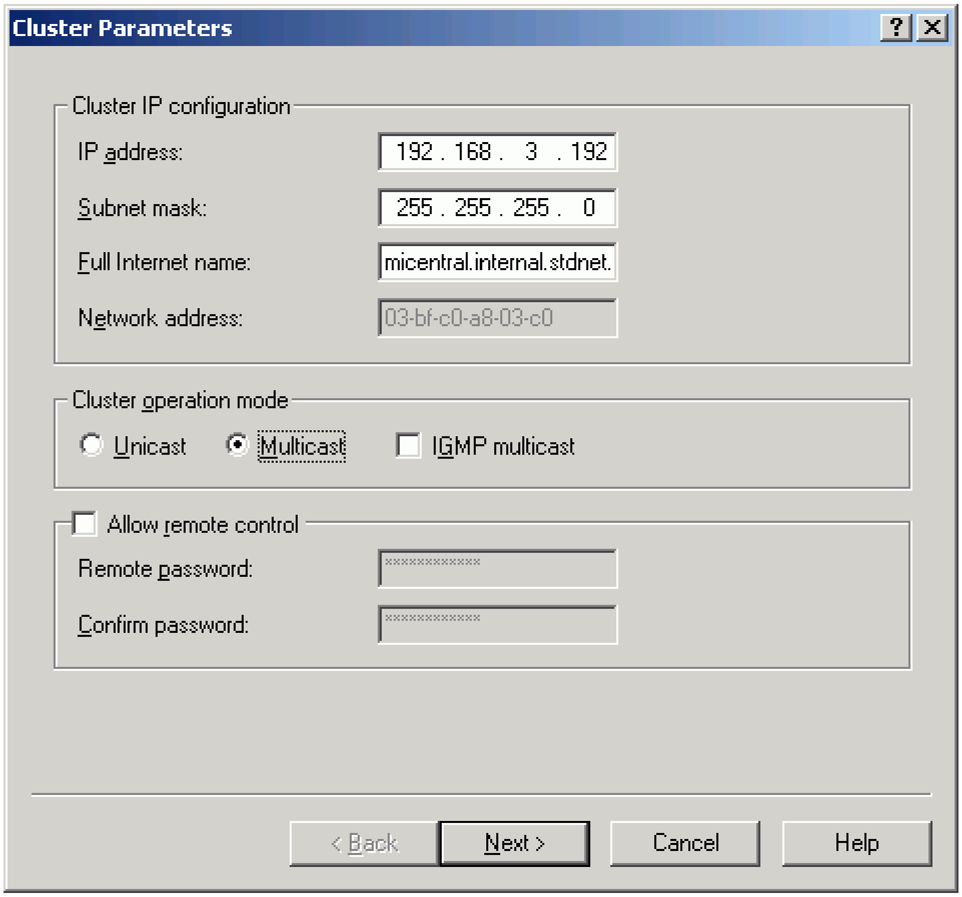
Then you'll get the main window:


Network Load Balancing Manager
File Cluster Host Options Help
Network Load Balancing Clusters
Cluster configuration for all known NLB clusters
Cluster name
Cluster IP address
Cluster IP subnet m

Log Entry	Date	Time	Cluster	Host	Description
0001	5/9/2005	2:10:56 PM			NLB Manager session started

d) Choose **Cluster** | **New** to be prompted with the "Cluster Parameters" window.

e) Enter the external IP address (configured in Advanced TCP/IP Settings above) which the MOVEit Centrals will share and choose **Multicast** for operation mode. Enter the subnet mask and domain name. Then choose **Next**.



Cluster Parameters

Cluster IP configuration

IP address: 192 . 168 . 3 . 192

Subnet mask: 255 . 255 . 255 . 0

Full Internet name: micentral.internal.stdnet.

Network address: 03-bf-c0-a8-03-c0

Cluster operation mode

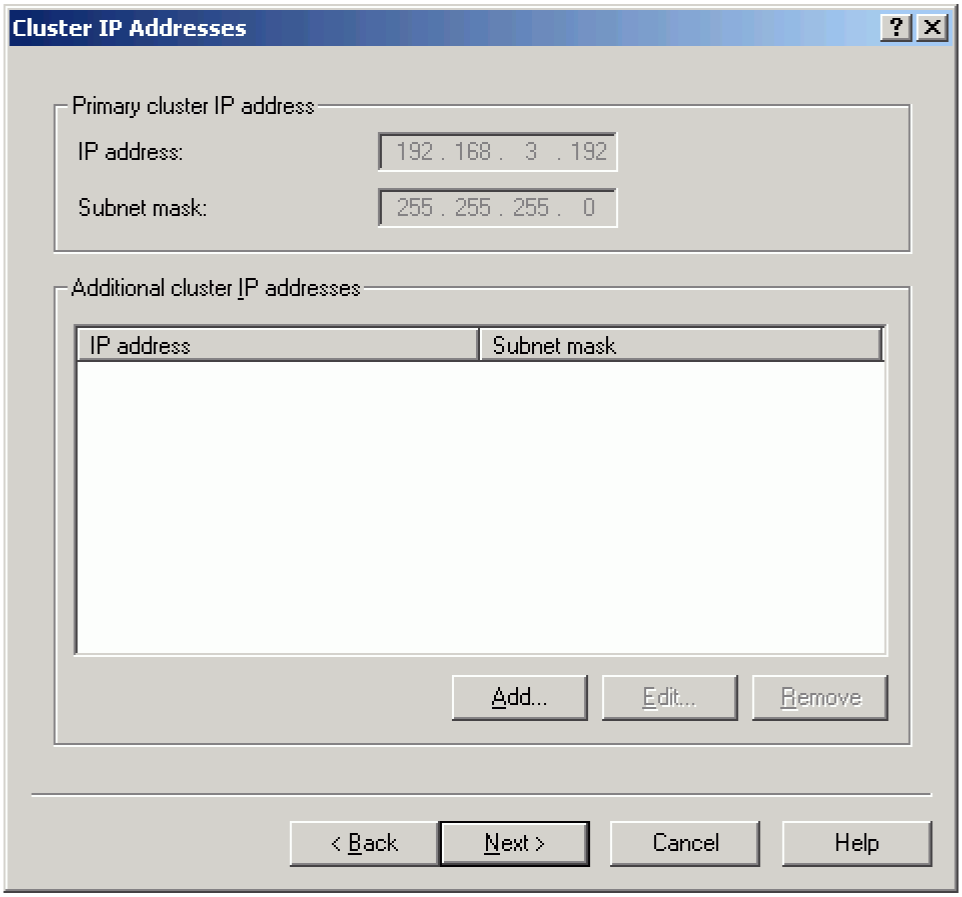
○ Unicast ● Multicast □ IGMP multicast

□ Allow remote control

Remote password: *************

Confirm password: *************

f) Do *not* enter any information into the Cluster IP Addresses dialog. Simply choose **Next**.



Cluster IP Addresses

Primary cluster IP address

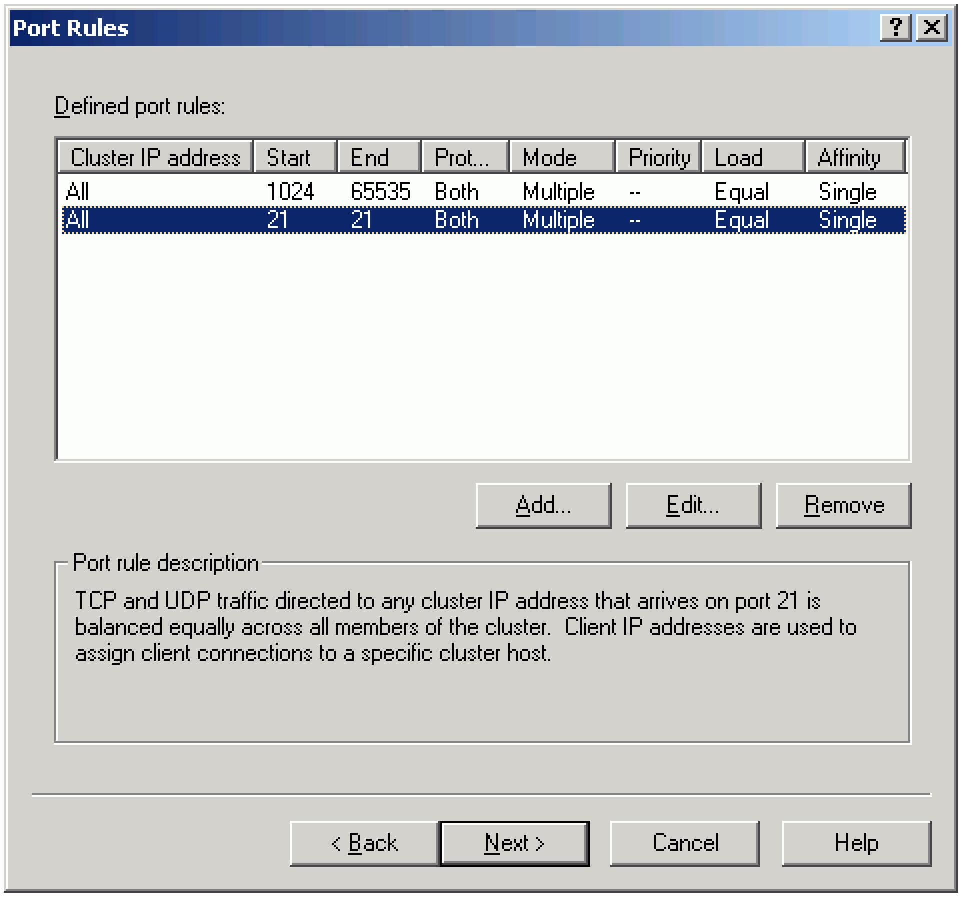
IP address: 192 . 168 . 3 . 192

Subnet mask: 255 . 255 . 255 . 0

Additional cluster IP addresses

IP address	Subnet mask

g) Configure your inbound port settings. In some situations, sticking with the default of "all ports" will be sufficient, but you will want to configure specific ports if you are using remote control software or a remote copy of MOVEit Central Admin to access each node in the MOVEit Central cluster. A more reliable setup is to only add the inbound ports needed by your FTP server. (For example: FTP control port 21 and the passive FTP data ports). Once you have the proper list, choose **Next**.



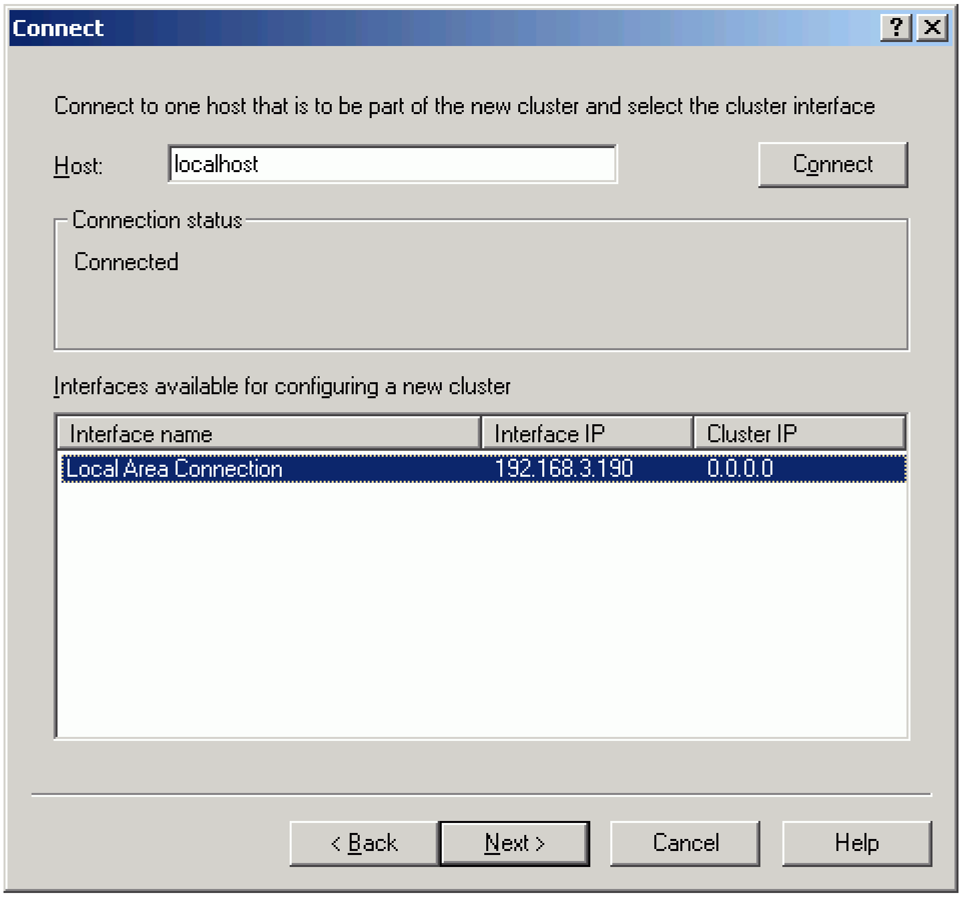
Defined port rules:

Cluster IP address	Start	End	Prot...	Mode	Priority	Load	Affinity
All	1024	65535	Both	Multiple	--	Equal	Single
All	21	21	Both	Multiple	--	Equal	Single

Port rule description

TCP and UDP traffic directed to any cluster IP address that arrives on port 21 is balanced equally across all members of the cluster. Client IP addresses are used to assign client connections to a specific cluster host.

h) At the Connect dialog, enter **localhost** and choose **Connect**. This will cause a list of network interfaces to appear. Select the external network interface and choose **Next**. (In the example below, there is only one interface.)



Connect

Connect to one host that is to be part of the new cluster and select the cluster interface

Host: localhost

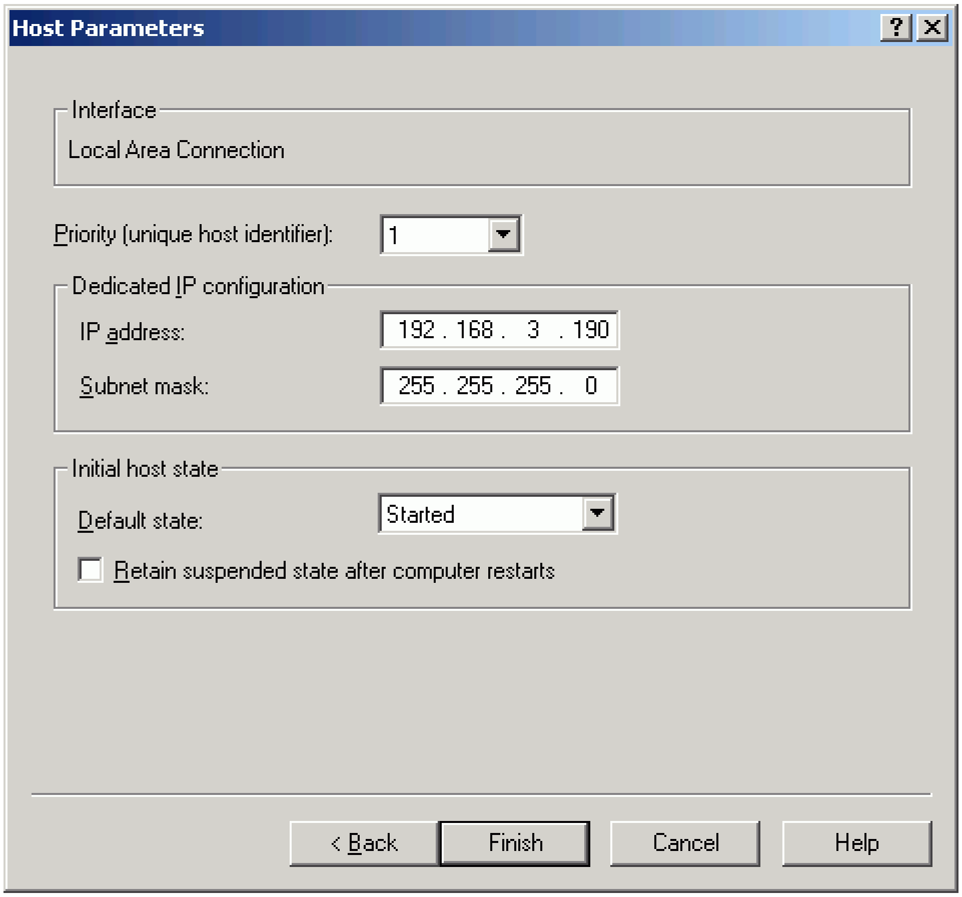
Connection status

Connected

Interfaces available for configuring a new cluster

Interface name	Interface IP	Cluster IP
Local Area Connection	192.168.3.190	0.0.0.0

i) In the Host Parameters dialog, set the dedicated IP address to the main IP address of this adapter. Set an appropriate subnet mask. Leave the other parameters at their default values. Choose **Finish** to complete the setup.



Host Parameters

Interface

Local Area Connection

Priority (unique host identifier): 1

Dedicated IP configuration

IP address: 192 . 168 . 3 . 190

Subnet mask: 255 . 255 . 255 . 0

Initial host state

Default state: Started

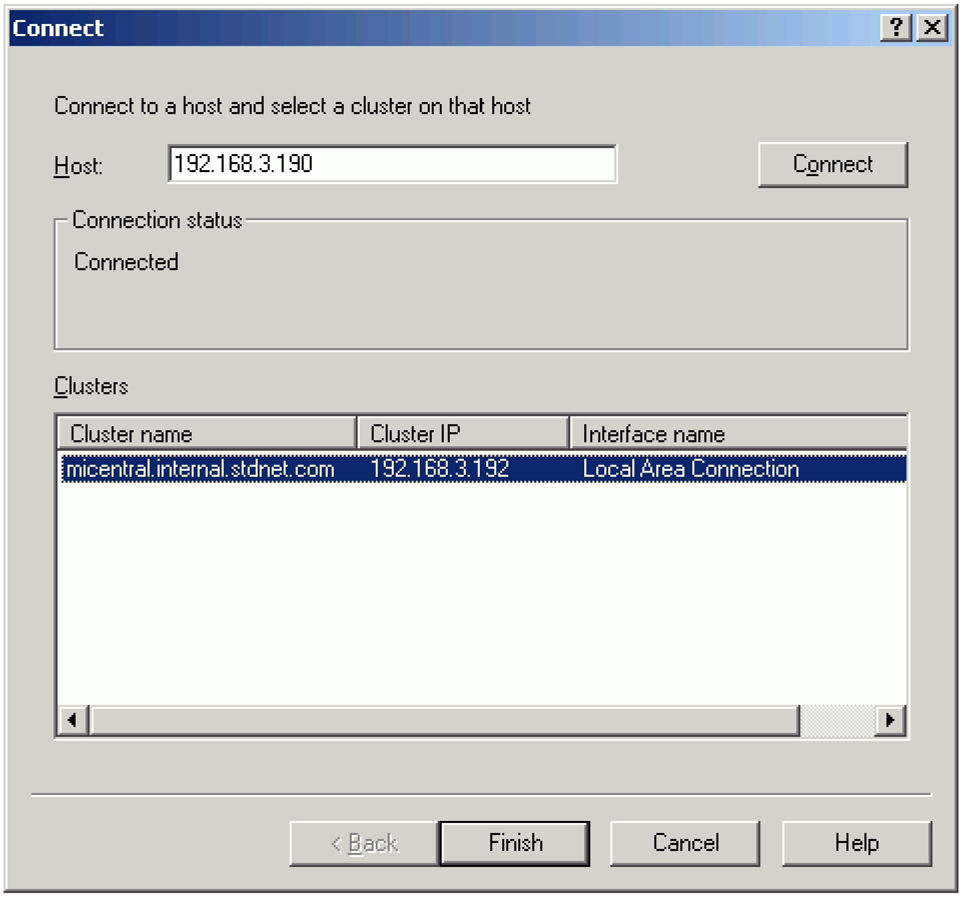
□ Retain suspended state after computer restarts

3 On the other MOVEit Central box, perform the following steps:

a) Enable Network Load Balancing, as above.

b) In Network Load Balancing Manager, use Cluster | Connect to Existing to bring up the Connect dialog.

c) Enter the IP address of the other computer that was configured above, and choose **Connect**. Select the cluster name corresponding to the one you just configured on the other computer, and choose **Finish**.



Connect to a host and select a cluster on that host

Host: 192.168.3.190

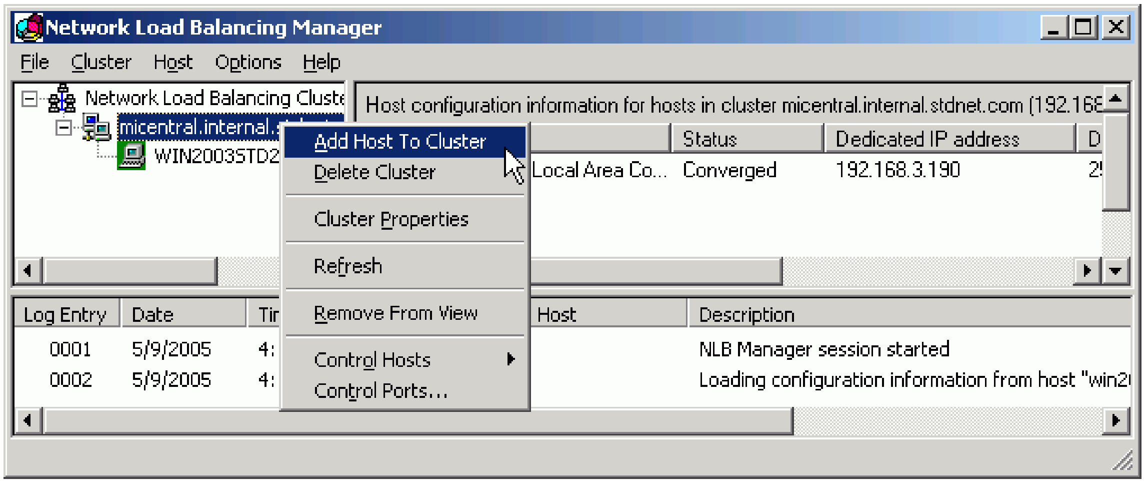
Connection status

Connected

Clusters

Cluster name	Cluster IP	Interface name
micentral.internal.stdnet.com	192.168.3.192	Local Area Connection

d) Right-click the name of the cluster, and choose **Add Host To Cluster**.

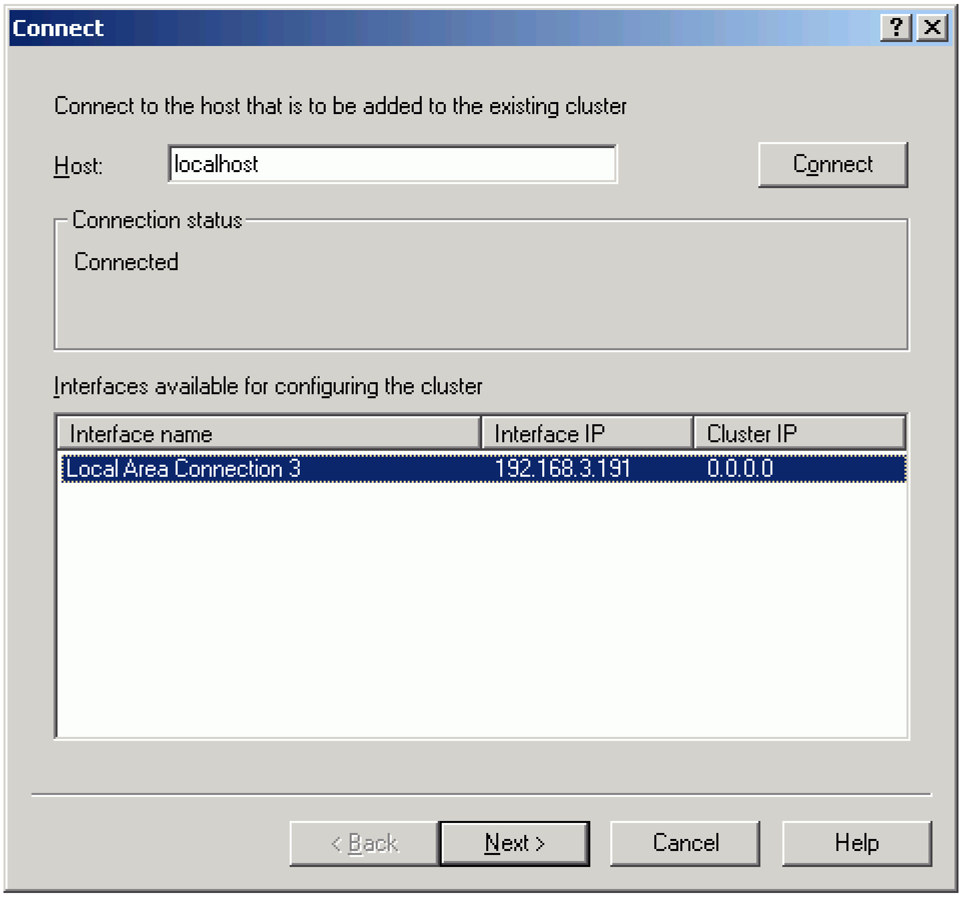


Host configuration information for hosts in cluster micentral.internal.stdnet.com (192.168

	Status	Dedicated IP address	D
Local Area Co...	Converged	192.168.3.190	2!

Log Entry	Date	Tir	Host	Description
0001	5/9/2005	4:		NLB Manager session started
0002	5/9/2005	4:		Loading configuration information from host "win2

e) Enter "localhost" as the host name, and choose **Connect**. Select the name of the external interface, and choose **Next**.



Connect to the host that is to be added to the existing cluster

Host: localhost

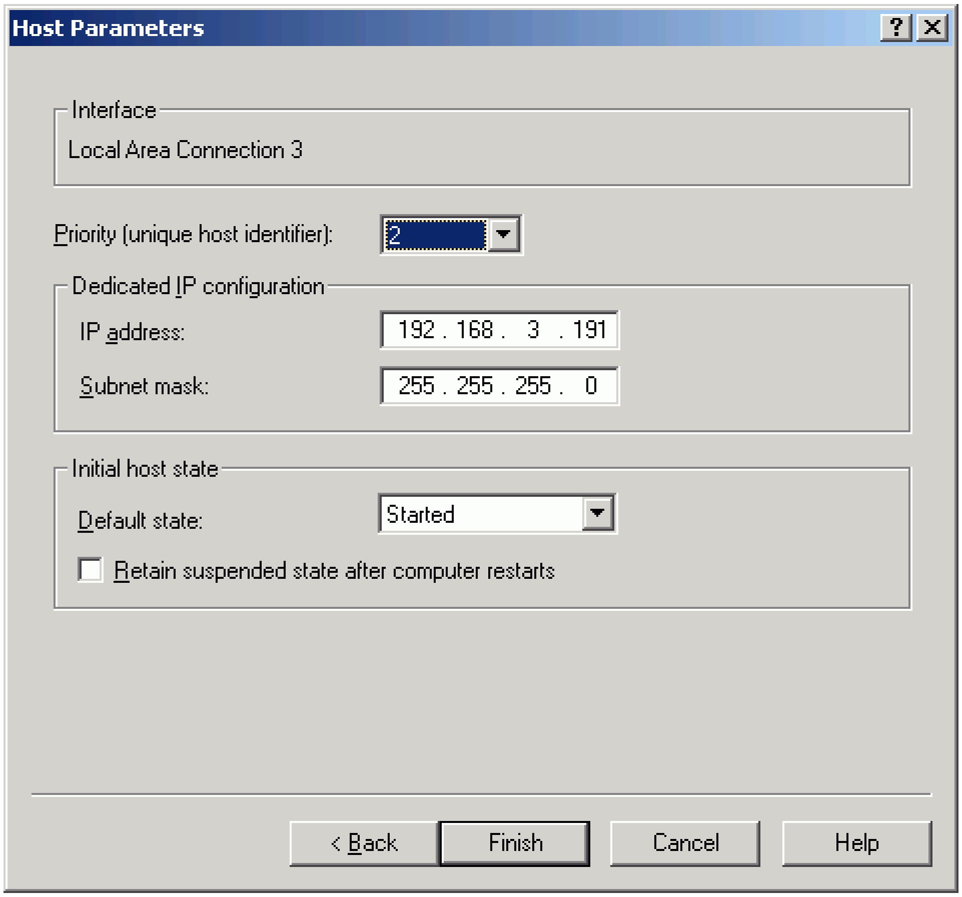
Connection status

Connected

Interfaces available for configuring the cluster

Interface name	Interface IP	Cluster IP
Local Area Connection 3	192.168.3.191	0.0.0.0

f) Accept the defaults for the Host Parameters, and choose **Finish**.



Host Parameters

Interface

Local Area Connection 3

Priority (unique host identifier): 2

Dedicated IP configuration

IP address: 192 . 168 . 3 . 191

Subnet mask: 255 . 255 . 255 . 0

Initial host state

Default state: Started

□ Retain suspended state after computer restarts

g) Use Network Connections | (connection name) | Properties | Internet Protocol (TCP/IP) | Properties | Advanced | Add... to add the cluster IP address to the list of addresses for your network adapter.

4 You may need to reboot the systems to clear NLB errors due to temporary issues with recognizing the cluster IP address.

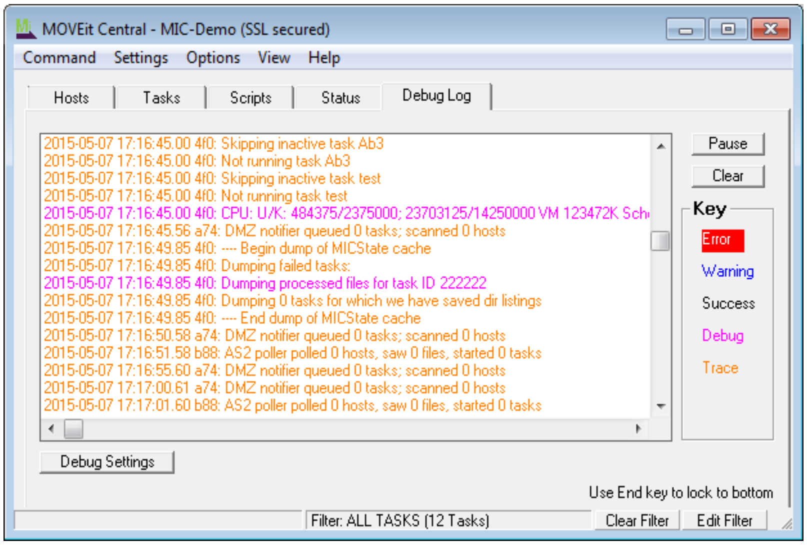
See also ***Failover Overview*** (on page 42).

Admin Console

Overview

The MOVEit Central Admin program is used to configure MOVEit Central's file transport/manipulation tasks and to monitor MOVEit Central activity. MOVEit Central Admin must have an authenticated connection to at least one MOVEit Central service, though it can manage multiple installations of MOVEit Central. It can reside on the same server as MOVEit Central or on a remote system.

Note: The new Web-based Admin program is now available for preview. It requires a separate installation process, described in the MOVEit Central Installation Guide.



```
2015-05-07 17:16:45.00 4f0: Skipping inactive task Ab3
2015-05-07 17:16:45.00 4f0: Not running task Ab3
2015-05-07 17:16:45.00 4f0: Skipping inactive task test
2015-05-07 17:16:45.00 4f0: Not running task test
2015-05-07 17:16:45.00 4f0: CPU: U/K: 484375/2375000; 23703125/14250000 VM 123472K Sch
2015-05-07 17:16:45.56 a74: DMZ notifier queued 0 tasks; scanned 0 hosts
2015-05-07 17:16:49.85 4f0: ---- Begin dump of MICState cache
2015-05-07 17:16:49.85 4f0: Dumping failed tasks:
2015-05-07 17:16:49.85 4f0: Dumping processed files for task ID 222222
2015-05-07 17:16:49.85 4f0: Dumping 0 tasks for which we have saved dir listings
2015-05-07 17:16:49.85 4f0: ---- End dump of MICState cache
2015-05-07 17:16:50.58 a74: DMZ notifier queued 0 tasks; scanned 0 hosts
2015-05-07 17:16:51.58 b88: AS2 poller polled 0 hosts, saw 0 files, started 0 tasks
2015-05-07 17:16:55.60 a74: DMZ notifier queued 0 tasks; scanned 0 hosts
2015-05-07 17:17:00.61 a74: DMZ notifier queued 0 tasks; scanned 0 hosts
2015-05-07 17:17:01.60 b88: AS2 poller polled 0 hosts, saw 0 files, started 0 tasks
```

Use End key to lock to bottom

Filter: ALL TASKS (12 Tasks)

The main screen of MOVEit Central Admin is broken into five or six tabs. Three are used to configure MOVEit Central and two are used to monitor MOVEit Central. One tab ("Failover") only appears if ***MOVEit Central Failover*** (on page 42) has been licensed.

- **Hosts** - Configures address and credentials used to access servers from various tasks.
- **Tasks** - Configures specific file transfer and manipulation tasks.
- **Scripts** - Configures file processing scripts.
- **Status** - Shows the current and last status of tasks.
- **Debug Log** - Monitors the debug log.
- **Failover** - Displays current failover status. Only available if ***MOVEit Central Failover*** (on page 42) has been licensed.

Titlebar

The top bar of the main MOVEit Central Admin dialog contains one or two interesting pieces of information about the current connection. All connections will show the hostname or IP address of the MOVEit Central to which MOVEit Central Admin is currently connected. If this value is "localhost", it means that the "connection" is local and SSL is not necessary. However, if this value is anything else either "(SSL secured)" or "(not secured)" will also be seen in the titlebar.

Firewall Considerations

MOVEit Central Admin only requires that it can connect to MOVEit Central on three TCP ports (3471, 3472, and 3473). All MOVEit Central Admin-to-MOVEit Central communication occurs over these ports, including "browse" actions to various hosts. (MOVEit Central is the machine actually doing the browsing in each case.) Because MOVEit Central Admin and MOVEit Central are often on the same "side" of a firewall, there is rarely a need to configure these ports into a firewall.

When MOVEit Central Admin traffic has been SSL encrypted (by installing an SSL certificate on MOVEit Central), these three channels will all be encrypted and will continue to use the same ports.

Requirements

The MOVEit Central Admin application is supported on the same operating systems specified for MOVEit Central Service requirements, and in addition, it is supported on Windows 7 Professional/Enterprise.

- **Hardware:** A standard PC. A Pentium-1GHz or faster processor, and 256 MB or more of memory are recommended.
- **Operating system:**
  - Windows 7 Professional/Enterprise
  - Windows Server 2008 R2 (64-bit English and German)
  - Windows Server 2012 R2

  - Windows Server 2012
  - Support for virtual servers running on VMware ESX (64-bit) and Microsoft Hyper-V 1.0 (64-bit)
- **Other components:** Internet Explorer 5.0 or later. MOVEit Central Admin does not use Internet Explorer directly, but it requires some of the libraries installed by Internet Explorer.
- **Supported browsers:** Internet Explorer 11 (Windows only); Mozilla Firefox (Windows, Mac, and Red Hat Linux); Chrome (Windows only); Safari (Mac only)

NOTICE: The new Web-based Admin program is now available for preview. It requires a separate installation process, described in the *MOVEit Central Installation Guid*e.

Installation

When you install or upgrade MOVEit Central using the MOVEit Central installation package, your local copy of MOVEit Central Admin will be removed. You must re-install the Admin Console if you want to run it from the MOVEit Central server.

Remote MOVEit Central Admin Users

Users who use MOVEit Central Admin to remotely connect to MOVEit Central must use the standalone MOVEit Central Admin installation to upgrade their clients.

1. Run the setup program. There are normally only two questions to answer:
   a) into which directory should the program be installed, and
   b) into which Start menu folder should the shortcuts be located.
2. MOVEit Central Admin may prompt you to also install Microsoft Installer and/or Microsoft XML. If you are prompted, please respond affirmatively, as both these entities are required. (If you are not prompted to install these entities, then the installation has detected that you have sufficient versions of these entities.)

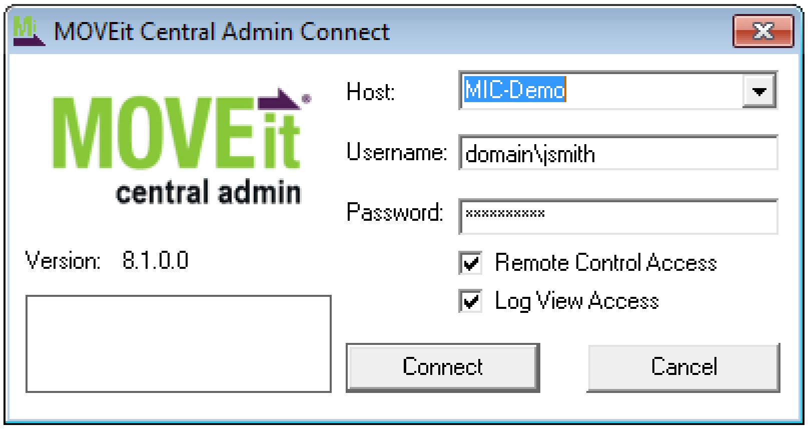
Remote MOVEit Central Admin Upgrades

Remote MOVEit Central Admin users should expect to upgrade MOVEit Central Admin each time MOVEit Central is upgraded; the only way to take advantage of new features in MOVEit Central is to configure them with a matching MOVEit Central Admin. In fact, recent versions of MOVEit Central Admin will only work with a particular range of MOVEit Central versions.

There are no special considerations when upgrading an existing MOVEit Central Admin. Almost all of Admin's configuration information (except for its recent host list) is obtained from MOVEit Central after connecting, so upgrades are easy and painless.

Connecting...

In order to configure hosts and tasks, and to view logs and status events, MOVEit Central Admin must first be connected to a running MOVEit Central server. The first dialog that shows up when MOVEit Central Admin is started, is the connection dialog.



MOVEit Central Admin Connect

Version: 8.1.0.0

Host: MIC-Demo

Username: domain\jsmith

Password: ***********

☑ Remote Control Access

☑ Log View Access

This dialog allows the operator to select a MOVEit Central by hostname or IP address, enter a username and password and connect/authenticate to that MOVEit Central.

When MOVEit Central Admin connects remotely, MOVEit Central will allow access only if:

- The user is a local Windows user or a user in the domain (including Active Directory)
- The user is a member of the MOVEit Admin, MOVEit Log or any of the MOVEit-User groups
- The correct password is provided for the user

The type of access allowed by MOVEit Central depends on the user's group membership. The "Remote Control" and "Log View" checkboxes will display or hide all configuration and monitoring functions, respectively. (Only check the "Log View" box if you are signing on to the secondary node of a MOVEit Central Failover cluster.)

NOTE:A user using MOVEit Central Admin to connect to a MOVEit Central server on the same machine (localhost) does not currently need to provide a username/password.

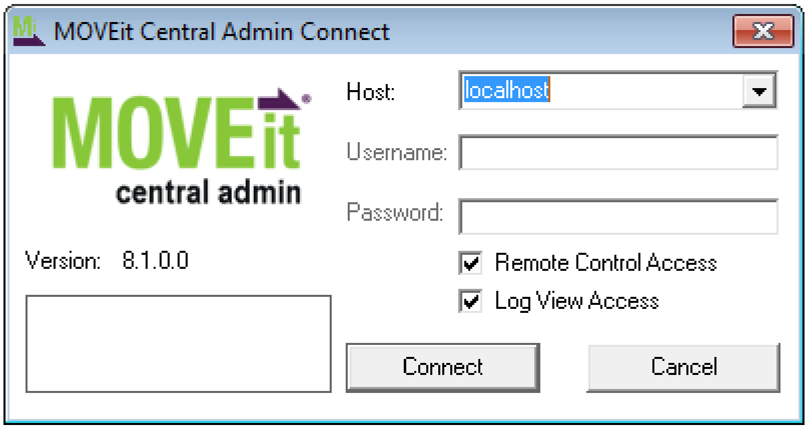
The proper syntax to use when signing on to MOVEit Central with a domain account is "[DOMAIN]\[username]", even if you regularly use syntax such as "[username]@[DOMAIN]".

Service Control

MOVEit Central Admin can provide basic service control when running on the same system as the MOVEit Central service. Central Admin will present a Start Service button, which will start the MOVEit Central service on the local system, assuming the following requirements are met:

- Host field is set to "localhost"
- MOVEit Central service is present and not running (and no running process exists that contains the string "MICentral")
- Current user has administrative rights

Once the service is running, the usual Connect button will be available. Service status will be displayed in the status window.



MOVEit Central Admin Connect

Version: 8.1.0.0

Host: localhost

Username:

Password:

☑ Remote Control Access

☑ Log View Access

Minimum Version

MOVEit Central requires that the version of MOVEit Central Admin be fairly recent. Each release of MOVEit Central requires a specific minimum version. If the version of MOVEit Central Admin is too old, MOVEit Central will reject the connection attempt with an error message. You can override the minimum version required by MOVEit Central on the server side; see ***System Internals*** (on page 415).

Access Control

MOVEit Central uses Windows authentication to control access to its configuration. Specifically, all remote users who authenticate to MOVEit Central will only be allowed access if:

- The user is a local Windows user or a user in the domain (including Active Directory)
- The user is a member of the MOVEit Admin, MOVEit Log or any of the MOVEit-User groups
- The correct password is provided for the user

MOVEit Central installs two new groups by default: MOVEit Admin and MOVEit Log. MOVEit Admin is the administrators group - users belonging to this group have full power over MOVEit Central. MOVEit Log is a "read-only" group - users belonging to this group may only monitor MOVEit Central. (It is not necessary for users to belong to both the MOVEit Admin and MOVEit Log groups; MOVEit Admin includes all the rights allowed MOVEit Log.)

Domain Authentication

It is possible to sign onto MOVEit Central through MOVEit Central Admin using a domain account, if you observe the following:

- the machine on which MOVEit Central is installed is part of the domain,
- the user the MOVEit Central service is running under is a domain account, and
- the users or groups you would like to control MOVEit Central have been added to the appropriate Windows user groups.

The proper syntax to use when signing on to MOVEit Central with a domain account is "[DOMAIN]\[username]", even if you regularly use syntax such as "[username]@[DOMAIN]".

"MOVEit-User" Groups

MOVEit Central also supports setting up additional groups with customized permissions. These groups are collectively known as "MOVEit-User" groups and are configured from the Settings menu in MOVEit Central Admin. (A user must be a member of the MOVEit Admin group to make changes to these settings.)

Users who sign into MOVEit Central Admin with a username that belongs to the "MOVEit Admin" Windows group can edit or start any task. To control access to tasks in specific task groups, operators can create restrictive administrative users based on site-specific Windows groups. These groups have names beginning with "MOVEit Users-". By default, a restricted user has no permissions.

Note: MOVEit Central Enterprise supports customized permissions by selecting Permissions on the Settings menu. Though this functionality is not available in the Corporate version, users of the Corporate version can manually create a MOVEit-User group, or add a user to the MOVEit Admin and MOVEit Log groups, by using Windows Computer Management.

Managing Permissions (Enterprise only)

1 Select the "Permissions" option in the ***Settings menu*** (on page 96) to open the Permissions dialog.

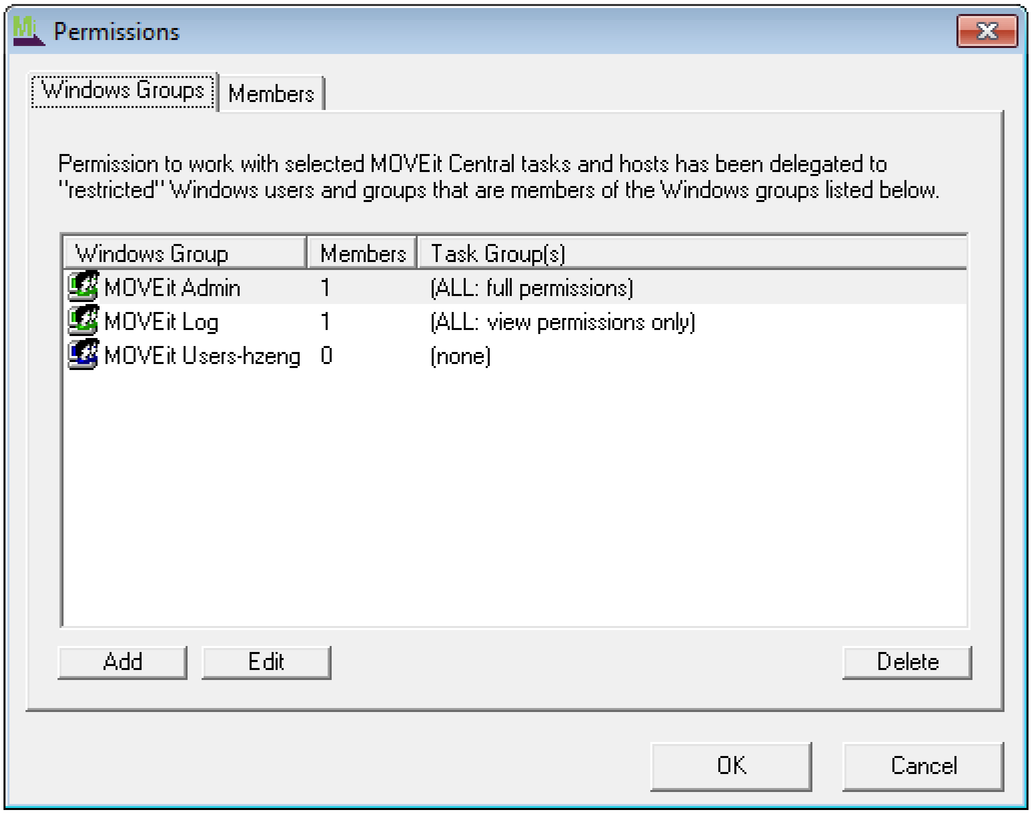
Here, the groups associated with MOVEit Central permissions will be listed in the Windows Groups tab, and the members of those groups in the Members tab.

2 On the Windows Groups tab:

a) To add new "MOVEit Users" groups, select the **Add** button.

b) To delete an existing group, select the **Delete** button.

c) To edit a group, double-click the group or select the group and then click the **Edit** button.



Permission to work with selected MOVEit Central tasks and hosts has been delegated to "restricted" Windows users and groups that are members of the Windows groups listed below.

Windows Group	Members	Task Group(s)
MOVEit Admin	1	(ALL: full permissions)
MOVEit Log	1	(ALL: view permissions only)
MOVEit Users-hzeng	0	(none)

3 On the Members tab, right-click a user:

a) To create new Windows users, click the **Add** button.

b) To delete an existing user that was created by MOVEit Central, from the menu select **Delete**.

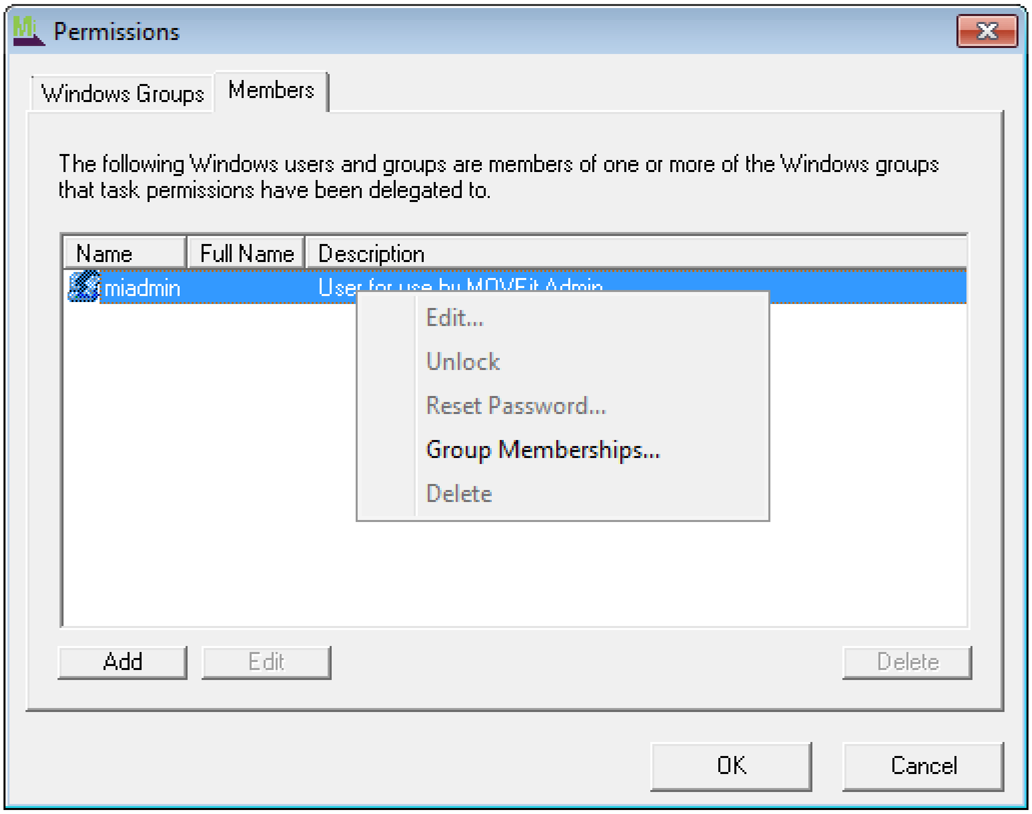
Administrators are not allowed to edit or delete Windows users that were not created by MOVEit Central.

c) To change the user's password, from the menu select **Reset Password**.

d) To unlock a locked user, from the menu select **Unlock**.

e) To change the group memberships of all Windows users and groups listed, click the **Groups** button.

Note: The only property you can change for the built-in user miadmin is Group Memberships.



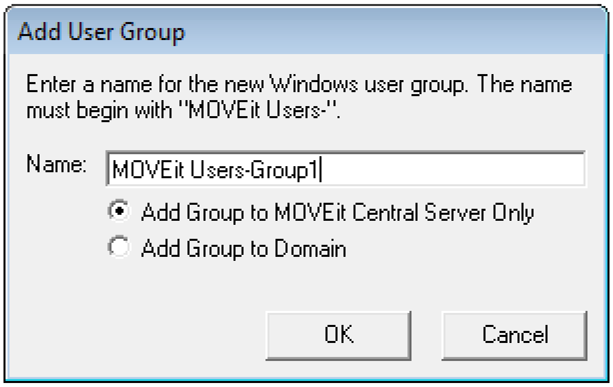
The following Windows users and groups are members of one or more of the Windows groups that task permissions have been delegated to.

Name	Full Name	Description
miadmin		User for use by MOVEit Admin

Adding Windows Groups

1 Click the Add button on the Windows Groups tab

The Add User Group dialog appears.



Enter a name for the new Windows user group. The name must begin with "MOVEit Users-".

Name: MOVEit Users-Group1

● Add Group to MOVEit Central Server Only

○ Add Group to Domain

2 Enter a name for the new group, and select whether the group will be added to the local system or to the domain where the Central server is a member.

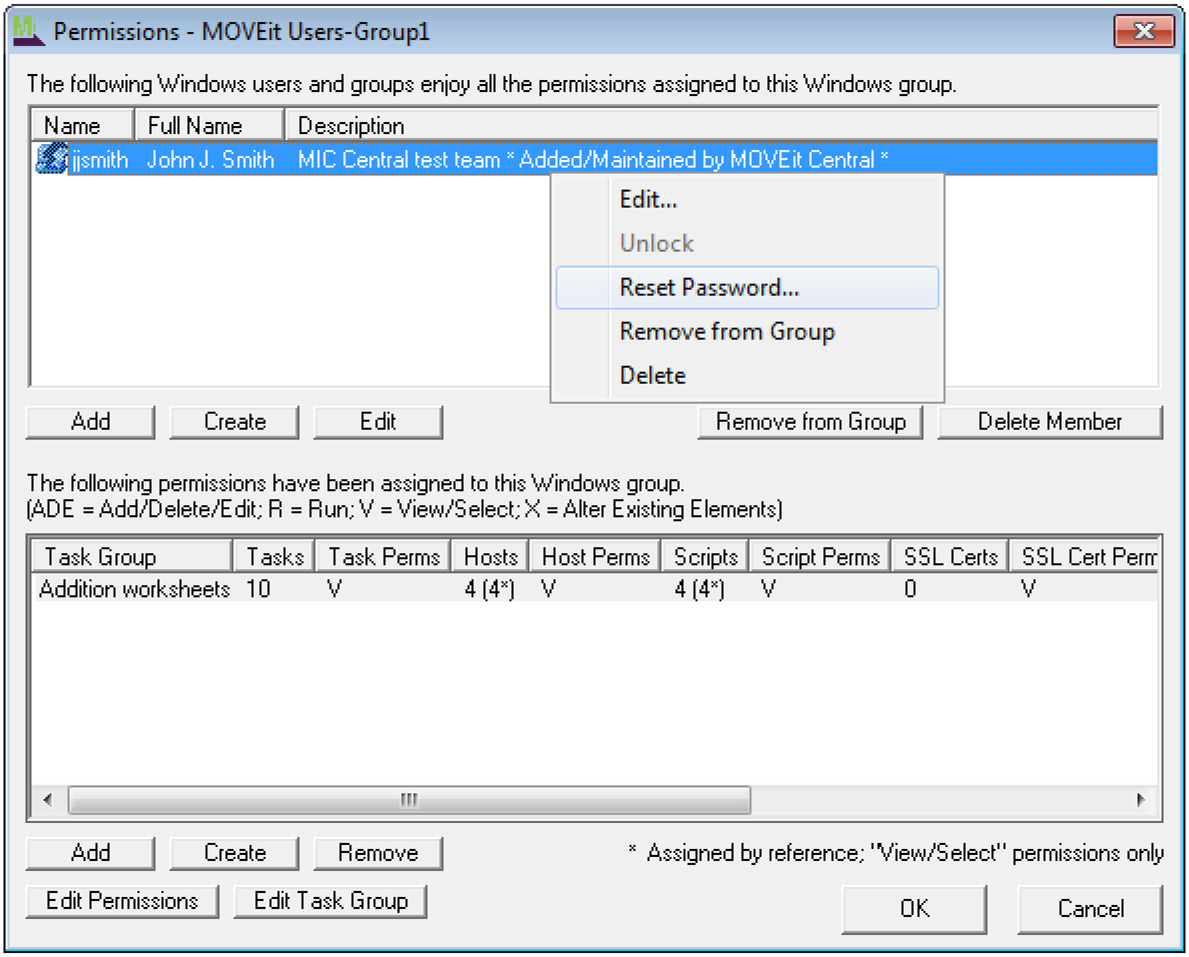
The name must begin with the string "MOVEit Users-" in order to be recognized as a MOVEit Central user group. If you enter a name that does not begin with this string, or a name that is already in use, an error message appears.

Editing Windows Groups

In addition to allowing a user to authenticate to MOVEit Central, membership in a MOVEit Central permissions group also determines which tasks, hosts, scripts, and other elements a user is allowed to view, use, and edit. While membership in the MOVEit Admin group allows full access to all tasks and other elements, and membership in the MOVEit Log group allows read-only access to all tasks and other elements, which tasks and elements a user in a MOVEit Users group has access to is determined by which task groups are associated with the MOVEit Users group, and which permissions are assigned to those task groups.

1 To view or edit the list of task groups associated with a MOVEit Users group, as well as the list of members of that Windows group, double-click a group in the Windows Group tab, or select it and click the **Edit** button.

The Permissions dialog for the group appears.



The following Windows users and groups enjoy all the permissions assigned to this Windows group.

Name	Full Name	Description
jjsmith	John J. Smith	MIC Central test team * Added/Maintained by MOVEit Central *

The following permissions have been assigned to this Windows group.
(ADE = Add/Delete/Edit; R = Run; V = View/Select; X = Alter Existing Elements)

Task Group	Tasks	Task Perms	Hosts	Host Perms	Scripts	Script Perms	SSL Certs	SSL Cert Perm
Addition worksheets	10	V	4 (4*)	V	4 (4*)	V	0	V

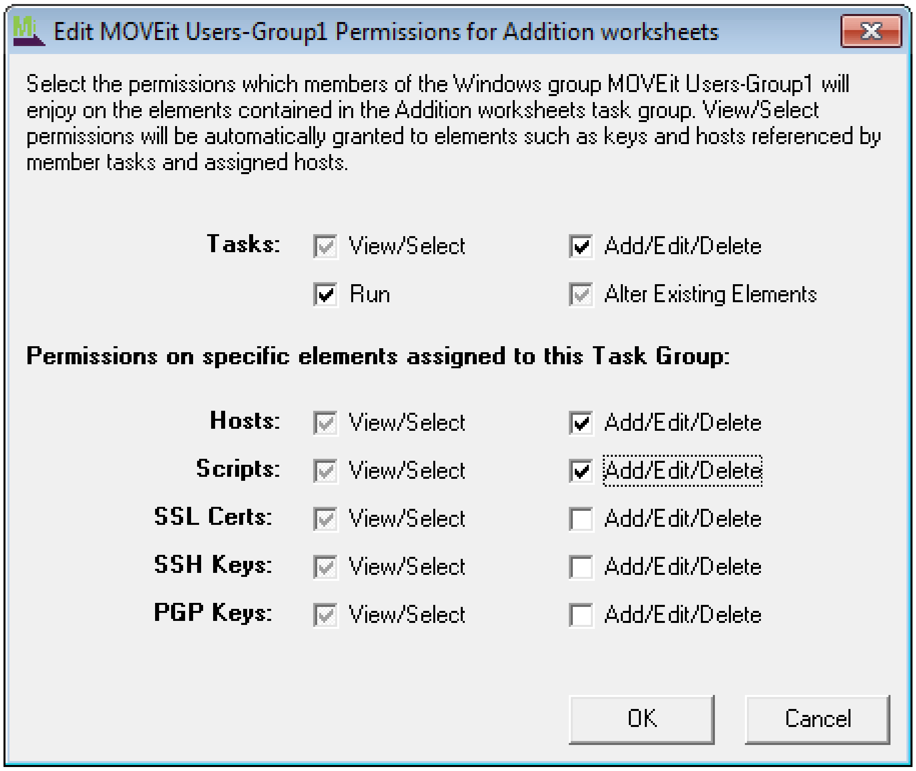
* Assigned by reference; "View/Select" permissions only

In this dialog, current members of the Windows group are listed, and members can be added, created, maintained, removed, or deleted. Only those users created through MOVEit Central will be fully editable. Task group associations are also listed and maintained here. Each task group associated with the Windows group is listed, along with counts of the various elements in the task group, and what permissions are assigned for each element type. Administrators may add existing task group associations, create new task groups, edit existing task group, edit the permissions of a task group association, and remove task group associations. Creating and editing task groups here is the same as creating and editing task groups through the Edit Task Groups dialog. See the ***Task Groups*** (on page 116) page for more information.

Task group associations have permissions assigned for each of the types of elements that can belong to a task group.

2 To change permissions, double-click a task group, or select a task group and click the **Edit Permissions** button.

The Edit Permissions dialog for the task group appears.



Edit MOVEit Users-Group1 Permissions for Addition worksheets

Select the permissions which members of the Windows group MOVEit Users-Group1 will enjoy on the elements contained in the Addition worksheets task group. View/Select permissions will be automatically granted to elements such as keys and hosts referenced by member tasks and assigned hosts.

Tasks: ☑ View/Select ☑ Add/Edit/Delete

☑ Run ☑ Alter Existing Elements

Permissions on specific elements assigned to this Task Group:

Hosts: ☑ View/Select ☑ Add/Edit/Delete

Scripts: ☑ View/Select ☑ Add/Edit/Delete

SSL Certs: ☑ View/Select □ Add/Edit/Delete

SSH Keys: ☑ View/Select □ Add/Edit/Delete

PGP Keys: ☑ View/Select □ Add/Edit/Delete

For tasks, there are four different permissions:

- **View/Select** - Allows users to see a task but not run or make any changes to it. This permission is always allowed and cannot be removed.
- **Run** - Allows users to manually run a task and stop a running task.
- **Add/Edit/Delete** - Allows users to add and remove tasks, and add and remove the various elements of tasks, such as sources, destinations, processes, and schedules.

- **Alter Existing Elements** - Allows users to change the settings of existing elements of tasks, such as sources and destinations, but does not allow them to add or remove task elements. This permission is completely overridden by the Add/Edit/Delete permissions.

For all other elements, there are only two different permissions:

- **View/Select** - Allows users to see an element of the given type and use it in a task, but not make any changes to it. This permission is always allowed and cannot be removed.
- **Add/Edit/Delete** - Allows users to add, edit, and remove a elements of the given type.

Managing Members

MOVEit Central permissions group memberships can be managed from the Members tab of the main Permissions dialog, or from the membership list on an individual Windows group permissions dialog. In both locations, existing users can be added as members, new users can be created as members, and existing members can have their password reset, be unlocked if they are marked as "locked out", or removed from the group, and even deleted. Only those users who were originally created through MOVEit Central will be fully editable. Otherwise, the Reset, Unlock, and Delete options will not be available. Users originally created through MOVEit Central are recognizable by the string "*Added/Maintained by MOVEit Central*" in the user's description.

Adding/Creating Members

1 To ***add or create new members*** (on page 85), from the Members tab of the MOVEit Central Permissions dialog click the **Add** or **Create** button.

The Add New Group Member dialog appears with the appropriate selection or creation option selected.

2 To select a domain group as the member, select the "Select existing group" option.

a) Select the group to which you want the member to belong from the list of available groups for the domain.

If the Add New Group Member dialog was opened from the main Permissions dialog, the "Group to add to" option to select which existing MOVEit Central permissions group the user should be added appears. Otherwise, if the dialog was opened from an individual Windows group permissions dialog, the selected user or group will be added to that group.

b) From the list of domain groups, choose a group.

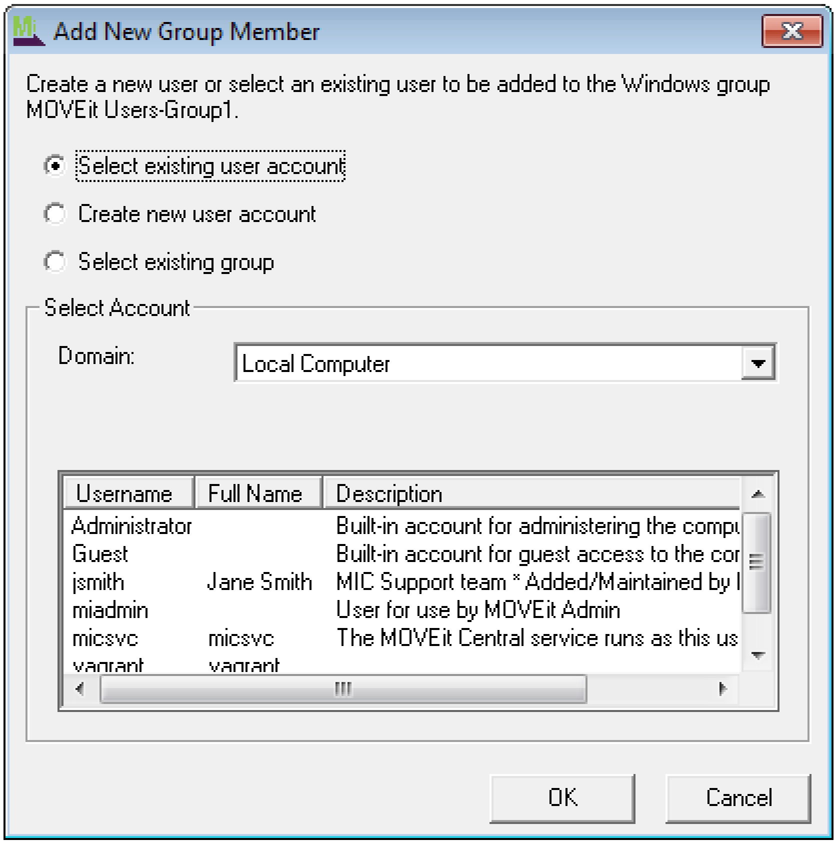
NOTE: Only domain groups can be selected from here - local Windows groups cannot be added as members of a MOVEit Central permissions group.

3 To select an existing user as a member, select the "Select existing user account" option.

a) If necessary, select the group to which you want the member to belong from the list of available groups for the domain.

If the Add New Group Member dialog was opened from the main Permissions dialog, the "Group to add to" option to select which existing MOVEit Central permissions group the user should be added appears. Otherwise, if the dialog was opened from an individual Windows group permissions dialog, the selected user or group will be added to that group.

b) Select a user from either the local system, or from the domain where the MOVEit Central server is a member.



Add New Group Member

Create a new user or select an existing user to be added to the Windows group MOVEit Users-Group1.

● Select existing user account

○ Create new user account

○ Select existing group

Select Account

Domain: Local Computer

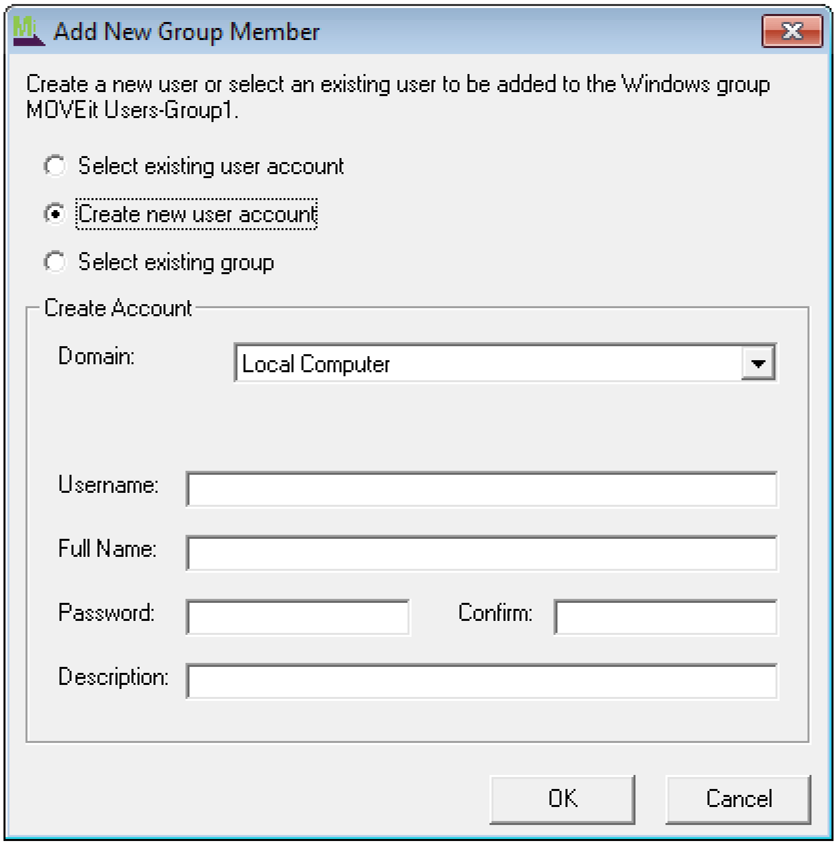
Username	Full Name	Description
Administrator		Built-in account for administering the compu
Guest		Built-in account for guest access to the cor
jsmith	Jane Smith	MIC Support team * Added/Maintained by I
miadmin		User for use by MOVEit Admin
micsvc	micsvc	The MOVEit Central service runs as this us
vagrant	vagrant	

4 To create a new user as a member, select the "Create new user account" option.:

a) If necessary, select the group to which you want the member to belong from the list of available groups for the domain.

If the Add New Group Member dialog was opened from the main Permissions dialog, the "Group to add to" option to select which existing MOVEit Central permissions group the user should be added appears. Otherwise, if the dialog was opened from an individual Windows group permissions dialog, the selected user or group will be added to that group.

b) Enter the appropriate user information in the provided fields. The user may be created on either the local system, or on the domain the MOVEit Central server is a member of.



Add New Group Member

Create a new user or select an existing user to be added to the Windows group MOVEit Users-Group1.

○ Select existing user account

● Create new user account

○ Select existing group

Create Account

Domain: Local Computer

Username:

Full Name:

Password: Confirm:

Description:

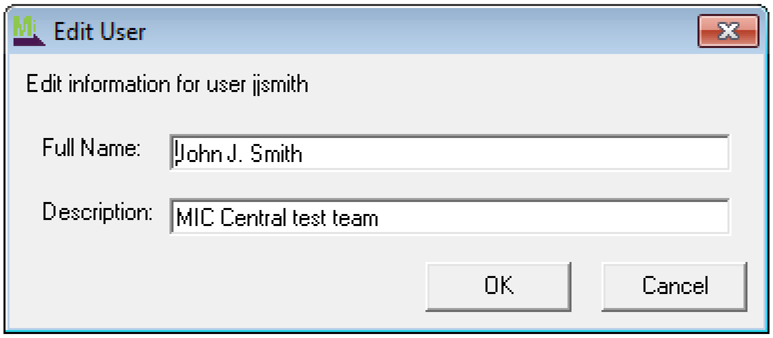
NOTE: For performance reasons, both the user and group selection lists are limited to displaying up to 2,000 entries. If you need to manage more users or groups than this, please use the Windows user management tools.

Editing Members

To change the full name and description of members originally created through MOVEit Central:

1 Select the user.

2 Click the **Edit** button.



Edit User

Edit information for user jjsmith

Full Name: John J. Smith

Description: MIC Central test team

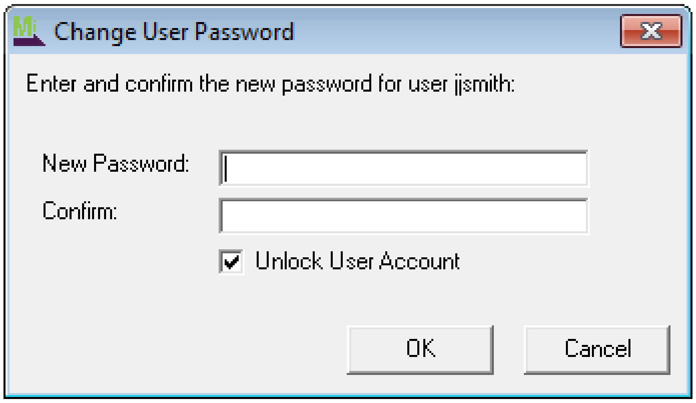
Resetting/Unlocking Members

To unlock or reset passwords of users originally created through MOVEit Central:

1 Select the user.

2 Click either the **Reset** or **Unlock** button.

If a user needs to be unlocked, clicking the Reset button to change the user's password will also provide an option to unlock the account.



Change User Password

Enter and confirm the new password for user jjsmith:

New Password:

Confirm:

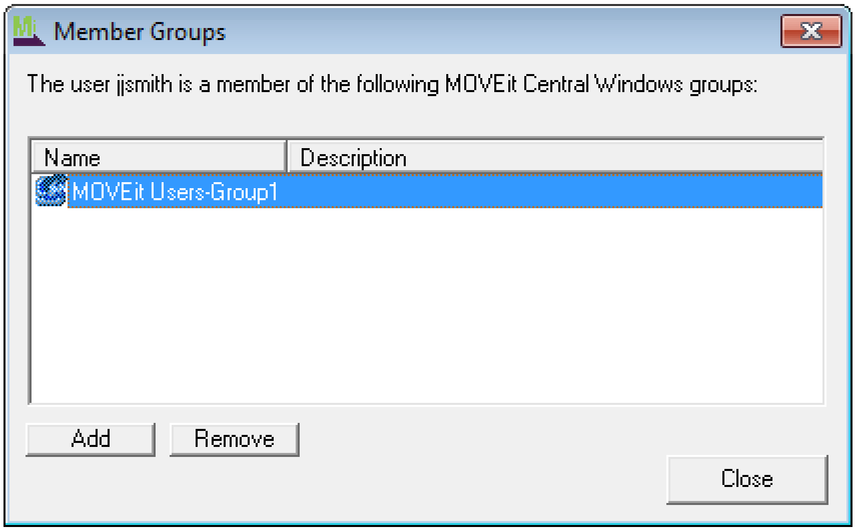
☑ Unlock User Account

Editing User Group Memberships

On the Members tab of the main Permissions dialog, an additional button is available which allows administrators to edit the group memberships of a select member.

1 Double-click a member, or select a member and click the **Groups** button.

The Member Groups dialog appears, with a list of all MOVEit Central permissions groups where the user or group is a member.



The user jjsmith is a member of the following MOVEit Central Windows groups:

MOVEit Users-Group1

2 To add the user or group to additional groups, click the **Add** button.

3 To remove the user or group from existing groups, click the **Remove** button.

Admin-specific Options

This section describes the following Admin-specific options menus:

- Command Menu
- Settings Menu
- Options Menu
- Tasks Menu
- View Menu
- Help Menu

Command Menu

The "Command" sub-menu is available from the Admin main menu located immediately beneath the application title bar. All options may not be available at all times depending on user permissions and the state of communication between MOVEit Central Admin and MOVEit Central.

- **Send Config** - Sends the current configuration that MOVEit Central Admin is working with to the MOVEit Central server it is currently connected to. When MOVEit Central receives this configuration, it writes it out to disk for storage and then implements it. The keyboard shortcut Ctrl-S will also run this command. Use of this command should usually not be necessary; MOVEit Central Admin automatically performs this activity as necessary as part of its normal operation.
- **Refresh Config** - Checks to see if the configuration that MOVEit Central Admin is working with is still current. If it is not, MOVEit Central Admin will then retrieve the latest configuration from MOVEit Central. If changes have been made to the configuration that MOVEit Central Admin is working with, Admin will ask the user if they would like to retrieve the latest configuration. Doing so will eliminate any changes made by the user. The keyboard shortcut Ctrl-R will also run this command. Use of this command should usually not be necessary; MOVEit Central Admin automatically performs this activity as necessary as part of its normal operation.
- **Import Config** - Takes an exported XML config file and reads it back into the system. Can be used to reinstall a backed-up configuration.
- **Export Config** - Writes out a copy of the XML config file currently loaded into MOVEit Central Admin. Can be used for backing-up configurations.
- **Disable Scheduler** (or when already disabled, Enable Scheduler) - Disables (or enables) MOVEit Central's task scheduler. No more tasks will be automatically started, although tasks can still be manually started by MOVEit Central Admin or MOVEit Central API. Any tasks already running will run to completion.

  If MOVEit Central is restarted, the MOVEit Central scheduler will automatically be restarted as well. If this is not desired, it is also possible to start the MOVEit Central service with the scheduler disabled; see the "-k" option in the "Running MOVEit Central in the Foreground" section of the "***Central: The Service - Running As...*** (see "***Running As...***" on page 14)" doc for information about this feature.
- **Shut Down Service** - Disables MOVEit Central's task scheduler, waits until no tasks are running, and then stops the MOVEit Central service. When the service stops, MOVEit Central Admin will display a "Host Disconnected" message: this is normal and expected.

  Use this feature to shut down MOVEit Central cleanly. This is generally preferable to simply stopping the service, because simply stopping the service will abruptly terminate any tasks that are running.

  Any tasks that are launched (or "looped") using Next Actions may need to be shut down individually through the "Status" tab because such tasks are not launched from the scheduler.

- **Test Antivirus** - This function will cause MOVEit Central to deposit a file (with a "*.tmp" extension) with a test virus signature (the "EICAR" test string) into MOVEit Central's cache directory. The test file is harmless, but it should be treated by any real-time antivirus package as an actual virus. If the test is successful you will see a message like "Success - AntiVirus test successful. Detected antivirus package 'Symantec AntiVirus'." pop up in MOVEit Central Admin.
- **Reset Tamper Detection** - Resets MOVEit Central's tamper detection mechanism so that it begins tamper checking audit and statistics entries from the point at which the command is issued. Any previous entries will no longer be covered by tamper detection.
- **Disconnect** - Ends the current session with MOVEit Central and returns the user to the signon window. From here, the user may select a different MOVEit Central server to connect to, or exit the program.
- **Exit** - Ends the current session with MOVEit Central and exits the program.

Settings Menu

The "Settings" sub-menu is available from the Admin main menu near the application title bar. All options may not be available at all times depending on user permissions and the state of communication between MOVEit Central Admin and MOVEit Central.

- **System Settings** - Opens the ***System Settings*** (see "***Related Settings***" on page 229) dialog, which is used to alter MOVEit Central system settings, such as debug level and log file size.
- **Permissions (Enterprise only)** - Opens the Permissions dialog, which is used to set task group permissions for Windows user groups. See the ***Access Control*** (on page 84) page for more information
- **Date Lists** - Opens the Date List Manager, which is used to create and edit date lists used in task schedules. See the ***Date Lists*** (on page 144) page for more information.
- **Task Groups** - Opens the Task Group Manager, which is used to create, edit, and populate task groups. See the ***Task Groups*** (on page 116) page for more information.
- **Certs/Keys**
  - **SSL Client Certificates** - Opens the Manage SSL Certs dialog, which is used to add and remove SSL client certificates, and view the information for existing certificates. See the ***SSL Client Certificates*** (on page 217) page for more information.
  - **SSH Public Keys** - Opens the Manage SSH Keys dialog, which is used to add, edit, and remove SSH client keys, and view information for existing keys. See the ***Importing Existing SSH Keys*** (see "***Importing SSH Client Keys***" on page 216) page for more information.
  - **PGP Keys** - Open the Manage PGP Keys dialog, which is used to add, export, and remove PGP keys. See the ***Managing PGP Keys*** (on page 219) page for more information.
- **Global Task Parameters** - Opens the Manage Global Task Parameters dialog, which allows you to configure parameters which are common to all tasks. See the ***Task Information*** (on page 108) page for more information.

Options Menu

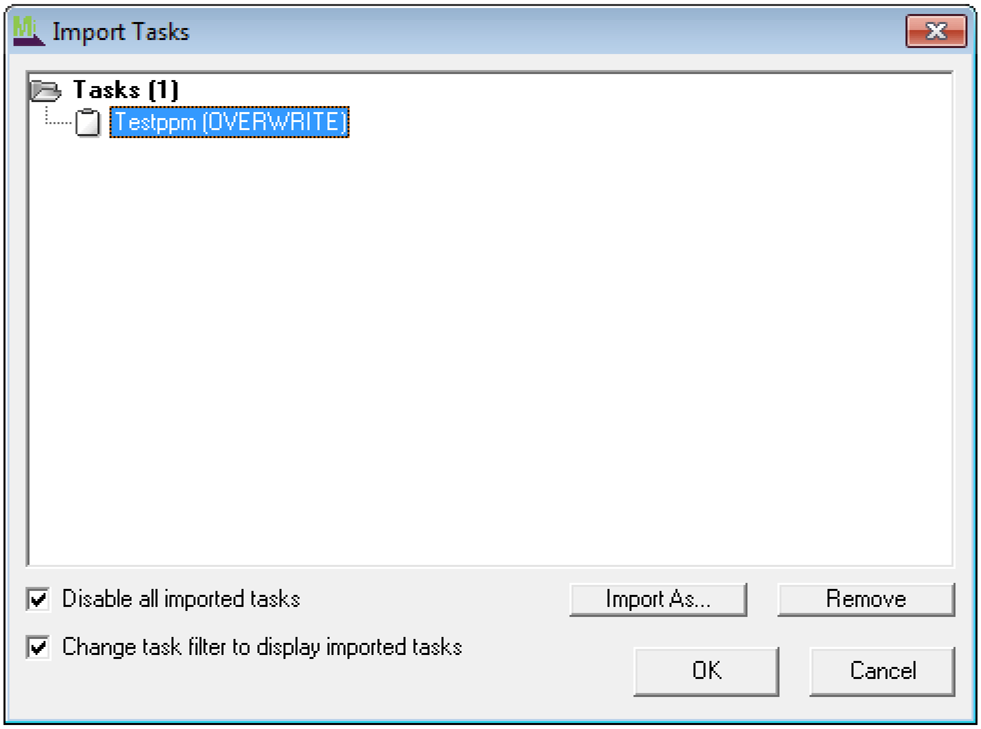
The "Options" sub-menu is available from the Admin main menu near the application title bar. All options may not be available at all times depending on user permissions and the state of communication between MOVEit Central Admin and MOVEit Central.

- **24-hour Time Display** - When checked, all times displayed in MOVEit Central Admin will be formatted as 24-hour times. (13:30 as opposed to 1:30PM)
- **Use Log Colors** - Different priority levels of log messages are shown as different colors in MOVEit Central Admin's Log window. This option may be used to turn off log colors in accordance with ADA requirements.
- **Hide Cleared Task Runs** - When checked, enables the option to select task runs in the ***Reports window*** (on page 241) and mark them as viewed ("clear" them). If the Hide Cleared Entries report filter option is set, cleared task runs will not be displayed in the task runs report.
- **Export Deleted Tasks** - When checked, MOVEit Central Admin will allow the user to export tasks before they are deleted. This applies to both single- and multiple-task deletions. Upon electing to delete one or more tasks, the user will be informed during the delete confirmation message that they will have a chance to export the tasks before they are deleted. Once the confirmation message has been accepted, the user will be prompted for a location to store the export file(s). If only a single task is being deleted, the user will be prompted to specify the location and filename of the export file. If multiple tasks are being deleted, the user will be prompted only for the location; each task will be individually exported to a separate file using the name of the task as the name of the file. As each task is successfully exported, it is then deleted. If an error occurs while exporting a task, the task is not deleted, and the deletion process stops at that point.
- **Default Report Range is Today** - When checked, MOVEit Central Admin will apply a default datetime range of "Today" to the reports filter, meaning only records added today will be displayed. This typically improves performance as the query executes faster and returns less data to be displayed. Unchecking the option will cause Admin to not apply the datetime filter, thus returning all records that match other filters in place. Note that Admin will not override an existing datetime filter if one is in place. This option only applies when a report is initially requested.
- **Reset Advanced Task Prompts** - When selected, MOVEit Central Admin will reset all preferences related to prompting the end user during the creation of Advanced Tasks to their original default values. MOVEit Central Admin will occasionally display prompt windows when adding/editing Advanced Tasks in order to assist in creating valid and/or desirable task definitions.

Tasks Menu

The "Tasks" sub-menu is ONLY available from the Admin main menu when the Tasks tab is selected. All options may not be available at all times depending on user permissions and the state of communication between MOVEit Central Admin and MOVEit Central.

- **Import Tasks** - Browses to an XML task export file and begins the import process. Once the export file has been identified, it will be loaded, and its contents displayed in the Import Tasks dialog.



Import Tasks

Tasks (1)

Testppm (OVERWRITE)

☑ Disable all imported tasks

☑ Change task filter to display imported tasks

From here, the user can see all the elements that are to be imported, and what their status is. If an element to be imported matches an existing element in the config, that element will be listed in regular text and have the phrase "(OVERWRITE)" appended to it. This indicates that that element will overwrite the existing element in the config if the user were to click the OK button. Otherwise, if an element does not match an existing element in the config, it will be listed in bold text and have the phrase "(NEW)" appended to it.

Before the import is OKed, the user may make changes to the list of elements to be imported using the Import As and Remove buttons. Any element to be imported may be removed from the import list by selecting it and clicking the Remove button. Note that this does not affect the export file, only the list of elements that will be imported into the config. Also, a user may select an element marked "(OVERWRITE)" and click the Import As button to change that element into a "new" element. This process creates a new ID for the element and prompts the user to enter a new name.

Finally, two checkbox options are available to modify the import process. The Disable All Imported Tasks option causes all task elements in the import to be marked as DISABLED once they are imported. This is useful to prevent an imported task which is not yet ready to begin production use from running before it can be edited. The Change Task Filter to Display Imported Tasks option modifies the task filter to display only the imported tasks. This makes it easier to find these tasks, especially if there are large numbers of existing tasks in the config.

- **Jump to Task** - Opens a quick search box to look for the provided search text in the current task list. This can make finding a task in a large list of tasks a little easier. Can also be opened with the hotkey sequence Ctrl-F.
- **Edit Filter** - Opens the ***Task Filter*** (on page 258) dialog.
- **Clear Filter** - Resets the ***Task Filter*** (on page 258) to show all tasks.
- **All Tasks in Filter** - All options in this submenu act against the tasks selected by the current task filter settings.
  - **Export** - Exports all currently visible tasks to an XML-formatted task export file. (The operator will be prompted for the location and filename to save to.) Related items associated with each task will also be exported, including host definitions, scripts, and certificates. PGP key and SSL certificate dependencies will also be exported. If private keys (including SSH client keys) are detected, the operator will be prompted whether they want to export private certificates/keys, and will have the option of password-protecting their private data. Note that special characters (e.g. "?" and ";") will be stripped from suggested filenames if present.
  - **Create Group** - Creates a new task group (the operator will be prompted to provide a name for the new task group) and adds all currently visible tasks as members.
  - **Enable** - Marks all currently visible tasks as ENABLED.
  - **Disable** - Marks all currently visible tasks as DISABLED.
  - **Delete** - Deletes all currently visible tasks. If the Export Deleted Tasks option is enabled, the user will be prompted to export the tasks before they are deleted. (See the ***Admin Console - Admin-Specific Options - Options Menu*** (see "***Options Menu***" on page 97) page for further details about the Export Deleted Tasks option.) Also, additional confirmation messages will appear if the current task list includes built-in tasks such as "Tamper Check".

View Menu

The "View" sub-menu is available from the Admin main menu near the application title bar. All options may not be available at all times depending on user permissions and the state of communication between MOVEit Central Admin and MOVEit Central.

- **Reports** - Opens and closes the "***Reports*** (on page 241)" window. The state of this option will be remembered between sessions.

Help Menu

The "Help" sub-menu is available from the Admin main menu near the application title bar.

- **Show Help** - Displays this help file.
- **About** - Shows the MOVEit Central Admin "About" window, which displays the version numbers of Admin and Central. Admin connects to Central to determine its version number.

Configuring Tasks

Overview

MOVEit Central **tasks** define how, where and when data is transmitted or manipulated. Traditional tasks tell MOVEit Central to pull files from specific ***sources*** (see "***Source***" on page 120) and push them to specific ***destinations*** (see "***Destination***" on page 126) at times designated by ***schedules*** (see "***Schedule***" on page 130).

Optional ***processes*** (see "***Process***" on page 132) can be added to react to or change data as it moves through MOVEit Central. Optional ***next actions*** (on page 136) can be used to react to failed, successful, or empty-handed tasks to run a different task and/or send email notifications to interested parties.

Traditional vs. Synchronization Tasks

MOVEit Central can replicate the contents of two folders to ensure the files and folder structures remain in sync. Any two folders on MOVEit Central's local hard drive, other Windows servers/shares, FTP servers, FTPS servers, SFTP servers and/or MOVEit DMZ servers may be involved in a single synchronization task.

Folder sync operations are configured in special "synchronization tasks". Instead of the sources and destinations found in a traditional task, a synchronization task consists of "Folder A", "Folder B" and a "sync direction" arrow.

More information about this can be found in the "***Synchronization*** (see "***Overview***" on page 283)" section of this documentation. Much of the information in this "Configuring Tasks" section assumes you are working with traditional tasks.

Traditional vs. Advanced Tasks

Like a Traditional Task, an Advanced Task can pull files from specific sources, push them to specific destinations, at times designated by schedules. Advanced Tasks can also use processes. In addition, an Advanced Task can use the two conditional elements (IF) and (FOR) to determine if and when the other elements are run. The conditional elements provide powerful job flow control without requiring programming or chained tasks.

Advanced Tasks provide conditional processing within a task. This means that you can build tasks that run a process, or transfer a file, after a specified condition is met, for example, files can be routed to different destinations based on the file extension.

Icon Legend

The following icons are in use throughout the MOVEit Central Admin interface to represent hosts and task steps.

Host Type	Color	Insecure Host	Secure Host	Task Source ("Download")	Task Destination ("Upload")
Windows File System	**Yellow**	🖥	- - -	⇩	⇧
MOVEit DMZ	**Green**	🖥	🖥🔒	⇩	⇧
FTP(S) Server	**Blue**	🖥	🖥🔒	⇩	⇧
SSH Server	**Purple**	- - -	🖥🔒	⇩	⇧
Mail Server	**Grey**	🖥	- - -	✉⇩	✉⇧
AS1 Partner *(via Email)*	**Grey**	AS	AS🔒	AS⇩	AS⇧
AS2 Partner *(via HTTP/S)*	**Green**	AS	AS🔒	AS⇩	AS⇧
AS3 Partner *(via FTP/S)*	**Blue**	AS	AS🔒	AS⇩	AS⇧

Different icons are also in use by tasks in different configuration and schedule states as well as the schedules which control them.

Task Type	Scheduled Task	Paused or Unscheduled Task	Incomplete Task	Schedule
Traditional Task	☑	⏸	☒	🕒
Synchronization Task	1:1 ☑	1:1 ⏸	1:1 ☒	🕒
Advanced Task	ADV ☑	ADV ⏸	ADV ☒	🕒

Process icons also vary.

Custom Process ("VBScript")	Built-In Process	Built-In Process (Missing Parameters)
⚙	◆	◆✗

Next Action icons can also take a number of different forms.

Next Action Type	On Failure (Only)	On Success (Only)	All Other Cases
Send Email	✉✗	✉✓	✉
Run Task	📋✗	📋✓	📋

Other Synchronization task icons: Instead of large colored-by-type-of-host arrows to indicate sources and destinations, synchronization tasks use colored-by-type-of-host folders. There are always two (and only two) folders listed in a synchronization task. Synchronization tasks also use small black arrows between the two folders to clearly indicate the sync direction.

🟨	**Windows File System or Share** sync folder
🟩	**MOVEit DMZ** sync folder
🟦	**FTP** or **FTPS** sync folder
🟪	**SFTP** sync folder
↓	**One-way** sync direction (from "Folder A" to "Folder B")
↓↑	**Two-way** sync direction

Advanced Tasks can also have the following icons:

File Loop	If Block	Else If	Rename Original	Delete Original
↻	IF	…	B	✗

Task Information

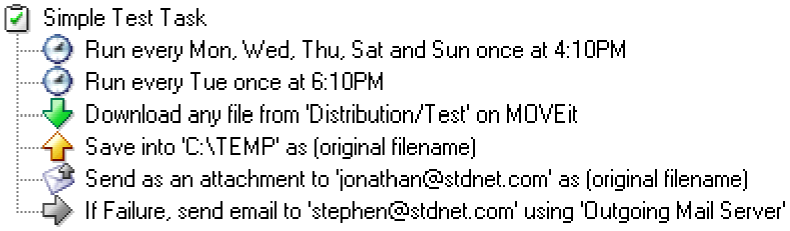
The action performed by a task and the time it is run are controlled by task **elements** such as sources, destinations, schedules, processes and next actions. A task's status (enabled or disabled), variable task parameters and other attributes are instead called task **information**.

All tasks (even ***sync tasks*** (see "***Overview***" on page 283)) are always "scheduled," "unscheduled," "disabled," or "incomplete."

An **incomplete** task is one that is incapable of being run automatically or manually. In essence, the task cannot do anything, meaning it does not have at least one process, or at least one source and destination. These tasks are marked with red X's.

Unscheduled and **disabled** tasks have at least one process, or at least one source and destination. These tasks will not be started by the scheduler or file events but can be run manually. Unscheduled tasks have no schedule. Disabled tasks usually do not have a schedule and will be marked with an extra "*** DISABLED ***" tag in their names on the Tasks tab. The primary use of the "disabled" designation is to allow operators to build and save tasks without worrying about the scheduler attempting to run unfinished configurations, and to allow operators to "pull out of production" certain tasks which they would rather not delete.

A **scheduled** task can be run either manually, or automatically. It has all necessary parts of the task defined: at least one process or at least one source and destination, and at least one schedule.

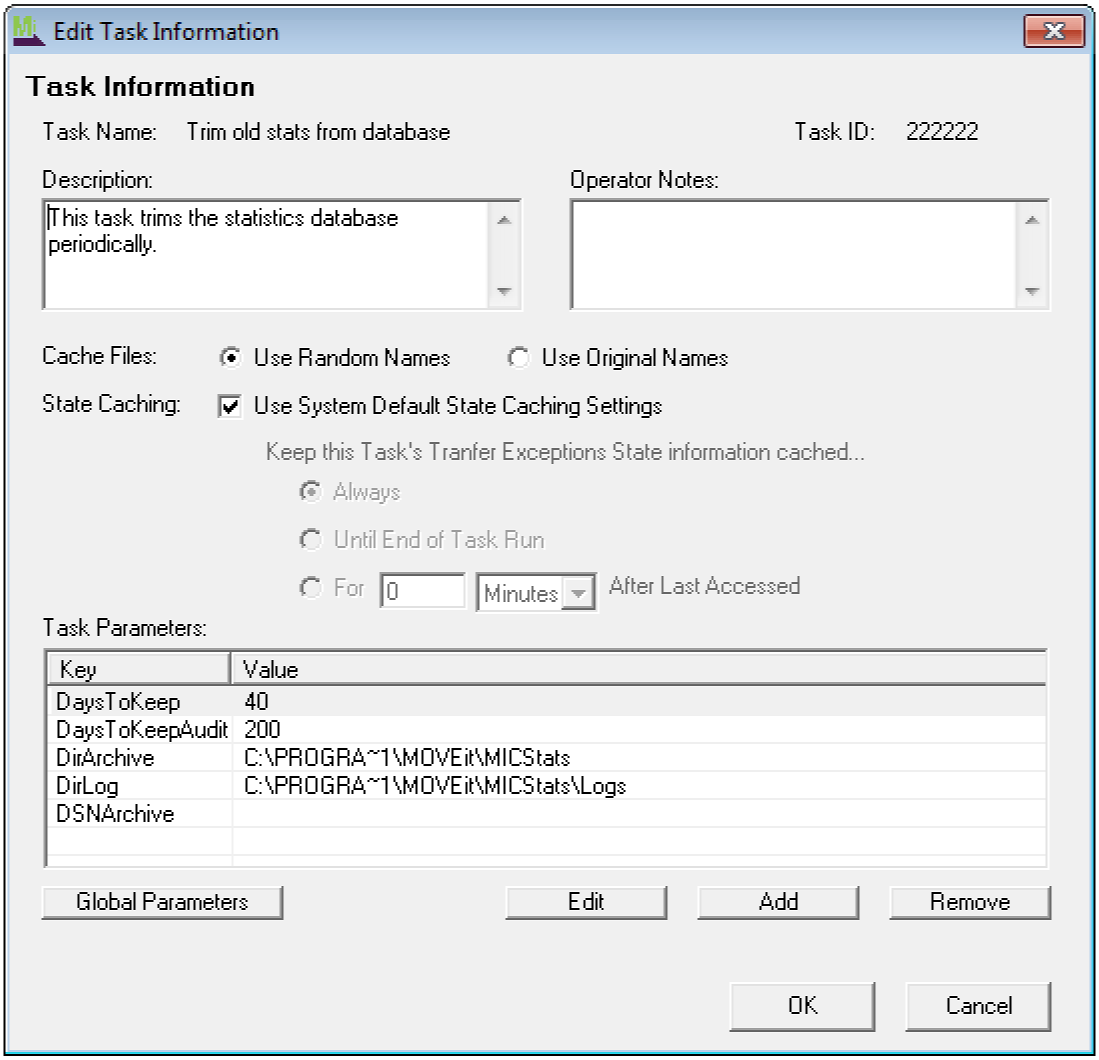


Simple Test Task
- Run every Mon, Wed, Thu, Sat and Sun once at 4:10PM
- Run every Tue once at 6:10PM
- Download any file from 'Distribution/Test' on MOVEit
- Save into 'C:\TEMP' as (original filename)
- Send as an attachment to 'jonathan@stdnet.com' as (original filename)
- If Failure, send email to 'stephen@stdnet.com' using 'Outgoing Mail Server'

A scheduled traditional task, featuring 1 source, 2 destinations, 1 next action, and 2 schedules.

Task Information

In addition to sources, processes, and destinations, tasks have several optional settings which apply to the task as a whole. These settings include a description, operator notes, cache file naming convention, state file caching, and a collection of name=value task parameters that can be accessed by scripts and macros. To access the Task Information dialog, right-click on a task and select the "Edit Task Info..." option.



Task Information

Task Name: Trim old stats from database

Task ID: 222222

Description: This task trims the statistics database periodically.

Operator Notes:

Cache Files: ● Use Random Names ○ Use Original Names

State Caching: ☑ Use System Default State Caching Settings

Keep this Task's Tranfer Exceptions State information cached...

● Always

○ Until End of Task Run

○ For 0 Minutes After Last Accessed

Task Parameters:

Key	Value
DaysToKeep	40
DaysToKeepAudit	200
DirArchive	C:\PROGRA~1\MOVEit\MICStats
DirLog	C:\PROGRA~1\MOVEit\MICStats\Logs
DSNArchive	

The description and operator notes fields can be used to contain any information about this task. The cache file setting determines whether MOVEit Central cache files will have automatically generated random names (for example, "atc0035.tmp"), or their original names, when stored in Central's cache directory for processing. If the Use Original Names option is selected, and one or more of the task sources use the "Include Subdirectories", files will be stored not only with their original name, but with the correct relative folder path as well (for example, "software\v2.6\installfile.exe"). This feature is useful when creating zip files of an arbitrary collection of files.

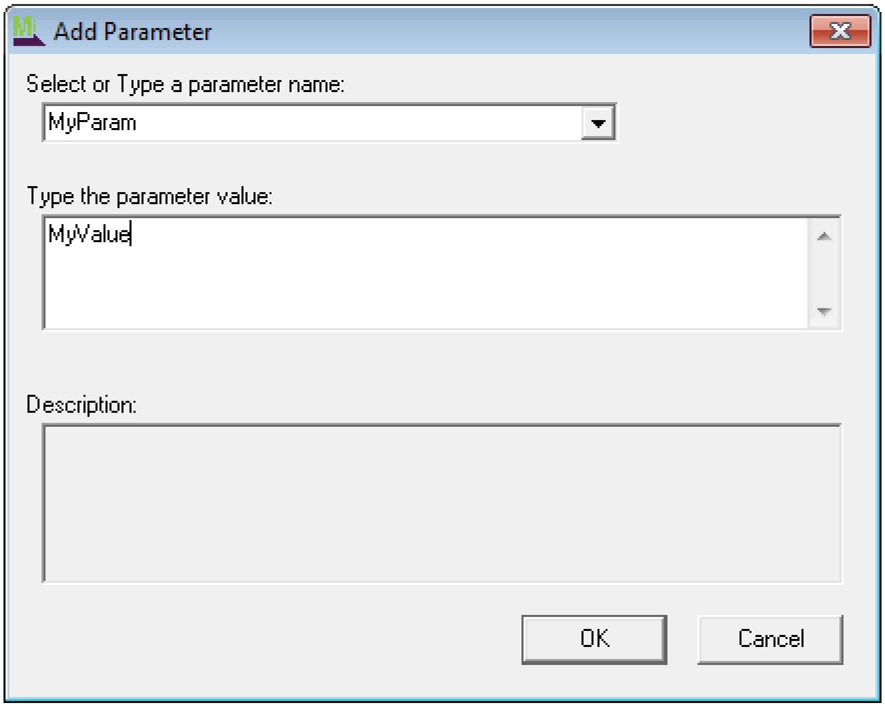
The Use Default State Caching Settings option, if checked, will cause this task to use the ***system's default State Caching settings*** (on page 234). If unchecked, the task will use the specified State Caching settings. By default, MOVEit Central always keeps state file information cached in memory in order to achieve maximum efficiency. In certain environments, however, this can become quite memory intensive. The State Caching settings can be used to remove state file information from memory after a task run or even after a specified amount of time.

Task parameters can be useful when you have a need to perform similar, but not identical, scripts processing in several different tasks. You can write a single script whose behavior is customized for the task at hand by examining task parameters.

To add a task parameter, click the Add button. This will open the Add Parameter dialog. Here, the user can enter a new parameter and a value to set for it, or select from one of the existing parameters used by any built-in processes that are loaded in MOVEit Central. Selecting an existing parameter will cause a short description of the parameter to be displayed, and, depending on the type of the parameter, change the value field to enforce specific values. Custom parameter names may only contain the following characters (including capital letters):

```
abcdefghijklmnopqrstuvwxyz._:
```

Different built-in task parameter types include the basic text type, a numeric type (which only allows entering of numbers), a choice-based type (which will display the available choices in a drop-down menu), and PGP Recipient and Sender key types. These last two types are used with PGP built-in processes to select PGP keys from the key selection dialog. Pressing the button to the right of the field will open this dialog.



Add Parameter

Select or Type a parameter name: MyParam

Type the parameter value: MyValue

Description:

Existing parameters can be edited by double-clicking on the parameter entry in the list. This will bring up a the Edit Parameter dialog, where the user can change the name or value of the parameter. Deleting a parameter can be done by selecting the parameter and clicking the Remove button.

You can read and/or set task parameters in processes with the "MIGetTaskParam" and "MISetTaskParam" commands. You can also use the value of a task parameter in any macro using "[Parm:ParameterName]" syntax.

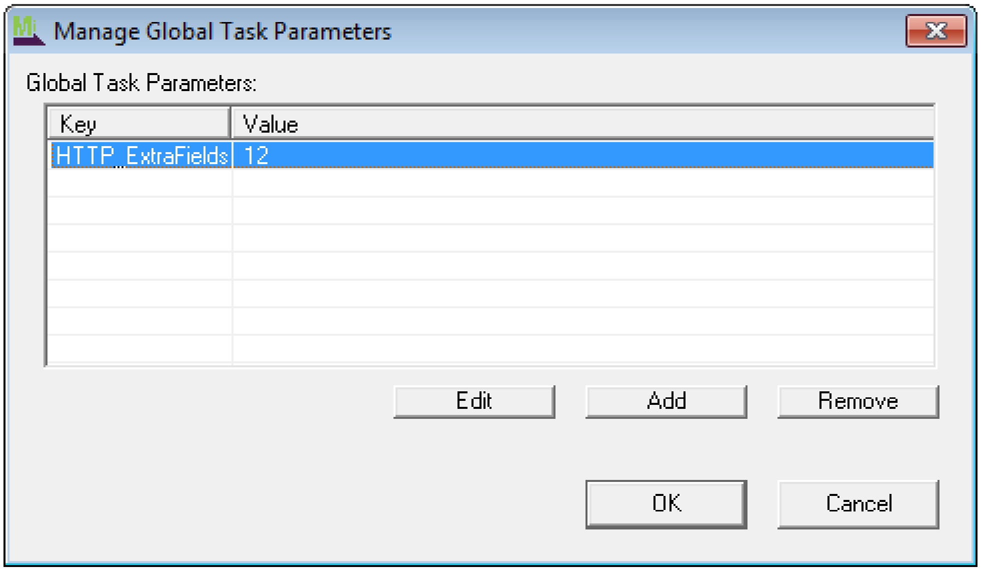
If a task parameter contains a ***macro*** (on page 137), the macro is automatically expanded when a task is run. For instance, a task parameter with a value of `The year is [YYYY]` would be treated as if it were `The year is 2005` (assuming the year is indeed 2005).

Global Task Parameters

In addition to individual task parameters, MOVEit Central also supports global task parameters that apply to all tasks. When a task makes a reference to a parameter, via either the [Parm:ParameterName] syntax or a script call to MIGetTaskParam(), MOVEit Central first looks in the information for that task for a parameter with that name. If it is found, that task parameter is used. Otherwise, MOVEit Central looks for a global task parameter with that name and uses it if available. If no parameter with that name is available, MOVEit Central uses an empty string.

Global task parameters can be useful when there are multiple tasks or Next Actions which use the same parameter. Examples of how built-in parameters can be used to define default or common settings across multiple tasks that use built-in MOVEit Central scripts include: PGP public/private key pair usually used to sign/encrypt PGP files, common ZIP process compression options, and common "email errors to" email address.

Global task parameters are either built-in parameters or custom parameters in the same way all scripts are either built-in scripts or custom scripts. By definition, a built-in global task parameter is the global setting for any parameter used by a built-in script. All other global task parameters are custom global task parameters. If a specific built-in script parameter is validated (usually, to be numeric) or selected through a drop-down menu, the built-in global task parameter will also be validated or displayed as a selectable item. (A description, if any, for built-in global task parameters will also be displayed when the item is created or changed.) The values of custom global task parameters must always be typed and are never validated.



Key	Value
HTTP_ExtraFields	12

Global task parameters are configured via the ***Settings menu*** (on page 96). The Global Task Parameters dialog is similar to the Task Parameters section of the Task Info dialog, and allows the user to add (using the same Add Parameter dialog as above), edit (using the same Edit Parameter dialog as above), or remove global parameters.

Using Global Task Parameters to Make Error Reporting Easier

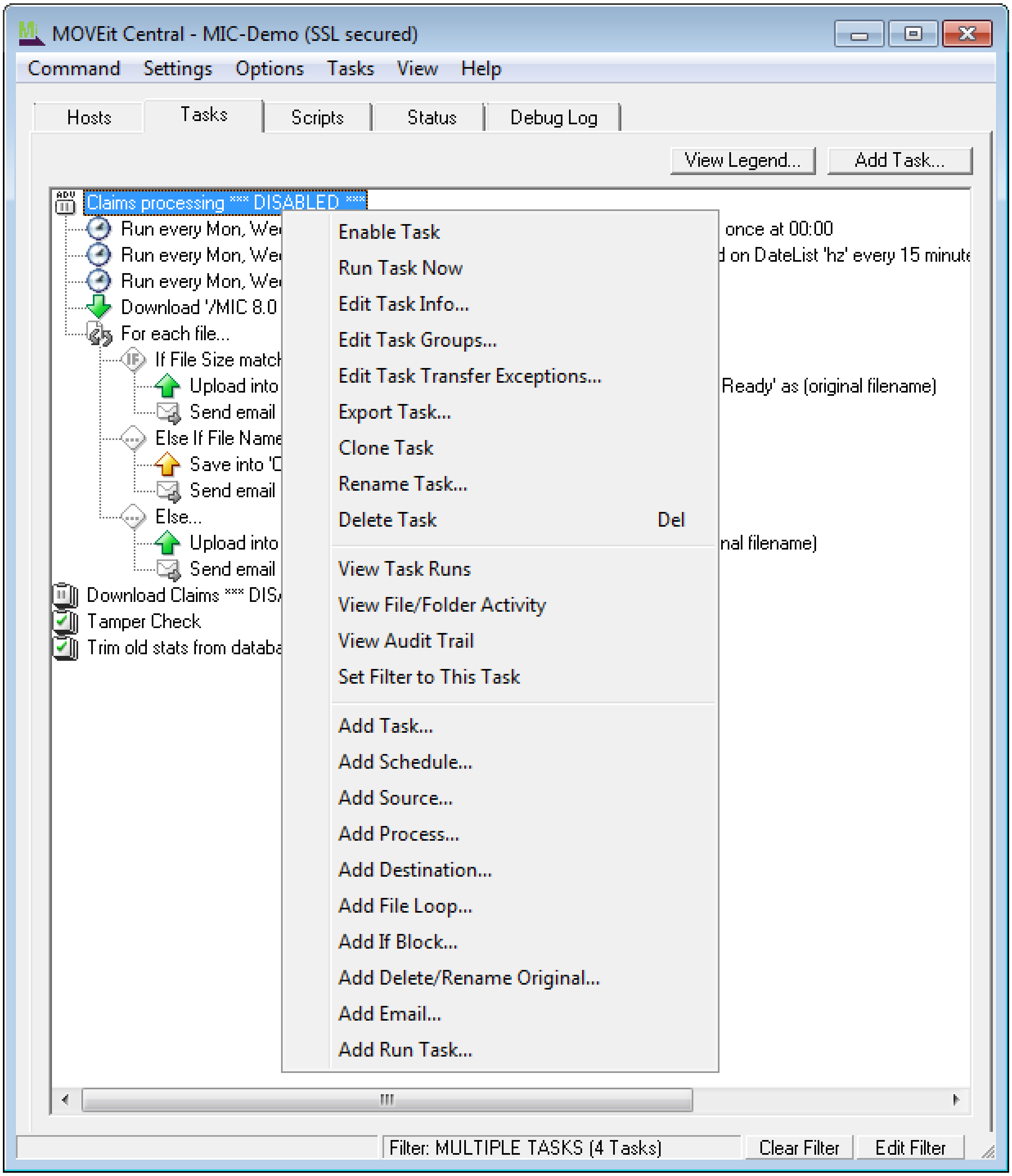
To use global task parameters to make error reporting through Next Action email messages easier, set up the following name/value pairs as global task parameters.

ERR_EMAIL =	single email address or a comma-separated list of email addresses)
ERR_SUBJECT =	ERROR - [Taskname] - [hh]:[tt]:[ss]
ERR_MESSAGE =	At [yyyy]-[mm]-[dd] [hh]:[tt]:[ss], task '[TaskName]' encountered error #[ErrorCodeFile] - [ErrorDescriptionFile] - while transporting '[OrigName]'

Then, on each task you want to send this error, set up a per-file, on errors Next Action that sends email to "[PARM:ERR_EMAIL]" with subject "[PARM:ERR_SUBJECT]" and a message "[PARM:ERR_MESSAGE]".

Tasks Tab

The Tasks tab is used to create, edit, delete, view and otherwise manage tasks. The ***"Edit Filter" button*** (see "***Task Filter***" on page 258) in the lower-left hand corner of MOVEit Central Admin should be used to filter which tasks are displayed on this page.


MOVEit Central - MIC-Demo (SSL secured)
Command
Settings
Options
Tasks
View
Help
Hosts
Tasks
Scripts
Status
Debug Log
View Legend...
Add Task...
Claims processing *** DISABLED ***
Run every Mon, We
Run every Mon, We
Run every Mon, We
Download '/MIC 8.0
For each file...
If File Size match
Upload into
Send email
Else If File Name
Save into 'C
Send email
Else...
Upload into
Send email
Download Claims *** DIS
Tamper Check
Trim old stats from databa
once at 00:00
d on DateList 'hz' every 15 minute
Ready' as (original filename)
nal filename)
Enable Task
Run Task Now
Edit Task Info...
Edit Task Groups...
Edit Task Transfer Exceptions...
Export Task...
Clone Task
Rename Task...
Delete Task Del
View Task Runs
View File/Folder Activity
View Audit Trail
Set Filter to This Task
Add Task...
Add Schedule...
Add Source...
Add Process...
Add Destination...
Add File Loop...
Add If Block...
Add Delete/Rename Original...
Add Email...
Add Run Task...
Filter: MULTIPLE TASKS (4 Tasks)
Clear Filter
Edit Filter

Note: The menu above includes the options available to Advanced Tasks. A subset of these options are available to Traditional Tasks.

A new but empty task is created simply by specifying a "friendly name" for the task. After you have created a task, you can add to it, and edit existing elements, by right-clicking on the task and selecting the proper menu item. (More than one source, destination, process, and schedule may be added.)

When adding a process, you refer to scripts you have already configured. When adding a source or destination, you refer to hosts that you have already configured. When adding a source or destination to a task, you have the opportunity to override properties of the host, such as username and password. For sources, you can also specify whether the files should be deleted from the source host after they have been transferred successfully.For destinations, you can specify the filenames that will be applied to outgoing files. You may choose to use the original name of the file, or you can use any combination of ***File Name Macros*** (see "***Macro***" on page 137), a powerful way to automate the generation of outgoing filenames.

Sources, destinations, schedules, and even entire tasks may also be cloned. Cloning creates a copy of the step that was cloned, maintaining all setting that were a part of that step. This can be useful when adding a number of very similar steps, as the operator doesn't need to enter the same information multiple times. (Process steps may not be cloned, as creating a process step involves only selecting the desired script) Cloning a task creates a copy of the entire task that was cloned, including all associated steps and schedules. The clone carries the same name as the original task with the word "Clone" appended to it and will initially be disabled to prevent the clone from working on the same files the original task should be working on.

If more than one source host is part of the task, files will be retrieved from all sources before any files are processed or sent to their final destinations. If more than one process is part of the task, the process will be run against all files that have been retrieved. If more than one destination host is part of the task, all files that have been retrieved will be sent to all hosts. If more than one schedule is part of the task, the task will run at all of the times specified by any of the schedules. (It is an "Or" rather than an "And".)

You can configure the task description, operator notes, and task parameters via the Edit Task Information dialog, accessible by right-clicking on the task in the Tasks pane.

Task Schedule Status

A task can one of three different "schedule status" values. Only "Scheduled" tasks will be run periodically by MOVEit Central's built-in scheduler or kicked off by file notification events.

- **Scheduled** (☑) - Scheduled tasks have either at least one source and one destination or at least one process. They also have a schedule. (All other elements are optional.) These are the only kind of tasks that will be run periodically by MOVEit Central's built-in scheduler or kicked off by file notification events. These tasks may also be started by "Run Now..." commands, Next Actions that kick off specific tasks or scripts that start specific tasks.
- **Disabled or Unscheduled** (⏸) - Like Scheduled tasks, Disabled and Unscheduled tasks have either at least one source and one destination or at least one process. However, neither of these kinds of tasks will be run periodically by MOVEit Central's built-in scheduler or kicked off by file notification events. Disabled tasks have been explicitly marked "Disabled" by an administrator or a task clone operation. Unscheduled tasks simply lack a schedule. In either case, these tasks may still be started by "Run Now..." commands, Next Actions that kick off specific tasks or scripts that start specific tasks. On the Tasks tab, disabled tasks may quickly be distinguished from unscheduled tasks because an additional "*** DISABLED ***" phrase will appear at the end of disabled task names.
- **Incomplete** (☒) - Incomplete tasks are missing some key task elements: either at least one source and one destination or at least one process. These tasks will not be run periodically by MOVEit Central's built-in scheduler or kicked off by file notification events. Attempts to start these tasks with "Run Now..." commands, Next Actions that kick off specific tasks or scripts that start specific tasks will fail.

Manipulating Tasks

A task can be **started** manually by right-clicking its name and choosing **Run Task Now**. Manual runs of tasks are not counted as a scheduled run, even if they take place during a schedule interval. The next scheduled run of a task will still take place.

When you are viewing the "Tasks" tab, a "Tasks" MENU option will also appear at the top of the dialog and allow you to perform actions such as importing and exporting individual tasks or task groups, or enabled and disabling all the tasks in your current view. See "***Admin Console Admin-Specific Options, Tasks Menu*** (see "***Tasks Menu***" on page 98)" for more information.

Task Permissions

Ordinarily, users wishing to edit or start tasks sign into MOVEit Central Admin with a username that belongs to the "MOVEit Admin" Windows user group. Membership in this group allows the user to edit or start any task. However, sites wishing finer-grained control over operators can use special site-specific Windows groups to control access to tasks. These groups have names starting with "MOVEit Users-". A user logging in with a Windows username that belongs to a Windows group with a name like "MOVEit Users-Detroit" (and which does not belong to the "MOVEit Admin" group) has limited capabilities. Permissions to edit and run tasks are set at the task group level (see ***User Permissions*** (on page 84)).

Task Groups

MOVEit Central Admin allows the operator to configure any number of "Task Groups" to help organize large numbers of tasks. Task groups are created and maintained using the "Task Groups" option in the ***Settings menu*** (on page 96). Once a task group is created, and tasks are added to it, the operator can select that task group in the Task Filter, and only the tasks that belong to that task group with be shown. See the ***Task Groups*** (on page 116) page for more information. Task group membership is also used in determining ***User Permissions*** (on page 84).

Viewing Task History

MOVEit Central Admin can display information about past task runs, the individual file transfers that took place during those runs, and any audit entries for a task using the database configured by MOVEit Central. From the task window, right-clicking on a task and selecting "View Task Runs" will bring up a list of past runs of a task. Selecting "View File Activity" will bring up a list of files the task has transferred. Selecting "View Audit Trail" will bring up a list of audit log entries for the task, indicating what actions have been taken against the task. Each of these reports will appear in the ***Reports Window*** (on page 241) which the focus will be moved to when one of the above options is clicked.

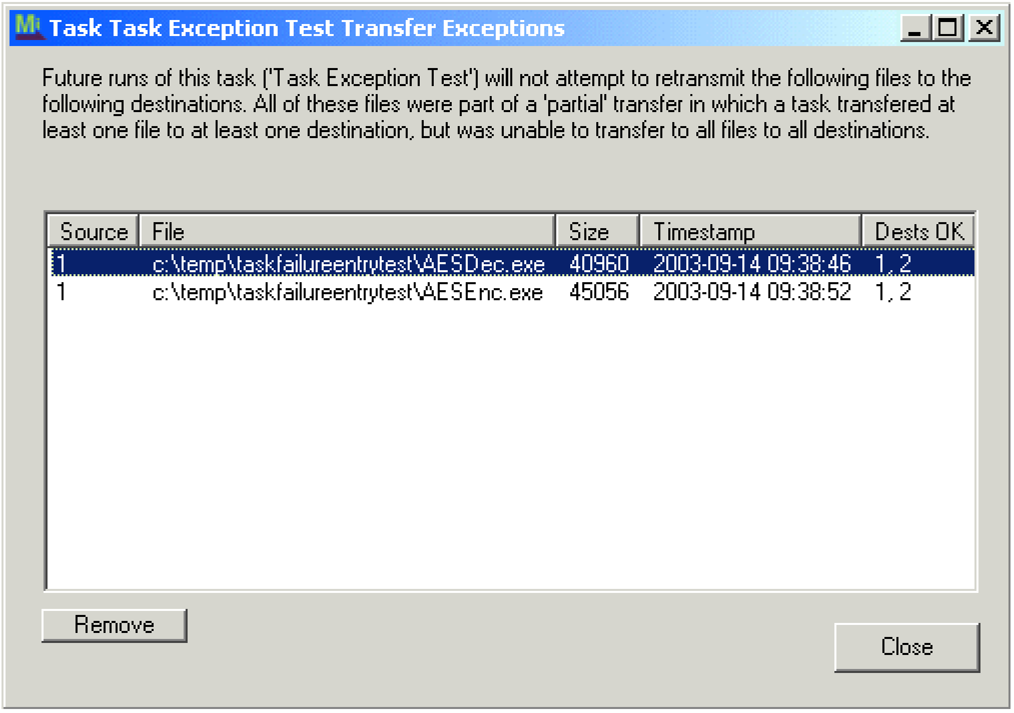
Editing Task Transfer Exceptions

The ability to edit "task transfer exceptions" is an advanced and rarely-used feature that allows you to control what a task does when it runs after a previous failure.

When a task fails after transferring some files, MOVEit Central creates an entry in its state file, listing the files that have been completely or partially processed. The next time the task runs, MOVEit Central will not perform duplicate processing on the files that were processed last time. This prevents "duplicate posting" of files. When a task succeeds, any task failure history is removed from the state file. These examples illustrate how this works:

- Let's say a task has two destinations. One day, it downloads files A and B, and sends them to destination 1 but is unable to send to destination 2. MOVEit Central will mark both these files as having been sent to destination 1, but not destination 2. Then the next time that task runs, it will download the files again but will send them only to destination 2.
- Let's say a task has one destination that is an unreliable FTP server. One day, it downloads files A and B and sends A successfully to the FTP server--but the FTP server crashes while B is being sent. MOVEit Central will mark file A has having been completely processed. Then the next time the task runs, file A will not be downloaded at all. File B will be downloaded and sent to its destination.

The "edit task transfer exceptions" feature allows you to remove entries from the list of files that have been processed by a previous, unsuccessful run of a task. Removing these entries means that the next time that the task runs, it will not remember that these files have been processed, and hence will process them again. Right-clicking on a task and choosing "Edit Task Transfer Exceptions..." brings up a dialog like this:



Future runs of this task ('Task Exception Test') will not attempt to retransmit the following files to the following destinations. All of these files were part of a 'partial' transfer in which a task transfered at least one file to at least one destination, but was unable to transfer to all files to all destinations.

Source	File	Size	Timestamp	Dests OK
1	c:\temp\taskfailureentrytest\AESDec.exe	40960	2003-09-14 09:38:46	1, 2
1	c:\temp\taskfailureentrytest\AESEnc.exe	45056	2003-09-14 09:38:52	1, 2

If the previous run of a task was successful, there will be no entries in this list. Select the entries you wish to delete and choose "Remove".

Realize that removing entries will likely cause files to be transmitted a second time. If you want to ignore a troublesome file altogether, and your source is marked "New Files Only", you can use the ***Editing Source Timestamps*** (on page 116) feature to edit the source host's timestamp to be just beyond the stamp of the troublesome file.

Editing Source Timestamps

You can modify the file that MOVEit Central uses to determine which files are new. For each combination of host, pathname, and filemask, MOVEit Central stores a date/time stamp of the most recent file in that directory that matches that mask and that has been successfully processed. For MOVEit DMZ, "Windows File System and Shares", FTP, and SSH hosts, MOVEit Central uses this information to determine whether a file is "new". This allows sources with the "Collect Only New Files" option selected to ignore old files. If you need to transfer a file again, even though it has already been processed successfully, you can edit the timestamp that applied to that file so that the file looks new to MOVEit Central.

For instance, suppose you have a task with a source that scans the FTP host "XYZ FTP Server", looking for files in path "/uploads" matching the mask "*.txt", with the "Collect Only New Files" option selected. Let's say that the task has run, and it transferred the new file report.txt that was last modified on 12 March 2004 at 2:15:00 pm. This would cause MOVEit Central to create an entry for the host "XYZ FTP Server", path "/uploads", mask "*.txt", with a most recent stamp of 2004-03-12 14:15:00. If for some reason you need to transfer the file again, running the task again will not suffice, since this file will no longer be new. One solution is to edit the timestamps for this source. In the Tasks tab, right-click the source "Download new '/uploads/*.txt' from 'XYZ FTP Server' ", and select "Edit Source Timestamps". Double-click the entry for "/uploads" with filemask "*.txt" and change the timestamp, perhaps to 2004-03-12 14:14:59. Then the next time this task is run, report.txt will appear to be new.

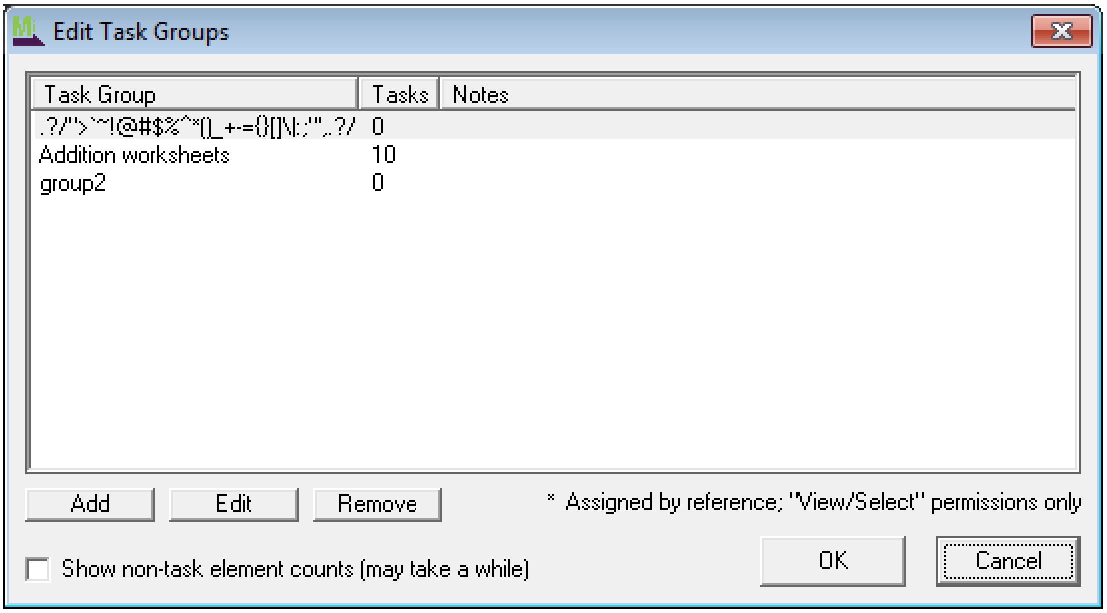
For a related, but obscure, feature, see ***Editing Task Transfer Exceptions*** (on page 114).

Task Groups

MOVEit Central Admin allows the operator to configure any number of "Task Groups" to help organize large numbers of tasks, hosts, scripts, and other elements. Task groups are created and maintained using the "Task Groups" option in the ***Settings menu*** (on page 96). Once a task group is created, and tasks are added to it, the operator can select that task group in the Task Filter, and only the tasks that belong to that task group will be shown. Task group membership is also used in determining ***User Permissions*** (on page 84).

Edit Task Groups Dialog

The Task Groups option in the Settings menu opens the Edit Task Groups dialog, where task groups are created and maintained. Here the current task groups are listed, along with the number of tasks in the group and any notes for the group. Task groups can be added, edited, and removed using the available buttons. Also, the "Show non-task element counts" option is available which causes counts of the other members of the task group to be displayed, in addition to the task counts. This option is off by default because it can take more time to compile and display this extra information.



Edit Task Groups

<table>
<tr><th>Task Group</th><th>Tasks</th><th>Notes</th></tr>
<tr><td>.?/'"&gt;`~!@#$%^*()_+-={}[]\|:;'",.?/</td><td>0</td><td></td></tr>
<tr><td>Addition worksheets</td><td>10</td><td></td></tr>
<tr><td>group2</td><td>0</td><td></td></tr>
</table>

* Assigned by reference; "View/Select" permissions only

□ Show non-task element counts (may take a while)

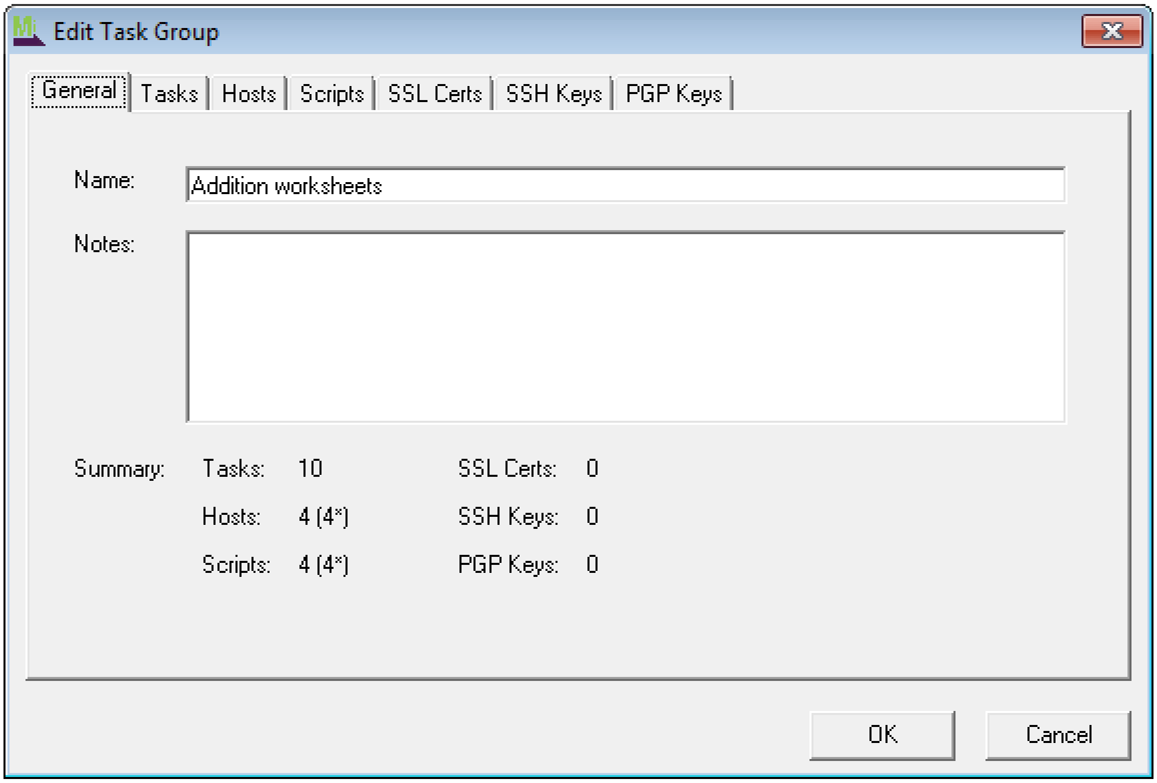
Adding and Removing Task Groups

Clicking the Add button prompts the user to enter a name for the new task group. If a valid name is entered, the new task group will be created and then opened in the Edit Task Group dialog, where the new group's settings and element memberships can be changed.

Selecting an existing task group and clicking the Remove button will cause the selected task group to be removed after a confirmation dialog is accepted.

Editing Task Groups

Double-clicking an existing task group, or selecting a group and clicking the Edit button will open the group in the Edit Task Group dialog.



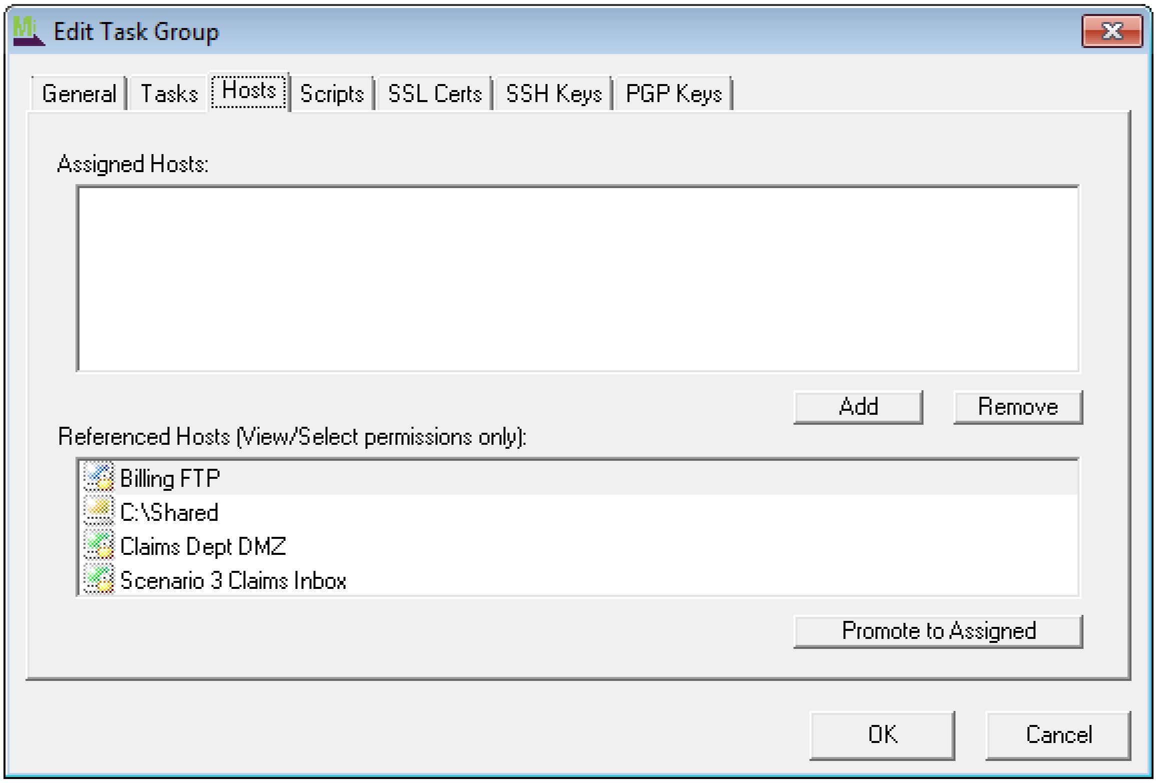
Name: Addition worksheets

Notes:

Summary:	Tasks:	10	SSL Certs:	0
	Hosts:	4 (4*)	SSH Keys:	0
	Scripts:	4 (4*)	PGP Keys:	0

The General tab is where the task name and notes can be changed. It also displays a summary of the various element memberships of the group. The summary shows how many total of each element is a member of the group. It also shows (by the asterisked number in parenthesis) how many of those elements are "referenced" members.

Task group memberships can be changed on the various other element tabs in the Edit Task Group dialog. With the exception of the Tasks tab, assigned members are show in the top list, and referenced members are shown in the bottom list. On the Tasks tab, only assigned tasks are displayed. Assigned members can be added and removed using the Add and Remove buttons. Referenced members can be promoted to assigned members using the Promote to Assigned button.



Referenced vs. Assigned Members

There are two types of members in task groups. First is an assigned member, meaning an administrator has explicitly added that element as a member of a task group. All tasks are assigned members, since they are the foundation of task groups. Other elements may be assigned on that element's associated tab.

The other member type is a referenced member. These members are not explicitly assigned, but are still considered members of the group because they are referenced by another member. For example, a task that has a source or destination that uses a specific host is said to "reference" that host. If that host is not an assigned member of a task group that task is a member of, it will be listed as a referenced member.

Referenced members cannot be explicitly added or removed from a task group, though they can be promoted to assigned members. Referenced members exist in order to provide read-only access to necessary task elements when using User Permissions. They are displayed as ghosted elements in the Referenced window on each element tab, except the Tasks tab.

Task Elements

This section describes the elements of tasks that define how, where and when data is transmitted or manipulated.

Source

A source is a reference to a host which defines a single location from which files are obtained for use in a task. A task may be configured with an unlimited number of sources.

Common Source Options:

- **Folder(s) -** Indicates the folder name or path in which MOVEit Central should look for files on the remote host. Note that to reference a remote filesystem share, you must have selected the MOVEit Central host that corresponds to that filesystem share. You may use ***Macros*** (see "***Macro***" on page 137) in this field.

  For filesystem, MOVEitDMZ, FTP, and SSH hosts, you may use wildcards here. For example, "/home/jal/data*/reports" will match any folder named "reports" which is a direct subfolder of a folder whose name starts with "data" and which is a subfolder of /home/jal. For example, both /home/jal/data/reports and /home/jal/dataaccounting/reports match, but /home/jal/reports does not.

Additionally, a special MOVEit Central-specific "**" wildcard operator is available. "**" matches any number of intermediate subfolders. For instance, "/home/jal/**/reports" matches any folder named reports which is a direct or indirect subfolder of jal. The folders /home/jal/data1/2005/07/reports, /home/jal/2005/reports, and /home/jal/reports all match this folder specification, but /home/jal/2005/report1 and /home/jal/2005/reports/mydata do not. (However, that last folder would match if "Include Subdirectories" were checked.) Note that a trailing ** means the same thing as checking "Include Subdirectories"; e.g. /home/jal/2005/** means the same thing as /home/jal/2005 with "Include Subdirectories" checked.

Full UNC paths cannot be used here when using the local filesystem host. In order to use a remote filesystem by UNC or mounted drive letter, the host must be added as a Share to the hosts list. If a UNC is entered, MOVEit Central Admin will attempt to find a matching Share host to use instead, and prompt the user to use that host.

- **Ignore Folder(s)** - When this option is checked, one or more folder masks may be entered. (See "Folders" above for exact syntax.) When MOVEit Central finds a folder name that matches one of the entered masks while searching subfolders recursively, it will be ignored. Note that the folder mask(s) match against the names of sub-folders in the current folder being searched, therefore the folder mask(s) should reflect folder names and NOT full or relative folder paths. You may use ***Macros*** (see "***Macro***" on page 137) in this field.
- **File(s)** - The filename (i.e. "readme.txt") or filemask (i.e. "*.txt") MOVEit Central should use to select files on the remote host. You may use Macros in this field.

There are two special wildcard characters:

*, which matches zero or more characters at that position in the filename

?, which matches exactly one character at that position in the filename

You may use multiple wildcard characters in a single mask.

For example, a*.rpt matches a.rpt, a1.rpt, and apple.rpt, but not apple.rp or lemon.rpt.
a?.rpt matches a1.rpt and aQ.rpt, but not a.rpt, a12.rpt, or a1.rp

You may also use multiple filenames or filemasks, separated by semi-colons (";"). The semi-colons act as an "Or" operator. For instance, the filemask "fred*.*;*.zip" will match fred7.txt and will also match sally.zip.

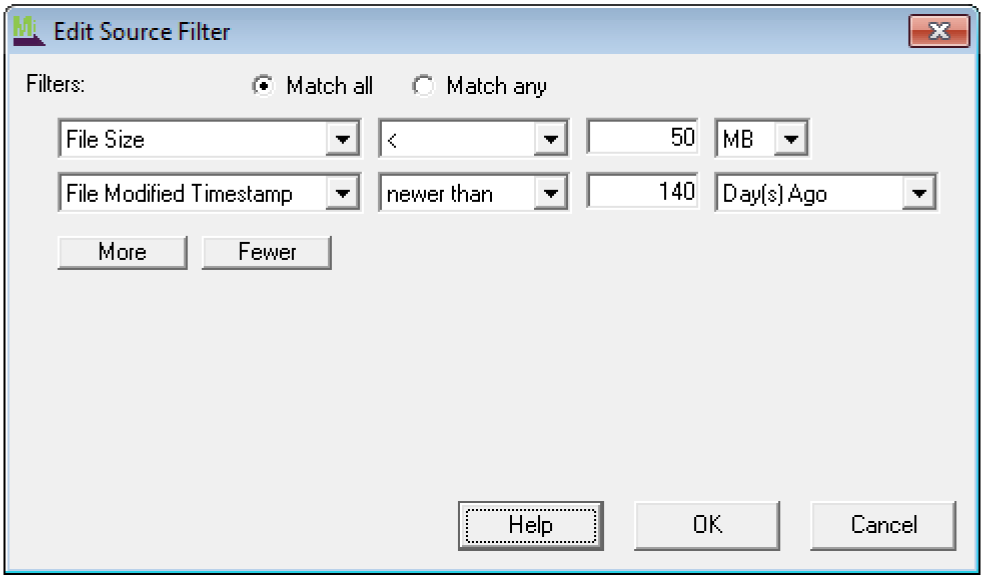
The ampersand operator ("&") acts as an "And" operator unless it is preceded by $. ("$&" means to match an ampersand literally.) For instance, given a filemask of "*.txt&ready.dat&final.log", MOVEit Central will not process any files on the source location unless "ready.txt", "final.log" and at least one "*.txt" file are available. A semi-colon (";") has a higher precedence than "&", so "*.txt;*.doc&*.zip" means "either *.txt or *.doc, AND ALSO *.zip".

If you want the task to wait until all filetypes in the mask are available from the source, also choose **Retry If No Files Found**.

Note: If the filemask on an existing source is changed, and the **Collect Only New Files** option is enabled, a confirmation message will be displayed warning the user that changing the filemask while collecting only new files could cause old files to be downloaded from the source host. This is because file collection timestamps are stored by filemask internally in MOVEit Central. Changing the filemask negates existing timestamps.

- **Ignore File(s)** - When this option is checked, one or more file masks may be entered. (See "Files" above for exact syntax.) When MOVEit Central finds a file that matches one of the entered masks, it will be ignored. Note that the ampersand operator ("&") has no context in this field and is therefore always treated as a literal. You may use ***Macros*** (see "***Macro***" on page 137) in this field.
- **Special Filter(s)** - When this option is checked, you may specify filters that allow MOVEit Central to select files based on their size and date/time of last modification.

  Filters are built in a pop-up window accessed through the nearby "Edit" button. Supported size filters are expressed in your choice of bytes, KB, MB or GB. Supported date/time filters are expressed the difference between now and some other date in hours, days, months or years. A "match all/any" selection controls whether files must match all or just one of the filter criteria.



Edit Source Filter

Filters: ● Match all ○ Match any

File Size	<	50	MB
File Modified Timestamp	newer than	140	Day(s) Ago

- **"Browse" Button** - The Browse button provides an easy way to select a folder on the remote host, which will automatically fill the Folder Name field. Files on the remote host can also be selected, which will automatically fill the Filemask field. If your source simply needs to download a specific file from a specific directory on the host, the Browse button is the easiest configuration method to use. If you need a more complex mask, however, the Filemask and Folder Name fields can still be edited after being filled by the Browse button.

  NOTE: If the source is using an FTP or SSH host with the Blind Downloads option enabled, the Browse button will not be available. Blind Downloads are used when the client is not allowed to do directory listings, or directory listings will not appear correctly. The Browse button usually will not function correctly in these situations, so it is disabled.

NOTE: browsing will not work if the username or password fields contain references to certain types of macros, such as non-global task parameters.

- **Collect Only New Files** - When checked, picks only those files that are "new" off the remote server. For filesystem, FTP, and SSH hosts, MOVEit Central maintains a database of most recent timestamps by host, directory, and filemask. See ***Editing Source Timestamps*** (on page 116) for how to edit this database. For MOVEit DMZ hosts, MOVEit Central versions prior to 3.2 relied upon MOVEit DMZ's interpretation of which files are new. Starting in version 3.2, MOVEit Central relies upon MOVEit DMZ's definition of newness only until the first new file is downloaded for any given folder. After that, MOVEit Central will use the same new file definition used by the other source types. In the case of filesystem files, MOVEit Central will use the Last Modified stamp when determining newness.

Note: State information for the "Collect Only New Files" option is now saved on a per-Task basis rather than per-Host. This change has been made in order to address various issues related to State files growing too large. Now, if the task has run previously and sent files, the files will be resent initially after turning on the option, if they still exist on the source.

- **After Successful Transfer** - Indicates what MOVEit Central should do with an original file if all process and destination steps are completed without problems. The selected action (if any) will be performed on a per-file basis as soon as MOVEit Central has delivered it or processed it through all steps successfully; there is no "mass delete" or "mass rename" step performed against source files. The options are:
  - **Do Nothing** - this is the default.
  - **Delete original(s)** - Delete the original file from the source. (This is an effective way to prevent "double-posts".)
  - **Rename original(s)** to: - Renames the original files to the given name. The name you specify may contain macros, such as [OrigName]. Some hosts (especially FTP hosts) will permit you to move source files across folders using this option and properly formatted paths.

  See ***POP3 Sources*** (on page 411) for the special case of deleting POP3 messages.
- **Include Subdirectories** - When checked, MOVEit Central will search subdirectories of the given folder for files matching the given file mask, in addition to the given folder itself.
- **Expand compressed (zip) file(s)** - When checked, tells MOVEit Central to attempt to uncompress any files ending in a .zip extension.
- **Retry If No Files Found** - If checked, times out and retries a directory listing if the previous listing was successful but resulted in no matching files. The usual retry count and retry timeout are used. This feature can be used to "wait" for a file to appear during the running of a task. If the maximum number of retries is reached and still no matching files are found, the task continues with the next step with no error flagged.

  If unchecked, a directory listing returning no files is not retried, and as a result, no files are downloaded from this source.

- **Sign On With Default Username** - If checked, this task will use the usual username and password for this host. If unchecked, operators may specific alternate credentials to use for this transfer.
- **Use Default Connect Timeout** - Gives the option to override the Connect Timeout setting for the specified host and set a different value. If this option is not checked, MOVEit Central will use the value entered in the Connect Timeout field. The Connect Timeout setting specifies how many seconds MOVEit Central will wait when attempting to connect to the host.
- **Use Default Data Timeout** - Gives the option to override the Data Timeout setting for the specified host and set a different value. If this option is not checked, MOVEit Central will use the value entered in the Data Timeout field. The Data Timeout setting specifies how many seconds MOVEit Central will wait when sending data to or receiving data from the host.
- **Use Default Retry Count** - Gives the option to override the Retry Count setting for the specified host and set a different value. If this option is not checked, MOVEit Central will use the value entered in the Retry Count field. The Retry Count setting specifies how many times MOVEit Central will attempt a step if it fails.
- **Use Default Retry Timeout** - Gives the option to override the Retry Timeout setting for the specified host and set a different value. If this option is not checked, MOVEit Central will use the value entered in the Retry Timeout field. The Retry Timeout setting specifies how many seconds MOVEit Central will wait between retry attempts of a step.

Specialized Source Options:

- **Sign On with Default Username** (*MOVEit DMZ, FTP, and SSH servers only*) - If checked, tells the program to sign on with the username and password configured in the host. If not checked, tells the program to use the username and password specified in the **Username** and **Password** boxes. In the case of FTP servers, this also applies to the little-used **Account** field. These fields may contain macro references.
- **Use Default Server Transfer Type** (*FTP servers only*) - If checked, causes MOVEit Central to use the transfer type configured in the host. If not checked, causes MOVEit Central to use the type (ASCII vs. Binary) selected.
- **Use Default FTP Transfer Mode** (*FTP servers only*) - If checked, causes MOVEit Central to use the transfer mode configured in the host. If not checked, causes MOVEit Central to use the mode (Active vs. Passive) selected. Passive is generally preferred, but not all servers support passive mode.
- **Transfer - Reuse SSL Session for Data Connections** *(FTP SSL servers)* - If checked, forces data connections to use the same SSL session as the existing control connection, which overrides the default unchecked setting on the Hosts Advanced options configurations. This allows you to comply with partner server settings that require reuse of an SSL session for data connections.
- **Use Default XSHA1 Setting** (*FTP servers only*) - If checked, causes MOVEit Central to use the XSHA1 setting configured in the host. If not checked, causes MOVEit Central to use the settings value selected.
- **Additional commands to execute before transfer** (*FTP servers only*) - "quote" commands to send to the server before each file is downloaded. This is in addition to the per-connection before-each-file "quote" commands specified in the host configuration. Macros may be used in this field.

- **Additional commands to execute after transfer** *(FTP servers only*) - "quote" commands to send to the server after each file is downloaded. This is in addition to the per-connection after-each-file "quote" commands specified in the host configuration. Macros may be used in this field.
- **Use Default Blind Download** (*FTP and SSH servers only*) - If checked, causes MOVEit Central to use the "blind downloads" setting configured in the host. If not checked, causes MOVEit Central to use the mode selected. This rarely-used setting is intended for unusual servers that have problematic implementations of commands like CWD and LIST commands.
- **Sign On with Default Client Key** (*SSH servers only*) - If checked, causes the public key defined in the host configuration to be used for authentication. (If no public key is configured, then public key authentication will not be used.) If unchecked, operators may choose an alternate public key using the "..." button. Most SSH servers require either a password or a client key; a few require both.
- **Sign On with Default Client Cert** (*MOVEit DMZ and FTP servers only*) - If checked, causes the SSL client certificate defined in the host to be used when connecting to the host. (If no client certificate is configured, then none will be used.) If unchecked, operators may choose an alternate certificate using the "..." button. See ***SSL Client Certificates*** (on page 217).
- **Rescan before Xfer** (*Filesystem, FTP and SSH servers only*) - This option helps prevent MOVEit Central from downloading "incomplete" files from servers that make such files available for download before they are closed. It specifies that once one or more files matching the download criteria have been identified, MOVEit Central should rescan the directory, looking for changes in the files' size and date. If a file has changed, the behavior of the task will be different depending on the task type:
    - Traditional/Advanced tasks: The file will be removed from the list of files to download. The purpose of this feature is to detect when another application is currently changing the files, so that MOVEit Central will not download a partial file. The value is the number of seconds to wait between scans.
    - Sync tasks: The task will continue rescanning until the files have have not changed in successive scans. If files are continuously changing, this option should not be used, or the task may get stuck. The purpose of this feature is to detect when the source has "settled down," so that the task does not need to run multiple times to capture and sync all of the changes in a directory.

      The value is the number of seconds to wait between scans. The default is 0, which deactivates the feature .A reasonable value for when you do need the feature might be 5 or 10 seconds. (This setting will be overriddent if specified in any source related to this host.)
- **MD5 Checking** (*FTP and SSH servers only*) - Specifies whether MOVEit Central should look for an MD5 file, containing MD5 hashes of source files on the FTP server, and what that MD5 file should be called (see the ***FTP Source Integrity*** (on page 399) page for more information). The following settings are available for checking for an MD5 file:
    - **Never** - Central will not look for an MD5 file.
    - **If Present** - Central will look for an MD5 file. If the file contains a hash for a source file, Central will check the file against the hash. If the file matches the hash, Central will allow the file to continue, otherwise it will generate an error. If Central does not find a hash for the source file, it will allow the file to continue.

  - **Required** - Central will look for an MD5 file and generate an error if it is not found. All files downloaded will be checked against the MD5 file. If a file does not match its hash, or a hash does not exist for the file, Central will generate an error.
- **Download Limits** (*MOVEit DMZ, FTP, SSH, and filesystem only*) - Limits the number of files that Central will download from this source in a single task run. The limit can be by file count or by byte count. In the case of a limit by byte count, Central will stop downloading files after the first file that causes the number of downloaded bytes to exceed the configured limit. A value of 0 means no limit. If Use Default is checked, the defaults configured for the associated host are used; otherwise, the values specified in the source are used.

  If the Re-Run Task Automatically option is enabled, Central will automatically re-run the task if the configured limits are exceeded, allowing Central to pick up the remaining source files without waiting for the next scheduled run of the task. Note that if this option is enabled and neither the Collect Only New Files or Delete/Rename After Successful Download options are enabled, the task could potentially end up looping indefinitely. For this reason, MOVEit Central Admin will display a warning message if it detects this condition while a source is being edited.
- **Use Default UNC Transfer Type** (*Share hosts only*) – If checked, causes MOVEit Central to use the Use Windows CopyFile API setting configured in the host. If not checked, causes MOVEit Central to use the selected Use Windows CopyFile API setting. By default, MOVEit Central uses the Windows CopyFileEx function to download files from UNC shares. Under certain conditions, the performance of this function can potentially suffer, especially when transferring large files. If bad performance is being experienced when downloading files from this UNC host, deselecting the Use Windows CopyFile API for UNC Transfers setting may help remedy the situation.

See also ***AS1, AS2, AS3*** (see "***AS1, AS2, AS3 (Enterprise Only)***" on page 148).

Destination

A destination is a reference to a host which defines a single location to which files will be sent. A task can have zero or more destinations. If there are no destinations, there must be at least one process for a task to be eligible to run (be "ready").

Common Destination Options:

- **Folder Name** or **Path** - Indicates the folder name or path in which MOVEit Central should save files on the remote host. You may use ***Macros*** (see "***Macro***" on page 137) in this field.

  Full UNC paths cannot be used here when using the local filesystem host. In order to use a remote filesystem by UNC or mounted drive letter, the host must be added as a Share to the hosts list. If a UNC is entered, MOVEit Central Admin will attempt to find a matching Share host to use instead, and prompt the user to use that host.

- **Filename** - The filename (i.e. "readme.txt") MOVEit Central should use to save files on the remote host. You may use Macros in this field.
- **"Browse" Button** - The Browse button provides an easy way to select a folder on the remote host, which will automatically fill the Folder Name field. If your destination simply needs to upload to a specific directory on the host, the Browse button is the easiest configuration method to use. If you need a more complex configuration, however, the Folder Name field can still be edited after being filled by the Browse button.

Note: browsing will not work if the username or password fields contain references to certain types of macros, such as non-global task parameters.

- **Use Original File Name(s)** - Indicates whether or not MOVEit Central should save the file with the name under which it was saved on the source. If this option is not checked, MOVEit Central will use the name defined in the Filename field. This name may contain macros.
- **Overwrite Setting** - Indicates how MOVEit Central should handle situations in which the files already exist on the destination. The available options depend on the host type.

  For MOVEit DMZ servers, the option is a checkbox:

  - **Overwrite Existing File(s) of Same Name** - Indicates whether or not MOVEit Central should silently overwrite existing files. If this option is left unchecked, the destination transfer will fail with a message indicating that the file already exists on the destination host.

    Important: Although it is unlikely that you would use FTP or SSH to upload to MOVEit DMZ, be aware that append is not supported in MOVEit DMZ.

  For FTP and SSH servers, and the filesystem, the options are:

  - **Overwrite existing file(s) of same name** - If a file already exists, it will be overwritten; otherwise, a new file will be created. This is the default.
  - **Leave existing file(s) of same name alone** - If a file already exists, the destination transfer will fail with a message indicating that the file already exists on the destination host.
  - **Append to existing file(s) of same name** - For both downloads and uploads, if a file already exists, the data being transferred will be written to the end of that file. For downloads, if the file does not already exist, a new file will be created. For uploads, if the file does not already exist, an error message is displayed, and a new file is not created.

    Note: If Append is chosen, and an error occurs while attempting to append, then no further appends will be attempted on the destination during that task run. This is to prevent appends from being attempted out-of-order.

- **Compress File(s) (Zip format)** - When selected, this will cause MOVEit Central to compress the file using Zip compression. Note: each file is individually compressed and a ".zip" extension is used in place of the filename extension specified in the "Filename" field. (For example, a value of "[OrigName]" in the "Filename" field will cause the zipped files to be saved as "[OnlyName].zip" . If the filename is "test.txt", then the zipped file would be "test.zip".) Use the ***Zip Advanced*** (on page 210) built-in script to zip multiple files together, and/or apply a password.
- **Use Relative Subdirectories** - When selected, and if one or more source elements have the "Include Subdirectories" option selected, files found in subdirectories of the source folder will be uploaded to the same subdirectory they were found in on the destination host.
- **Create Directories if Necessary** - If checked, causes MOVEit Central to create the directory named in "Path" (or the relative subdirectory if "Use Relative Subdirectories" is enabled) if it does not exist. Otherwise, if the server directory does not exist, the transfer fails.
- **Use Default Connect Timeout** - Gives the option to override the Connect Timeout setting for the specified host and set a different value. If this option is not checked, MOVEit Central will use the value entered in the Connect Timeout field. The Connect Timeout setting specifies how many seconds MOVEit Central will wait when attempting to connect to the host.
- **Use Default Data Timeout** - Gives the option to override the Data Timeout setting for the specified host and set a different value. If this option is not checked, MOVEit Central will use the value entered in the Data Timeout field. The Data Timeout setting specifies how many seconds MOVEit Central will wait when sending data to or receiving data from the host.
- **Use Default Retry Count** - Gives the option to override the Retry Count setting for the specified host and set a different value. If this option is not checked, MOVEit Central will use the value entered in the Retry Count field. The Retry Count setting specifies how many times MOVEit Central will attempt a step if it fails.
- **Use Default Retry Timeout** - Gives the option to override the Retry Timeout setting for the specified host and set a different value. If this option is not checked, MOVEit Central will use the value entered in the Retry Timeout field. The Retry Timeout setting specifies how many seconds MOVEit Central will wait between retry attempts of a step.

Specialized Destination Options:

- **Optional Note** (*MOVEit DMZ servers only*) - The comment to associate with files uploaded to this destination. This note will appear in the Web interface to MOVEit DMZ when the user is viewing details of a file.
- **Sign On with Default Username** (*MOVEit DMZ, FTP, and SSH servers only*) - If checked, tells the program to sign on with the username and password configured in the host. If not checked, tells the program to use the username and password specified in the **Username** and **Password** boxes. In the case of FTP servers, this also applies to the little-used **Account** field. These fields may contain macro references.
- **Use Default Server Transfer Type** (*FTP servers only*) - If checked, causes MOVEit Central to use the transfer type configured in the host. If not checked, causes MOVEit Central to use the type (ASCII vs. Binary) selected.

- **Use Default FTP Transfer Mode** (*FTP servers only*) - If checked, causes MOVEit Central to use the transfer mode configured in the host. If not checked, causes MOVEit Central to use the mode (Active vs. Passive) selected. Passive is generally preferred, but not all servers support passive mode.
- **Transfer - Reuse SSL Session for Data Connections** *(FTP SSL servers)* - If checked, forces data connections to use the same SSL session as the existing control connection, which overrides the default unchecked setting on the Hosts Advanced options configurations. This allows you to comply with partner server settings that require reuse of an SSL session for data connections.
- **Use Default XSHA1 Setting** (*FTP servers only*) - If checked, causes MOVEit Central to use the XSHA1 setting configured in the host. If not checked, causes MOVEit Central to use the settings value selected.
- **Additional commands to execute before transfer** (*FTP servers only*) - "quote" commands to send to the server before each file is uploaded. This is in addition to the per-connection before-each-file "quote" commands specified in the host configuration. Macros may be used in this field.
- **Additional commands to execute after transfer** (*FTP servers only*) - "quote" commands to send to the server after each file is uploaded. This is in addition to the per-connection after-each-file "quote" commands specified in the host configuration. Macros may be used in this field.
- **Use Default Blind Upload** (*FTP servers only*) - If checked, causes MOVEit Central to use the "blind uploads" setting configured in the host. If not checked, causes MOVEit Central to use the mode selected. This setting is intended for unusual servers that have problematic implementations of commands like CWD and LIST commands.
- **Sign On with Default Client Key** (*SSH servers only*) - If checked, causes the public key defined in the host configuration to be used for authentication. (If no public key is configured, then public key authentication will not be used.) If unchecked, operators may choose an alternate public key using the "..." button. Most SSH servers require either a password or a client key; a few require both.
- **Sign On with Default Client Cert** (*MOVEit DMZ and FTP servers only*) - If checked, causes the SSL client certificate defined in the host to be used when connecting to the host. (If no client certificate is configured, then none will be used.) If unchecked, operators may choose an alternate certificate using the "..." button. See ***SSL Client Certificates*** (on page 217).
- **Use Default File Attribute Settings** (*SSH servers only*) – If checked, causes MOVEit Central to use the File Attribute settings configured in the host. If unchecked, causes MOVEit Central to apply the specified Unix-style file attributes to a file after a successful upload. This setting only affects hosts that are based on Unix-like file systems.
- **Use Default UNC Transfer Type** (*Share hosts only*) – If checked, causes MOVEit Central to use the Use Windows CopyFile API setting configured in the host. If not checked, causes MOVEit Central to use the selected Use Windows CopyFile API setting. By default, MOVEit Central uses the Windows CopyFileEx function to upload files to UNC shares. Under certain conditions, the performance of this function can potentially suffer, especially when transferring large files. If bad performance is being experienced when uploading files to this UNC host, deselecting the Use Windows CopyFile API for UNC Transfers setting may help remedy the situation.

See also ***AS1, AS2, AS3*** (see "***AS1, AS2, AS3 (Enterprise Only)***" on page 148).

Schedule

A **schedule** specifies when the task will be run. A task may have more than one schedule associated with it, but must always have at least one in order to be run automatically. Tasks can also be run manually by the operator; a task need not have a schedule to be run manually.

How Schedules Work

MOVEit Central checks for new tasks to run once a minute. Each time a check occurs, the scheduler scans all tasks to see which ones are eligible to run this minute. A task is eligible to run if ANY of its schedules lists the current minute as a valid time to run. The same task will not be run multiple times in a minute, even if more than one of its schedules matches the current minute.

If the ***Maximum Running Tasks*** (see "***Related Settings***" on page 229) setting is 0, which is the default, then all eligible tasks are started simultaneously. Otherwise, the scheduler will immediately start only as many eligible tasks as it can without exceeding the specified maximum number of simultaneous tasks. The other tasks will be queued, and will be run as soon as currently-running tasks complete. In any case, each task runs in its own thread so as not to interfere with any other task.

A task will not be run if a previous copy of the task is still running. Missed runs will be "made-up" the next time that the scheduler runs and sees that another copy of the task is not running. However, no more than one missed run will be made up. For instance, if a task is scheduled to be run at 9:00, 9:05, 9:10, 9:15, and 9:20, and the 9:00 task takes 16.5 minutes to run, then the 9:05 and 9:10 runs of the task will be skipped. At 9:17, the scheduler will run the 9:15 task two minutes late.

The scheduler will never run a task that was scheduled to run prior to the time that MOVEit Central was started. So, in the above example, if MOVEit Central is started at 9:17, it would not run the task until 9:20, completely skipping the 9:00, 9:05, 9:10, and 9:15 runs.

Schedules and Event-Driven Tasks

Schedules also control when event-driven tasks are run. Events that arrive for an interested task will be ignored unless they arrive during a scheduled window of time. "Missed" files are handled by an automatic task run performed automatically when the task enters its next scheduled window.

For example, consider a task listening for events every day from 3am to 7am. A file arrives at 2am; this file is ignored and the task is not started at that time. At 3am MOVEit Central automatically runs the task to look for missed files, finds the "2am file" and downloads it. A second file arrives at 4am. As soon as this file is complete, MOVEit Central runs the task to download it. Finally, a third file arrives at 8am. This file is ignored; unless manual action is taken this file will automatically be picked up by the task tomorrow morning.

The "Run even if notifications are enabled for the host" scheduling option (discussed below) allows you to schedule tasks on a periodic and event-driven basis. To schedule a task to ignore file events, you must set it up to "run once" at specific times.

At startup, and when a secondary failover node becomes primary, MOVEit Central will run all event-driven tasks whose schedule covers the current date and time. It does this to ensure that files that arrived when Central was not running will be processed.

Configuring Schedules

Unlike hosts and scripts, schedules are part of a task, not separate entities that are simply referred to by tasks.A schedule specifies both the days a task should run and the times it should run.

Specified days can be either days of the week (Sunday, Monday, Tuesday, etc.), days of the month (1-28), or a pre-configured ***Date List*** (on page 144). Days of the week and days of the month can only be positively added to a schedule; you can not tell a schedule NOT to run on a day of the week or month. Date Lists can be added to a schedule either positively or negatively; a date list can either tell Central to run a task on the specified days, or not run a task on the specified days. A negatively added date list will overrule all other days in the schedule.

Times are expressed either as one specific time of day, or a range: every X minutes between two times of the day.

For example, specifying "Monday and Tuesday", and "Every 30 minutes between 3:00PM and 4:00PM" means that the task will run every Monday at 3:00PM, 3:30PM, and 4:00PM, and every Tuesday at 3:00PM, 3:30PM, and 4:00PM.

If you want a task to run at two dissimilar times, for example, Mondays at 8:00AM and Thursdays at 11:00AM, two separate schedules will be required, one for each day.

Schedule Options

In addition to the time-of-day settings, schedules may contain these options:

- **Repeat only until first success**. If this option is chosen, the task will be run at the normal intervals as long as no previous run in that schedule has successfully downloaded and processed files. Once a task succeeds in retrieving and processing at least one file, all further runs in that schedule are suppressed until the next day. This feature can be useful in reducing the load on remote servers, and on MOVEit Central itself, if you know that only one batch of files will appear within a given time range. This option is ignored if all sources are subject to ***file notifications*** (on page 160).
- **Log failure if no files found during scheduled run**. If this option is chosen, then during the last run of a task during the schedule, the run will fail if no runs during that schedule have succeeded in downloading and processing at least one file. This can be useful if, for instance, you expect a customer to place a file on a server every Friday between 1:00AM and 5:00AM. You can schedule a task to run, say, every 10 minutes during that time. If by the last run in that period (at 5:00 AM), no file has appeared, MOVEit Central will declare that run to have failed. If you choose this option, you will probably want to designate a Next Action / Failure setting for the task.

- **Run even if notifications are enabled for the host**. If this option is chosen, then the task will be run according to this schedule even if all associated source hosts have file notifications enabled. See ***file notifications*** (on page 160) for more information.

Multiple Copies of a Task

Although the scheduler will not run a task if a copy of the task is already running, it is possible to run multiple simultaneous copies of a task outside the scheduler. A second or subsequent instance of a task can be run in these cases:

- AS2 receives
- Manual (and Central API automated) task starts
- Next Actions
- When the "Re-run task automatically if limits are encountered" option in Download Limits is selected

This capability was introduced in MOVEit Central 5.5.

Process

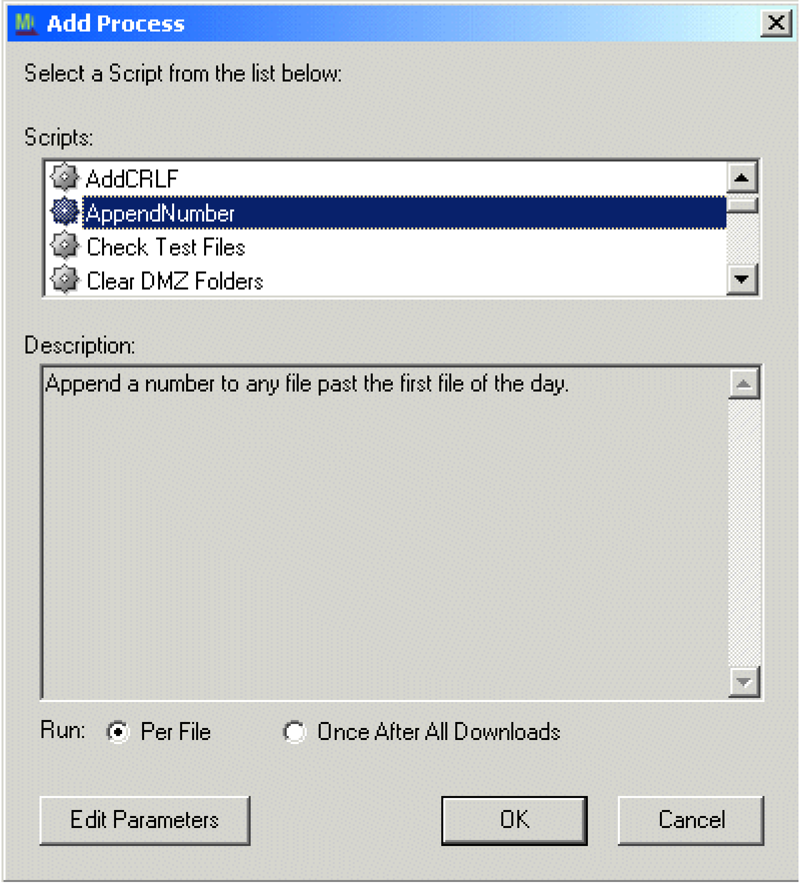
Processes allow administrators to configure specific file manipulation or processing behavior into MOVEit Central tasks. A single process runs a single built-in script or custom (VBScript) script. Processes are also frequently used to run command-line applications or scripts.

Behind the scenes, MOVEit Central runs built-in scripts and custom scripts in a very similar manner, but way the two types of scripts are updated and configured is quite different.

Built-in scripts have been written, tested and documented by Ipswitch. They cannot be changed by MOVEit Central users but they are automatically updated with each new release of MOVEit Central. MOVEit Central Admin is aware of the parameters each script requires and provides a clickable, often drop-down interface for operators to add and configured built-in scripts as a part of their MOVEit Central tasks. Global built-in script parameters also benefit from the same clickable, user-friendly interface.

Custom scripts are VBScripts which have been manually coded and imported into MOVEit Central through the "Script" panel of the "Settings" page. (Custom scripts are available only in MOVEit Central Enterprise.) Custom script parameters must be configured through the "Task Info..." dialog or manually keyed in as global custom script parameters.

Command-line applications and scripts are typically invoked by selecting MOVEit Central's "Command Line App" built-in script and specifying both the application and command-line parameters to be used when calling the application.



Append a number to any file past the first file of the day.

Run Per File vs. Run Once After All Downloads

Both built-in scripts and custom scripts offer a "Run" option which indicates whether this particular script should be run against each file or only after all files have been downloaded from all sources. Typically, the "Run" option should be set to "Per File"; "Once After All Downloads" is handy when a task needs to do something like zipping multiple files into a single archive.

Setting the option to Per File causes the process to be run once for each file downloaded from all sources, before the file goes out to any destination hosts. If there are no sources, the process will be run once.

Setting the option to Once After All Downloads causes the process to run once, and only once, after all source files have been downloaded, and before any files are uploaded to any destination hosts. The process will be run once even if no files have been downloaded. Such a process can determine whether any files were downloading by looking to see whether the **MICacheFiles**() function returns an empty string.

Built-in scripts feature an "Edit Parameters" button which will allow operators to select required and optional parameters for the selected script from a drop-down menu.

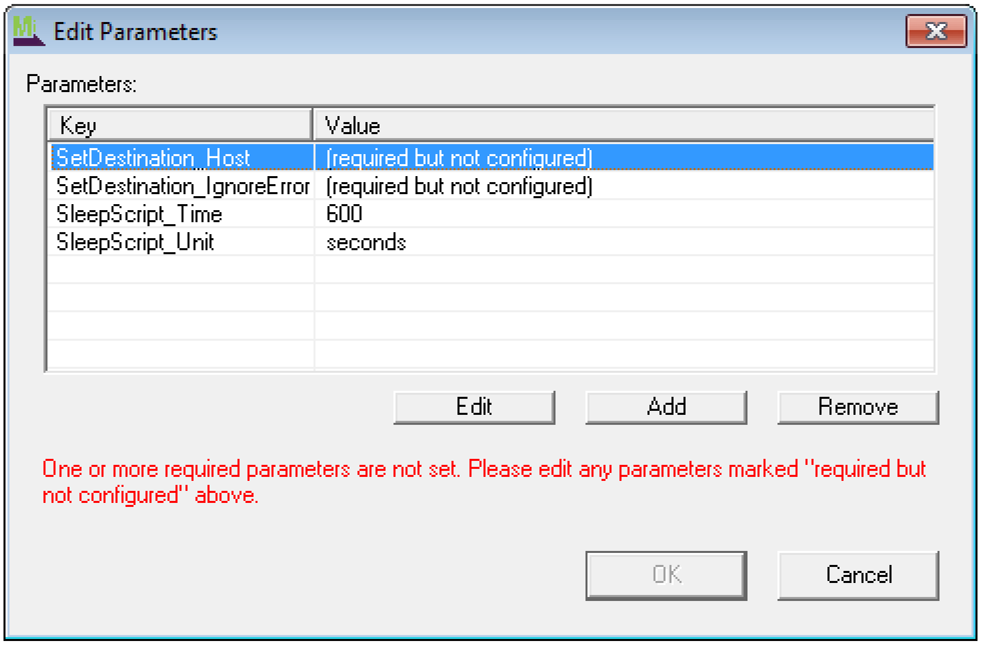
This Script Behaves As A Destination

MOVEit Central will refuse to download a file if a previous run has already sent it to all destinations. Unfortunately, the logical result of this is that if there are no destinations, by definition the file has already been sent to all of them. This means that if a task has no destinations but does have processes, and one fails, then the downloaded files are not downloaded again next time.

Check this box to force this process step to behave as a destination when you have a transfer exception. This will cause files to be downloaded if the process failed last time.

Edit Parameters

The Edit Parameters button on the Add/Edit Parameters dialog provides access to the parameters currently configured for the selected task. If a built-in script has been selected, and one or more required parameters have not been set, the user will be forced into the Edit Parameters dialog upon clicking OK in the Add/Edit Parameters dialog.



Key	Value
SetDestination_Host	(required but not configured)
SetDestination_IgnoreError	(required but not configured)
SleepScript_Time	600
SleepScript_Unit	seconds

One or more required parameters are not set. Please edit any parameters marked "required but not configured" above.

The Edit Parameters dialog is similar to the ***Global Parameters*** (on page 108) dialog, and allows the user to add, edit, or remove task parameters. For custom scripts, all parameters are treated as strings. For built-in scripts, parameters may be one of several types: strings, numbers, drop-down selections and keys/certificates. (Operators will be given a browse dialog to select appropriate PGP keys, SSL certificates, etc.)

Furthermore, for built-in scripts, parameters may be marked as required, meaning that you must have either a global parameter or a task-specific parameter of that name before the process will be allowed to run. The dialog will inform the user if any required parameters have not been set either globally or on the selected task. The user will not be able to leave the dialog through a click of the "OK" button until all required parameters are set. Double-click parameters in the list marked "(required but not configured)" to set their values.

Next Action

A next action setting defines an action to take following the completion of a task. The action can be to either send an email message to a specified recipient or list of recipients, or to run another task.

A next action setting can be configured to run after any combination of the following task results:

- **Success** - The task found files to operate on and successfully operated on them.
- **Failure** - The task found files to operate on but failed to operate on them.
- **No Action** - The task did not find any files to operate on or the files it found were "ignored" by a process.

A next action can also be configured to run after the Task, which will cause the next action to run once after completion of the entire task, or after Each File, which will cause the next action to run after each file is completely processed.

When sending an email following completion of a task, there are four settings to configure:

- **SMTP Host** - The SMTP host to use for sending email. At least one SMTP host must be configured in the Hosts section in order to send an email.
- **AddressTo** - A single email address or a comma-separated list of email addresses to send an email to. You may use Macros in this field.
- **Subject** - Subject of the email message. You may use Macros in this field.
- **Message** - Main body of the email message. You may use Macros in this field.

When starting another task following completion of a task, there are two settings to configure:

- **Task To Run** - The task to run.
- **Parameters** - A list of task parameters to forward on to the next task. Adding and removing parameters from the list can be done using the Add and Remove button below the list.

If the selected task is already running when MOVEit Central tries to start it via Next Action, MOVEit Central will wait until the running instance of the task is completed before it starts the task.

Using Error Macros in Next Actions

As of MOVEit Central 3.2, the built-in "[Error..." macros can be used to send the error code and description of any error which happened in the subject or body of a Next Action notification.

For example, a Next Action message body of:

```
At [yyyy]-[mm]-[dd] [hh]:[tt]:[ss], task '[TaskName]' encountered error
#[ErrorCodeFile] - [ErrorDescriptionFile] - while transporting '[OrigName]' (FYI,
the current task error is #[ErrorCodeTask] - [ErrorDescriptionTask])
```

...will be interpreted as:

```
At 2005-01-07 12:37:26, task 'Test Error Macros' encountered error #2234 - CopyFile
returned Access is denied. - while transporting 'readme.txt' (FYI, the current task
error is #2234 - CopyFile returned Access is denied.)
```

If you settle on a preferred combination of messages using error macros, you may want to propagate their use by setting them up as ***Global Parameters*** (on page 108) and configure your tasks' Next Actions to work off global parameters rather than a different message for each task.

Next Action Tips

Please note that Next Actions can by themselves generate failures. For example, if a task successfully transfers 5 files but cannot send the email to notify the operator, then the whole task will be marked failed. To prevent this kind of behavior, be sure to point your mail host to a reliable external server or to the localhost SMTP server when using email-based Next Actions.

Macro

Macros are not really a type of host element, but are instead configuration snippets used in source, destination and next action elements to represent dates, times, filenames and task parameters. For example, a task using a macro of "data[yyyy].log" would run against a value of "data2003.log" instead.

Macros can be used in the following places:

- Source Folder Name
- Source Filemask
- Destination Path
- Destination Filename
- Email Message Address To
- Email Message Subject
- Email Message Body
- FTP QUOTE Fields
- Parameters consumed by built-in or custom scripts

Macro keywords are always found in square brackets ("[","]"). Macro arguments (usually a DateSpec or an integer) follow macro keywords after a colon (":").

In some cases, task or global parameters may contain macros. These are still interpreted as macros. For example, if a global parameter named "Error_Subject" is set with a value of "ERROR in '[TaskName]' at [hh]:[mm]:[ss]", a Next Action subject set to "[Parm:Error_Subject]" would be interpreted as "ERROR in 'Get TPS Reports' at 12:34:56" when the task is run.

Macro Keywords

Attribute	Description	Applicable Host Types
DestFileName	The filename of the most recent destination file, not including any directory names. For example: "report12.txt". This is used primarily in per-file Next Actions.	All
DestFolderPath	The folder path, including all folder components but not the filename, of the most recent destination file. For example: "/pub/reports". This is used primarily in per-file Next Actions.	All
ErrorCodeFile	The last error code encountered for the current file, or 0 if no error. See "***Next Actions*** (on page 136)" for an example of how to use this macro to report errors.	All
ErrorDescriptionFile	The last error description encountered for the current file, or empty if no error. See "***Next Actions*** (on page 136)" for an example of how to use this macro to report errors.	All
ErrorCodeTask	The last error code encountered for this task, or 0 if no error. See "***Next Actions*** (on page 136)" for an example of how to use this macro to report errors.	All
ErrorDescriptionTask	The last error description encountered for this task, or empty if no error. See "***Next Actions*** (on page 136)" for an example of how to use this macro to report errors.	All
FileDateStamp	The date stamp of the file as recorded by the source, in the form YYYY-MM-DD HH:MM:SS. Not all sources provide date stamps. When using this macro in a destination filename or folder name, you will usually want to combine it with macro string functions. For example, "[LEFT([FileDateStamp],10)]" will yield the "YYYY-MM-DD" date part and "[MID([FileDateStamp],12,2)]" will yield the hour from the original source file's date and time information.	Filesystem, FTP (most), MOVEit, SSH
FileSize	The size of the file, in bytes, as recorded by the source. Note: some unusual FTP servers do not provide the file size; in these cases, a size of 0 will be used.	Filesystem, FTP (most), MOVEit, SSH

Attribute	Description	Applicable Host Types
FolderID	Unique number identifying a MOVEit folder. For example: "1236518".	MOVEit
FolderName	Name of remote folder. Note that this macro returns only the "last" part of the path. Example: Given a full remote path of "frog\dog\cat", this macro returns "cat".	Filesystem, FTP, MOVEit, SSH
FullPath	The full path of the file as it was on the source, including all directories and the filename.	Filesystem, FTP, MOVEit, SSH
ID	Unique number identifying a MOVEit file. For example: "251660214".	MOVEit
NominalStart	Time this task was "officially" started in "YYYY-MM-DD HH:MM:SS" format (e.g., "2006-07-18 11:33:16"). This value combined with the TaskID will yield a key that uniquely identifies a single task run (e.g., in the "stats" database table).	All
OrigComment	The upload comment specified when the file was uploaded. (This is often blank.)	MOVEit
OrigName	Original name of this file. Example: "Example.txt"	Filesystem, FTP, MOVEit, SSH
OrigUser	The username of the user who uploaded the file	MOVEit
OrigUserEmail	The email address of the user who uploaded the file	MOVEit, POP3
OrigUserFull	The full name of the user who uploaded the file	MOVEit
OrigUserID	The UserID of the user who uploaded the file, if the MOVEit DMZ host is version 5.5 or later. If the MOVEit DMZ host is an earlier version, this will be the empty string. (The UserID is typically a long string starting with the username; a typical UserID might be "fred9zyupmuxa6dk".)	MOVEit

Attribute	Description	Applicable Host Types
OnlyName	The original filename minus the extension and the period. Example: Given "frog.txt", this macro returns "frog".	Filesystem, FTP, MOVEit, SSH
OnlyExt	The original filename extension. Example: Given "frog.txt", this macro returns "txt".	Filesystem, FTP, MOVEit, SSH
Parm:*ParmName*	Returns the task parameter named ParmName. If there is no such parameter, the empty string is returned.	All
RelativePath	The pathname of the directory for this file, relative to the originally specified source path. This applies only when Include Subdirectories is selected, and cannot be used for source paths. For instance, if the source path is C:\outgoing and the file in question is C:\outgoing\reports\Fred.txt, then when used in a destination path, [RelativePath] is "reports".	Filesystem, FTP, MOVEit, SSH
Rnd	A random decimal number. Use the format [Rnd:len] where len is the desired number of digits. The random number generator is of cryptographic quality.	All
SyncReport()	Synchronization tasks offer a special "[SyncReport()]" macro that allows a complete report of all synchronization actions to be sent in a Next Action email notification. Please see the ***Synchronization - Next Actions*** (see "***Next Actions***" on page 294) documentation for more information.	Next Actions Following Sync Tasks
TaskID	The ID of the task that is running. This number is used internally in the configuration files and the database to identify tasks. A typical value would be a nine-digit number such as "618116254".	All
TaskName	The name of the task that is running	All

Attribute	Description	Applicable Host Types
TaskStatus	The status of the task that is running. This string will have one of three values: "Success" if the task encountered no errors and processed at least one file or ran at least one script, "Failure" if the task encountered one or more errors, or "No xfers" if the task encountered no errors but did not process any files or run any scripts.	All
Date specification (see below)	Current date and time. Example: Given a time of "10:06" and a macro of "[HH][TT]", the macro will return "1006".	Filesystem, FTP, MOVEit, SSH
Macro function (see below)	Returns the results of a string operation	All

Examples: (Given "January 3, 2002 13:11:01", original filename="myfile.txt")

- "[WW][AAA].[OnlyExt]": 00Thu.txt
- "gotit[JJJ]-[YYYY].log": gotit002-2002.log
- "[OrigName]": myfile.txt
- "[OnlyName]_[MM]-[DD]-[YY].[OnlyExt]": myfile_01-03-02.txt
- "ReallyBigText [AAA], [MM]-[DD]-[YY]": ReallyBigText Tue, 01-03-02

Macro Date and Time Syntax

The Macro Date and Time Syntax allows operators to specify how date and time elements should be represented in their filenames and messages. The different types of date/time elements supported include day-of-week, day-of-month, day-of-year (aka "Julian"), hour, minute, second, month, week-of-year and year.

Operators such as the minus sign normally apply to all times and dates in a macro phrase. To apply operators to only part of a macro phrase, use double-quotes to delimit phrases. For example, if today is currently July 5, 2007, a macro of:

- [dd][mm-][yyyy] [dd][mm][yyyy] yields 05062007 05062007
- "[dd][mm-][yyyy]" [dd][mm][yyyy] yields "05062007" 05072007

Attribute	Description
A	DAY-OF-WEEK; minimal numeric. Example: "2" (Sunday=0)
AAA	DAY-OF-WEEK; three-letter abbreviation. Example: "Tue"
AAAA	DAY-OF-WEEK; full. Example: "Tuesday"
B	DAY-OF-WEEK; minimal numeric. Example: "2" (Sunday=1)
D	DAY-OF-MONTH; minimal representation. Example: "7"
DD	DAY-OF-MONTH; two-digit representation. Example: "07"
H	HOUR; minimal representation, 24-hour clock. Example: "7"
HH	HOUR; two-digit representation, 24-hour clock. Example: "07"
HHH	HOUR; minimal representation, 12-hour clock. Example: "7"
HHHH	HOUR; two-digit representation, 12-hour clock. Example: "07"
II	am/pm; two-digit representation of "am" or "pm" designation. Example: "pm"
J	JULIAN DATE; minimal representation. Example: "7" First day of year is 0.
JJJ	JULIAN DATE; three-digit representation. Example: "007" First day of year is 0.
K	JULIAN DATE; minimal representation. Example: "7" First day of year is 1.

Attribute	Description
KKK	JULIAN DATE; three-digit representation. Example: "007" First day of year is 1.
M	MONTH; minimal numeric representation. Example: "7" First month is 1.
MM	MONTH; two-digit numeric representation. Example: "07" First month is 1.
MMM	MONTH; short representation. Example: "Jan"
MMMM	MONTH; full representation. Example: "January"
S	SECOND; minimal representation. Example: "7"
SS	SECOND; two-digit representation. Example: "07"
T	MINUTE; minimal representation. Example: "7"
TT	MINUTE; two-digit representation. Example: "07"
W	WEEK-OF-YEAR; minimal representation. First week is numbered 0. Example: "2"
WW	WEEK-OF-YEAR; two-digit representation. First week is numbered 0. Example: "02"
X	WEEK-OF-YEAR; minimal representation. First week is numbered 1. Example: "2"
XX	WEEK-OF-YEAR; two-digit representation. First week is numbered 1. Example: "02"
YY	YEAR; two-digit representation. Example: "02"
YYYY	YEAR; four-digit representation. Example: "2002"
+	The "+" symbol following any date designation will increment the current date by one unit of time, namely amount of time implied by the designation. The entire date is affected, with rollover from day-to-day, month-to-month, year-to-year, etc. as required. A + after a day designation increments the date by one day; a + after a month designation increments the date by one month, etc. For instance, on June 30, 2003, "[MMM] [DD], [YYYY]" is rendered "Jun 30, 2003", but "[MMM] [DD+], [YYYY]" is rendered "Jul 1, 2003".
-	The "-" symbol following any date designation will decrement the current date by one unit of time, namely the amount of time implied by the designation. The entire date is affected, as with "+". Hence, [MMM-] decrements the date by one month, etc.

Macro Functions

Macro functions are built-in functions that perform string operations on their arguments.

These functions are patterned after the identically-named functions in Basic.

Macro function references must start with a [, then the name of the function, then a (.

Function name	Description
LEFT(arg, count)	Returns the leftmost "count" characters of "arg". If arg is less than count characters long, the entire string is returned.
LEN(arg)	Returns the number of characters in "arg", as a decimal number.
MID(arg, start, count)	Returns "count" characters from "arg", starting at position "start" (where 1 is the first character). If ", count" is omitted, then the function returns the characters starting at "start" and going through the end of "arg". For example, if the original filename is ABCDE.TXT, then the value of the macro [MID([OrigName], 2, 3)] is BCD and the value of [MID([OrigName],2)] is BCDE.TXT.
RIGHT(arg, count)	Returns the rightmost "count" characters of "arg". If arg is less than count characters long, the entire string is returned.

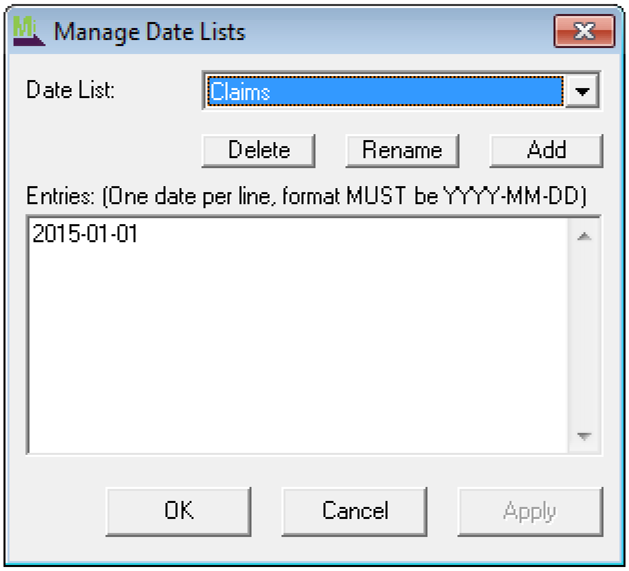
Date List

In addition to day-of-the-week and day-of-the-month schedule processing, MOVEit Central can also run tasks (or keep from running tasks) on days specified in a Date List. Date lists are simply that, lists of dates. These date lists are created separately from tasks, similarly to scripts, and referenced by schedules that use them.

Creating, editing, and removing date lists can be done from the Date List Manager in MOVEit Central Admin. The Manager can be accessed from the ***Settings menu*** (on page 96).

Adding a Date List

To add a new date list, click the Add button in the Date List Manager. Enter a name for the new date list when prompted. Choose a descriptive name, so that users setting up schedules will know what the date list contains. After choosing a name, the date list will be created.



Date List: Claims

Entries: (One date per line, format MUST be YYYY-MM-DD)

2015-01-01

Populating a Date List

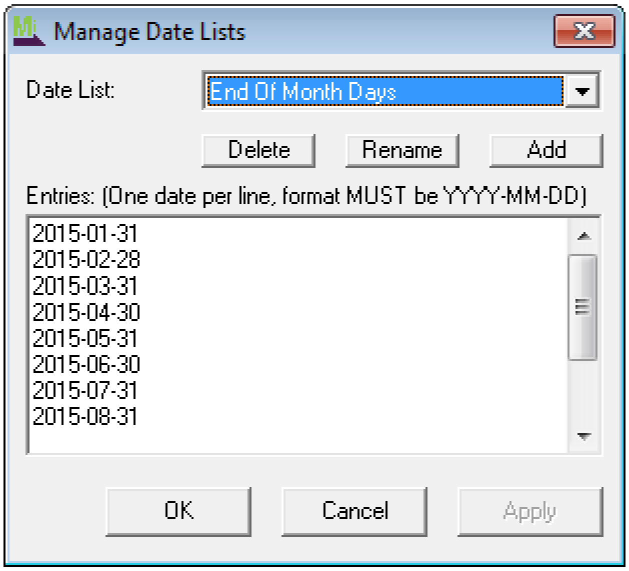
Populating the date list is done through the Entries text box. The data for a date list is simply a list of dates, one date per line. The date format MUST be in the format YYYY-MM-DD. An asterisk ("*") wildcard is allowed in the year and month places. Entries not of this format will generate an error, requiring you to fix the entry before saving the date list.

Blank lines and lines starting with the # character will be ignored by MOVEit Central when using the date list. These lines will be saved as part of the date list, but will not affect its operation, thus allowing for better readability and documentation. An example date list is shown below:

```
#

# Holidays Date List

#

# New Years Day

*-01-01

# St. Valentine's Day

*-02-14

# U.S. Independence Day

*-07-04

# U.S. Independence Day, Observed

2004-07-05

# Halloween

*-10-31

# Christmas Eve

*-12-24

# Christmas Day

*-12-25

# New Years Eve

*-12-31
```

Editing a Date List

Editing an existing date list is simply a matter of selecting the date list you wish to edit, and then making the appropriate changes in the Entries text box. Renaming a date list can be accomplished by clicking the Rename button.



Date List: End Of Month Days

Entries: (One date per line, format MUST be YYYY-MM-DD)

```
2015-01-31
2015-02-28
2015-03-31
2015-04-30
2015-05-31
2015-06-30
2015-07-31
2015-08-31
```

Once the date list changes are made, there are three ways to save the changes to Central. First, you can click the OK button in the Date List Manager to save the recent changes and exit the Manager. You can also click the Apply button in the Date List Manager to save the current changes without exiting the Manager. Finally, you can select a different date list to edit. When a new date list is selected before saving changes to a previous one, you will be prompted to save the changes before moving on. Click the Yes button in the dialog to save the changes and move to the next date list. Click No to ignore the changes and move to the next date list. Click Cancel to stay on the current date list.

Deleting a Date List

Deleting an existing date list can be accomplished by selecting the date list you wish to delete, and then clicking the Delete button. A confirmation dialog will prompt you to make sure you wish to delete the date list. Clicking Yes in this dialog will cause the date list to be removed from Central, along with all references to it in any existing schedules.

AS1, AS2, AS3 (Enterprise Only)

By nature, sources and destinations involving AS1, AS2, and AS3 file transfers have several different options from those involving other host types. When configuring an AS1, AS2, or AS3 source or destination, some options will appear familiar, but most will be specific to the host type, or AS1, AS2, and AS3 hosts in general.

For an overview of AS1, AS2, and AS3 file transfers, see the ***AS1, AS2, AS3 - Overview*** (see "***Overview***" on page 337) page.

For more details about AS1, AS2, and AS3 source and destination options, see the following pages:

- ***AS1, AS2, AS3 - Tasks - AS1 - Source*** (on page 389)
- ***AS1, AS2, AS3 - Tasks - AS1 - Destination*** (on page 390)
- ***AS1, AS2, AS3 - Tasks - AS2 - Source*** (on page 392)
- ***AS1, AS2, AS3 - Tasks - AS2 - Destination*** (on page 393)
- ***AS1, AS2, AS3 - Tasks - AS3 - Source*** (on page 395)
- ***AS1, AS2, AS3 - Tasks - AS3 - Destination*** (on page 397)

Hosts

This section describes endpoint servers or hosts where MOVEit Central picks up or drops off files.

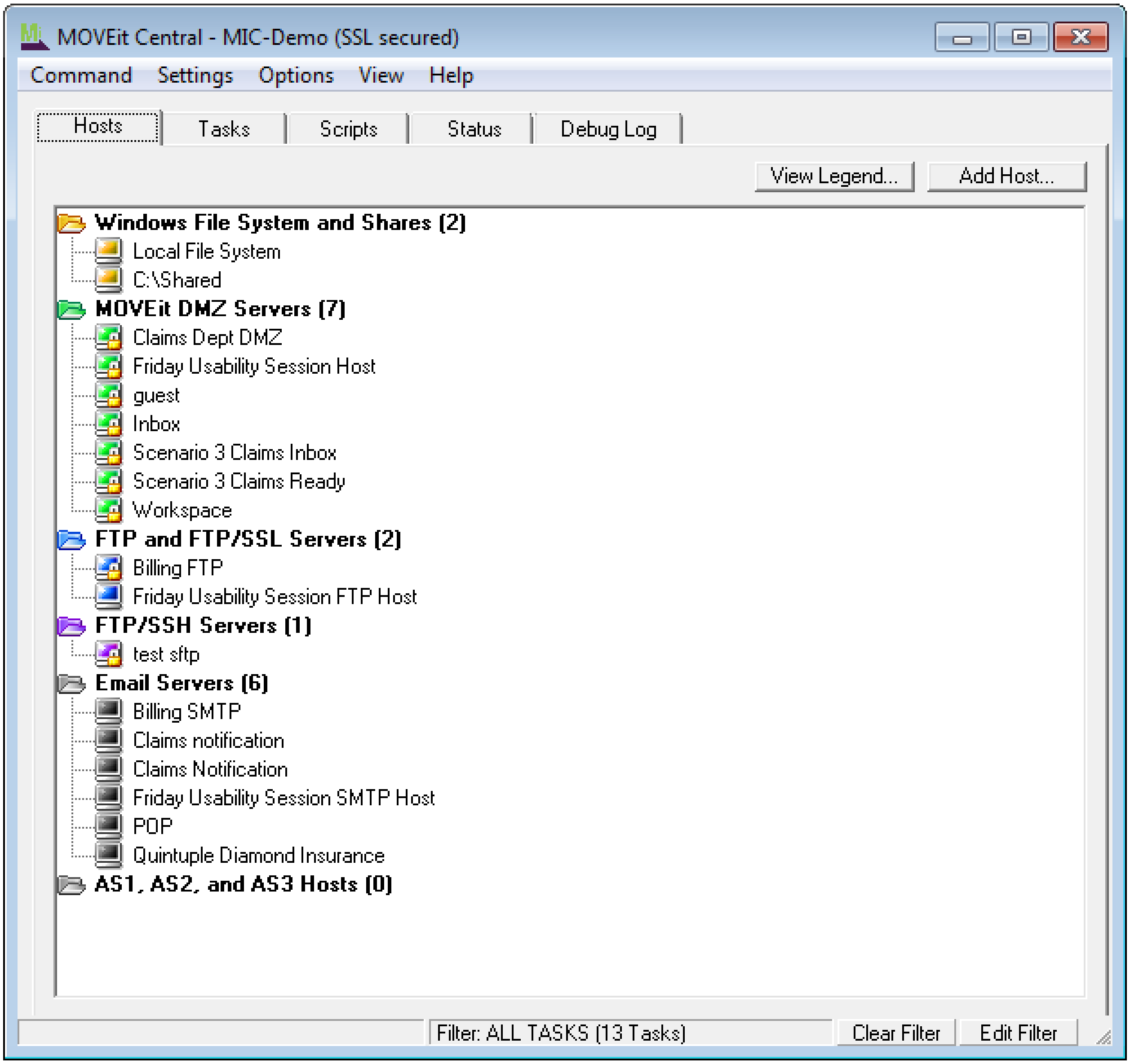
Overview

Hosts define "endpoint" servers where MOVEit Central can pick up files or drop files off. Sources and destinations directly depend on host definitions; they can override some information (such as the credentials presented) on a task-by-task basis, but the IP address, port number and other information must be defined in the underlying host definition.

Changes made to a host definition immediately affect all sources and destinations which depend on that definition. This is beneficial when configuring many tasks to go to the same host, especially if that host changes its IP address.

Hosts Tab

MOVEit Central Admin displays all hosts defined on a MOVEit Central system on the Hosts tab. Each host may be of only one type (SSH, FTP(S), MOVEit DMZ, FileSystem or SMTP/Mail), and known hosts are organized by host type in the Hosts tab display. See also ***Host Operations*** (on page 159).


MOVEit Central - MIC-Demo (SSL secured)
Command Settings Options View Help
Hosts Tasks Scripts Status Debug Log
View Legend... Add Host...
Windows File System and Shares (2)
Local File System
C:\Shared
MOVEit DMZ Servers (7)
Claims Dept DMZ
Friday Usability Session Host
guest
Inbox
Scenario 3 Claims Inbox
Scenario 3 Claims Ready
Workspace
FTP and FTP/SSL Servers (2)
Billing FTP
Friday Usability Session FTP Host
FTP/SSH Servers (1)
test sftp
Email Servers (6)
Billing SMTP
Claims notification
Claims Notification
Friday Usability Session SMTP Host
POP
Quintuple Diamond Insurance
AS1, AS2, and AS3 Hosts (0)
Filter: ALL TASKS (13 Tasks)
Clear Filter
Edit Filter

The following types of hosts are currently supported:

- **Windows File System and Shares** - The local computer on which MOVEit Central is running. This "placeholder" host includes the local filesystem, and any remote Windows shares MOVEit Central is configured to access. If you want to access files on a network share, either click the "Add Host..." button or right-click on the Windows File System and Shares host type and choose "Map Network Drive" to configure access to the remote share.
- **MOVEit DMZ** - A MOVEit DMZ server accessible via HTTPS usually over TCP port 443.
- **FTP Server** - A plain FTP server or FTP over SSL server, usually accessible over TCP port 21. (Note: The most common TCP port used for FTP over SSL in implicit mode is 990.)
- **SSH Server** - An FTP over SSH server, usually accessible over TCP port 22.
- **SMTP Server** - An outbound email server usually accessible over TCP port 25.
- **POP3 Server** - An inbound email server usually accessible over TCP port 110.
- **AS1** - An AS1 trading partner relationship. AS1 uses email (SMTP and POP3) transports, often with SSL transport security.
- **AS2** - An AS2 trading partner relationship. AS2 uses mostly web (HTTP) transport, often with SSL transport security.
- **AS3** - An AS3 trading partner relationship. AS3 uses FTP transport, often with SSL transport security.

The following elements typically define a host:

- **Hostname or IP Address** - The full hostname (i.e. "MOVEit.stdnet.com") or IP address (i.e. "192.168.1.1") of the remote server.
- **Name** - This will be the name associated with this host in all tasks. Feel free to change this name at any time; hosts are really linked to tasks through the use of an invisible, unchanging host ID.
- **Username and Password** - Authentication credentials. These are always stored encrypted on disk. A username is usually required. In the case of SSH hosts, a password is optional if you are using public key authentication. (Some SSH hosts may require both public key and password authentication, but this is unusual.) Both username and password may contain macro references.

  For Share hosts, the permissions of the current user MOVEit Central is running as can be used instead of a specified username and password by selecting the "Use MOVEit Central Run-As credentials" option.

- **Port** - Offers the opportunity to connect to a server offering its services on an unusual port.
- **Default Connect Timeout** - The default number of seconds to wait when attempting to connect to the host.
- **Default Data Timeout** - The default number of seconds to wait when sending data to or receiving data from the host.
- **Default Retry Count** - The default number of extra times that a transfer (get or put) should be retried before MOVEit Central gives up. This defaults to 0-meaning try just once-and can be overridden by individual tasks.
- **Default Retry Timeout** - The number of seconds between retries. This defaults to 120 seconds, and can be overridden by individual tasks.
- **Host ID** - The automatically-generated unique ID for the host. This value is not editable.
- **Description** - A description field for the host. This field does not affect the operation of the host and is used simply to provide operators with information about the host.

The following elements are also used with specific types of hosts. Many of these settings can be overridden by individual task sources or destinations. (AS1, AS2 and AS3 hosts are different enough to warrant their ***own section*** (see "***AS1, AS2, AS3 (Enterprise Only)***" on page 162).)

Note: Depending on the host type, some of these options appear on the Host options dialog, and some on the Advanced options dialog, which is accessed from the Host options dialog. The Host options dialog is accessed from the Hosts tab by clicking Add Host, or by selecting an existing host and selecting Edit Host from the right-mouse menu.

Note: If any of the options are "greyed out," or if the Advanced Options button is greyed out, this indicates that your license does not include that feature.

- **Send Email As** (*SMTP Server only*) - MOVEit Central will send attachments and message email through this server using this "from" address.
- **Default Transfer Type** (*FTP Server only*) - FTP transfers can be performed in ASCII or BINARY mode. This option allows operators to configure the default setting for any FTP host. (This setting will be OVERRIDDEN if specified in any source/destination related to this host.)
- **Default Transfer Mode** (*FTP Server only*) - FTP transfers can be performed in Active or Passive mode. Active mode is the normal mode of operation for FTP transfers, while Passive mode is generally used for FTP clients located behind a firewall. This feature allows operators to configure the default setting for any FTP host. (This setting will be OVERRIDDEN if specified in any source/destination related to this host.)
- **Account** (*FTP Server only*) - Supplies the FTP "account" for this server. A few FTP servers require that an account be entered during login, after the username and password. In most cases, though, you will leave this empty. The account may contain macro references.

- **Additional Commands to Execute Upon Signon** (*FTP Server only*) - Several FTP servers (especially those in front of enterprise servers or legacy equipment) work best if presented with special "quote" block formatting and file type commands before file transfers are performed. (Commands listed in this area will be executed IN ADDITION TO any additional commands specified in any source/destination related to this host.) Macros are supported in this field.

  AS/400 (iSeries) FTP Server Hint: Enter a value of "SITE LISTFMT 1" here to ask the AS/400 to use a standard (Unix-like) listing format, which can be automatically recognized by MOVEit Central.
- **Additional Commands to Execute Per File Before Transfer** (*FTP Server only*) - Several FTP servers (especially those in front of enterprise servers or legacy equipment) work best if presented with special "quote" block formatting and file type commands before file transfers are performed. (Commands listed in this area will be executed IN ADDITION TO any additional commands specified in any source/destination related to this host.) Macros are supported in this field.
- **Additional Commands to Execute Per File After Transfer** (*FTP Server only*) - Specifies "quote" commands to send to the FTP server immediately after a successful transfer. (Commands listed in this area will be executed IN ADDITION TO any additional commands specified in any source/destination related to this host.) Macros are supported in this field.
- **Blind Downloads (skip directory listing)** (*FTP and SSH hosts only*) - Specifies that when downloading from this host, MOVEit Central should not use any directory listing commands. In the case of FTP servers, this includes "change directory" (CWD) and "list directory" (LIST) commands. Instead, the "FileMask" specified in the source is actually a single filename, not a mask, and the program should download the file without first checking to see if it exists. This rarely-used option is intended primarily to accommodate unusual FTP servers.
- **Blind Uploads** (*FTP Server only*) - Specifies that when uploading to this host, MOVEit Central should interpret all destination paths as absolute. In this case, the most that MOVEit Central should be doing is issuing a CWD to the path specified, and then doing a PUT to save the file in that location. This rarely-used option is intended primarily to accommodate unusual FTP servers.
- **Upload as TempFile then Rename** and **Temp Upload Filename** (*FTP, SSH and Filesystem hosts only*) - This feature allows MOVEit Central to upload a file under a temporary filename, and then rename the just-uploaded file to something else. The most common reason for using this option is to avoid triggering another automation system which depends on the existence of a certain filename but which cannot detect the difference between open/closed or started/finished files. The checkbox field enables or disables this option. (It is off by default.) The text field allows an administrator to provide a specific pattern for the name of temporary files. By default a value of "CTMP[Rnd:4]" is used (this will yield values like "CTMP9243" and "CTMP2495"). If a different value is used, care should be taken to avoid duplicate temporary filenames. (Relying on minute-second timestamps may not be reliable for this purpose, but derivations of filenames may be reliable.) Renames will occur on a file-by-file basis as soon as each file has been uploaded; there is no "mass rename" step after all files have been uploaded.

- **Host adjusts timestamps for Daylight Savings Time** (*FTP, SSH, Filesystem, and Share hosts only*) - Warns MOVEit Central that the host will automatically change the apparent time of existing files when Daylight Savings Time comes into effect, or reverts to Standard Time. The Windows filesystem, for instance, will do this if (as is usually the case) the host computer has the Windows setting "Automatically adjust clock for daylight savings changes" selected.

  If this "Host adjusts timestamps" setting is selected, MOVEit Central changes the way that the "Collect Only New Files" source option is processed, and it also changes the way that synchronization works. In these situations, MOVEit Central compensates for the changes made by the host by adjusting the apparent timestamps of files by one hour. This is to prevent the unnecessary transfer of files that appear new because their apparent times have changed since they were last observed. For example, consider a file that is modified in January (during Standard Time) at 8:00AM. When Daylight Savings Time comes into effect in the spring, after months of having appeared to be modified at 8:00AM, the file's apparent modification time will suddenly change to 9:00AM. If "Host adjusts timestamps" is selected, MOVEit Central will internally adjust its view of the file's time back to 8:00AM for comparison purposes, and will not consider the file to be new.

  Similar adjustments are made by MOVEit Central during the transition from Daylight Savings Time to Standard Time, in order to compensate for file timestamp changes made by the host computer on which the file resides.
- **Rescan before Xfer** (*Filesystem, FTP and SSH servers only*) - This option helps prevent MOVEit Central from downloading "incomplete" files from servers that make such files available for download before they are closed. It specifies that once one or more files matching the download criteria have been identified, MOVEit Central should rescan the directory, looking for changes in the files' size and date. If a file has changed, the behavior of the task will be different depending on the task type:
  - Traditional/Advanced tasks: The file will be removed from the list of files to download. The purpose of this feature is to detect when another application is currently changing the files, so that MOVEit Central will not download a partial file. The value is the number of seconds to wait between scans.
  - Sync tasks: The task will continue rescanning until the files have have not changed in successive scans. If files are continuously changing, this option should not be used, or the task may get stuck. The purpose of this feature is to detect when the source has "settled down," so that the task does not need to run multiple times to capture and sync all of the changes in a directory.

    The value is the number of seconds to wait between scans. The default is 0, which deactivates the feature .A reasonable value for when you do need the feature might be 5 or 10 seconds. (This setting will be overridden if specified in any source related to this host.)

- **IIS Virtual Directory** (*MOVEit DMZ Server only*) - It is perfectly legal to install MOVEit DMZ into a subdirectory of another web site. (An installation may already host another secure web site on the same machine, for example.) However, MOVEit Central needs to know about any alternate locations used and this box provides the interface to define this location. (e.g., "/mysubdir/"; set this to "/" if you are unsure)
- **Secure** (*MOVEit DMZ Server only*) - When checked, this enables secure communications between MOVEit Central and the remote host. Secure MOVEit DMZ connections are usually initiated on port 433 rather than insecure port 80.
- **Secure Connection** (*FTP Server only*) - Selects the style of encryption used when connecting to the FTP server. Your choice will depend on the styles offered by the particular FTP server.

Encryption style	**Meaning**
None	No encryption
TLS-P	Both the control connection and any data connections are encrypted. (Note to experts: MOVEit Central actually does an AUTH TLS, followed by an explicit PROT P.)
TLS-C	Only the control connection is encrypted.
Implicit	Both the control connection and any data connections are encrypted. This type of connection is usually done to port 990. This style is considered to be obsolete.

- **Cleartext after connection (CCC)** (*FTP Server only*) - After connecting and signing on securely, switch to unencrypted mode for the control connection. This option applies only to the encrypted FTP options above.

  The CCC option is slightly less secure, because it allows an opponent to see the names of the files you transfer. However, if the FTP server is behind a firewall that does NATing, this option allows the firewall to rewrite the responses to PASV commands, thus allowing MOVEit Central to transparently connect to the correct IP address.

  This CCC option is rarely needed, because the "Ignore PASV IP in passive mode" option, which is on by default, accomplishes much the same thing.

- **Ignore Cert Errors** (*FTP Server and MOVEit DMZ Server only*) - When checked, ignores SSL certificate problems. These problems include the certificate being expired, having the wrong hostname, or having been issued by an untrusted authority. This is used primarily during testing, when you have only a temporary test certificate. It applies only if Secure is checked. If this box is not checked and questionable certificate is detected, MOVEit Central will not connect to the host, and an error will be logged.
- **SSH Host Key** (*SSH Server only*) - Specifies the host key expected from the SSH server. If "Specific Key" is checked, then if the public key presented by the SSH host does not match the approved key, or if no approved key has been designated, MOVEit Central will refuse to connect to the host, under the assumption that there may be a security problem. (For instance, another server may be masquerading as the original server.)

  The "Any Key" option is the SSH equivalent of the SSL-oriented "Ignore Cert Errors" option. The difference is that SSL certificate errors pertain to attributes of the certificate itself, so MOVEit Central can detect problems (such as a hostname mismatch or an expired certificate) by inspecting the certificate itself. By contrast, SSH public keys are simpler and potential problems can be checked only by noticing changes. By choosing "Any Key", you are instructing MOVEit Central to accept any key presented by the host. This option makes it impossible for MOVEit Central to detect when a rouge SSH server has been substituted for the legitimate SSH server.

  When an administrator sets up an SSH/FTP host, s/he normally obtains the host's current public key by choosing the "Specific Key / New" button, and marks it as approved via the Verify Host Fingerprint dialog. On subsequent connections to the host, MOVEit Central compares the public key presented by the host to the approved key.
- **SSH Client Key** (*SSH Servers only*) - Specifies the optional SSH client key associated with this user. Typically, SSH servers will require either a username and password, or a username and client key. If you want to use client key authentication, choose the "..." button and either choose a previously-generated client key via the "Current Key" drop-down box, or create or import a new key via the "Add" button.

  If you choose the Add button, you must enter a name for the key; the name you choose is for your own convenience and has no bearing on the authentication process. Then you will see the Add SSH Key dialog. You can choose "Generate new key" to create a new key, or "Import existing key" to ***import*** (see "***Importing SSH Client Keys***" on page 216) a key that has already been generated on a remote machine and downloaded to your PC.

  Once you select, generate, or import a key, characteristics of the key are shown in the "Fingerprint (MD5)" and "Public Key" text boxes. The "Format" radio button controls whether you see the public key in SSH or OpenSSH format.

  Note that the remote server must be configured to ***authorize the key for logon*** (see "***Importing SSH Client Keys***" on page 216).

- **Client Certificate** (*MOVEit DMZ and FTP Servers only*) - Specifies the SSL client certificate to use when establishing connections. MOVEit DMZ 4.0 and later servers can be configured to accept or require client certificates, although this is not the default. Some FTP servers also use SSL client certificates, although this is rare.
- **Client NAT Settings** (*FTP Servers only*) - Specifies Network Address Translation (NAT) options to use in certain unusual network configurations.

  Client External IP is the IP address that MOVEit Central should send to the FTP server when in active mode. Normally MOVEit Central will send its real IP address, but if there is a router between MOVEit Central and the FTP server that is doing NAT, it may be necessary to use a different "external" IP address.

  Ignore PASV IP in passive mode means that when in passive mode, MOVEit Central should ignore the IP address given by the FTP server and instead use the IP address associated with the host configuration. This option is used to accommodate incorrectly configured networks.

  Both of these options are rarely used.
- **Use Notifications** (*MOVEit DMZ, Filesystem, and Share hosts only*) - Specifies that tasks accessing this host will be run when files arrive, rather than periodically by the scheduler. Choosing this option is recommended. See ***File Notifications*** (on page 160).
- **Default File Sorting** (*MOVEit DMZ Server only*) - Specifies how file listings should be sorted when retrieving listings from a MOVEit DMZ server. Files will be downloaded in the order they are listed, so this setting provides the ability to define which files should be downloaded first. Available options are "By Filename", "By Date/Time", and "By Size", each with an "Ascending" or "Descending" option.
- **Custom Parsing** (*FTP and SSH Servers only*) - Specifies whether MOVEit Central's automatic directory listing recognition should be overridden with an explicit configuration. This feature is needed only for unusual brands of FTP and SSH servers. See ***Custom Directory Parsing*** (on page 400).
- **MD5 Checking** (*FTP and SSH Servers only*) - Specifies whether MOVEit Central should look for an MD5 file, containing MD5 hashes of source files on the FTP server, and what that MD5 file should be called (see the ***FTP Source Integrity*** (on page 399) page for more information). The following settings are available for checking for an MD5 file:
  - **Never** - Central will not look for an MD5 file.
  - **If Present** - Central will look for an MD5 file. If the file contains a hash for a source file, Central will check the file against the hash. If the file matches the hash, Central will allow the file to continue, otherwise it will generate an error. If Central does not find a hash for the source file, it will allow the file to continue.
  - **Required** - Central will look for an MD5 file and generate an error if it is not found. All files downloaded will be checked against the MD5 file. If a file does not match its hash, or a hash does not exist for the file, Central will generate an error.

- **Download Limits** (*MOVEit DMZ, FTP, SSH, Filesystem, and Share hosts only*) - Limits the number of files that Central will download from a source in a single task run against this host. The limit can be by file count or by byte count. In the case of a limit by byte count, Central will stop downloading files after the first file that causes the number of downloaded bytes to exceed the configured limit. If the limit is exceeded, the task will automatically be rerun. A value of 0 means no limit.

  This option is useful in production only when the source has "new files only" or delete or rename after successful transfer set. Otherwise, the same files will be downloaded over and over.
- **Encryption Algorithm** (*SSH Servers only*) – By default, when negotiating an encryption algorithm with an SSH server, MOVEit Central will try AES first, then 3DES, then Blowfish. This setting can be used to specify which type of encryption algorithm is allowed when attempting to connect to this server.
- **Transport - Disable SSH Compression** (*SSH Servers only*) - Turns off compression for all communications with the SSH server. This is recommended only for a few, rare SSH servers which do not support compression.
- **Transfer – Use Windows CopyFile API** (*Share hosts only*) – By default, MOVEit Central uses the Windows CopyFileEx function to transfer files to and from UNC share hosts (with the exception of Synchronization tasks). Under certain conditions, the performance of this function can potentially suffer, especially when transferring large files. If bad performance is being experienced when transferring files to/from this UNC host, deselecting this option may help remedy the situation.
- **Transfer - Use XSHA1 Command (if available)** (*FTP Servers only*) - Enables the use of the XSHA1 command if the FTP server supports it. This allows Central to compare the file it received or transmitted with the copy that the server has by comparing SHA1 hashes of the file.
- **Transfer - Resume Partial Transfers (if possible)** (*FTP, SSH Servers*) - During a task run, enables MOVEit Central to resume an FTP upload or download that has failed. If the file is a binary file and the Default Retry Count is greater than zero, MOVEit Central tries to resume the transfer. Transfers will pick up where a previous one failed. The number of resume attempts is set by Default Retry Count. This setting can be overridden on sources and destinations.
- **Transfer - Reuse SSL Session for Data Connections** *(FTP SSL servers)* - If checked, forces data connections to use the same SSL session as the existing control connection. You can override the default unchecked setting here for a given source or destination task element configuration. This allows you to comply with partner server settings that require reuse of an SSL session for data connections.
- **File Attributes** (*SSH servers only*) – Allows setting Unix-style file attributes on a file after a successful upload. The desired file attributes can either be specified by entering a valid 3-digit octal numeric representation, or by selecting individual check boxes corresponding to specific permissions. This setting only affects SSH hosts that are based on a Unix-like file system.

- **Alternate Host - Select Host** (*Enterprise only*) - designates a secondary host to "rollover" to when the primary host is not available. When running a task, MOVEit Central will use the alternate host if, after the designated number of retries, it encounters problems connecting or logging in to the primary host. MOVEit Central will not rollover if there are other problems, such as if the directory does not exist, or if there are insufficient permissions to access a file; these cases will instead cause an error. Also, this feature applies to an individual host, making it different from the failover feature that applies to nodes. Note: In order for a host to appear in this drop-down, you must create it in the Hosts tab of the MOVEit Central admin window. The alternate host must be the same type of host (FTP server, SSH server) as the primary host.
- **State File – Delete State After X Days** - When this host is assigned as a task source that uses Collect Only New Files, MOVEit Central will save file stamp state information that is specific to this host and the task source's folder path and file mask. If the source's folder path and/or file mask contains a non-static macro (for instance [DD] or other data/time macros), then the actual source folder path/file mask combination can potentially be different every time the task runs, which in turn can cause the saved state information for this host to grow very large and without bounds. This setting can be used to automatically delete state information for this host that is older than the specified number of days, which prevents state information from growing uncontrollably.
- **State File – Use Default State Caching Settings** - If checked, this host will use the system's default State Caching settings. If unchecked, the host will use the specified State Caching settings. By default, MOVEit Central always keeps state file information cached in memory in order to achieve maximum efficiency. In certain environments, however, this can become quite memory intensive. The State Caching settings can be used to remove state file information from memory after a task run or even after a specified amount of time.

For a list of icons used to represent hosts, sources, and destinations, see ***Configuring Tasks - Overview*** (see "***Overview***" on page 101).

Testing Hosts

All remote host types provide a testing option, to allow the administrator to check the current host configuration. Once the host settings are entered, click the Test button in the lower left corner of the Define Host dialog to test the host. The test results will be reported with a popup information dialog when the test is complete. Note that the test may take several seconds depending on the accessibility and speed of the host.

The following tests are executed, based on the type of the host:

- **MOVEit DMZ Servers** - Attempt to sign on to the configured host and port using the configured security settings and username and password. If successful, attempt to execute a directory listing on the root directory.
- **FTP Servers** - Attempt to sign on to the configured host and port using the configured security settings, transfer mode, username, password, and account. Use any advanced options configured, such as client certificate and/or NAT settings. If successful, attempt to execute a directory listing on the current directory returned by the signon transaction.

- **SSH Servers** - Attempt to sign on to the configured host and port using the configured host key setting and username and password. If a client key is configured in the advanced options, it will be used. If successful, attempt to execute a directory listing on the current directory returned by the signon transaction.
- **SMTP Servers** - First prompt for an email address to send a test email message to. Attempt to sign on to the configured host and port and send an email message using the configured sender address and the provided recipient address.

  Note: A successful test here merely indicates that MOVEit Central was able to connect to the SMTP server and ask it to send an email message to the provided recipient address. Final confirmation of a successful test requires checking the provided recipient address to make sure the test message was accepted and delivered.
- **POP3 Servers** - Attempt to sign on to the configured host and port using the configured username and password. If successful, attempt to get a count of waiting messages.

Host Operations

You can perform various operations on hosts in the Hosts tab. To perform an operation on a host, right-click on a specific host or a host type, and choose from the resulting menu. You can also get this menu by highlighting a host and pressing Shift-spacebar. See also ***Hosts Tab*** (on page 149).

Available operations

- **Add Host...** allows you to specify a new host. You will be presented with several dialogs, in which you type the parameters for this host.
- **Edit Host...** allows you to modify an existing host. You can also get the Edit Host dialog by left double-clicking the host.
- **Rename Host** allows to you change the name by which MOVEit Central refers to the host. The Internet hostname is not changed this way; use Edit Host to change the domain name of the host (if applicable).
- **Remove Host** removes the host from the configuration, as well as any sources or destinations that refer to it.
- **Map Network Drive** allows you to connect to a remote fileserver, optionally mapping a drive letter. MOVEit Central will attempt to map the share immediately. If it cannot do so--for instance, if the drive letter is in use, or if you are already connected to that server with a different username--then the mapping will not take effect until MOVEit Central is restarted. This option is available only when the "Windows File System and Shares" host type is selected. (You can also add drive maps and UNCs from the usual "Add Host..." button.)
- **Edit Share...** allows you to change information associated with a mounted share. Mounted shares appear under the "Windows File System and Shares" host type. MOVEit Central will attempt to make the change immediately. If it cannot do so, you will be shown an explanatory message. In that case, changes you make will not go into effect until MOVEit Central is restarted.

- **Remove Share** allows you to delete a shared network path. This option is available only for mounted shares, which are listed under the "Windows File System and Shares" host type. The change will not go into effect until MOVEit Central is restarted.
- **View Audit Trail** - Displays a view of all current Audit entries for the selected host on the Reports window.
- **Set Filter To This Host/Share** - Sets the task filter to show only those tasks that involve the selected host or share.

File Notifications

File notifications are a mechanism that MOVEit Central can use to start a task almost immediately, based on the arrival of a file in a directory. This feature is available only for MOVEit DMZ and filesystem sources, and is also known as "event-driven transfers".

File Notifications vs. Scheduler

Prior to the introduction of file notifications in MOVEit Central 3.1, in order for a task to notice a file, the task had to be scheduled to run repeatedly. Each time the task was run, it would check for files matching a given mask. Oftentimes, no such files had arrived, so no action was taken, and the task would be run again later by the scheduler. In order for a task to see a file shortly after its arrival, the task had to be scheduled to run often, causing extra overhead for both the remote server and MOVEit Central itself.

By contrast, file notifications allow you to run a task only when files it's interested in are actually available. And with file notifications, the task runs almost immediately after the arrival of a file.

The MOVEit Central component that implements file notifications is called the "notifier".

Enabling File Notifications

File notifications are enabled on a host-by-host basis.

To enable file notifications for all tasks accessing a given MOVEit DMZ host, use MOVEit Central Admin to edit that host and check the "Use Notifications" checkbox.

Note: The MOVEit DMZ server must be running MOVEit DMZ 3.1 or later. If it is not, MOVEit Central will figure it out during operation, and will disable notifications for that host. If you later upgrade that MOVEit DMZ server, you will have to stop and start MOVEit Central for it to notice the new capability on that server.

To enable file notifications for a Windows directory or remote share, you must edit a Windows File System and Shares host. To enable file notifications for all tasks accessing a remote mapped drive (share), edit that share and choose "Use Notifications". To enable file notifications for local drives, edit the "(Local)" FileSystem entry and choose "Use Notifications".

Note: On remote filesystems, file notifications work only for remote servers running modern Windows operating systems. Remote servers running Windows 9x or a non-Microsoft operating system will usually not provide file notifications even though they may still be able to share files.

Scheduler Ramification

Like the scheduler, the MOVEit Central file notifier requires a task to have a schedule in order to run that task. As with the scheduler, the notifier will run the task only during the scheduled intervals.

However, tasks for which all sources use notifications are run much less frequently than when file notifications are not used. Those tasks will not be run periodically as specified by the task interval (e.g., "every 15 minutes"). Instead, with a few exceptions, the task will be run only when files that match one of that task's sources actually arrive. Also, the "Repeat only until first success" option on a schedule is ignored if all sources are subject to file notifications.

The exceptions are these:

- In order to catch files that arrived outside the scheduled hours, MOVEit Central always runs a task at the beginning of each schedule associated with that task, even when no notifications have arrived.
- At startup, MOVEit Central runs all tasks that are subject to notifications and whose schedule spans the time that MOVEit Central is starting. This is to catch files which arrived during the time that MOVEit Central was not running.
- If a schedule spans midnight (e.g., 20:00 to 04:00), then the task is always run at midnight.
- If a schedule is marked "Log failure if no files found during scheduled run" and no files have been found yet during the schedule, the task is run at the end of the schedule, so that it may fail if necessary.
- Finally, schedules marked "Run even if notifications are enabled for the host" cause the task to run even if notifications are enabled. Note that a task may have multiple schedules, and each has its own "Run even if notifications are enabled for the host" setting.

If, for instance, a task is scheduled to run every 15 minutes between 08:00 and 17:00, and all of its sources are marked to use notifications, then the "every 15 minutes" portion of the scheduling information is ignored. Instead, the task is run at 08:00 (in order to catch any files that may have arrived overnight), and thereafter the task is run only when a file arrives.

If only some of a task's sources correspond to hosts for which notifications have been enabled, then the task will be run both by the normal scheduler and by the notifier.

The arrival of a given file may cause several tasks to run, if those tasks are all watching the same directory. The notifier respects the "Include Subdirectories" option.

The simultaneous arrival of multiple files that are being looked for by a task will not necessarily cause that task to be run multiple times. However, if a task is already running when files for that task arrive, the notifier will queue a request to run the task again when the task completes.

Implementation

MOVEit Central learns of files arriving on MOVEit DMZ by periodically contacting MOVEit DMZ servers and asking for a list of recently-arrived files. The frequency of this polling is governed by the Global Settings option "Notification Polling Interval". The default is 5 seconds; the minimum is 1 second and the maximum is 3600 seconds. One request per MOVEit DMZ server is made during each interval.

Because only one request is made per interval, regardless of the number of tasks affected, and because MOVEit Central does not need to signon and signoff each for each request, this process is much more efficient than having many tasks each run and check for themselves.

Note: The MOVEit Central notifier uses the username and password associated directly with the host. Tasks with sources that override this username may not be notified properly.

If this username cannot signon, MOVEit Central will wait for a period of 60 times the notification interval (up to a maximum of 3600 seconds) before trying again. This extra delay is intended to prevent MOVEit DMZ from locking out the user or IP address.

For filesystem notifications, the notifier uses Windows directory change notifications (using ReadDirectoryChangesW). When a file arrives, MOVEit Central waits until the file is no longer locked by another process before it runs the corresponding task(s). Generally, this prevents problems in which MOVEit Central tries to read an incomplete file being created by a program on the remote computer.

AS1, AS2, AS3 (Enterprise Only)

A single AS1, AS2 or AS3 host definition covers negotiable partner parameters such as formal organization names, encryption methods, signing methods, hostnames and other AS "partner connection" options. Within each MOVEit Central Task, AS source and destination elements control path/file settings, MDN requests and similar "per transfer" options. Traditional Task schedules control the timing of the transfers.

By nature, AS1, AS2, and AS3 hosts have several different options from other host types. When configuring an AS1, AS2, or AS3 host, some options will appear familiar, but most will be specific to the host type, or AS1, AS2, and AS3 hosts in general.

For an overview of AS1, AS2, and AS3 file transfers, see the ***AS1, AS2, AS3 - Overview*** (see "***Overview***" on page 337) page.

For more details about AS1, AS2, and AS3 host options, see the following pages:

- ***AS1, AS2, AS3 - Hosts - AS1*** (see "***AS1***" on page 376)
- ***AS1, AS2, AS3 - Hosts - AS2*** (see "***AS2***" on page 379)
- ***AS1, AS2, AS3 - Hosts - AS3*** (see "***AS3***" on page 387)

Processes/Scripts

The section describes how scripts may affect processes.

Overview

A single process indicates that a built-in script or custom script should be run by itself, against each file or against all files retrieved during a single traditional task run. (Synchronization tasks cannot run processes.) There are two types of scripts: built-in and custom.

Built-in scripts are installed and updated along with MOVEit Central, and their source code may not be viewed or altered. A complete list of built-in scripts available in this version is available in the ***Processes/Scripts - Built-In Overview*** (see "***Built-in Scripts Overview***" on page 173), but examples of built-in script functions include PGP encryption/decryption, advanced ZIP, find-and-replace operations and invocation of command-line applications.

Custom scripts are just that: they are VBScript scripts written by you or imported from the directory of sample scripts installed with MOVEit Central Admin. (Custom scripts are available only in the MOVEit Central Enterprise.) The source code of any custom script may be viewed or changed at any time, as long the user who wished to view or change the code has been properly authenticated through MOVEit Central Admin. (Custom scripts are stored encrypted in the MOVEit Central configuration file so a hacker who gains access to the MOVEit Central hard drive cannot alter processes.)

Built-in scripts are available automatically as soon as you install MOVEit Central. By contrast, to use a custom script, you must load it into MOVEit Central. A custom script is loaded into MOVEIt Central when an administrator selects a VBScript source code file (*.vbs) and associates a "friendly name" with this script. Once loaded, the original script file is no longer used and can be deleted. (If changes to the script need to be made, an administrator can retrieve a copy of the saved script using MOVEit Central Admin, make changes and reload the script back into MOVEit Central.)

When defining a process, you choose these options:

- Which script to use
- When to run the script. Your choices are:
  - Once, after all files have been downloaded from Sources and before any files have been uploaded to Destinations.
  - Per file, immediately before each file is uploaded. If no sources are defined for the task, "per-file" processes are run once.

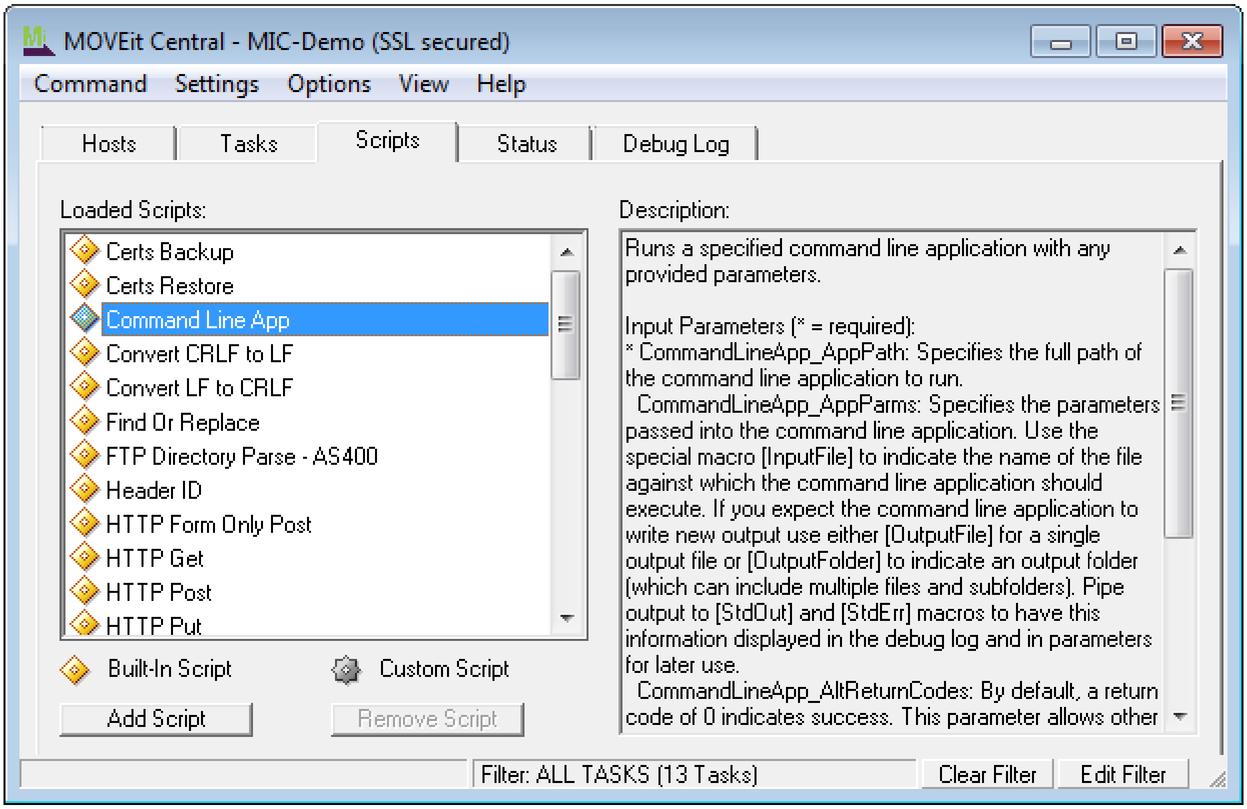
- Which task parameters to use (if any), and their values. This is optional; not all tasks require task parameters.

See ***Configuring Tasks - Tasks Elements - Process*** (see "***Process***" on page 132).

A script may call any function defined by VBScript. It may also instantiate and invoke COM objects, such as the useful "Scripting.FileSystemObject" and command-line applications using the "MIRunCommand" function. In addition, there are several ***MOVEit Central-specific functions*** (see "***Syntax (Enterprise Only)***" on page 165) that allow you integrate seamlessly with MOVEit Central's cache files and make your own task log entries.

Scripts Tab

Custom scripts are added and maintained in the "Scripts" panel of the Settings tab. (Custom scripts are available only in MOVEit Central Enterprise.)



Loaded Scripts:

- Certs Backup
- Certs Restore
- Command Line App
- Convert CRLF to LF
- Convert LF to CRLF
- Find Or Replace
- FTP Directory Parse - AS400
- Header ID
- HTTP Form Only Post
- HTTP Get
- HTTP Post
- HTTP Put

Description:

Runs a specified command line application with any provided parameters.

Input Parameters (* = required):
* CommandLineApp_AppPath: Specifies the full path of the command line application to run.
 CommandLineApp_AppParms: Specifies the parameters passed into the command line application. Use the special macro [InputFile] to indicate the name of the file against which the command line application should execute. If you expect the command line application to write new output use either [OutputFile] for a single output file or [OutputFolder] to indicate an output folder (which can include multiple files and subfolders). Pipe output to [StdOut] and [StdErr] macros to have this information displayed in the debug log and in parameters for later use.
 CommandLineApp_AltReturnCodes: By default, a return code of 0 indicates success. This parameter allows other

Filter: ALL TASKS (13 Tasks)

Custom scripts are stored encrypted in MOVEit Central's configuration file. Buttons and a right-click pop-up menu on the script list offer the following options:

- **Add Script** - Adds a new custom script to the script collection. Prompts allow administrators to create a new blank script, create a new script which reads a text file in all at once, create a new script which reads a text file in line by line or import an existing script. (To work with the enclosed samples oc custom scripts, use the "Add Script" function and select the desired script.)
- **Edit Definition** - Pops up a dialog which allows changes to a custom script's name and description.
- **Get Local Copy** - Downloads the selected custom script to a local location.
- **Edit Script** - Downloads the selected custom script to a local location and opens your "*.vbs" registered editor (if any).
- **Reload Script** - Reloads the selected custom script from the a local location.
- **Remove Script** - Deletes the current custom script (after confirmation, of course.)
- **View Audit Trail** - Displays a view of all current Audit entries for the selected script on the Reports window.
- **Set Filter To This Script** - Sets the task filter to show only those tasks that involve the selected script.

Syntax (Enterprise Only)

MOVEit Central custom scripts use Microsoft VBScript. (Custom scripts are available only in MOVEit Central Enterprise). Above and beyond the basic functions provided by that environment, however, MOVEit Central also makes available a number of application-specific functions. In alphabetical order, the functions and subroutines are:

- **MIAddFile** CacheFilename, AssignedFilename
- DirName = **MICacheDir**()
- FileName = **MICacheFilename**()
- FilesString = **MICacheFiles**()
- bOK = **MIDeleteFileSecure**(Filename)
- **MIDirAddEntry** FilenameToMatch, Date, Size, bIsDir, FilenameForGet, FilenameOriginal
- sDirListing = **MIDirGetListing**()
- DbgLevel = **MIGetDebugLevel**()
- OriginalFilename=**MIGetOriginalFilename**()
- Result = **MIGetTaskInfo**(InfoString)
- ParamValue = **MIGetTaskParam**(ParamName)
- **MIIgnoreFiles** [bDeleteOrigIfCfg [,bKeepAsNew]]
- **MIIgnoreThisFile** [bDeleteOrigIfCfg [,bKeepAsNew]]
- **MILogMsg** Message
- MyString = **MIMacro**(MacroText)
- FileName = **MINewCacheFilename**()

- bOK = **MIReplaceCacheFile**(Filename)
- retval = **MIRunCommand**(Command)
- errcode = **MISetDestHost**(ConfiguredHostName [,idest])
- errcode = **MISetDestPath**(NewPath [,idest])
- **MISetErrorCode** NumericErrorCode
- **MISetErrorDescription** ErrorDescription
- **MISetFilename** NewFilename
- **MISetStatus** StatusText
- **MISetTaskParam** ParamName,ParamValue
- **MISleep** Milliseconds
- ErrCode = **MIStartTask**(TaskNameOrID [,TaskParams])
- TaskGroups = **MITaskGroups**()
- TaskName = **MITaskname**()

In more detail:

- **MIAddFile** CacheFilename, AssignedFilename

  Adds a file to the list of files to be sent to destinations. CacheFilename is the name of the temporary file to send; you should first call MINewCacheFilename() and create this file. AssignedFilename is the name the file is to be given on the destination server. It may include / or \ characters, in which case the name will be considered a folder path and filename relative to the destination path. Scripts are not currently run on files added via MIAddFile, to prevent infinite loops.

- DirName = **MICacheDir**()

  Returns the full path of the directory where MOVEit Central keeps its temporary files.

- FileName = **MICacheFilename**()

  Returns the name of the temporary copy of the file. This file can be overwritten if the custom script needs to change the contents of the file before it is transferred.

- FilesString = **MICacheFiles**()

  Returns a string containing the subdirectories and filenames for all active files in the cache. These names are relative to MICacheDir and reflect the actual names on disk in the cache directory, not the original names from the sources. The names are separated by the | character. The last file does not have a | at the end. This list is empty immediately after a call to MIIgnoreFiles. The list does not include, for instance, the names of zip files that have been downloaded from sources marked "Uncompress Archives".

- bOK = **MIDeleteFileSecure**(Filename)

  Deletes the specified file, first overwriting it with random bytes. Returns True if successful.

- **MIDirAddEntry** FilenameToMatch, Date, Size, bIsDir, FilenameForGet, FilenameOriginal

  Adds an entry to the FTP or SSH directory listing being parsed. This should be called only from custom directory parsing scripts; see ***Custom Directory Parsing*** (on page 400).

- sDirListing = **MIDirGetListing**()

  Returns the entire verbatim listing from the FTP or SSH server. This should be called only from custom directory parsing scripts; see ***Custom Directory Parsing*** (on page 400).

- DbgLevel = **MIGetDebugLevel**()

  Returns the debug level currently set in MOVEit Central. The possible values are:

Level	Meaning
0	Internal errors
10	Task/File Errors
20	Task/File Warnings
30	Task Completions
40	File Completions
50	Some Debug
60	More Debug
70	All Debug

- OriginalFilename=**MIGetOriginalFilename**()

  Returns the original filename of the file.

- Result = **MIGetTaskInfo**(InfoString)

  Returns the specified information about the current task. InfoString can have the values:

InfoString	Value returned by MIGetTaskInfo
"CacheUsesOriginalNames"	True if the task is configured to use original filenames in the cache directory, else False if the task is configured to use random filenames.
"NSources"	The number of sources in the task.
"ProcessIsPerFile"	True if the current process is run for each file, else False if the current process is run once after all downloads.
"ShouldStop"	True if an operator has requested that the task be stopped.

- ParamValue = **MIGetTaskParam**(ParamName)

  Returns the value of the specified task parameter. If the current task has no such parameter, the empty string is returned.

- **MIIgnoreFiles** [bDeleteOrigIfCfg [,bKeepAsNew]]

  Causes all files already downloaded or added via MIAddFile to be ignored in subsequent processing steps. You might call this if, for instance, your custom script creates a zip file containing the downloaded files, and you do not want the downloaded files to be sent.

Parameter	Meaning
bDeleteOrigIfCfg	Whether to delete the original files if the Delete Original File(s) After Successful Transfer option has been set in the source. Defaults to True.
bKeepAsNew	Whether to continue to regard these files as new in the next task run even if the task succeeds. This is meaningful only if Collect Only New Files is set in the source. Defaults to False.

- **MIIgnoreThisFile** [bDeleteOrigIfCfg [,bKeepAsNew]]

  Causes the current file to be ignored in subsequent processing steps. You might call this if, for instance, your custom script wishes to ignore zero-length files. When called without parameters, this method is equivalent to calling MISetErrorCode 5000. This should be called only in per-file processes.

Parameter	Meaning
bDeleteOrigIfCfg	Whether to delete the original file if the Delete Original File(s) After Successful Transfer option has been set in the source. Defaults to False.
bKeepAsNew	Whether to continue to regard this file as new in the next task run even if the task succeeds. This is meaningful only if Collect Only New Files is set in the source. Defaults to False.

- **MILogMsg** Message

  Logs a message to the debug window and debug log file. The message is preceded by the task name.

- MyString = **MIMacro**(MacroText)

  Evaluates the macro MacroText and returns the resulting text. MacroText may contain any combination of ***macros*** (see "***Macro***" on page 137).

- FileName = **MINewCacheFilename**()

  Returns a new, unique temporary filename. The filename will be a full path and will be in the cache folder

- bOK = **MIReplaceCacheFile**(Filename)

  Securely deletes the current temporary cache file, and replaces it with the contents of Filename. You use this if you want to send a different file--probably one you just created--instead of the downloaded file. Typically you will first call MINewCacheFilename() to get a filename, use the FileSystemObject to create the file based on the contents of the file in the cache, then call MIReplaceCacheFile() to tell MOVEit Central to use the new file.

- retval = **MIRunCommand**(Command)

  Runs a system command through the system command interpreter. Command is a command, such as "Notepad MyFile.txt". This can be the name of a command, such as a .exe or .bat file, or the name of a file with an associated extension, such as .vbs, or a built-in CMD.EXE command such as DIR.

  MIRunCommand will wait until the command is complete. If you want the custom script to continue running while the command runs, use the Windows START command to launch the program.

MIRunCommand returns a long integer: -1 if the program could not be found, or else the return code from the program. Programs typically return 0 upon success, or >0 upon failure.

MIRunCommand does always not work well with pathnames that contain spaces. To avoid these situations, use the "Scripting.FileSystemObject" to look up "safe" versions of paths before passing them to MIRunCommand. For example:

```
Set fso = CreateObject("Scripting.FileSystemObject")
AppPath = "C:\Program Files\My App"
AppExe = AppPath & "\" & "runit.exe"
SafeAppPath = fso.GetFolder(AppPath).ShortPath
SafeAppExe = fso.GetFile(AppExe).ShortPath
ErrorCode = MIRunCommand(SafeAppExe & " " & " -o " & SafeAppPath &
"\out.txt")
```

- errcode = **MISetDestHost**(ConfiguredHostName [,idest])

  Changes the current file's view of one of the task's destinations so that it points to the given configured host. ConfiguredHostName is the name of one of the configured hosts such as "XYZ Corp FTP Server", not an Internet host domain name. The new host need not be the same type as the destination being changed; for instance, the destination may be of type FileSystem, but you can change it to point to an FTP server. Only the current file being processed (if any), and any files added via MIAddFile during this run of the process, are affected.

  If you are using this command to switch between hosts of different types (for example, between FTPS and MOVEit DMZ servers) you should also use the "MISetDestPath" command to ensure that destination paths are properly parsed.

  Use a value of "(default)" to indicate a Windows file system host; in this case your path value should either begin with a drive letter (e.g., "C:\") or a UNC (e.g., "\\server\share\").

  idest is the ordinal number of the destination to change. The default for this optional parameter is 1, which means the first destination in the task. (Most tasks have only one destination.)

  Returns an error code which is 0 for success, 2540 if the named host does not exist, or 2850 if idest is out of range.

- errcode = **MISetDestPath**(NewPath [,idest])

  Changes the current file's view of one of the task's destinations so that it points to a different path. NewPath is the new path or directory name. idest has the same meaning that it does for MISetDestHost. Only the current file being processed (if any), and any files added via MIAddFile during this run of the process, are affected.

  Returns an error code which is 0 for success, or 2850 if idest is out of range.

- **MISetErrorCode** NumericErrorCode
  MISetErrorDescription ErrorDescription

  Sets the error code and error description for this process.

If the custom script determines that the file should not be transferred, it should call MISetErrorCode with a non-zero numeric error code and MISetErrorDescription with a textual description of the error. This information will be recorded by MOVEit Central, and the file will not be sent.

If the special value 5000 is set by MISetErrorCode, MOVEit Central will ignore the file. That is, it will not send the file, will not delete the original file, and will not flag an error which would cause the task to fail. Returning error code 5000 can be used to ignore unwanted files without alarming operators by having the task marked as unsuccessful. See also **MIIgnoreThisFile**

If the special value 5010 is set by MISetErrorCode, MOVEit Central will not count this process as having been run. Ordinarily, MOVEit Central will mark a task has having completed successfully (as opposed to "No actions taken") if any process runs, even if no files were downloaded or uploaded. But if all processes in a task end up calling MISetErrorCode 5010, and no files are transferred, then that task run is considered to have completed with "No actions taken". This affects which NextActions are executed at the end of the task.

- **MISetFilename** NewFilename

  Changes the name under which the file should be stored at the destination. The new filename should not contain a path.

- **MISetStatus** StatusText

  Set the status text to be displayed by MOVEit Central Admin while the script is running. This can be used by long-running scripts to inform the operator the status of the process. If MISetStatus is not called, the message "Running script scriptname" will be displayed.

- **MISetTaskParam** ParamName, ParamValue

  Sets the value of the specified task parameter. If the current task has no such parameter, a parameter of that name is created. Parameter names are not case-sensitive.

- **MISleep** Milliseconds

  Suspends the custom script for the specified number of milliseconds. Very little processor time is consumed during the pause.

- ErrCode = **MIStartTask**(TaskNameOrID [,TaskParams])

  Starts the specified task. The first parameter is either a task name (this is checked first) or a task ID. The optional second parameter allows you to specify values for task parameters. If a parameter name matches the name of a parameters configured in the task definition, the new value overwrites the configured value.

  The format of TaskParams is *ParamName1=ParamVal1|ParamName2=ParamVal2*|... The trailing | at the end of the last task parameter is optional.

  Here is an example in which a task called "SendSummaryFile" is started with two task parameters computed from within the script: ID and CheckNum.

  blnResult = MIStartTask("SendSummaryFile", "ID=" & strID & "|CheckNum=" & intCheckNum)

  Returns 0 if the task was started. Note: the task will probably still be running when this function returns; a 0 return code does not mean that the task will successfully run to completion.

- TaskName = **MITaskname**()

  Returns the name of the task.

- TaskGroups = **MITaskGroups**()

  Returns the names of the task groups to which the task belongs. This is a string containing the names of all applicable groups, separated by |. For instance, the result might be "Daily|For Argus Bank|By Fred", or just "". You can process this easily in VBScript by creating an array from it using the Split function.

Sample Scripts (Enterprise Only)

MOVEit Central Admin installs several different sample scripts into a "sample scripts" subfolder. Several of these are "example only" but a few are generalized versions of production scripts used by several MOVEit Central data center customers. A description of all of these scripts can be found below.

To see VERY basic script examples of just reading in and processing files, you may simply want to use the "Add Script" wizard to create a simple "all at once" or "line-by-line" example.

Finally, it is worth noting that each script runs in a separate thread, so errors in one script will not hurt MOVEit Central or the other tasks MOVEit Central is working on.

"Play" Scripts

- **CvtCatalog.vbs** - Performs simple XML processing against a file read in line by line.
- **Custom Errors.vbs** - Example of how to generate custom error codes and messages from a script.
- **FixLen Record In.vbs** - Reads in a fixed (line) length file, parses it, totals a few columns of numbers, and generates an exception report. Built to work with the files created by "FixLen Record Out.vbs"
- **FixLen Record Out.vbs** - Randomly generates fixed (line) length data sets to be consumed by "FixLen Record Out.vbs"
- **Reverse File.vbs** - Reads in a file and writes out the complete contents backwards. (e.g. "fox" becomes "xof")
- **StripLF.vbs** - Removes newlines from a file.
- **Task Groups.vbs** - Overwrites a file with the name of the task that is running, and the list of task groups the task belongs to.

Production Scripts

- **Clean IIS Web Logs.vbs** - Used to strip "local" addresses and non-interesting files out of IIS web server logs. Ipswitch uses this script to pre-process the logs from its marketing sites.
- **CleanupFolder.vbs** - Used to search through a folder and delete any files that were last modified more than n days ago and any empty folders (regardless of age). This script may be used on the local Windows file system only. To delete remote files use a "No Op" task and configure a filter to only download files older than n days. (See "***Configuring Tasks - Processes/Scripts - Built-In - No Op*** (see "***No Op***" on page 197)" for an example.) Parameters used by this script include:
  - folderPath - The path to the folder to cleanup.
  - fileAgeDays - Files older than (this value) days will be deleted.
  - includeSubfolders - If true, recurse through subfolders. (default=false)
  - deleteEmptyFolders - If true, it will delete any folders that are empty. (default=false)
  - logToFile - If true, a file named CleanupFolder_yyyy-mm-dd.log will be created in the "folderPath" directory. This log file will record each file considered and whether it was deleted or not. (default=false)
- **FileSize.vbs** - Used to obtain the file size from a single transferred file. This can be used in conjunction with Next Actions. Works with only one file or last file transferred.
- **IgnoreSmallFile.vbs** - Checks the size of each file processed against a minimum file size specified by a task parameter. Any files smaller than that value are ignored.
- **Kick Off Task.vbs** - Reads in from a file a "shared secret", a list of task names and runs all the named tasks. Used by a few large companies who like to "kick off" tasks from a mainframe process. (The source in this case is a file on the mainframe's FTP server marked to be deleted after successful transfer; there is no destination.)
- **OrigNames.vbs** - Compiles a complete list of all the files used by task into a comma-delimited list. Used by people who wish to have a complete list of all files processed by a task sent to them in Next Action emails. (The Next Action message body contains the macro "[Parm:OrigNames]")
- **Ping.vbs** - Pings several remote hosts to make sure they are still responding; generates an error message if one or more of these hosts goes down. (Used in a task with a single process and one or more Next Actions.)
- **PKZipWithPass.vbs** - Uses PKZip to compress a file and secure the compressed file with a password. Requires the PKZip application from PKWare.
- **PurgeStats.vbs** - Purges all entries from the statistics database older than a specified limit. (Note: this sample script was reimplemented as the built-in "Trim Statistics DB" script.)
- **Run DOS Command.vbs** - Executes a command specified by a task parameter, with arguments also specified by task parameters. The command is something that would normally be run at the command line, like "zip.exe" or "copy". (Note: The functions of this script are also available in the built-in "Command Line App" script.)

- **TrimStatsDB.vbs** - Goes through the MOVEit Central statistics database and purges entries older than X days. Purged entries may be deleted, copied to text files, or sent to another database. This script is run daily by most heavy Central users, included most datacenters. (Note: this sample script was reimplemented as the built-in "Trim Statistics DB" script.) See ***Trimming the database*** (see "***Trimming***" on page 466).
- **WordCount.vbs** - Counts the number of times a particular word appears in source files. The word MOVEit Central looks for is configured in a task parameter; the word count, a brief report and other information is written back into other task parameters. (Note: The functions of this script are also available in the built-in "Find Or Replace" script.)
- **ZipAllFiles.vbs** - Calls a command-line zip utility to zip up a collection of downloaded files and replace them with the zip file, so that only the zip file gets sent to the task destinations. When used with the "Run Process Once" and "Use Original Names for Cache Files" features, this task allows you to zip up an arbitrary collection of files and folders in one task, compared with two or more tasks for previous methods. (Note: The functions of this script are also available in the built-in "ZipAdvanced" script.)
- **ZipDir.vbs** - Calls a command-line zip utility to zip a local folder and its contents. Adds the zip file to the list of sources to be processed to destinations. (Note: The functions of this script are also available in the built-in "ZipAdvanced" script.)
- **ZipExe.vbs** - Uses MOVEit Central's command-line facility to demonstrate how to zip multiple source files into a single ZIP archive. (Note: The functions of this script are also available in the built-in "ZipAdvanced" script.)

Built-in

This section describes the built-in scripts available with MOVEit Central.

Built-in Scripts Overview

Built-in scripts are installed and updated along with MOVEit Central, and their source code may not be viewed or altered. Built-in scripts are available automatically as soon as you install MOVEit Central. By contrast, to use a custom script, you must load it into MOVEit Central.

There are two types of built-in script:

- Scripts that can be run as processes in tasks. This is the more common type.
- Scripts that can be used to parse the output from an unusual FTP or SSH server. These are used by specifying them in the configuration of an FTP or SSH host.

The following built-in process scripts are currently available.

- ***Certs Backup*** (on page 175) - Extracts client certificates from Windows and saves them to two files for backup purposes.
- ***Certs Restore*** (on page 176) - accepts as input PFX files created by the "Certs Backup" script, and imports them into Windows.
- ***Command Line App*** (on page 177) - Runs a command line application. Parameter placeholders to indicate input file and output file/folder allow for seamless integration into MOVEit Central tasks.
- ***Find Or Replace*** (on page 180) - Finds (i.e., counts) or replaces particular words or phrases in files. Also can strip or replace special characters such as tabs and line feeds.
- ***Header ID*** (on page 182) - Reads the first (Header) line of a file, determines the ID from a set character position and passes this as a new task parameter. Also can strip the first line.
- ***HTTP Get*** (on page 183) - Downloads a file from a webserver, using the GET verb.
- ***HTTP Post*** (on page 184) - Uploads a file to a webserver, using the POST verb.
- ***HTTP Put*** (on page 185) - Uploads a file to a webserver, using the somewhat uncommon PUT verb.
- ***HTTP SharePoint Get*** (on page 186) - Downloads a file from a Microsoft SharePoint server.
- ***HTTP SharePoint Put*** (on page 186) - Uploads a file to a Microsoft SharePoint server.
- ***Ignore All Files*** (on page 187) - Causes all files already downloaded or added via a script to be ignored in subsequent processing steps.
- ***Look Up*** (on page 188) - Looks up one or more values from a table given a key such as a file name, uploading username or source path.
- ***MessageWay Translation*** (on page 195) - Sends a file to a MessageWay server for translation or data format conversion.
- ***No Op*** (on page 197) - "No Operation". Generally used to force MOVEit Central to delete files from a source without transferring them.
- ***Prepend Lines*** (on page 200) - Inserts up to four lines at the beginning of a file.
- ***Report Long Running Tasks*** (on page 201) - Queries the micstats database and reports back information about any tasks that have been running longer than the specified time interval.
- ***Set Destination*** (on page 202) - Changes the host definition (and optionally, the path) of the destination used in this task run.
- ***Sleep*** (on page 203) - Pauses task operation for a specified number of seconds or milliseconds.
- ***SMIME Receive*** (on page 204) - Retrieves and decrypts an S/MIME encoded email attachment.
- ***SMIME Send*** (on page 205) - Encrypts a file and sends it as an S/MIME email attachment.
- ***Tamper Detect*** (on page 206) - Checks for tampering in the audit and activity history tables.
- ***Trim Statistics DB*** (on page 207) - Archives old MOVEit Central log records into a flat file every few days.
- ***Unzip Advanced*** (on page 209) - Unzips ZIP archives with an optional ZIP password.
- ***XSL Transform*** (on page 209) - Transforms XML documents with XSL stylesheets/templates.

- ***Zip Advanced*** (on page 210) - Creates ZIP archives with one or multiple files, configurable level of compression and an optional ZIP password.

These built-in process scripts are also available when a MOVEit Central PGP license has been enabled. More information about how to use MOVEit Central to encrypt and decrypt PGP files may be found in the ***MOVEit Central PGP documentation*** (on page 325).

- ***PGP Decrypt*** (on page 198) - Used to decrypt PGP files.
- ***PGP Encrypt and Sign*** (on page 199) - Used to encrypt and sign PGP files.
- ***PGP Encrypt Only*** (on page 200) - Used to encrypt but not sign PGP files.

The following built-in directory parsing scripts are available:

- **FTP Directory Parse - AS400**. This can be configured as a directory parsing script on the Advanced Options dialog when configuring an FTP host. It should be used only if the FTP server is a standard IBM AS/400 (iSeries) server. However, it is recommended that instead of using this parsing script, you configure the host with the value SITE LISTFMT 1 for the "Additional commands to execute upon signon" setting available on the same Host configuration dialog. This asks the AS/400 to use a more standard listing format, which can be automatically recognized by MOVEit Central.

Certs Backup

"Certs Backup" extracts MOVEit Central's client certificates from its Windows Certificate Store and saves them to two files so they can be saved/sent to a destination for backup purposes. The related "***Certs Restore*** (on page 176)" built-in script is used to restore the certificates in these files.

To use this script, first configure a source-less task with a per-task process that runs this script. Then configure one or more destinations to save the files to their final locations.

An example of a complete task and a recommendation on its use can be found in the "***Central Service - Backup - Automated Configuration Replication*** (on page 39)" documentation.

Input Parameters

- **Certs_Password** (*Required*) - The password that will encrypt the output PFX files.
- **Certs_Filename_Personal** - The filename (no path) of the output PFX file containing the certificates (with private keys) from the My Certs/Personal store. Default value is "CertsPersonal.pfx". Date macros are allowed.
- **Certs_Filename_OtherPeople** - The filename (no path) of the output PFX file containing the certificates (no private keys) from the Other Certs/Other People store. (Currently used only for SMIME recipients and some AS1/AS2/AS3 certificates.) Default value is "CertsOtherPeople.pfx". Date macros are allowed.

Notes

When MOVEit Central is running as a foreground application, this script will generally not work properly because a different users' Windows Certificate Store will generally be used in foreground mode than when MOVEit Central is running as a service.

Certs Restore

"Certs Restore" imports client certificates from input PFX files created by the "Certs Backup" built-in script into the Windows Certificate Store used by MOVEit Central.

To use it, configure a task with a source that downloads the two files created by the "Certs Backup" built-in script. Then configure a per-file process to run this script to restore the certificates in those two files.

An example of a complete task and a recommendation on its use can be found in the "***Central Service - Backup - Automated Configuration Replication*** (on page 39)" documentation.

Input Parameters

- **Certs_Password** (*Required*) - The password that the built-in "***Certs Backup*** (on page 175)" script used to encrypt the PFX files.

Notes

When MOVEit Central is running as a foreground application, this script will generally not work properly because a different users' Windows Certificate Store will generally be used in foreground mode than when MOVEit Central is running as a service.

Command Line App

"Command Line App" runs a command line application. Parameter placeholders to indicate input and output files allow for seamless integration into MOVEit Central tasks.

Input Parameters

- **CommandLineApp_AppPath** (*Required*) - Specifies the full path of the command line application to run.
- **CommandLineApp_AppParms** - Specifies the parameters passed into the command line application. Use the special macro [InputFile] to indicate the name of the file against which the command line application should execute. If you expect the command line application to write new output use either [OutputFile] for a single output file or [OutputFolder] to indicate an output folder (which can include multiple files and subfolders). Pipe output to [StdOut] and [StdErr] macros to have this information displayed in the debug log and in parameters for later use.
- **CommandLineApp_AltReturnCodes** - By default, a return code of 0 indicates success. This parameter allows other return codes besides zero to also indicate success. Alternate values must be separated with commas. For example, a value of "0,3,7" in this parameter indicates that zero and two other return codes all signal success. Note: If zero if not specified as an alternate return code and any other alternate return codes are specified, zero will not be considered a successful return code.

Notes

The "[InputFile]", "[OutputFile]", "[OutputFolder]", "[StdOut]" and "[StdErr]" macros used with this built-in process are not available for general use in other MOVEit Central sources, destinations, processes or next actions.

When the "[OutputFolder]" macro is used, any "[InputFile]" cache files will be ignored in the final output. For example, if CommandLineApp was used to run "unzip.exe [InputFile] -d [OutputFolder]", the Zip file indicated by the "[InputFile]" parameter would not be included in the set of files sent to the destination.

To record any "standard" or "error" output written by your command line application, append the following phrase to your usual CommandLineApp_AppParms value.
> [StdOut] 2> [StdErr]
For example, if your original CommandLineApp_AppParms value is "a c:\windows\system32\eula.txt", you can record output with a revised CommandLineApp_AppParms value of "a c:\windows\system32\eula.txt > [StdOut] 2> [StdErr]". Any "StdErr" output will appear in the debug log at the "Warnings" level and higher and any "StdOut" output will appear in the debug log at the "Some Debug" level and higher. To use the first 8192 characters of each type of output in your Next Actions, use the related "[Parm:CommandLineApp_StdOut]" and "[Parm:CommandLineApp_StdErr]" output parameters.

This built-in script may be run per-file or once-after-all-files. This built-in script may be run as the first step of a task.

Date macros (on page 142) are frequently used with command line arguments. Remember that operators (such as the minus sign) normally apply to all times and dates in a macro phrase. To apply operators to only part of a macro phrase, use double-quotes to delimit phrases. For example, if today is currently July 5, 2007, a macro of:

- [dd][mm-][yyyy] [dd][mm][yyyy] yields 05062007 05062007
- "[dd][mm-][yyyy]" [dd][mm][yyyy] yields "05062007" 05072007

Example #1

Joe would like to run a command line application to read files passing through MOVEit Central and make sure they contain valid data. His application will NOT change the contents of the files. The syntax used by his application is "checkapp.exe -verify *(input file)*" and his application is installed into his "C:\Program Files\VerifyIt" folder.

To integrate this application with MOVEit Central, Joe should...

1. Create a new task with a source, process, destination and schedule.
2. Select "Command Line App" as his process
3. Set process parameters:
   - CommandLineApp_AppPath = "C:\Program Files\VerifyIt\checkapp.exe"
   - *(Add)* CommandLineApp_AppParms = "-verify [InputFile]"

If Joe also wanted to see any standard or error output generated by his command line application as it ran, he could also have added the phrase " > [StdOut] 2> [StdErr]" to the end of his CommandLineApp_AppPath value. This would have allowed him to see this output in his debug log: command line errors at the "Warning" level or higher and other output at the "Some Debug" level or higher.

If Joe also wanted to see this kind of output in an email or send it to another task, he could also have used the output macros "[Parm:CommandLineApp_StdOut]" and "[Parm:CommandLineApp_StdErr]".

Example #2

Nancy would like to run a command line application to process files passing through MOVEit Central. Her application will change the contents of the files if they are valid and will return a non-zero error code if the files are not valid. The syntax used by her application is "alterapp.exe -x207 -i=*(input file)* -o=*(output file)*" and her application is installed into her "D:\AlterProg" folder.

To integrate this application with MOVEit Central, Nancy should...

1. Create a new task with a source, process, destination and schedule.
2. Select "Command Line App" as her process
3. Set process parameters:

- CommandLineApp_AppPath = "D:\AlterProg\alterapp.exe"
- *(Add)* CommandLineApp_AppParms = "-x207 -i=[InputFile] -o=[OutputFile]"

Example #3

Pedro would like MOVEit Central to transfer reports created by a stand-alone command-line application. His application does not need a "source file" and will return a non-zero error code if it cannot create its reports. The syntax used by his application is "makereports.exe -repcode=76 *(output file)*" and his application is installed into his "C:\Program Files\DBExtracts" folder.

To integrate this application with MOVEit Central, Pedro should...

1. Create a new task with a process, destination and schedule. (No source!)
2. Select "Command Line App" as his process
3. Set process parameters:
   - CommandLineApp_AppPath = "C:\Program Files\DBExtracts\makereports.exe"
   - *(Add)* CommandLineApp_AppParms = "-repcode=76 [OutputFile]"

Example #4

Paul would like to run a command line "unzip with odd encryption" application on files passing through MOVEit Central. Each original archive file may contain one or more files, perhaps including files in archived subfolders. The syntax used by his application is "oddzip.exe -enc=codfish -ifil=*(input file)* -ofol=*(output folder)*" and her application is installed into her "D:\OddZip" folder.

To integrate this application with MOVEit Central, Nancy should...

1. Create a new task with a source, process, destination and schedule.
2. Select "Command Line App" as her process
3. Set process parameters:
   - CommandLineApp_AppPath = "D:\OddZip\oddzip.exe"
   - (Add) CommandLineApp_AppParms = "-enc=codfish -ifil=[InputFile] -ofol=[OutputFolder]"

Paul will control whether or not he wants to respect the subfolders the archive file's members were stored in in his Destination element (by checking/unchecking the "Use Relative Subdirectories" option).

Find Or Replace

"Find Or Replace" Finds (i.e., counts) or replaces particular words or phrases in files. It can also handle special characters such as tabs and line feeds.

Input Parameters

- **FindOrReplace_Find** (*Required*) - Specifies a value to find.
- **FindOrReplace_Replace** - Specifies a value to replace. (Ignored if Action is "Find".)
- **FindOrReplace_Action** (*Required*) - Specifies whether to just find (and count) instances or replace them as well.
- **FindOrReplace_CaseSensitive** (*Required*) - Specifies whether comparisons are case sensitive or not.
- **FindOrReplace_SkipFileSizeMB** - If a file is larger than this (MB) and if special characters are being used, then skip that file (for performance reasons). The default is 100; maximum value is 500 (500MB).

Output Parameters

- **FindOrReplace_Count** - Returns the number of times the Find value appeared in this file.
- **FindOrReplace_CountTask** - Returns the number of times the Find value appeared in all files encountered during this task run.

Special Characters

FindOrReplace can handle special character operations such replacing all tabs with three spaces or stripping carriage returns from a file. To work with special characters, you must represent them using special character "macros" in your FindOrReplace_Find or FindOrReplace_Replace parameters as appropriate.

The following special character macros are supported.

- **[char_cr]** - Carriage return (ASCII 13)
- **[char_lf]** - Line feed (ASCII 10)
- **[char_crlf]** - Carriage return followed by a line feed (ASCII 13+10)
- **[char_tab]** - Tab (ASCII 9)
- **[char_ff]** - Form feed (ASCII 12)
- **[char_null]** - Null (ASCII 0)
- **[char_###]** - ASCII code ###

For example, to:

- ...replace tabs with three spaces, configure:
  - FindOrReplace_Find = "[char_tab]"
  - FindOrReplace_Replace = " "

- ...strip line feeds, configure:
  - FindOrReplace_Find = "[char_lf]"
  - FindOrReplace_Replace = ""
- ...add a carriage return to the end of each line feed, configure:
  - FindOrReplace_Find = "[char_lf]"
  - FindOrReplace_Replace = "[char_crlf]"
- ...replace "doAg" with "BonE", configure:
  - FindOrReplace_Find = "do[char_65]g"
  - FindOrReplace_Replace = "[char_66]on[char_69]"

Notes

Please only use the replace operation this against text files as replacing text in a binary file could have unforeseen consequences.

This built-in script may only be run per-file. This built-in script may not be run as the first step of a task.

Example #1

Ed would like email listing how many times the word "- PAGE" appears in files that pass through MOVEit Central.

To perform this operation with MOVEit Central, Ed should...

1. Create a new task with a source, process, destination, schedule and next action.
2. Select "Find Or Replace" as his process
3. Set process parameters:
   - FindOrReplace_Action = "Find"
   - FindOrReplace_Find = "- PAGE"
   - FindOrReplace_CaseSensitive = "Yes"
4. Configure his next action to:
   - send him an email with the macro "[Parm:FindOrReplace_Count]" in the message body.
   - run per-file (not per-task).

Example #2

Jane would like to replace all instances of "bubbler" with "drinking fountain" in files that pass through MOVEit Central.

To perform this operation with MOVEit Central, Jane should...

1. Create a new task with a source, process, destination and schedule.
2. Select "Find Or Replace" as her process

3. Set process parameters:
   - FindOrReplace_Action = "Replace"
   - FindOrReplace_Find = "bubbler"
   - FindOrReplace_CaseSensitive = "No"
   - *(Add)* FindOrReplace_Replace = "drinking fountain"

Header ID

"Header ID" reads a text string on the first (Header) line of a file from a set character position. A new task parameter called HeaderID_Value can be used for integration into MOVEit Central tasks.

Input Parameters

- **HeaderID_Length** (*Required*) - Specifies the number of characters (length) to read from the first line of the file.
- **HeaderID_Start** (*Required*) - Specifies the starting character position (column) from which to read the text string value.
- **HeaderID_Strip** - Set this optional parameter to "Yes" if you would like to remove the entire first line after capturing the Header ID_Value.

Output Parameter

- **HeaderID_Value** - Returns the text string found on the first line, beginning at HeaderID_Start and continuing for HeaderID_Length characters.

Example #1

Bill would like to read a value from the first line of a file starting in column 1 and continuing 8 characters and then use this text string to rename the file on the task's destination (with a date stamp extension).

To integrate this application with MOVEit Central, Bill should...

1. Create a new task with a source, process, destination and schedule.
2. Select "Header ID" as his process
3. Set process parameters:
   - HeaderID_Start = 1
   - HeaderID_Start = 8
4. Edit the Destination to set FileName to [Parm:HeaderID_Value].[YYYY][MM][DD]

Example #2

Cheryl would like to read a value from the first line starting in column 5 and continuing 6 characters. She wants to discard this first line and use the HeaderID_Value in conjunction with a LookUp process to find which folder on a FTP server each respective file should go.

To integrate this application with MOVEit Central, Cheryl should...

1. Create a new task with a source, process, destination and schedule.
2. Select "Header ID" as her 1st process
3. Set the Header ID process parameters:
   - HeaderID_Start = 5
   - HeaderID_Start = 6
4. Add a second process, choosing the built in "Look Up" script
5. Set the Look Up process parameters:
   - LookUp_Key = [Parm:HeaderID_Value]
   - LookUp_FilePath = C:\LookUp\List1.txt (Note: this is just an example)
   - LookUp_ActionIfKeyNotMatched = Throw_Error
   - LookUp_MatchType = Require_Exact_Match
6. Edit the Destination to set Folder to [Parm:LookUp_Value]

HTTP Get

"HTTP Get" downloads a file from a website, using HTTP[S] with the GET verb. This script is not suitable for files larger than a few dozen megabytes, because it loads the entire file into memory before saving it.

Use this script like a source. Then configure one or destinations to save the files to their final locations.

Input Parameters

- **HTTP_URL** *(Required)* - The full URL of the file; e.g., https://myserver/reports/Daily.txt. Date and parameter macros are permitted.
- **HTTP_IgnoreCertProblems** - Whether problems with the remote server certificate (such as signer not trusted) should be ignored. Defaults to False.
- **HTTP_User** - The username, for HTTP authentication.
- **HTTP_Password** - The password, for HTTP authentication.
- **HTTP_DestFilename** - The destination filename. If not specified, the filename from the URL will be used. Date and parameter macros are permitted.

Notes

This script will work only when the website requires either no authentication, or HTTP authentication. Unfortunately, many websites require the user to signon via a web form, and/or to navigate through the site in order to access the download page. This script will not support websites like that.

HTTP Post

"HTTP Post" uploads a file to a website, using HTTP[S] with the POST verb. POST is the mechanism used by most websites that accept browser-based uploads.

Use this script like a destination, as a per-file process. Typically you would use this in a task with one or more sources.

Input Parameters

- **HTTP_URL** (*Required*) - The URL to post to; e.g., https://myserver/cust/upload.aspx. May include macros.
- **HTTP_IgnoreCertProblems** - Whether problems with the remote server certificate (such as signer not trusted) should be ignored. Defaults to False.
- **HTTP_User** - The username, for HTTP authentication. If the website uses form-based authentication rather than HTTP authentication, then this script will not work.
- **HTTP_Password** - The password, for HTTP authentication.
- **HTTP_DestFilename** - The destination filename. If not specified, the original filename is used.
- **HTTP_FileFormField** (*Required*) - The name of the form field for the file contents. May include macros.
- **HTTP_ExtraFields** - The names and values of optional extra form fields to be provided along with the POSTed file. This is very application-specific. The format is a string like fldname1=value1|fldname2=value2|... May include macros.
- **HTTP_MaxFileSizeMB** - If a file is larger than this (MB), then skip that file and signal an error. Default 100; max value 500.

Notes

This script will work only when the website requires either no authentication, or HTTP authentication. Unfortunately, many websites require the user to signon via a web form to authenticate. This script will not support websites like that.

This script is not suitable for files larger than a few dozen megabytes, because it loads the entire file into memory before saving it.

HTTP Put

"HTTP Put" uploads a file to a website, using HTTP[S] with the PUT verb. Note that PUT is not the usual way to upload files, and is not accepted by many websites. The ***HTTP Post*** (on page 184) script may work as an alternative for these sites. However, when available, the HTTP PUT technique is preferable because it is simpler.

Use this script like a destination, as a per-file process. Typically you would use this in a task with one or more sources.

Input Parameters

- **HTTP_URL** (*Required*) - The URL of the folder to upload to; e.g., https://myserver/reports. May include macros.
- **HTTP_IgnoreCertProblems** - Whether problems with the remote server certificate (such as signer not trusted) should be ignored. Defaults to False.
- **HTTP_User** - The username, for HTTP authentication.
- **HTTP_Password** - The password, for HTTP authentication.
- **HTTP_DestFilename** - The destination filename. If not specified, the original filename is used.
- **HTTP_MaxFileSizeMB** - If a file is larger than this (MB), then skip that file and signal an error. Default 100; max value 500.

Notes

This script will work only when the website requires either no authentication, or HTTP authentication. Unfortunately, many websites require the user to signon via a web form to authenticate. This script will not support websites like that.

To enable PUT on a remote webserver running Microsoft IIS 6.0, use IIS Manager on that webserver to enable the WebDAV Web Service Extension, and turn on Write access to the virtual directory.

This script is not suitable for files larger than a few dozen megabytes, because it loads the entire file into memory before saving it.

HTTP SharePoint Get

"HTTP SharePoint Get" downloads files from a Windows SharePoint Server website, using HTTP[S]. This script is not suitable for files larger than a few dozen megabytes, because it loads the entire file into memory before saving it.

Use this script like a source. Then configure one or destinations to save the files to their final locations.

Input Parameters

- **SharePoint_BaseURL** (*Required*) - The base URL of the website. For SharePoint 2003, this will be something like https://server. For SharePoint 2007, this will be something like https://server/Docs.
- **SharePoint_DeleteAfterDownload** - Whether the source file should be deleted from SharePoint after a successful download. Defaults to False.
- **SharePoint_IgnoreCertProblems** - Whether problems with the remote server certificate (such as signer not trusted) should be ignored. Defaults to False.
- **SharePoint_HTTPUser** - The username, for HTTP authentication.
- **SharePoint_HTTPPassword** - The password, for HTTP authentication.
- **SharePoint_Folder** (*Required*) - The name of the SharePoint folder, including parent folders if applicable. For SharePoint 2003, use "Shared Documents" for the default library. For SharePoint 2007, use "Documents" for the default library. Date and parameter macros are permitted.
- **SharePoint_FileMask** (*Required*) - The filemask specifying which files to download; e.g., *.txt. Date and parameter macros are permitted.

HTTP SharePoint Put

"HTTP SharePoint Put" uploads a file to a Windows SharePoint Server website, using HTTP[S]. This script is not suitable for files larger than a few dozen megabytes, because it loads the entire file into memory before sending it.

Use this script like a destination, as a per-file process. Typically you would use this in a task with one or more sources.

Input Parameters

- **SharePoint_BaseURL** (*Required*) - The base URL of the website. For SharePoint 2003, this will be something like https://server. For SharePoint 2007, this will be something like https://server/Docs.
- **SharePoint_IgnoreCertProblems** - Whether problems with the remote server certificate (such as signer not trusted) should be ignored. Defaults to False.
- **SharePoint_HTTPUser** - The username, for HTTP authentication.
- **SharePoint_HTTPPassword** - The password, for HTTP authentication.
- **SharePoint_Folder** (*Required*) - The name of the SharePoint folder, including parent folders if applicable. Macros are permitted. For SharePoint 2003, use "Shared Documents" for the default library. For SharePoint 2007, use "Documents" for the default library.
- **SharePoint_Filename** - The name to be given to the file. If not specified, the original filename is used. Macros are permitted.
- **SharePoint_MaxFileSizeMB** - If a file is larger than this (MB), then skip that file and signal an error. Default 100; max value 500.

Ignore All Files

This script causes all files already downloaded or added via a script to be ignored in subsequent processing steps.

Input Parameters

- **IgnoreAllFiles_Error5010** (*Required*): Affects which "Next Action" is executed at the end of the task, and allows you to select how subsequent processing occurs. Determines whether the script should return error 5010 to indicate No Files. Defaults to *False* which returns 0 to indicate Success. When a task checks multiple sources for files, but finds no files, the IgnoreAllFiles script returns a Success message, which could be confusing. When you set this parameter to *True*, it will always return error 5010, whether files were found or not.

Example #1

You use trigger files to determine which source files need to be transferred, and you want to exclude the trigger files from the source list.

To perform this operation with MOVEit Central, you...

1. Download X trigger files from a source.
2. For each trigger file, run custom "Process Trigger Files" script, which reads each trigger file and builds a list of files to download into a custom task parameter.
3. Run Ignore All Files to clear the trigger files from the file processing list.
4. Download all files specified by the custom task parameter built from the trigger files.
5. Upload files to the target destination.

Look Up

"Look Up" looks up a key, usually expressed with a macro, against a text file filled with one column of keys and up to five columns of values.

For example, given a file name of "report56.txt" (in the Lookup_Key parameter) and the path to a file containing the following keys and values (in the Lookup_FilePath parameter), the Look Up built-in script would return a value of "customer13.rpt" (in the Lookup_Value parameter). To obtain this Lookup_Value, the Look Up built-in script would compare Lookup_Key to the "file keys" and return the related value from the **first matching line**.

```
report44.txt,customer01.ttk
report56.txt,customer13.rpt
report66.txt,customer87.lml
```

Input Parameters

- **LookUp_Key** (*Required*) - The value that needs to be looked up.
- **LookUp_FilePath** (*Required*) - Specifies where the "lookup file" containing delimited keys and values may be found.
- **LookUp_NumValues** - Specifies the number of value columns that the script should attempt to look for within the lookup table. The default is 5 value columns.
- **LookUp_CaseSensitive** (*Required*) - Specifies whether or not key comparisons are case-sensitive or not. (The default value is "No".) This parameter applies no matter which value of LookUp_MatchType is selected.
- **LookUp_Delimiter** - Specifies an alternate column delimiter. (The default value is a comma, i.e., ",".) For example, if a single line of keys and values looked like "753|blue|large", this parameter would need to be set to a vertical bar, i.e., "|".
- **LookUp_CommentChar** - Specifies an alternate character to indicate a line is a comment line, not a data line. (The default value is a single quote, i.e., "'".) For example, if a single line of comment looked like "# This is a comment", this parameter would need to be set to a pound sign, i.e., "#".
- **LookUp_ActionIfKeyNotMatched** (*Required*) - Specifies what to do if LookUp_Key does not match any values in the table. There are four possible values if no match is found for LookUp_Key.
  - **Throw_Error** (*Default*) - This task run and/or file transfer will end with an error (#120).
  - **Ignore_File** - This task run and/or file transfer will end with an "ignore this file" status code. Normally, you should only use this option if your Lookup script has been set to run "per file" so individual files can be ignored.
  - **Return_Key_in_Values** - This task run and/or file transfer will continue without error and the value of LookUp_Key will be copied into all the LookUp_Value* parameters.
  - **Return_Blank_Values** - This task run and/or file transfer will continue without error and the LookUp_Value* parameters will be set to a blank value.

- **LookUp_MatchType** (*Required*) - Specifies how LookUp_Key should be looked up against keys in the file table. There are three possible values. The term "file key" refers to the values in column 1 in the lookup file.
    - **Require_Exact_Match** (*Default*) - This means that LookUp_Key must exactly match keys in the file. Example: LookUp_Key "dog.txt" will match file key "dog.txt", but not file key "do". Also, LookUp_Key "do" will not match file key "dog.txt".
    - **Allow_Partial_Match_of_LookUp_Key** - This means that LookUp_Key will be treated as a "partial key" and will match file keys if they appear anywhere in the file keys. Example: A LookUp_Key of "dog.txt" or "dog" will match file key "dog.txt", but not file key "do". Wildcards are permitted (see below).
    - **Allow_Partial_Match_of_File_Keys** - This means that file keys will be treated as "partial keys" and will match LookUp_Key if they appear anywhere in the lookup key. Example: LookUp_Key "dog" will match file key "do", but not file key "dog.txt". Wildcards are permitted (see below).
- **LookUp_ReturnAs** - Optional, alternate name for LookUp_Value return value. For example, if LookUp_ReturnAs="AltFolder" and LookUp_Value="\another\fol", then the macro "[Parm:AltFolder]" will be interpreted as "\another\fol" during the rest of the task run.

Wildcards

Lookup keys may contain wildcards, except when "Require_Exact_Match" is in effect. The wildcard syntax is similar to Windows filename masks, with some enhancements:

Wildcard char	Meaning
*	Match zero or more of any character
?	Match exactly one of any character
@	Match exactly one alphabetic character
#	Match exactly one digit
anything else	Match exactly that character

Some examples:

dog#	Matches "dog3", but not "dog" or "dogs3"
dog*7	Matches "dog7", "dog37" and ")dog/7PP" but not "dog" or "do7".

Output Parameters

- **LookUp_Value** - Value found by looking up LookUp_Key. If there are multiple data columns in the lookup table, this is the value from the first column. If LookUp_Key was not matched, this value is controlled by the LookUp_MatchType parameter.
- **LookUp_Value2** - Similar to LookUp_Value, except from data column 2, if available.
- **LookUp_Value3** - Similar to LookUp_Value, except from data column 3, if available.
- **LookUp_Value4** - Similar to LookUp_Value, except from data column 4, if available.
- **LookUp_Value5** - Similar to LookUp_Value, except from data column 5, if available.
- **LookUp_ValueN** - Similar to LookUp_Value, except from data column N, if available.
- **(Value of LookUp_ReturnAs)** - If a value has been provided in the LookUp_ReturnAs parameter, the value of LookUp_Value will also be returned as a parameter bearing that name. For example, if LookUp_ReturnAs="AltFolder" and LookUp_Value="\another\fol", then the macro "[Parm:AltFolder]" will be interpreted as "\another\fol" during the rest of the task run.

Notes

In most production cases, you will probably use macros such as "[OrigName]", "[OnlyName]", "[RelativePath]" or "[MID([OrigName], 2, 3)]" in your "LookUp_Key" parameter.

This built-in script may be run wherever processes are allowed, including alone in its own task.

Example #1

Fred would like look up a specific internal folder based on the username that uploaded a file. If a record for a particular username cannot be found, an error should be logged.

To perform this operation with MOVEit Central, Fred should...

1. Create a "lookup table" file containing content similar to the following and save it as "d:\customer2folder\fred.txt"

   ```
   ' Format is username,folder
   jack,D:\blue\2134
   diane,D:\red\3734
   american,D:\blue\3357
   kids,D:\red\1651
   heartland,D:\red\2162
   ```

2. Create a new task with a source, process, destination, and schedule.
3. Select "Look Up" as his process.
4. Set process parameters:
   - LookUp_Key = "[OrigUser]"
     (Username of user who uploaded the file; only works on MOVEit DMZ sources.)
   - LookUp_FilePath = "d:\customer2folder\fred.txt"
   - LookUp_CaseSensitive = "No"
   - LookUp_MatchType = "Require_Exact_Match"
   - LookUp_ActionIfKeyNotMatched = "Throw_Error"
5. Configure his destination to:
   - use the macro "[Parm:LookUp_Value]" in the "Path" field.

Given the contents of "fred.txt" displayed above, the following uploader usernames would cause the following values to be placed into the LookUp_Value parameter.

Uploader Username	LookUp_Value
diane	D:\red\3734
heartland	D:\red\2162
congress	*(NONE - ERROR)*

Example #2

Nancy would like to change the names that several of her files are saved as, but many file names will already bear the correct names.

To perform this operation with MOVEit Central, Nancy should...

1. Create a "lookup table" file containing content similar to the following and save it as "d:\correctoddfiles\nancy.txt"

   ```
   ' Format is incoming filename, corrected filename
   JHJ45KK,nice_J45.dat
   JTE_KTR_67,nice_K67.dat
   K_P0KX_R89,nice_L89.dat
   ```

2. Create a new task with a source, process, destination, and schedule.
3. Select "Look Up" as his process.
4. Set process parameters:
   - LookUp_Key = "[OrigName]"
   - LookUp_FilePath = "d:\correctoddfiles\nancy.txt"
   - LookUp_CaseSensitive = "Yes"
   - LookUp_MatchType = "Require_Exact_Match"
   - LookUp_ActionIfKeyNotMatched = "Return_Key_in_Values"
     (If there is no match, let the original file name "fall through".)
5. Configure her destination to:
   - use the macro "[Parm:LookUp_Value]" in the "Filename" field.

Given the contents of "nancy.txt" displayed above, the following filenames would cause the following values to be placed into the LookUp_Value parameter.

Source File Name	LookUp_Value
JHJ45KK	nice_J45.dat
hello.txt	hello.txt
K_POKX_R89	nice_L89.dat
K_pokx_R89	K_pokx_R89

Example #3

Ed would like to set FTP mainframe parameters based on the names of files MOVEit Central has just downloaded. He wants to be able to handle both specific filenames (e.g., "four.txt"), general extension (e.g., ".txt") and provide a "catch-all" value.

To perform this operation with MOVEit Central, Ed should...

1. Create a "lookup table" file containing content similar to the following and save it as "d:\blocking\ed.txt"

   ```
   ' List specific filenames first
   four.txt,80,4
   ' Next, list specific extensions
   .txt,80,10
   .dat,133,5
   ' Finally, provide a catch-all case
   ' (this assumes all incoming filenames will contain a period)
   .,80,10
   ```

2. Create a new task with a source, process, destination, and schedule.
3. Select "Look Up" as his process.
4. Set process parameters:
   - LookUp_Key = "[OrigName]"
   - LookUp_FilePath = "d:\blocking\ed.txt"
   - LookUp_CaseSensitive = "No"
   - LookUp_MatchType = "Allow_Partial_Match_of_File_Keys"
     (This will allow "five.txt" to match the ".txt" file record.)
   - LookUp_ActionIfKeyNotMatched = "Return_Blank_Values"
5. Configure his FTP destination to:
   - use the macros "[Parm:LookUp_Value]" and "[Parm:LookUp_Value]" in the "additional commands to execute before transfer" field.

Given the contents of "ed.txt" displayed above, the following source file names would cause the following values to be placed into the LookUp_Value and LookUp_Value2 parameters.

Source File Name	**LookUp_Value**	**LookUp_Value2**
four.txt	80	4
five.txt	80	10
six.dat	133	5
seven.rpt	80	10

Example #4

Ralph would like to scan an entire folder structure and only transfer files that match names in his lookup table file. Files that do match should usually be renamed.

To perform this operation with MOVEit Central, Ralph should...

1. Create a "lookup table" file containing content similar to the following and save it as "d:\onlysome\ralph.txt"

    ```
    ' List specific filenames first
    ur.txt,rrr[OnlyName].xtx
    ' Next, list specific extensions
    .txt,[OrigName]
    .dat,[OnlyName].tad
    ```

2. Create a new task with a source, process, destination, and schedule.
3. Select "Look Up" as his process.
4. Set process parameters:
    - LookUp_Key = "[OrigName]"
    - LookUp_FilePath = "d:\onlysome\ralph.txt"
    - LookUp_CaseSensitive = "No"
    - LookUp_MatchType = "Allow_Partial_Match_of_File_Keys"
      (This will allow "five.txt" to match the ".txt" file record.)
    - LookUp_ActionIfKeyNotMatched = "Ignore_Files"
5. Configure his destination to:
    - use the macro "[Parm:LookUp_Value]" in the destination "filename" field.

Given the contents of "ralph.txt" displayed above, the following source file names would cause the following files to appear on the destination with the following names.

Source File Name	Destination File Name
four.txt	rrrfour.xtx
five.txt	five.txt
six.dat	six.tad
seven.rpt	*(file ignored)*

MessageWay Translation

"MessageWay Translation" sends a file to a MessageWay server for translation or data format conversion.

The resulting output files are added to MOVEit Central's list of files to process, which typically means they are sent to one or more destinations, depending on the task's configuration. The original input file is ignored, which means that the task will do no further processing on it, and it will not be sent to task destinations.

Depending on the input file and the translation rules configured on the MessageWay server, a single input file may result in multiple output files. On the other hand, if no processing rules match the input file, or if errors occur, no output files may be created.

The MessageWay translation engine is very powerful, and the various EDI (Electronic Data Interchange) standards governing data format are complex. Consult the translation-related MessageWay manuals, such as *MessageWay Translator Workbench* User's *Guide and Reference*, for detailed information on how to set up a MessageWay server for translation.

For more information about the script itself, see the topic ***"Common Applications - MessageWay Translation."*** (on page 277)

Input Parameters

- **MWayConn_Host** (*Required*) - Hostname of the MessageWay server.
- **MWayConn_SSL** - Whether SSL is to be used. Default: True.
  Note: if you use SSL, you must specify the MessageWay server's certificate's fingerprint in MWayConn_SSLFingerprint. If the server is on the same computer as MOVEit Central, you can safely specify False here and avoid having to know the certificate's fingerprint.
- **MWayConn_Port** - TCP port number. Default: 6280 if not SSL, or 6243 if SSL. You generally do not need to specify this parameter.
- **MWayConn_SSLFingerprint** - Hexadecimal fingerprint (MD5 or SHA1) of the server's certificate. Required if MWayConn_SSL is True. (There is no way to specify that any certificate should be accepted.) The string consists of groups of 2 hex characters separated by spaces.
- **MWayConn_User** (*Required*) - MessageWay username.
- **MWayConn_Password** (*Required*) - MessageWay user's password.
- **MWayConn_Recipient** - Destination of translated files. For example, the destination "translate:moveit" means that there must be a translation location named "translate" and a mailbox named "moveit" configured in MessageWay. The specified user must have sufficient access to these locations.
- **MWayConn_Sender** - Arbitrary sender's name. May include macros. The MessageWay translation engine may base its translation rules partly on the sender's name.
- **MWayConn_MIMEType** - Arbitrary MIME type string. May include macros.
- **MWayConn_RetryCount** - Maximum number of retries to connect to MessageWay. Defaults to 0. The script will retry only if certain types of errors occur, such as an inability to connect to the MessageWay server.

- **MWayConn_RetrySeconds** - Number of seconds between attempts to connect to MessageWay. Defaults to 30.
- **MWayConn_MaxSeconds** - The maximum number of seconds to wait for MessageWay to process the file. A value of 0 means no limit. May include macros. Defaults to 7200 (two hours).
- **MWayConn_PollIntervalSeconds** - The number of seconds to wait between queries to MessageWay to determine whether processing has completed. May include macros. Defaults to 5 seconds.
- **MWayConn_ExceptionsInsteadOfData** - Tells the script how to behave when any exception occurs (meaning poorly formatted data). True means no data files should be returned; instead, the exception report files are returned. Defaults to False, which means only data files are returned. If False and exceptions do occur, you will have to look up the exception reports directly through MessageWay.
- **MWayConn_TraceFilename** - The full path to a file which will receive a detailed trace log of the script's communications with the MessageWay server. For example, C:\tmp\MWTrace.txt. Use this parameter only to debug problems interacting with the MessageWay server.

Debugging Parameters

The following parameters are rarely used, and are primarily used during product development.

- **MWayConn_ResultsDebugFilename** - The full path to a filename which will receive a copy of the results file from the MessageWay helper utility. May include macros. By default, no debug copy of the results file is made.
- **MWayConn_ForceAtLeastSeconds** - The minimum number of seconds to wait after downloading results from MessageWay, prior to processing the files. This parameter was implemented to allow testing features like progress bars. By default, no additional waiting is done.

Output Parameters

- **MWayConn_Report** - Contains the last translation exception report file returned from MessageWay. (Typically, only one report file is returned.) This parameter will be empty if no report files are returned. Note: if the report is too long to fit in a task parameter, it may be truncated.

Error handling

This script returns error 5300 if the translation takes place, but returns one of the following error statuses:

- Partially Accepted
- Accepted with Errors
- Rejected

When running a Traditional task, MOVEit Central will regard a script returning error 5300 as a successful process, which, depending on circumstances, may not be the desired behavior. For maximum flexibility, it is recommended that you use this script with Advanced rather than Traditional tasks. This is especially recommended if you set MWayConn_ExceptionsInsteadOfData to True, because in this case, if translation exceptions occur, the output from the task will be report files rather than data files. You may very well want to send report files to a different destination; if this is the case, using an Advanced Task and checking for a process error code of 5300 is recommended.

See also ***"Advanced Topics - MessageWay CLI."*** (on page 431)

No Op

"No Op" means "No Operation". "No Op" is a dummy task that always completes successfully. It is most often used in a task whose role is to delete files; files successfully downloaded by a task with a "NoOp" process will be deleted if the "delete after successful transfer" option has been checked on the source.

It neither takes nor outputs any parameters.

Notes

This built-in script may be run per-file or once-after-all-files. This built-in script may be run as the first step of a task.

Example #1

Jack would like MOVEit Central to delete any files from a remote directory that end with an "*.tmp" extension.

To perform this operation with MOVEit Central, Jack should...

1. Create a new task with a source, process and schedule. (No destination!)
2. Check the "Delete Originals After Success Transfer" option and specify "*.tmp" as his file mask on his source.
3. Select "No Op" as his process.

When this task executes, all *.tmp files will be downloaded from Jack's source into the MOVEit Central cache. The NoOp process will execute and MOVEit Central will then delete all the files it just downloaded from the source. No files will be retained permanently or transferred to any destination.

PGP Decrypt

Decrypts a message using PGP. This built-in script will only be active if a valid MOVEit Central PGP License is available.

See ***MOVEit Central PGP documentation*** (on page 325) for much more information.

This script does not require any PGP key parameters. An encrypted PGP file "self-describes" itself to the point where MOVEit Central can figure out what settings it needs to decrypt the file as long as the appropriate PGP keys have been set up in MOVEit Central.

Input Parameters

- **PGPPreserveName** - Set this to "True" if the name of the unencrypted file that results from the PGP Decrypt process should be based on the "preserved" name also passed in the encrypted PGP file. (Not all PGP packages preserve original file names, so this option is not on by default.)
- **PGPPreferredDecryptionKey** - If there are a large number of private keys available to MOVEit Central, set this parameter to the preferred key to use for decrypting files. This key will be used first to decrypt files handed to the script. If decryption fails, the rest of the available keys will be used in turn to attempt to decrypt the file.
- **PGPCheckSignature** - Set this to "True" if the signature should be checked (requires that the message be signed). As not all PGP encrypted files are also "signed," this option is not on by default.

PGP Encrypt and Sign

"PGP Encrypt and Sign" Encrypts and signs a file using PGP. This built-in script will only be active if a valid MOVEit Central PGP License is available.

Normally, this script should be run as a per-file process. If run as a per-task process, it will encrypt the last file added to the cache. Thus, this script can be chained with a script like ZipAdvanced.

See ***MOVEit Central PGP documentation*** (on page 325) for much more information.

Input Parameters

- **PGPRecipientKey** (*Required*) - The key of the recipient. A PGP key selection pop-up will be provided for this value. Multiple recipients are allowed.
- **PGPSignerKey** (*Required*) - The private/public key pair (a.k.a., "secret key") to be used for signing. A PGP key selection pop-up will be provided for this value.
- **PGPASCIIArmor** - True if the output file should be ASCII-armored, else False for binary. The default, if not specified, is False.
- **PGPTextMode** - True if the output file should be encoded for automatic text mode conversion. The default, if not specified, is False.
- **PGPForceV3Sigs** - True if the output file should be signed using the old version 3 signatures -- often required by McAfee E-Business Server. The default, if not specified, is False.
- **PGPSigningHash** - The hash algorithm to be used for signing -- often useful for compatibility with out of date PGP clients. The default, if not specified, is SHA1.

For the symmetric encryption algorithm (e.g., AES256 or 3DES), MOVEit Central will use the algorithm associated with the first recipient's key.

PGP Encrypt Only

"PGP Encrypt Only" Encrypts (but does not sign) a file using PGP. This built-in script will only be active if a valid MOVEit Central PGP License is available.

Normally, this script should be run as a per-file process. If run as a per-task process, it will encrypt the last file added to the cache. Thus, this script can be chained with a script like ZipAdvanced.

See ***MOVEit Central PGP documentation*** (on page 325) for much more information.

Input Parameters

- **PGPRecipientKey** (*Required*) - The key of the recipient. A PGP key selection pop-up will be provided for this value. Multiple recipients are allowed.
- **PGPASCIIArmor** - True if the output file should be ASCII-armored, else False for binary. The default, if not specified, is False.
- **PGPTextMode** - True if the output file should be encoded for automatic text mode conversion. The default, if not specified, is False.

For the symmetric encryption algorithm (e.g., AES256 or 3DES), MOVEit Central will use the algorithm associated with the first recipient's key.

Prepend Lines

"Prepend Lines" inserts lines at the beginning of a file. Up to four different lines can be inserted, including blank lines.

Input Parameters

- **PrependLines_Line1** (*Required*) - Specifies the first line to insert into the file. This field may contain macros. Blank lines may be specified using the string "(blank)".
- **PrependLines_Line2** - Specifies the second line to insert into the file. This field may contain macros. Blank lines may be specified using the string "(blank)".
- **PrependLines_Line3** - Specifies the third line to insert into the file. This field may contain macros. Blank lines may be specified using the string "(blank)".
- **PrependLines_Line4** - Specifies the fourth line to insert into the file. This field may contain macros. Blank lines may be specified using the string "(blank)".

Output Parameters

- **PrependLines_LineCount** - Returns the number of lines added by this run of PrependLines. (Could be zero or blank if an error occurs.)

Notes

Please only use the prepend operation this against text files as prepending text in a binary file could have unforeseen consequences.

This built-in script may only be run per-file. This built-in script may not be run as the first step of a task.

Example #1

Ed would like to insert a note with today's date followed by a blank line into archived log files that are moved from one server to another.

To perform this operation with MOVEit Central, Ed should...

1. Create a new task with a source, process, destination, and schedule.
2. Select "Prepend Lines" as his process
3. Set process parameters:
   - PrependLines_Line1 = "Archived log file processed on [yyyy]-[mm]-[dd]"
   - PrependLines_Line2 = "(blank)"

Report Long Running Tasks

"Report Long Running Tasks" will query the micstats database and report back information about any tasks that have be running longer than the specified time interval.

Input Parameters

- **ReportLongTasks_Time** (*Required*) - Specifies the number of hours or days a task has to have been running to be included in the report.
- **ReportLongTasks_Unit** (*Required*) - Specifies whether the ReportLongTasks_Time parameter is in hours or days.
- **ReportLongTasks_CommandTimeout** - The timeout in seconds to use when performing database queries. Default is 3 minutes.

Output Parameters

- **ReportLongTasks_Results** - Returns a list of tasks that have been running longer than the specified length of time, or a blank string if there were errors.

Notes

The output parameter ReportLongTasks_Results should most commonly be used in a message body for a Send Email step that occurs after the Run Script step for Report Long Running Tasks.

Set Destination

"Set Destination" changes the host definition (and optionally, the path) of the destination used in this task run.

This built-in script will almost always be used with macros. Three common scenarios in which it may play a role are briefly described below.

- **Partial Paths or Filenames** - If you have hosts named "FTP1" and "FTP2", you might use a macro like "[LEFT([OrigName], 4)]" in the "SetDestination_Host" parameter against a filename like "FTP2_report025245.dat" to select different hosts at runtime.
- **After Look Up** - If you have hosts named "Remote Company FTP" and "SSH for Brooklyn", you might use the built-in Look Up script first to figure out which host to use based on incoming filenames, file sizes, file paths, etc. and then use a macro like "[Parm:LookUp_Value]" in the "SetDestination_Host" parameter to select different hosts at runtime.
- **With MOVEit Central API** - MOVEit Central's ability to pass parameters to any task it runs allow you to use a macro like "[Parm:HostFromAPI]" in the "SetDestination_Host" parameter to let your MOVEit Central API application select different hosts at runtime.

Input Parameters

- **SetDestination_Host** (*Required*) - The "friendly" name of the destination host. The host you select does not need to be currently defined in the task, nor does it need to be of the same type. (e.g., You can use this parameter to switch the destination to a MOVEit DMZ server even if the task's destination is currently a single FTP server.) However, if you use this parameter to switch between hosts of different types (for example, between FTPS and MOVEit DMZ servers) you MUST also use the "SetDestination_Path" parameter to ensure that destination paths are properly parsed. Use a value of "(default)" to indicate a Windows file system host; in this case your "SetDestination_Path" value should either begin with a drive letter (e.g., "C:\") or a UNC (e.g., "\\server\share\").
- **SetDestination_Path** (*Optional*) - Sets the Destination path. Ignored if blank. Macros are allowed (and encouraged) in this field.
- **SetDestination_IgnoreError** (*Required*) - Specifies whether errors in setting host and path are ignored (set this to "ON" only if you have a fallback destination configured).

Notes

This built-in script may be run per-file or once-after-all-files. This built-in script may be run as the first step of a task.

Sleep

"Sleep" pauses the current task between file transfers for a specified number of seconds or milliseconds.

Input Parameters

- **SleepScript_Time** (*Required*) - Specifies the number of seconds or milliseconds the script should sleep. Maximum is 16000.
- **SleepScript_Unit** (*Required*) - Specifies whether to count off time in milliseconds or seconds. Default is seconds.

Notes

This built-in script may be run per-file or once-after-all-files. This built-in script may be run as the first step of a task.

Example #1

Kara has noticed that a particular application on a remote server "chokes" when MOVEit Central uploads files to it as fast as MOVEit Central can. Kara would like to introduce an artificial pause into the MOVEit Central file transfer task that points to the flaky destination to give the remote application time to digest each file. After some trial-and-error, Kara has decided that a 5 second pause usually clears up the remote application's issues.

To make this happen in her MOVEit Central task, Kara should...

1. Select her existing task, which already has a source, destination and schedule.
2. Add a new process: "Sleep", and make sure the process is set to run "per-file"
3. Set process parameters:
    - SleepScript_Unit = "seconds"
    - SleepScript_Time = "5"

SMIME Receive

"SMIME Receive" retrieves messages from a POP3 server, decrypts them if necessary using a certificate in the Windows certificate store, and adds the attachments, if any, to the list of files to be processed.

Input Parameters

- **SMIME_POPAddress** (*Required*) - The address of the POP3 server; e.g., mail.mycompany.com.
- **SMIME_Username** (*Required*) - The username for accessing the above POP3 server; e.g., joeuser.
- **SMIME_Password** - The password for the above POP3 user account.
- **SMIME_DelWhenDone** - Whether to delete messages when done processing them (default: True).
- **SMIME_DelMsgWOAttach** - Whether to delete messages found on the POP3 account that do not contain attachments. If SMIME_DelWhenDone is True, messages will be deleted anyway. (default: False).

If the script fails to run and returns an error, it is most likely due to a configuration error. See the list of error codes below to determine what the problem might be:

Error Code	**Meaning**
500	A required task parameter was not found
501	Could not access POP3 server
502	Error while retrieving a message
503	Error decrypting a message
504	Error verifying a message signature
505	Error saving attachment file

SMIME Send

"SMIME Send" encrypts and/or signs files, and sends them as email using an SMTP server.

Input Parameters

- **SMIME_SMTPAddress** (*Required*) - The address of the SMTP server; e.g., mail.mycompany.com.
- **SMIME_Sender** (*Required*) - The email address of the sender; e.g., joe@mycompany.com.
- **SMIME_Recipient** - The email address of the recipient; e.g., mary@shinythings.com.
- **SMIME_Subject** - Email message subject text (default: "File from MOVEit Central is attached").
- **SMIME_Body** - Email message body text (default: "This message should have come with a file attached by MOVEit Central.").
- **SMIME_RecipientCert** - The subject of the recipient's certificate (default: recipient email address).
- **SMIME_SenderCert** - The subject of the sender's certificate (default: sender email address).
- **SMIME_Sign** - Whether the message should be cryptographically signed (default: True).
- **SMIME_Encrypt** - Whether the message should be encrypted (default: True).

If the script fails to run and returns an error, it is most likely due to a configuration error. See the list of error codes below to determine what the problem might be:

Error Code	Meaning
500	A required task parameter was not found
501	File attachment failure
502	Could not find a certificate matching the provided subject(s)
503	Error sending the email message to the specified SMTP server

Tamper Detect

"Tamper Detect" performs ***tamper detection*** (on page 466) on the three main MOVEit Central "audit" tables. It is used by the built-in task "Tamper Detect". There should not be a need to use this script in any other task.

This script will normally email administrators if it suspects tampering. A daily report of its activity will be found in the most current "Audit" view as well as usual appearances in the "Task Runs" and "File Activity" views.

Input Parameters

- **TamperCheck_EmailOperator** - Specifies when the script should email a tamper detection report to the email address configured in Errors tab of the MOVEit Central configuration utility. The allowable values are:
  - Never - Never email the report.
  - OnError - Email the report only if errors are detected. This is the default.
  - Always - Always email the report.

Notes

This built-in script should be run as the first step of a task.

The report generated by this script is an ASCII file or message that is typically about 30 lines long. The first line of the message will clearly indicate whether any errors were found.

Trim Statistics DB

"Trim Statistics DB" deletes all MOVEit Central audit records older than a certain number of days, and optionally saves them to tab-separated files.

Input Parameters

- **DirLog** (*Required*) - The folder into which to write the debug and error logs. During a fresh install, this is set to "\Program Files\MOVEit\MICStats\Logs". Set this to an empty value if you don't want debug and error logs.
- **DirArchive** - The optional folder into which to write the tab-delimited archives. During a fresh install, this is set to "\Program Files\MOVEit\MICStats". Set this to an empty value if you don't want deleted records archived to a text file.
- **TrimStatsDB_DaysToRetainArchive** - The number of days to retain the tab-delimited archive files. Log files older than this number of days found in "\Program Files\MOVEit\MICStats\Logs" (or the value of DirLog) will be deleted. Use this setting carefully as deleted files are not put into the Recycle Bin.
- **DSNArchive** - The optional ODBC DSN into which to save a copy of the records being deleted. During a fresh install, this is set to an empty string, meaning that the delete database records will not be written to another database.
- **DaysToKeep** (*Required*) - The number of days to retain records. During a fresh install, this is set to 40.
- **DaysToKeepNoXfers** - The number of days to retain TaskRuns records marked "No Xfers". If not supplied, no special action is taken. If you have many tasks that run frequently, you may wish to set this parameter to a small number of days in order to reduce the size of the database and increase its performance. The default is empty, which means no special processing is done for these records.
- **TrimStatsDB_ArchiveNoXfers** - Specifies whether TaskRuns records marked "No Xfers" should be archived or simply discarded. The default is "No," which will prevent archiving of these records."
- **TrimStatsDB_DaysToKeepAudit** - The number of days to retain Audit records. If not supplied, default value of DaysToKeep is used.
- **TrimStatsDB_DateFormat** - The date format MOVEit Central should assume is in use. Usually only used on Windows systems outside the United States. The legal values are MonthDayYear (the default) and DayMonthYear.
- **TrimStatsDB_CommandTimeout** - The number of seconds a client connection to the database will remain active without timing out. The default value is 180 seconds (3 minutes).

Notes

This built-in script should only be run as the first (and only) step of a task. (Process-level per-file or once-after-all-files settings will be ignored.)

Over time, the statistics database can accumulate many records, slowing performance and using megabytes of disk space. To prevent this, MOVEit Central is typically configured to run this built-in script periodically, optionally saving them to a file or another database before deletion.

Beginning with version 3.0, during a fresh install, MOVEit Central began to automatically install and schedule a custom script to perform the same actions detailed here. Beginning with version 3.1.5, the custom script was converted to and replaced with a built-in script that could no longer be viewed or modified but was much easier to upgrade.

Older versions of Trim Statistics DB may have used a parameter named DSNMICStats. If DSNMICStats appears in the task parameter listing it will be ignored and so it is safe to delete it.

Example #1

Bob has noticed that the various task history dialogs in MOVEit Central have been "sluggish" lately and asks Ipswitch for some advice. Ipswitch notices that Bob has more than two hundred tasks that "poll" FTP servers every five minutes, all day long. Most (98%) of these polls do not yield files, but MOVEit Central will faithfully log this information during each poll. Over the course of a single day, this means that more than 55,000 "no xfer" actions will have been logged to the database. Bob knows that "no xfer" information can be of value in debugging, but Ipswitch would prefer he remove them after a few days and only retain "success" or "failure" audit entries for long periods of time. Bob and Ipswitch settle on retaining one week of "no xfer" records, and still decide to keep a full 60 days of "success" and "failure" logs in the database. He will not save the "no xfer" records to the longer term archive logs.

To accomplish this with MOVEit Central, Bob should...

1. Select his existing "Trim Stats DB" task, which already has a process and schedule.
2. Set process parameters:
   - DaysToKeep = "60"
   - *(Add)* DaysToKeepNoXfers = "7"

Unzip Advanced

"Unzip Advanced" unzips an single archive containing one or more files, with an optional ZIP password. It can work with archives that contain nested folders and can also handle the "bzip2" encryption type put into common use with the WinZip 9.0 file compression utility.

Use "Unzip Advanced" instead of the source-level "Expand compressed (zip) files" checkbox if you need to decrypt entries in the zip file.

Input Parameters

- **UnzipAdvanced_Password** - Specifies an optional password to apply to the Zip file. Default value is blank, which indicates no decryption is to be done. (CAUTION: Using a password to defend a Zip archive is not usually enough protection to thwart a determined hacker.)

Output Parameters

- **ZipFileSize** - Number of bytes in the zip file. This and other size parameters will be populated whether or not the Zip file is successfully unzipped. If more than one zip file is encountered, this parameter will only contain the size of the last zip file processed by this task run.
- **ZipFileSizeKB** - Number of kilobytes (KB) in the zip file.
- **ZipFileSizeMB** - Number of megabytes (MB) in the zip file.
- **ZipFileSizeGB** - Number of gigabytes (GB) in the zip file.

Notes

This built-in script must be run as a once-after-all-files process. This built-in script may not be run as the first step of a task.

The task's "Cache Files" option must be set to "Use Random Names".

XSL Transform

"XSL Transform" transforms XML documents downloaded from a source using a specific XSL stylesheet.

Input Parameters

- **XSLTransform_XSLPath** (*Required*) - Specifies the path from which MOVEit Central should obtain the XSL stylesheet.
- **XSLTransform_XSLFile** (*Required*) - Specifies the name of the XSL stylesheet file.

Notes

This built-in script must be run per-file (not once-after-all-files). This built-in script may not be run as the first step of a task.

Example #1

Xavier wants to automate the XSL transformation of several XML files. In this instance, he wants to transform incoming XML files using an XSL template called "example.xsl". This XSL template is located in the "d:\projects\templates" folder on MOVEit Central.

To integrate this application with MOVEit Central, Xavier should...

1. Create a new task with a source, process, destination and schedule.
2. Select "XSL Transform" as his process
3. Set process parameters:
   - XSLTransform_XSLPath = "d:\projects\templates"
   - XSLTransform_XSLFile = "example.xsl"

If Xavier decides to use MOVEit Central to perform other XSL transformations, he should consider setting "XSLTransform_XSLPath" as a global parameter so he would not need to set it on every task he sets up.

Zip Advanced

"Zip Advanced" zips one or more files into a single archive with a configurable level of compression and an optional ZIP password.

Use "Zip Advanced" instead of the destination-level "Zip" checkbox if any of the following zip features are needed.

- **Password** - Although not very secure, Zip Advanced can apply a password to a zip archive.
- **Multiple Files** - The destination-level Zip checkbox will zip each file into its own individual zip archive. If you need to zip multiple files together instead, use Zip Advanced as a "run once after all downloads" process instead.
- **Specific Zip Filename** - To come up with a "zip filename", the destination-level Zip checkbox will strip any given file extension and plug ".zip" on the filename instead. If you need to preserve the entire original filename in the name of the zip archive or want to substitute it with something else, use the Zip Advanced process and apply whatever name you want in the appropriate destination configuration.

Input Parameters

- **ZipAdvanced_Password** - Specifies an optional password to apply to the Zip file. Default value is blank, which indicates no password is to set on the Zip archive. (CAUTION: Using a password to defend a Zip archive is not usually enough protection to thwart a determined hacker.)
- **ZipAdvanced_Compression** - Specifies the level of compression. (More compression takes more time.) The default level is "Normal". Other values include "None", "Low" and "High". All levels involve vendor-neutral Zip compression standards; you should not run into incompatibilities with one level or another.

Output Parameters

- **ZipFileSize** - Number of bytes in the zip file. This and other size parameters will only be populated if the Zip file is successfully created.
- **ZipFileSizeKB** - Number of kilobytes (KB) in the zip file.
- **ZipFileSizeMB** - Number of megabytes (MB) in the zip file.
- **ZipFileSizeGB** - Number of gigabytes (GB) in the zip file.

Notes

Zip Advanced will recursively include subfolders in its archives if the "Include Subfolders" option has been set on any task sources.

Zip Advanced requires that the task-level "Cache Files" option be set to "Use Original Names". This option may be set by selecting "Edit Task Info..." from a task's "right-click" menu.

This built-in script may be run per-file or once-after-all-files. This built-in script may not be run as the first step of a task.

Example #1

Al would like to download several "*.rpt" files from an FTP server, include a "readme" from his local computer and zip the entire package together in a highly compressed Zip archive.

To accomplish this with MOVEit Central, Al should...

1. Create a new task with a source, process, destination and schedule.
2. Point his new source to his FTP server and use "*.rpt" as his file mask.
3. Select "Zip Advanced" as his process
4. Set process parameters:
   - ZipAdvanced_Compression = "High"
   - Run = "Once After All Downloads"
5. Add a second source to the task and point it at the local "readme.txt" file.

Al's final task will have two sources (one FTP server and one local), the Zip Advanced process (set to run after material is downloaded from all sources), and whatever destination Al deems necessary.

Keys and Certs

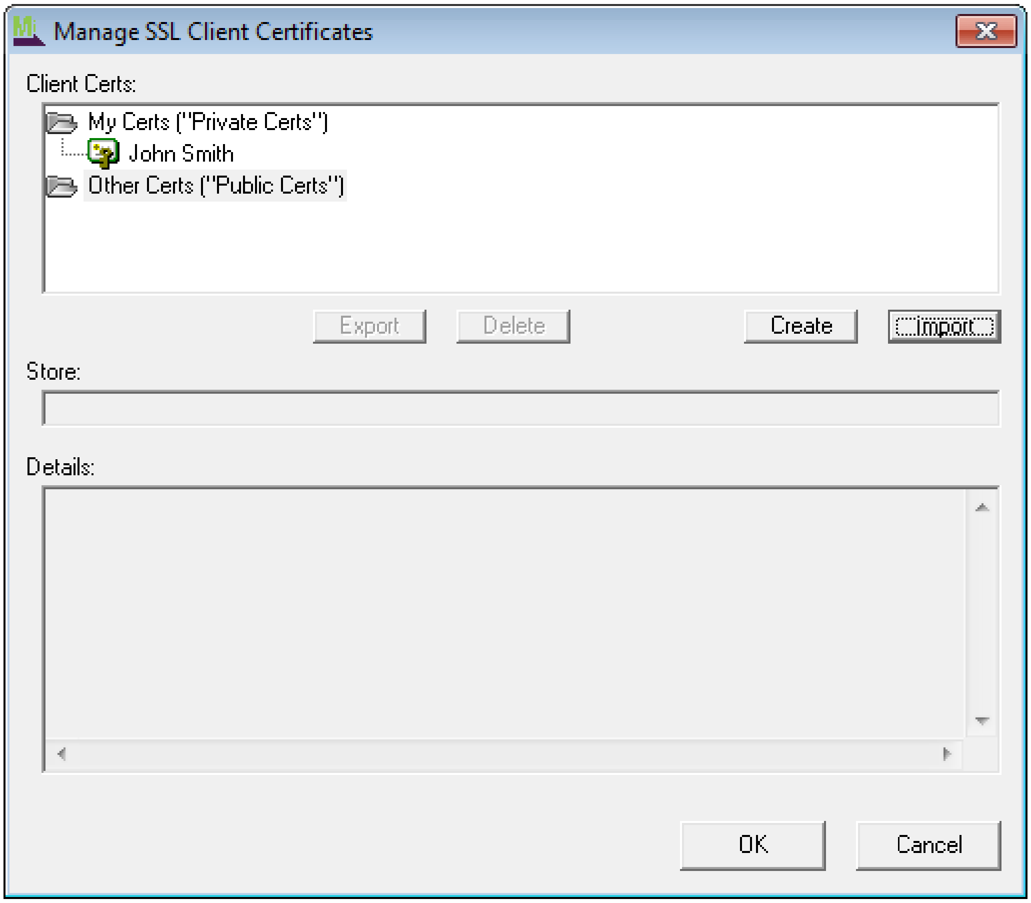
This section describes how to use the Cert/Key manager in MOVEit Central Admin to manage security keys and certificates.

Key/Cert Manager

Managing SSL certificates, SSH keys, and PGP keys is done using the Cert/Key manager in MOVEit Central Admin. This dialog is available by choosing the Settings menu, selecting Certs/Keys, and selecting the key/cert type you wish to manage. From here, keys and certs can be listed, details about individual entries shown, new keys created or imported, and existing keys removed. There are also more options available for specific key/cert types.

SSL Client Certificates

SSL client certificates (on page 217) are listed here under the particular store the certificate is installed under. Personal client certificates (those including private keys) are generally shown in My Certs store (corresponding to the "Personal" or "My" store in Windows). Client certificates for other people (those not including private keys) are generally shown in the Other Certs store (corresponding to the "Other People" or "AddressBook" store in Windows).


Manage SSL Client Certificates
Client Certs:
My Certs ("Private Certs")
John Smith
Other Certs ("Public Certs")
Export
Delete
Create
Import
Store:
Details:
OK
Cancel

Choosing a certificate in the list will display information about that certificate in the Details field. Certificate fields such as issuer, expiration date, and thumbprint are displayed here. A selected certificate can also be deleted by clicking the Delete button.

Existing certificates can be added to the system by choosing the Import button. The user will be prompted to select a certificate file from their local system to be imported. Files ending with a ".pfx" or ".p12" extension are assumed to contain private keys, and the user will be prompted for the password securing those keys. If no such password is set, simply leave the password field blank and click OK. Files ending with other extensions are assumed to contain only public certificates, so the user will not be prompted for a password.

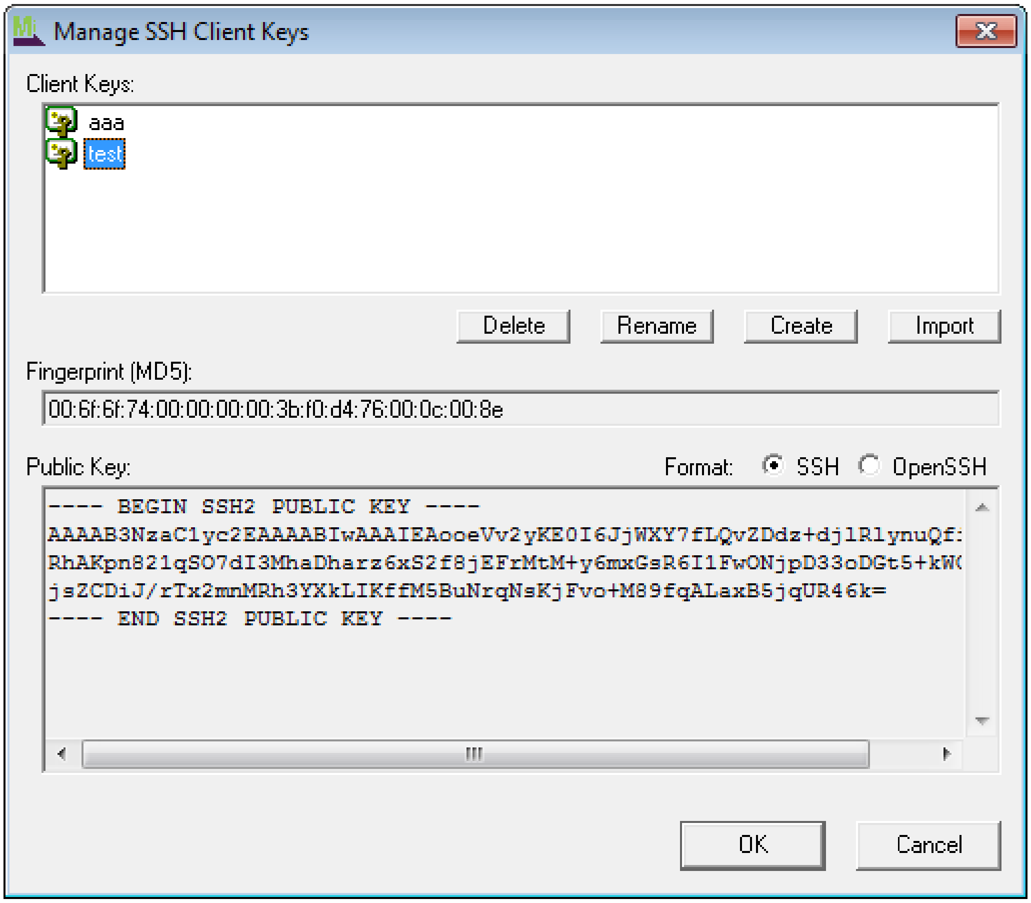
New certificates can be generated and added to the system by choosing the Create button. The user will be prompted for various fields; the only required field is Name, also known as Common Name or CN. Users may also select the key length: 1024 (default), 2048, 3072, 4096. The certificates generated in this way are "self-signed" and unlike certificates issued by well-known certificating authorities, will not automatically be trusted by other sites.

NOTE: Use of self-signed certificates is not recommended for securing web servers like IIS, as they will cause trust errors to occur with end users who visit a site configured with one. Self-signed certificates are suitable for testing, for securing communications between MOVEit Central and MOVEit Central Admin, and in some cases for production use in applications like AS2.

NOTE: If you have access to MOVEit DMZ as an administrator, you can also generate self-signed SSL certificates through the MOVEit DMZ web interface.

SSH Client Keys

SSH client keys available in MOVEit Central are listed here. choosing a key in the list will display the key fingerprint in the Fingerprint (MD5) field, and the text content of the key in the Public Key field. Use the Format radio options to select the displayed key content format in the Public Key field. SSH and OpenSSH formats are supported.



Fingerprint (MD5): 00:6f:6f:74:00:00:00:00:3b:f0:d4:76:00:0c:00:8e

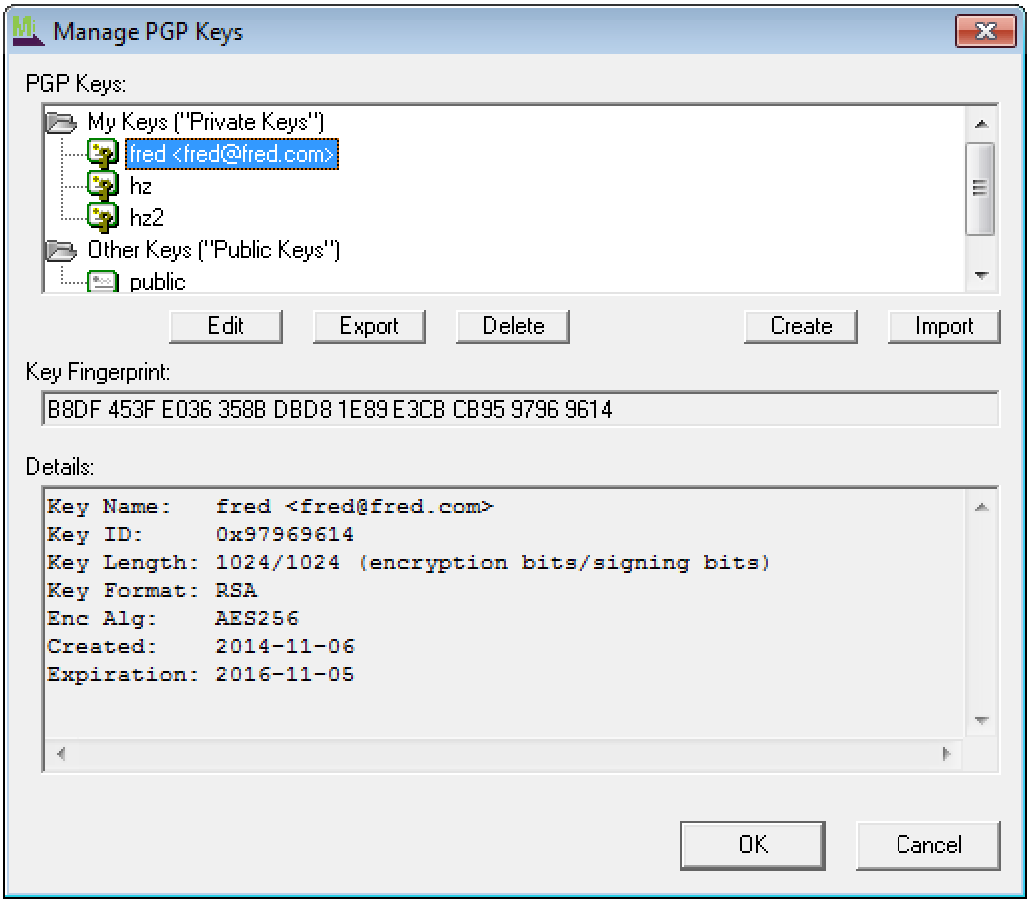
Public Key: Format: ● SSH ○ OpenSSH

```
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAABIwAAAIEAooeVv2yKE0I6JjWXY7fLQvZDdz+dj1R1ynuQf:
RhAKpn821qSO7dI3MhaDharz6xS2f8jEFrMtM+y6mxGsR6I1FwONjpD33oDGt5+kW(
jsZCDiJ/rTx2mnMRh3YXkLIKffM5BuNrqNsKjFvo+M89fqALaxB5jqUR46k=
---- END SSH2 PUBLIC KEY ----
```

A selected key can be renamed by clicking the Rename button. The new name will be prompted for. A selected key can also be deleted by clicking the Delete button.

New keys can be added by choosing the Create or Import buttons. First, the user will be prompted to enter a name for the new key. Users may also select the key type, RSA (default) or DSA, and the key length, 1024 (default), 2048, 3072, or 4096. Next, if the user clicked the Create Key button, MOVEit Central will generate a new key and add it to its internal key collection. If the Import button was clicked, the user will be prompted for a key file, and then a passphrase. The data from the provided key file will then be imported into MOVEit Central's key collection.

PGP Keys



B8DF 453F E036 358B DBD8 1E89 E3CB CB95 9796 9614

```
Key Name:    fred <fred@fred.com>
Key ID:      0x97969614
Key Length: 1024/1024 (encryption bits/signing bits)
Key Format: RSA
Enc Alg:     AES256
Created:     2014-11-06
Expiration: 2016-11-05
```

PGP keys are listed here in two sections, related to the key types. Personal PGP keys (those containing public and private keys) are listed in the My Keys section, while other PGP keys (those containing only public keys) are listed in the Other Keys section. choosing a key in the list will display the key fingerprint in the Fingerprint field, as well as information about that key in the Details field. Key fields such as name, size, format, and expiration date are displayed here.

For more information about actions available for PGP keys, see the ***Managing PGP Keys*** (on page 219) page in this section.

Importing SSH Client Keys

In addition to generating new SSH client keys, MOVEit Central can import existing keys that have been obtained from remote servers. The specifics of how servers generate and store SSH private keys vary from vendor to vendor. However, the most common SSH implementation, OpenSSH, generates its keys via "ssh-keygen" and stores the keys in files named $HOME/.ssh/id_dsa or $HOME/.ssh/id_rsa, where $HOME is the home directory of the user in question. Here's a sample Linux session which generates a key:

```
$ ssh-keygen -t rsa

Generating public/private rsa key pair.

Enter file in which to save the key (/home/fred/.ssh/id_rsa):

Created directory '/home/fred/.ssh'.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/fred/.ssh/id_rsa.

Your public key has been saved in /home/fred/.ssh/id_rsa.pub.

The key fingerprint is: 18:37:c3:bc:10:f0:c0:38:19:3e:80:7b:73:79:15:9c
fred@linuxsrv1

$
```

To import such a key into MOVEit Central, transfer the key (the file that does not end in .pub) to the computer running MOVEit Central Admin. (You might use FTP or FTP over SSH to do this transfer.) Then in the Hosts tab, double-click on the SSH host name. In the Define SSH Host dialog, choose the "..." button next to "SSH Client Key". In the resulting Manage SSH Keys dialog, choose Import. In the Enter Name dialog, choose an arbitrary name for the key and click OK. (This name is used only as a label within MOVEit Central) Then, select the key file that you just transferred from the SSH server. If the key file was encrypted on the server (this is rare, and would have been specified when the user ran ssh-keygen), enter the encryption password when prompted. Otherwise, leave the password field blank and simply click OK.

The key will be imported into MOVEit Central. It can now be ***selected as the default SSH client key*** (see "***Hosts Tab***" on page 149) for this or any host, and can be selected as the SSH client key in tasks that override the default SSH client key for a host.

Configuring the key on the SSH server

Once a key has been created, the SSH server must be configured to authorize the key for logon. The procedure for this depends on the type of SSH software running on the server.

- For OpenSSH, the OpenSSH version of the public key (one very long line of text) should be appended to the file ~/.ssh/authorized_keys on the user's UNIX machine.
- For SSH.com, a line like "Key mykey.pub" should be appended to the file ~/.ssh2/authorization, and the file ~/.ssh2/mykey.pub should be created with the contents of the SSH format of the key.
- For SSH.com Tectia Server, the SSH version of the public key should be uploaded to the user's authorized_keys directory on the server, with an arbitrary filename. This is typically $HOME/.ssh2/authorized_keys on Unix and %USERPROFILE%\.ssh2\authorized_keys on Windows.

For other servers, consult the documentation for that server.

PuTTY Key Generator

By default, the PuTTY Key Generator exports TWO files; one for a private key and one for a public key. However, to generate a file format for use in MOVEit Central's SSH client, you must opt to export your PuTTY key as an "OpenSSH Key" (using the "Conversions" menu, if available). The passphrase you designate in the provided fields will carry over to the exported OpenSSH key as well.

"ssh.com" Key Import

MOVEit Central allows the import of "ssh.com" keys, but such keys must NOT have been protected with a password; imports of "Password Protected ssh.com" keys will always fail. ("Blank password OpenSSH" and "Password Protected OpenSSH" keys can be imported without problems.)

SSL Client Certificates

MOVEit Central uses client certificates for FTP/S and MOVEit DMZ authentication, S/MIME signing/encryption and AS1/AS2/AS3 authentication/signing/encryption. This section discusses issues related to obtaining and installing certificates, prior to using them in MOVEit Central.

An X.509 digital certificate is a document that verifies the identity of the holder of the certificate. Digital certificates are often issued by and vouched for by Certification Authorities (CAs), but may also be "self-signed". Every certificate contains two keys used by public/private key cryptography.

A certificate used for client authentication conceptually consists of three components:

- The public component of the certificate, which contains the name of the client and the public key.
- The private component of the certificate, which contains an encrypted version of the private key. Though it is possible to have a certificate without the private component, such a certificate cannot be used as a client certificate.
- A password, which protects the private key.

To use client certificate with MOVEit Central, you must:

- Obtain a certificate from a server administrator, a CA or by generating one yourself.
- If necessary, convert the certificate into a form understood by Microsoft software (*.cer or *.pfx).
- Install the certificate into MOVEit Central through MOVEit Central Admin.
- Configure a MOVEit Central host to use the certificate when communicating with a particular FTP server, MOVEit DMZ server, AS2 partner, etc.

These steps are covered in more detail in the following topics.

Obtaining a Certificate

Let's say you ask the administrator of an FTP server for a certificate. This certificate must be registered with the FTP server; presumably, the administrator will have done this by the time the certificate is delivered to you. The certificate will likely be delivered to you either in the form of two ASCII files with extensions .crt and .key (or perhaps .cer and .key), or one binary file with an extension .p12 (or perhaps .pfx). Place these file(s) on the computer running MOVEit Central. If you are using a network file transfer mechanism to transmit the certificate file(s), be sure to choose the proper ASCII vs. binary transfer method.

Regardless of the file type, there will also be a password, which you must know before you can use the certificate.

Converting the Certificate

Microsoft software imports client certificates from .p12 (also known as .pfx) files. If you received .crt and .key files instead of a .p12 file, you must convert them to .p12 format. You can do this with the free program OpenSSL.exe from the ***OpenSSL Project*** (see http://www.openssl.org **-** ***http://www.openssl.org***).

Suppose that you received the files fred.crt and fred.key, and wish to convert them to a single fred.p12 file. You would use a command like:

```
openssl pkcs12 -inkey fred.key -in fred.crt -export -out fred.p12
```

This command prompts for the password to the fred.key file before writing the fred.p12 file.

Installing the Certificate into Windows

On a Windows system, certificates are registered with the operating system, usually in one of two locations: the Local Machine store, or the Current User store. (This store is also known as the "Personal" or "My" store.) The Local Machine store contains certificates that may be accessed by anyone on the local computer. Only administrators may add or modify certificates in this store. The Current User store contains certificates that may be accessed only by the currently signed on user. The current user has full access to the store and may add or modify certificates in the store. MOVEit Central accesses the Current User store when looking for certificates, and has the ability to install (or import) a certificate into this store.

To do so, first log on to the Central server using the Admin program. Once logged on, select Options | Cert Key Managers | SSL Client Certificates. Click the Add button to add a new Certificate. Browse to the certificate file and select it. Enter the password protecting the certificate when prompted. The certificate data will be sent to the Central server, where it will be added to the Current User certificate store of the user the Central server is currently running under.

Configuring MOVEit Central to Use the Certificate

In MOVEit Central Admin, edit the properties of the certificate-related host, or the properties of any sources or destinations that use that host, and select the newly-installed client certificate.

Managing PGP Keys

MOVEit Central allows operators to create, delete, import and export locally stored PGP keys through MOVEit Central Admin. There is no need to "shell out", issue command-line arguments or use a third-party PGP key management utility. Behind the scenes, MOVEit Central stores PGP keys in files called "keyrings", but the interface MOVEit Central Admin uses to manage PGP keys is intentionally similar to the interface used to manage SSH keys and SSL certificates.

There are two types of PGP keys: PGP public keys and PGP private/public keypairs.

PGP Public Keys

Public keys are non-secret keys that are often widely distributed to other users. To encrypt a file to send to someone, you must have a copy of their public key. If you sign the file, the recipient must have a copy of your public key in order to check the signature.

Typically you will "import" the public keys of several other users into your keyring, and "export" your own public key to send to other users. There is usually little security risk associated with distributing your public key. (In fact, some people attach their PGP public key to every email message they send!)

Operators may perform both import and export operations through MOVEit Central Admin, of course. In MOVEit Central Admin, public PGP keys (for which you lack a private key) are displayed as "Other Keys" because other people have the private keys associated with the "Other Keys".

PGP Private/Public Keypairs

Private/public keypairs (also known as **secret keys** or just **private keys**) are secret keys that are generated by you and that contain information that must not be given to other users. A secret key also contains a copy of an associated public key. Though you will rarely export your entire private/public keypairs (except possibly for backup purposes), you will need to export the public component of your private/public keypair in order to allow others to encrypt files to be sent to you.

Although not strictly necessary, private/public keypairs are generally encrypted with a password, so that if the private/public keypair file falls into the wrong hands, it cannot be used.

Although it is possible to have multiple private/public keypairs--just as it is possible to have multiple email addresses--to prevent confusion, it is recommended that you minimize the number of different secret keys.

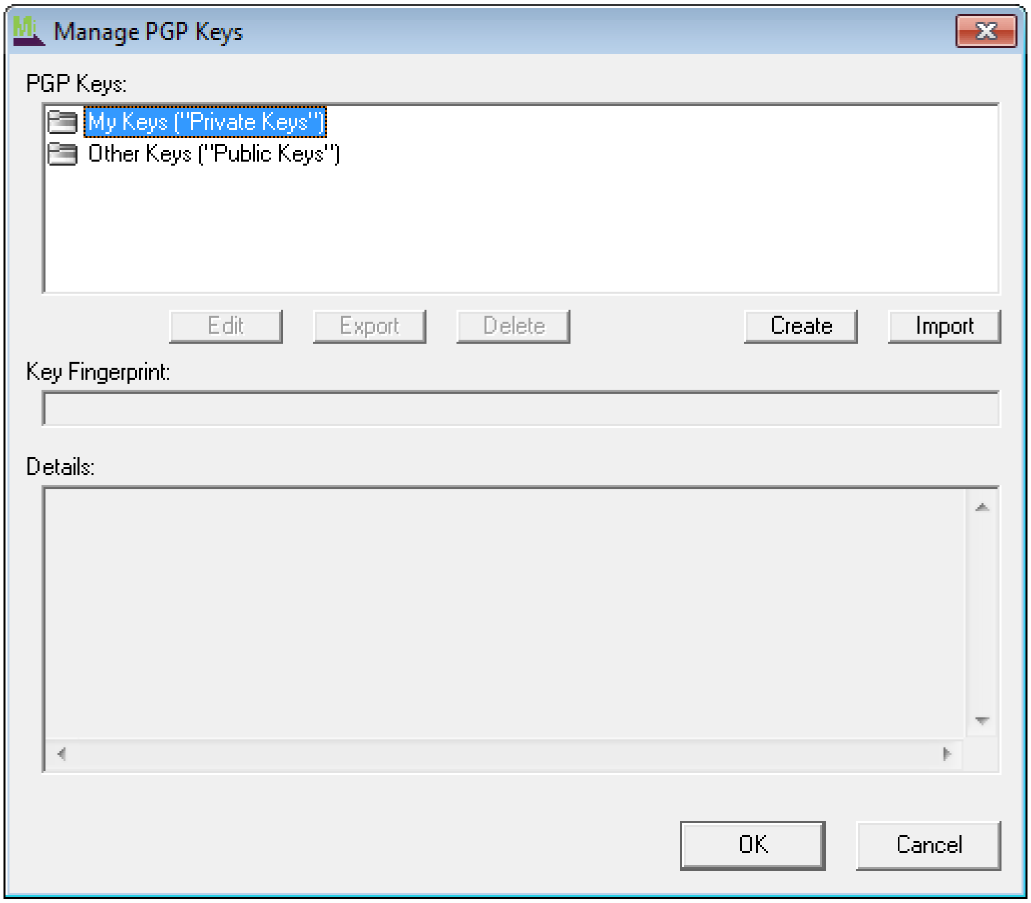
In MOVEit Central Admin, private/public keypairs are displayed as "My Keys" because you have the private keys.

Managing Keys

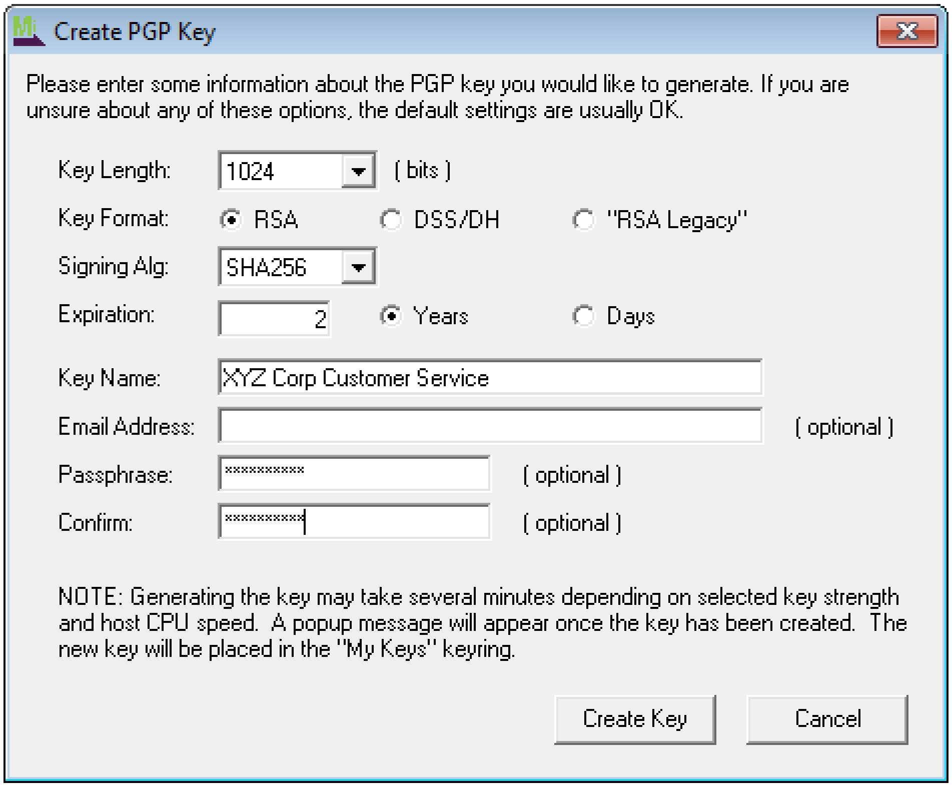
PGP keys are managed through the "Manage PGP Keys" dialog, which is accessed via Admin's Options | Cert/Key Managers | PGP Keys menu entry. This dialog shows all PGP keys. MOVEit Central Admin identifies secret keys as "My Keys" and public keys as "Other Keys". Select a key to see that key's details, such as expiration date and fingerprint.

Creating a Private/Public Keypair

To get started with PGP, you must have at least one private/public keypair in your "My Keys" collection. If you have already have a private/public keypair in some other PGP software, you can export it from that software and import it into MOVEit Central. Otherwise, you should generate a key. Use the Create button to create a new key:



In the Create Key dialog, you will be prompted for these items:



Create PGP Key

Please enter some information about the PGP key you would like to generate. If you are unsure about any of these options, the default settings are usually OK.

Key Length: 1024 (bits)

Key Format: ● RSA ○ DSS/DH ○ "RSA Legacy"

Signing Alg: SHA256

Expiration: 2 ● Years ○ Days

Key Name: XYZ Corp Customer Service

Email Address: (optional)

Passphrase: ********** (optional)

Confirm: ********** (optional)

NOTE: Generating the key may take several minutes depending on selected key strength and host CPU speed. A popup message will appear once the key has been created. The new key will be placed in the "My Keys" keyring.

- **Key Length** - the length of the key in bits. The longer the key, the more secure it is, but the more processing time is required for cryptographic operations. 1024 bits is probably enough, but many experts prefer 2048 bits to play it safe. 4096 bits is quite long; generating a key of this length may take over 10 minutes.
- **Key Format** - Both RSA and DSS/DH (Digital Signature Standard / Diffie-Hellman) are widely supported. "RSA Legacy" may be necessary if you are exchanging encrypted files with someone who is using a very old version of PGP.

IMPORTANT: The previous PGP module for MOVEit Central, Authora EDGE PGP Library, has been replaced by Didisoft OpenPGP Library for .NET in order to address various limitations. Didisoft does not support generating DSS or "RSA Legacy" keys, which are options that EDGE SDK does support. For backward compatibility, these options are still visible in MOVEit Central Admin for version 8.1. However if you try to generate a DSS or "RSA Legacy" key using the new IPSP/Didisoft components, you will receive a friendly error message stating that "This version of MOVEit Central doesn't support generating xxxxx keys".

- **Signing Alg** - The hash algorithm used for signing the key. The default for DSS keys is SHA1, because some older PGP applications do not support algorithms other than SHA1 for DSS keys. The default for RSA keys is the more secure SHA256, but you may need to choose SHA1 for backwards compatibility with older applications. For the best security, you may wish to choose SHA512. You may not configure the hash algorithm used to sign RSA legacy keys.
- **Expiration** - Shorter expiration times are more secure, because they reduce the amount of damage that could be done if an opponent somehow gains access to your key. However, shorter expiration times are less convenient, because when the key approaches its expiration date, you must generate a new one and send its public component to your correspondents.
- **Key Name** - This is an arbitrary name associated with the key. It is similar to the Common Name on an SSL certificate.
- **Email Address** - If provided, this is incorporated into the name of the key. Despite its name, this field is usually not used to address PGP-encrypted email, but instead serves as a point of contact for technical issues involving that PGP key.
- **Passphrase** - The passphrase used to encrypt the secret key. MOVEit Central will record this passphrase in its encrypted settings file, so you do not have to reenter it when signing or decrypting files. This passphrase will also be displayed each time a private/public keypair is exported.

Exporting Keys from Other Applications

If you have been using another PGP application, you have already established a keyring. You will probably want to transfer some or all of the keys in this keyring to MOVEit Central, so you can continue to use the same keys without additional coordination with your correspondents.

Before you can import these keys into MOVEit Central, you must export them from the other PGP application. This section describes how to export keys from two popular PGP applications. Note: the act of exporting keys does not remove them from the original application, so you can continue to use the keys with the old application if you like.

Exporting from GNU Privacy Guard

To export a single public key from GnuPG, use a command line like:

```
gpg -a --export "Fred Smith" >fredsmith-public-key.asc
```

To export all public keys from GnuPG, use a command line like:

```
gpg -a --export >all-public-keys.asc
```

To export a single private key from GnuPG, use a command line like:

```
gpg -a --export-secret-keys "Fred Smith" >fredsmith-private-key.asc
```

To export all private keys from GnuPG, use a command line like:

```
gpg -a --export-secret-keys >all-private-keys.asc
```

Note: unlike some other applications, GnuPG does not export the public key when it exports the private key. To export both the private key and the public key for a user, use a sequence like:

```
gpg -a --export "Fred Smith" >fredsmith-both.asc gpg -a --export-secret-keys "Fred
Smith" >>fredsmith-both.asc
```

Exporting from PGP Corporation's PGP Command Line

To export a single public key from PGP, use a command line like:

```
pgp --export "Mary Jones" --output maryjones-public-key.asc
```

To export a single public/private keypair from PGP, use a command line like:

```
pgp --export-key-pair "Mary Jones" --output maryjones-both.asc
```

There does not appear to be a single PGP Command Line command which will export all keys.

Importing Keys into MOVEit Central

Once you have exported one or more keys from another PGP application, you can use MOVEit Central Admin to import the key(s) into MOVEit Central. To import a PGP key, use the "Import" button in the Manage PGP Keys dialog. Select the file to which the other application exported the key(s). The same procedure is used to import secret keys and public keys; MOVEit Central will figure out which type a given key is. If you are importing a public key--which is the typical case--then do not enter a passphrase when prompted. You will typically import secret keys only if you are converting from another PGP application and have already established keys with that application. Once the key file has been successfully imported, a popup message will detail which keys were imported from the file.

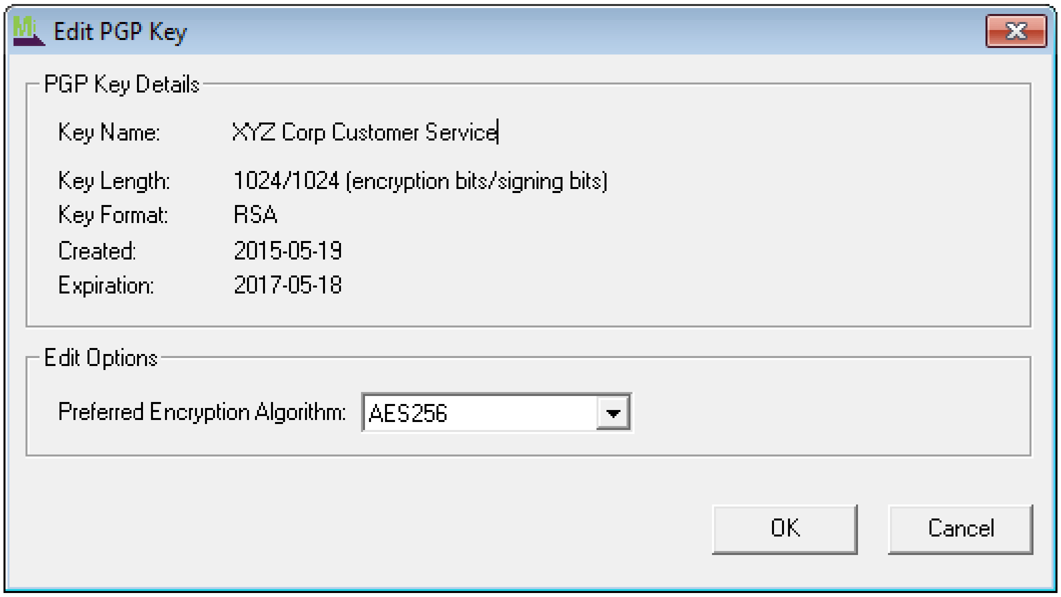
Exporting Keys from MOVEit Central

To export a key, select it in the Manage PGP Keys dialog and choose the Export button. You will see these options:

- **Export Private Key** - If the key in question is a secret key (keypair), you have the option of exporting the secret component as well as the public component. You should choose this option only if you are saving the key for your own purposes; do not give the secret key to others. If you do choose to export a private key, MOVEit Central Admin will remind you of the passphrase. You will need this passphrase to use the key for signing or decryption purposes on the system to which the private key is being exported.
- **Export to File** - Specifies the filename on the MOVEit Central Admin computer to which the exported key should be written. The file will be "ASCII Armored"--in other words, it will be a text file.
- **Also email copy to** - If you have at least one SMTP host defined, you may have MOVEit Central email the key as an attachment. Enter the recipient's email address. For security reasons, this option is available only for public keys.
- **using SMTP Host** - Choose one of the SMTP hosts that you have configured in the Hosts tab. This determines both the email server used, and the "From:" address in the message.

Editing Keys to Select Symmetric Algorith

When encrypting, MOVEit Central uses the symmetric encryption algorithm associated with public key of the first recipient. (Prior to version 3.4, the algorithm was specified as part of the Process task element; during an upgrade to MOVEit Central 3.4, these preferences are copied to the recipient key settings.) The "Edit" button allows you to choose which algorithm should be used for this public key.



Key Name: XYZ Corp Customer Service

Key Length: 1024/1024 (encryption bits/signing bits)

Key Format: RSA

Created: 2015-05-19

Expiration: 2017-05-18

Preferred Encryption Algorithm: AES256

The choices are:

- Default - Use the default preferred algorithm specified in the PGP public key itself. All of the other choices cause MOVEit Central to explicitly override this algorithm.
- 3DES - Triple DES: three rounds of the well-known 56-bit 1977-vintage DES algorithm.
- AES128 - 128-bit AES. AES is the Advanced Encryption Standard approved by the US National Institute of Standards and Technology in 2001.
- AES192 - 192-bit AES.
- AES256 - 256-bit AES.
- CAST5 - 128-bit CAST5, an algorithm rarely used outside the context of PGP.
- IDEA - 128-bit IDEA, an algorithm rarely used outside the context of PGP because it is proprietary.
- TWOFISH - a free 1999-vintage algorithm similar in security to AES, and designed by a team of well-known cryptographers, including Bruce Schneier.

All of these algorithms are considered secure, though AES256 and TWOFISH may have an edge over the others. Your choice will probably be made on the basis of compatibility with the recipient's software. "Default" is probably the safest choice.

Deleting Keys

To remove a key from your keyring, select it in the list of keys and choose the Delete button. Be cautious about deleting keys from "My Keys". If you do not have a backup copy of the key, you will not be able to decrypt messages encrypted by the sender with the public component of that key.

Monitoring Tasks

Overview

MOVEit Central offers several ways to monitor the file transfer and manipulation tasks. The most commonly used are provided in the MOVEit Central Admin interface.

- ***Debug Log Tab*** (on page 240) - Monitors the debug log.
- ***Status Tab*** (on page 238) - Provides access to current status and last run information.
- ***Reports Window*** (on page 241) - Provides access to current status and statistics about previous runs.

MOVEit Central also offers several other way to keep tabs on task status such as ***email alerts*** (see "***Email Notification***" on page 264), ***event log messages*** (see "***Event Log***" on page 262) and ***direct access*** (on page 264) to the Central log file and database.

Related Settings

There are several settings in MOVEit Central's "Central Config" program and MOVEit Central Admin which control what information is actually recorded by MOVEit Central.

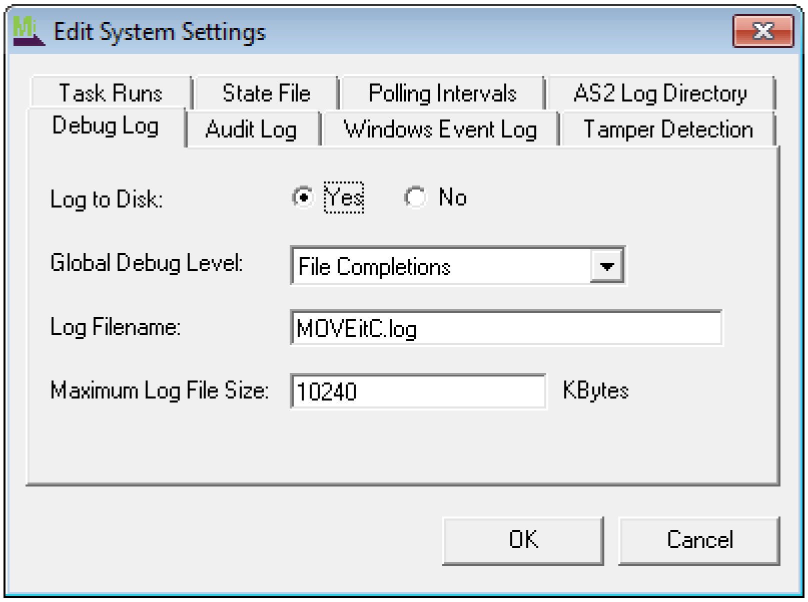
"Central Config" Settings

The only monitor setting set in the "Central Config" program is the ODBC Data Source Name (DSN) of the database to which MOVEit Central writes all its task statistics. (More information about the exact format of this database is found in the "Advanced Topics" section.) Normally the value of this setting is "MICStats".

System Settings

MOVEit Central Admin's monitor settings are found on the Edit System Settings dialog, which can be accessed from the Settings menu by clicking the System Settings option. The settings are grouped with related settings in tabs. There are also a number of other settings here that control how MOVEit Central works.

Debug Log



Log to Disk: ● Yes ○ No

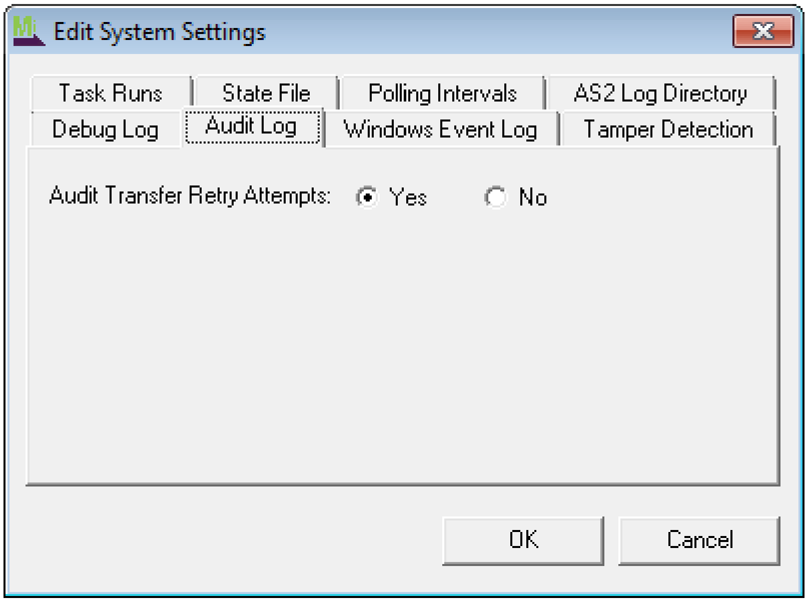
Global Debug Level: File Completions

Log Filename: MOVEitC.log

Maximum Log File Size: 10240 KBytes

- **Log to Disk** - Controls whether or not MOVEit Central writes its log file to disk. (The scrolling display on the Log tab of MOVEit Central Admin is not affected by this setting.)
- **Global Debug Level** - Controls how much information is logged to disk and is displayed in the "Log" tab if no task filter is set.
- **Log Filename** - Controls the name of the log file. The default value is "MoveITC.log". If no path is provided, the file will be written out to the same folder in which MOVEit Central has been installed. A complete file path (e.g., "D:\moveit\logs\central.log") can be used to write the log file on another drive. A file will only be written if "Log to Disk" is "yes".
- **Maximum Log File Size** - Controls how big log files are allowed to grow before they are automatically rolled. (Old log files are retained for one generation as ".old" files. Only applies if "Log to Disk" is "yes")

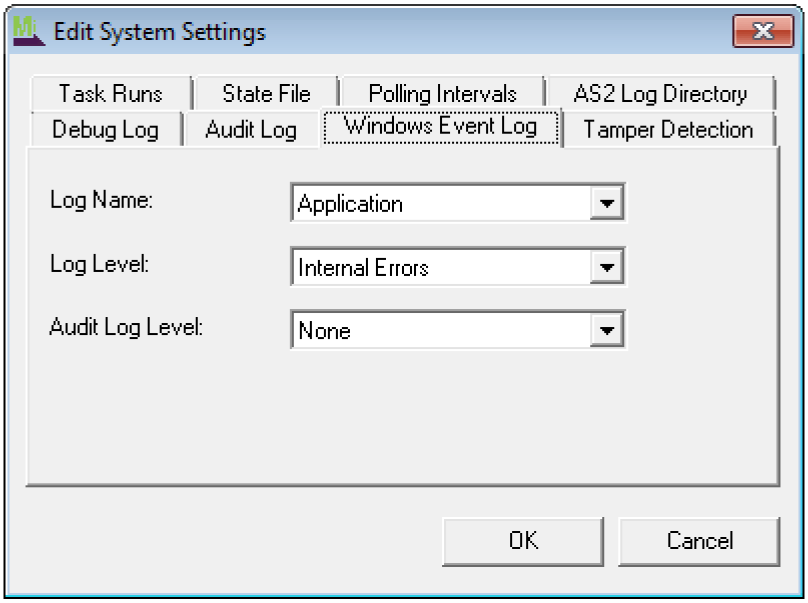
Audit Log



Audit Transfer Retry Attempts: ● Yes ○ No

- **Audit Transfer Retry Attempts** - When set to Yes, MOVEit Central will audit log each individual retry attempt to the database when issues are encountered during a file transfer. When set to No, only a single audit entry is logged after all retry attempts have completed.

Windows Event Log



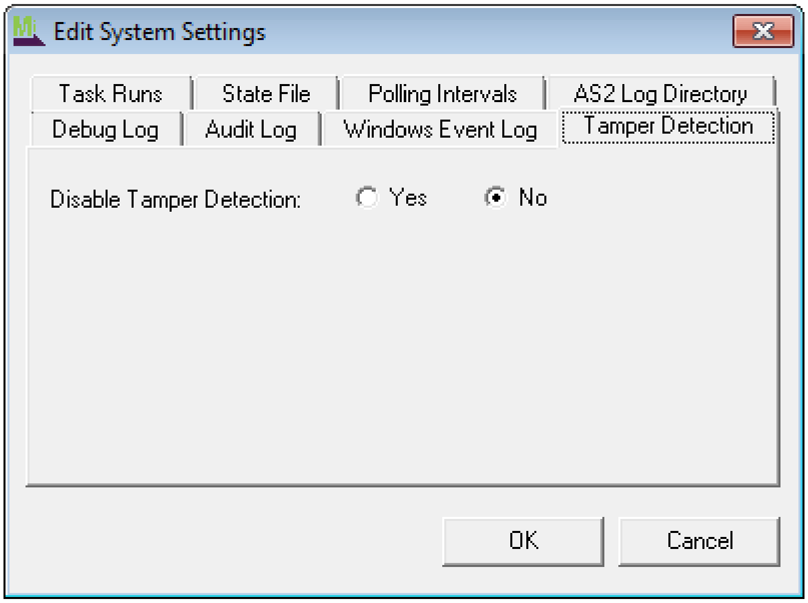
Log Name: Application

Log Level: Internal Errors

Audit Log Level: None

- **Log Name** - Controls which Windows Event Log is used. (In previous versions, MOVEit Central always logged to the built-in Windows "Application" Event Log.)
- **Log Level** - Controls how much information is logged to the local Windows Event Log.
- **Audit Log Level** - Controls how much audit log information is logged to the local Windows Event Log.

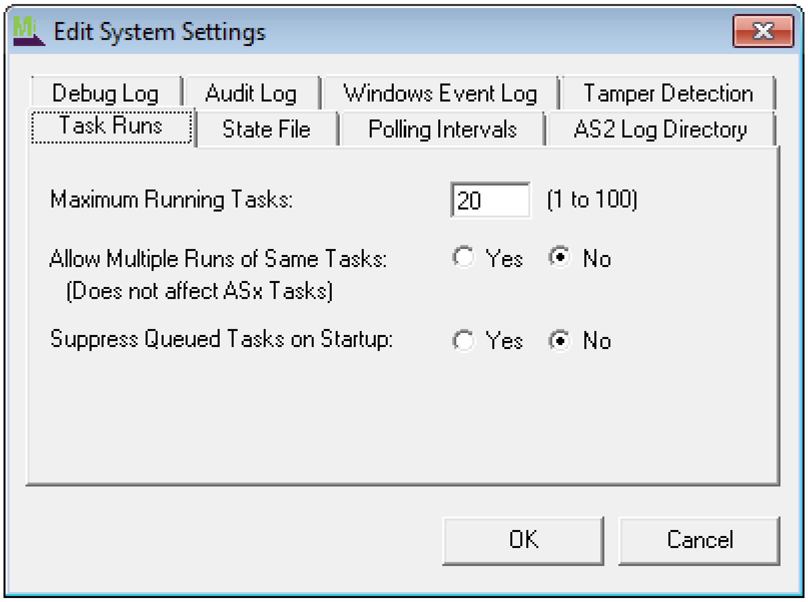
Tamper Detection



Disable Tamper Detection: ○ Yes ● No

- **Disable Tamper Detection** - Controls whether or not tamper evident protection is used. Setting this to "Yes" will slightly increase performance and avoid false positives.

Task Runs



Maximum Running Tasks: 20 (1 to 100)

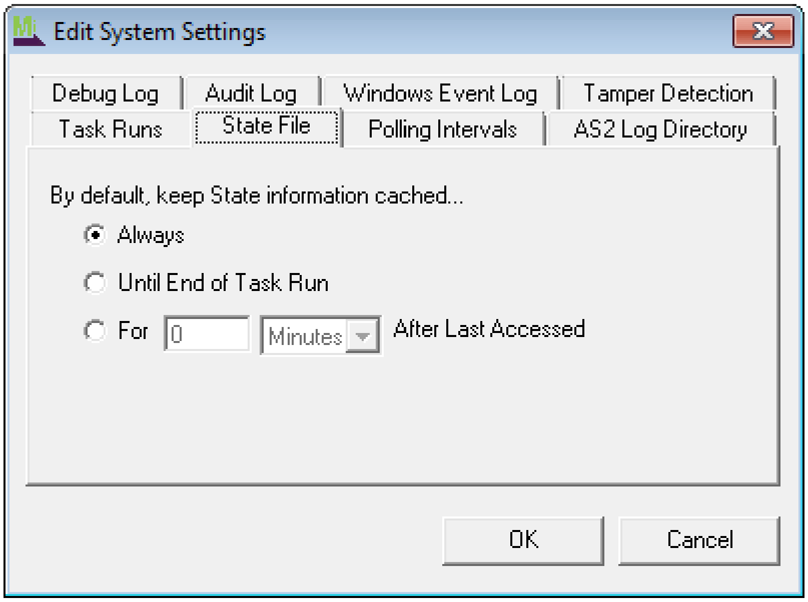
Allow Multiple Runs of Same Tasks: (Does not affect ASx Tasks) ○ Yes ● No

Suppress Queued Tasks on Startup: ○ Yes ● No

- **Maximum Running Tasks** - Controls the maximum number of tasks MOVEit Central will run at any given time. This setting is often useful on machines that otherwise attempt to launch hundreds of tasks all at once as it essentially implements a task run throttle. Tasks prevented from running immediately are queued; queued tasks are taken and started from this queue in FIFO order whenever the number of tasks currently running drops below the maximum value set here. The default value for this setting is 20.

  Note that this method of throttling task runs only limits tasks run directly by the MOVEit Central scheduler. Tasks started manually by either MOVEit Central Admin or MOVEit Central API, or tasks started via a Next Action step of another task will ignore the running tasks limit and insert themselves in front of any queued scheduled tasks.
- **Allow Multiple Runs of Same Tasks** - Controls whether multiple runs of a task will be allowed to run at the same time. Setting this to "No" will prevent a task from being run more than once at a time. This does not affect tasks that use AS2 hosts, and can be overridden when starting a task manually.
- **Suppress Queued Tasks on Startup** - When enabled, MOVEit Central will suppress automatic running, at startup, of tasks that are subject to notification. This also affects running of these tasks when a secondary fails over to being the primary. Enabling this option gives better startup performance, but may result in the delayed retrieval of "new" files.

State File



By default, keep State information cached...

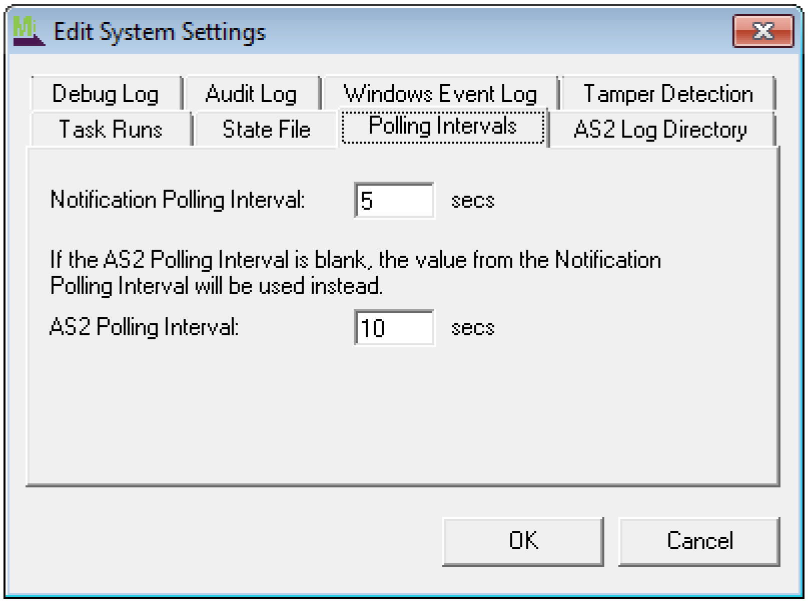
● Always

○ Until End of Task Run

○ For 0 Minutes After Last Accessed

- **Default State Caching Settings** – The default State Caching settings are inherited by new Hosts/Tasks and any existing Hosts/Tasks that are assigned to use the system's Default State Caching Settings. By default, MOVEit Central always keeps state file information cached in memory in order to achieve maximum efficiency. In certain environments, however, this can become quite memory intensive. The State Caching settings can be used to remove state file information from memory after a task run or even after a specified amount of time.

Polling Intervals



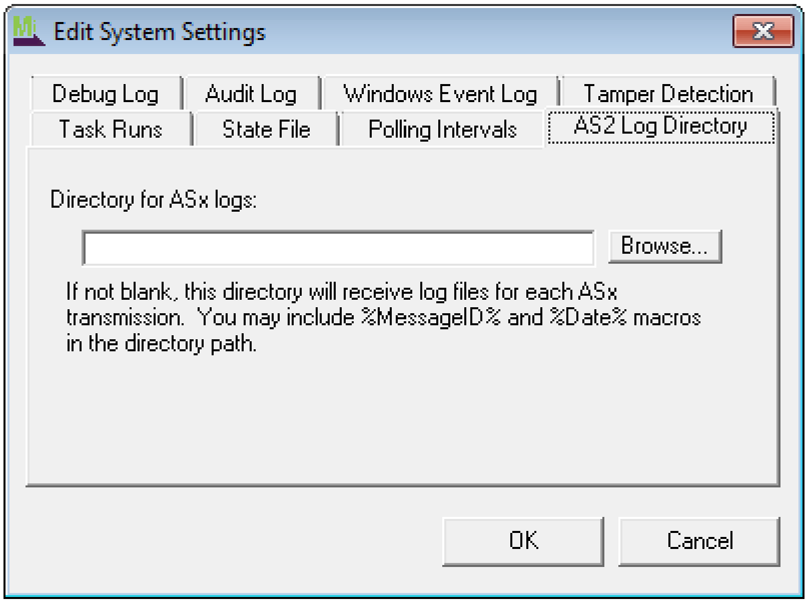
Notification Polling Interval: 5 secs

If the AS2 Polling Interval is blank, the value from the Notification Polling Interval will be used instead.

AS2 Polling Interval: 10 secs

- **Notification Polling Interval** - Controls how often MOVEit Central polls target servers that use the File Notification option for new files.
- **AS2 Polling Interval** - If the AS1/AS2/AS3 module is licensed, the additional AS2 Polling Interval option will be present here as well. This controls how often MOVEit Central polls an AS2-linked MOVEit DMZ server for incoming AS2 messages.

AS2 Log Directory



Directory for ASx logs:

If not blank, this directory will receive log files for each ASx transmission. You may include %MessageID% and %Date% macros in the directory path.

- **Directory for ASx Logs** - You can enter a directory which will receive log files for each ASx transmission. You can include the %MessageID% and %Date% macros in the directory path so that logs will be written to separate directories for each MessageID and Date. This directory can also be on a UNC path. Make sure that the account that the MOVEit Central service is running as (the default account is called "micsvc") has permissions for the specified directory, otherwise the AS2 Task will fail when it attempts to access the directory.

Troubleshooting

A few MOVEit Central troubleshooting hints are provided below.

Issues Encountered While Starting MOVEit Central

- **Startup "hangs" or takes a long time...** - During startup, MOVEit Central performs some analysis against its statistics database. If this database is very large (>100 megabytes) this analysis may take several minutes. To reduce this time, use the "PurgeStats.vbs" script to periodically purge and save off old entries from your statistics database.

Issues Encountered While Connecting to MOVEit Central

- **"Could not connect" error** - MOVEit Central may not be running. If MOVEit Central is running, your connection is likely being blocked by a personal firewall, port-filtering router, gateway firewall or some other device. See the "Connecting..." section of MOVEit Central Admin for information about connecting from remote locations.
- **"Bad username or password" error** - Means what it says. Either the user doesn't exist, the password is bad, or the user isn't in the domain/machine you thought it was.
- **"User not in MOVEit Admin group" error** - The user has been authenticated, but it doesn't belong to a MOVEit Admin, MOVEit Log or MOVEit-Users group. Therefore, MOVEit Central cannot grant this user any permissions and will deny the connection.
- **"RPC Server is unavailable" error** - The user under which the MOVEit Central runs as a service is not a member of a domain, but the user you are trying to authenticate with is.

Task Failure Issues

The first thing to do with any failed task is as follows:

1. Set the task filter to view only that task.
2. Run that task again after setting the debug level to "All Debug" on the Log tab.

There are many clues in the debug log as to why a particular task failed.

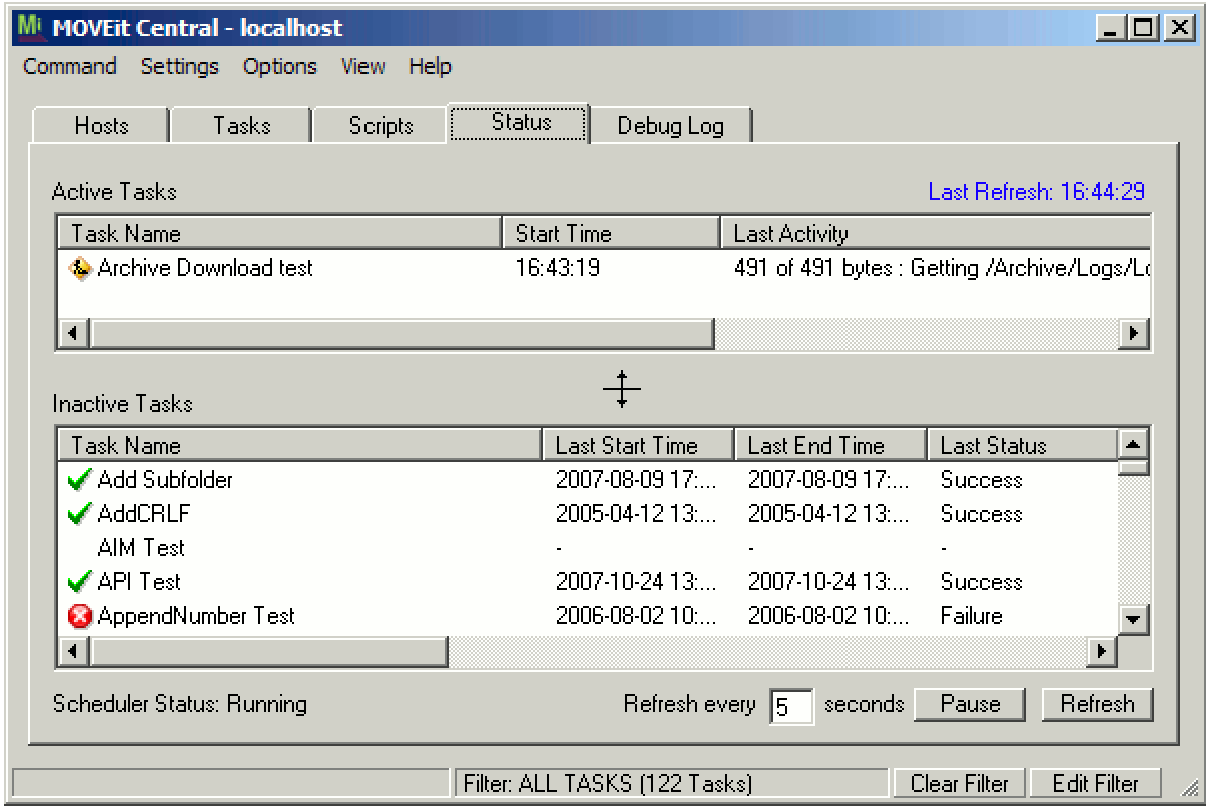
- **"Could not connect" or "time out during connect" errors -** Either the remote server is not alive or access to that remote server is blocked by a firewall.
- **"Could not negotiate SSL" errors -** Either MOVEit Central is required to provide an SSL client certificate but configured to not provide one or there is something terribly wrong with the SSL server certificate on the remote site. However, if this message is coming from an FTP/SSL site, this error could also be caused by corruption of the data stream by an intermediate firewall that performs application proxy functions but isn't familiar with FTP/SSL (e.g., early versions of Checkpoint firewalls).
- **"Bad username or password" errors -** Check your credentials.
- **"Abort" errors -** Either the client (MOVEit Central) or the remote server shut the connection prematurely. If it happens consistently, it may be an issue with a proxy server or a software bug.
- **"Nothing Happened" -** Check to make sure your source is configured to look in the correct location (host, folder, pathname). Also make sure there are actually files to pick up (adjust "delete original" option accordingly) and that the "collect only new files" option is set as expected.
- **"Cannot create log file in directory" -** Check that the account that the MOVEit Central service is running as (the default account is called "micsvc") has permissions to access the directory specified in "Directory for ASx logs"; this is set in the System settings > AS2 Log Directory tab.

...With Admin

This section describes monitoring options available with the Admin Console.

Status Tab

The Status tab contains two windows, Active Tasks, which displays a list of currently running tasks, and Inactive Tasks, which displays a list of tasks that are not currently running. These views allow operators to quickly determine the most recent status of the various tasks that have been configured in MOVEit Central. Also displayed on this tab is the status of the Scheduler module in the current MOVEit Central server, as well as a refresh interval setting and buttons to pause/resume status updates and update the status view immediately. The configured refresh interval will be remembered across MOVEit Central Admin sessions.



Active Tasks

Last Refresh: 16:44:29

Task Name	Start Time	Last Activity
Archive Download test	16:43:19	491 of 491 bytes : Getting /Archive/Logs/Lo

Inactive Tasks

Task Name	Last Start Time	Last End Time	Last Status
✓ Add Subfolder	2007-08-09 17:...	2007-08-09 17:...	Success
✓ AddCRLF	2005-04-12 13:...	2005-04-12 13:...	Success
AIM Test	-	-	-
✓ API Test	2007-10-24 13:...	2007-10-24 13:...	Success
✗ AppendNumber Test	2006-08-02 10:...	2006-08-02 10:...	Failure

Scheduler Status: Running

Refresh every 5 seconds

Filter: ALL TASKS (122 Tasks)

You can right-click the name of a task in either the Active Tasks or Inactive Tasks windows to bring up a menu with these options:

- **Run Task Now** - Allows you to start the task. This option is only available in the Inactive Tasks window..
- **Stop Task** - Allows you to stop a task. This option is only available in the Active Tasks window.
- **Kill Task** - Allows you to kill a task. This option is only available in the Active Tasks window.
- **Edit Task** - Allows you to change the task. You can modify, add, or remove source, destinations, and other task entities.
- **View Task Runs** - Displays a report of all runs of this task in the ***Report window*** (on page 241).
- **View File Activity** - Displays a report of all files transferred by this task in the Report window.
- **View Audit Trail** - Displays a report of all audited events against this task in the Report window.
- **Set Filter to This Task** - Sets the task filter to only display this task.

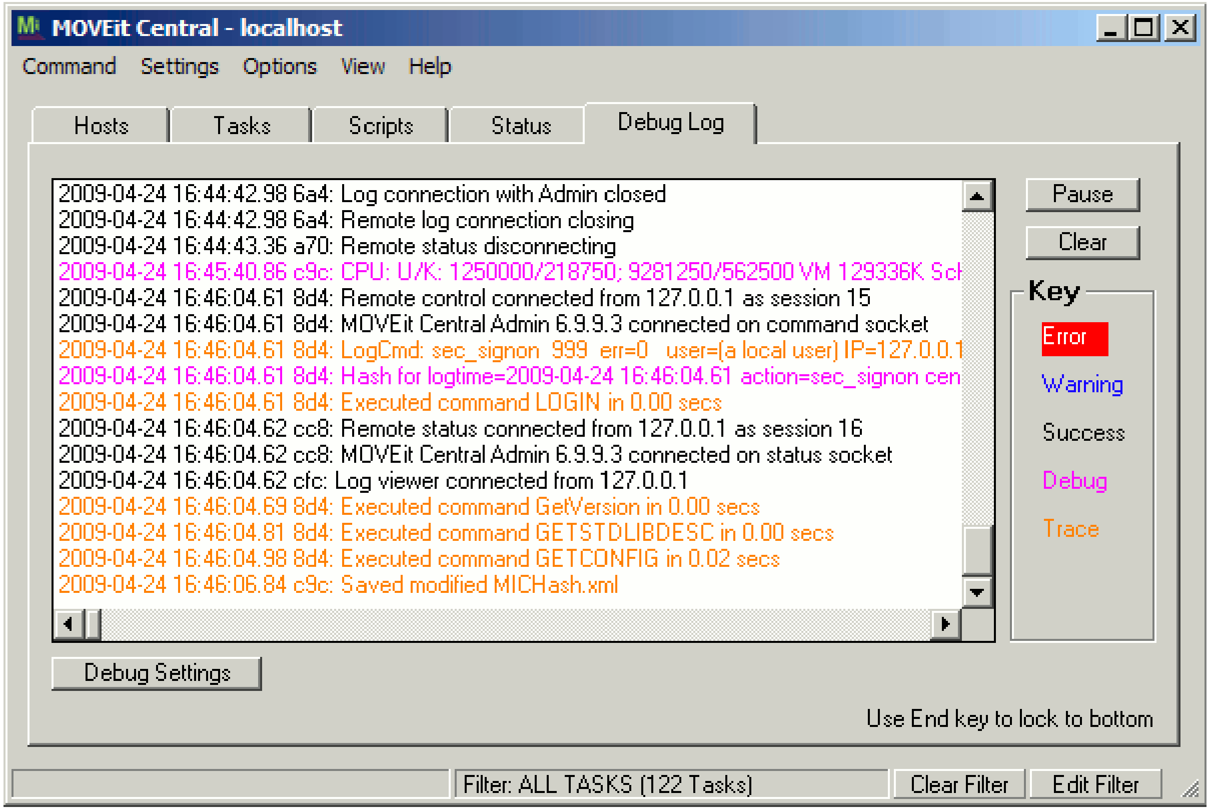
The cross control with arrows on its top and bottom is used to control how much of the screen is used to display active tasks and how much is used to display inactive tasks.

Finding "Idle" Tasks

One handy way to use the "Inactive Tasks" window is to sort on "Last Start Time" and look for any tasks that have not run recently. (These tasks will show "-" instead of a real time in this category.) By examining this list of tasks you can often get an idea of which tasks may be idle and candidates for deletion.

Debug Log Tab

MOVEit Central Admin displays MOVEit Central activity in real time through its debug log facility.



```
2009-04-24 16:44:42.98 6a4: Log connection with Admin closed
2009-04-24 16:44:42.98 6a4: Remote log connection closing
2009-04-24 16:44:43.36 a70: Remote status disconnecting
2009-04-24 16:45:40.86 c9c: CPU: U/K: 1250000/218750; 9281250/562500 VM 129336K Sch
2009-04-24 16:46:04.61 8d4: Remote control connected from 127.0.0.1 as session 15
2009-04-24 16:46:04.61 8d4: MOVEit Central Admin 6.9.9.3 connected on command socket
2009-04-24 16:46:04.61 8d4: LogCmd: sec_signon  999  err=0   user=(a local user) IP=127.0.0.1
2009-04-24 16:46:04.61 8d4: Hash for logtime=2009-04-24 16:46:04.61 action=sec_signon cen
2009-04-24 16:46:04.61 8d4: Executed command LOGIN in 0.00 secs
2009-04-24 16:46:04.62 cc8: Remote status connected from 127.0.0.1 as session 16
2009-04-24 16:46:04.62 cc8: MOVEit Central Admin 6.9.9.3 connected on status socket
2009-04-24 16:46:04.62 cfc: Log viewer connected from 127.0.0.1
2009-04-24 16:46:04.69 8d4: Executed command GetVersion in 0.00 secs
2009-04-24 16:46:04.81 8d4: Executed command GETSTDLIBDESC in 0.00 secs
2009-04-24 16:46:04.98 8d4: Executed command GETCONFIG in 0.02 secs
2009-04-24 16:46:06.84 c9c: Saved modified MICHash.xml
```

Filter: ALL TASKS (122 Tasks)

When MOVEit Central Admin successfully connects to MOVEit Central, MOVEit Central Admin's log window will display several recent, but past log entries made by MOVEit Central before displaying live entries. This feature allows operators to review a short period of recent history online as well as monitor current activities.

Using the mouse, you can select text in the log window, copy it using <CTRL>+<C> and paste it into any other application. (Most email clients and word processors will retain line colors during a copy.)

If a task filter is currently set, the log entries will be filtered down to those entries related to the task or task group. Optionally, system log entries (such as notification messages) may also be shown. The custom debug level option will also appear if a task filter is set, allowing the user to define a temporary custom debug level for the selected task or task group. See the ***Per-Task Debugging section of the Task Filter*** (see "***Task Filter***" on page 258) page for more details.

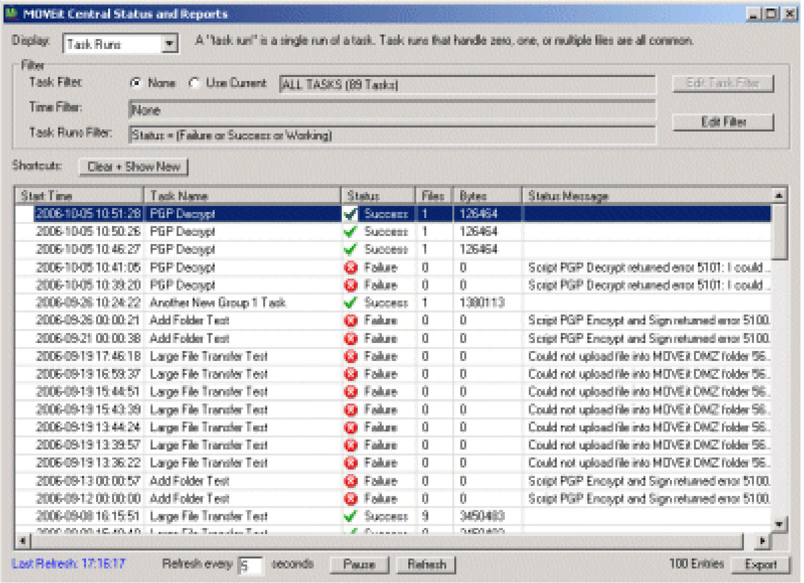
If a task filter is not currently set, a convenience button will be present which will open the ***System Settings*** (see "***Related Settings***" on page 229) dialog, to allow the user to alter the global debug level.

Access Control

Users belonging to the MOVEit Admin, MOVEit Log and any of the restricted "MOVEit Users-*" are allowed to use this tab. However, restricted users will only see tasks that they are allowed to run or edit.

Reports Window

The Reports window provides access to current status and recorded statistics in a convenient report format. Three different report display types are available, each with many user-selectable information columns and filter options. Report data is typically refreshed periodically, and the displayed data can be exported to several different formats.



Display: Task Runs

A "task run" is a single run of a task. Task runs that handle zero, one, or multiple files are all common.

Filter

Task Filter: ● None ○ Use Current ALL TASKS (89 Tasks)

Time Filter: None

Task Runs Filter: Status = (Failure or Success or Working)

Shortcuts:

Start Time	Task Name	Status	Files	Bytes	Status Message
2006-10-05 10:51:28	PGP Decrypt	✓ Success	1	126464	
2006-10-05 10:50:26	PGP Decrypt	✓ Success	1	126464	
2006-10-05 10:46:27	PGP Decrypt	✓ Success	1	126464	
2006-10-05 10:41:05	PGP Decrypt	☒ Failure	0	0	Script PGP Decrypt returned error 5101: I could ...
2006-10-05 10:39:20	PGP Decrypt	☒ Failure	0	0	Script PGP Decrypt returned error 5101: I could ...
2006-09-26 10:24:22	Another New Group 1 Task	✓ Success	1	1380113	
2006-09-26 00:00:21	Add Folder Test	☒ Failure	0	0	Script PGP Encrypt and Sign returned error 5100.
2006-09-21 00:00:38	Add Folder Test	☒ Failure	0	0	Script PGP Encrypt and Sign returned error 5100.
2006-09-19 17:46:18	Large File Transfer Test	☒ Failure	0	0	Could not upload file into MOVEit DMZ folder 56...
2006-09-19 16:59:37	Large File Transfer Test	☒ Failure	0	0	Could not upload file into MOVEit DMZ folder 56...
2006-09-19 15:44:51	Large File Transfer Test	☒ Failure	0	0	Could not upload file into MOVEit DMZ folder 56...
2006-09-19 15:43:39	Large File Transfer Test	☒ Failure	0	0	Could not upload file into MOVEit DMZ folder 56...
2006-09-19 13:44:24	Large File Transfer Test	☒ Failure	0	0	Could not upload file into MOVEit DMZ folder 56...
2006-09-19 13:39:57	Large File Transfer Test	☒ Failure	0	0	Could not upload file into MOVEit DMZ folder 56...
2006-09-19 13:36:22	Large File Transfer Test	☒ Failure	0	0	Could not upload file into MOVEit DMZ folder 56...
2006-09-13 00:00:57	Add Folder Test	☒ Failure	0	0	Script PGP Encrypt and Sign returned error 5100.
2006-09-12 00:00:00	Add Folder Test	☒ Failure	0	0	Script PGP Encrypt and Sign returned error 5100.
2006-09-08 16:15:51	Large File Transfer Test	✓ Success	9	3450480	

Last Refresh: 17:16:17 Refresh every 5 seconds

100 Entries

Report Options

The Reports window provides many options that are available for each report type, as well as some options which are specific to each report.

- **Display**: Selects the type of information to display in the report window. Available options are "Task Runs", "File/Folder Activity", and "Audit". See the ***Report Types*** (on page 244) following section for more information about each report type.
- **Filter**
  - **Task Filter**: Allows the user to use the same ***task filter*** (on page 258) currently in use by the main MOVEit Central Admin window to filter the reports display. When the Use Current option is selected, the current task filter will be applied. The current task filter is displayed in the textbox next to these options, and an Edit Task Filter button is available as well, when the Use Current option is selected.
  - **Time Filter**: Displays the current date/time filter being applied to the reports display. Editing of both this and the report-type-specific filter can be done by clicking the Edit Filter button. By default, the time filter is set to show entries starting at midnight on the current day, however this behavior can be disabled by turning off the Default Report Range Is Today option from the ***Options menu*** (on page 97). Also, viewing entries for a specific task, host, or script by right-clicking the element and selecting one of the View Entries options will reset the time filter to show all entries.
  - **Report-Type-Specific Filter**: Displays the current report-type-specific filter being applied to the reports display. Editing of both this and the date/time filter can be done by clicking the Edit Filter button.
- **Shortcuts**
  - **Hide Cleared Task Runs (see "Options Menu" on page 97) Option Enabled**:
    - **Clear Selected**: Marks all currently selected task runs as Cleared. If the Hide Cleared Entries report filter option is set, cleared task runs will not be displayed in the task runs report. Task runs may be selected by clicking the checkbox for the task run data row. Checkboxes will only be visible when the Hide Cleared Task Runs option is enabled.
    - **Select/Unselect All**: Selects or unselects all currently listed task runs.
  - **Hide Cleared Task Runs Option Disabled**:
    - **Clear + Show New**: Clicking this button will clear the current reports display and change the current report-type-specific filter to only show entries with entry IDs greater than the currently most recent entry. This button is useful for clearing out entries that no longer interest the user so they can more easily focus on new entries that arrive.

  - **Both**:
    - **Reset Filter**: Resets the current report filter back to its default value.
- **Right-Click Options**
  - **Shared Options**: These options are present regardless of the report type that is currently selected.
    - **View ... Details**: If a data entry is selected, the right-click menu will include a specific View ... Details option, which will open a details window for the currently selected entry. The details window can also be opened by double-clicking a data entry in the File/Folder Activity and Audit report views.
    - **Select Columns**: This option will be present regardless of whether a data entry is present or selected, and allows the user to specify which columns will be displayed in the reports display. The selected column list for each report type will be stored in the registry for the current user and remembered the next time MOVEit Central Admin is run.
  - **Task Runs Options**: These options are present when the selected report type is Task Runs and a data entry is selected.
    - **View Task Run File Activity**: Changes the selected report type to File/Folder Activity and sets the file activity filter to the specific task run selected. The resulting report display will show all the file transfer activities that the selected task run performed. This action can also be triggered by double-clicking a data entry.
    - **Run/Stop/Kill Tas**k **Now**: For non-running tasks, the Run Task Now option will be present which will command Central to run the task immediately. For running tasks, the Stop Task Now option will be present which will command Central to stop the task as soon as possible. For running tasks for which a Stop Task Now command has already been executed, the Kill Task Now option will be present which will forcibly remove the task run from the list of running tasks and audit log the fact that the task run has ended.
    - **Edit Task**: Switches focus back to the main MOVEit Central Admin window, changes to the Tasks tab, and selects the task which the selected task run entry references.
    - **View Task Runs**: Changes the task runs filter to show only task runs of the same task as the specific task run selected. The resulting report display will show all the task runs of the same task as the selected task run.
    - **View Task File Activity**: Changes the selected report type to File/Folder Activity and sets the file activity filter to the task of the specific task run selected. The resulting report display will show all the file transfer activities for all of the task runs of the same task as the selected task run.
  - **File/Folder Activity Options**: These options are present when the selected report type is File/Folder Activity and a data entry is selected.

    - **Back to Task Runs**: Changes the selected report type to Task Runs. The most recently used task runs filter will be applied.
    - **Edit Task**: Switches focus back to the main MOVEit Central Admin window, changes to the Tasks tab, and selects the task which the selected file/folder activity entry references.
    - **View Task File Activity**: Changes the file/folder activity filter to the task which the specific file/folder activity entry references. The resulting report display will show all the file transfer activities for all of the task runs of the task which the selected file/folder activity entry references.
  - **Audit Options**: These options are present when the selected report type is Audit and a data entry is selected.
    - **Edit Task/Host/Script**: If a selected audit entry references a specific task, host, or script, this option will be present and will switch focus back to the main MOVEit Central Admin window, switch to whatever tab the element is displayed in, and select the referenced element.
- **Refresh Every X Seconds**: This value determines how often the current data will refresh itself. The configured value will be remembered across MOVEit Central Admin sessions.
- **Pause/Resume**: Pauses or resumes the data refresh.
- **Refresh**: Causes the data to refresh immediately.
- **Export**: Exports the current data in a user-selected format. Available formats are CSV (comma-separated values), and XML. If CSV is chosen, the delimiter character and the text-qualifier character will be editable.

Report Types

This section describes the types of reports available when you use Central Admin.

Task Runs

Task Runs reports include information about when a task ran, and what the result was.

Available report columns are:

- **Log Time**: Date and time the entry was logged
- **Scheduled Time**: Date and time the task run was scheduled to run
- **Start Time**: Actual date and time the task run started
- **End Time**: Actual date and time the task run ended
- **Node**: MOVEit Central failover node number
- **Task Name**: Name of the entry's associated task
- **Task ID**: Numeric ID of the entry's associated task
- **Log ID**: Log entry's unique, numeric ID
- **Started By**: Whether or not the task was started manually
- **Status**: Whether or not the attempt succeeded
- **Files**: Count of all files uploaded to various destinations by the task run
- **Bytes**: Total size of all files uploaded to various destinations by the task run
- **Status Code**: Numeric error code (or 0 if no error)
- **Status Message**: Error or status message

File/Folder Activity

File/Folder Activity reports include information about individual file transfers. They may also include non-task-related entries, such as when a sync preview operation creates a folder. In these cases, special phrases will be displayed in the Task Name field to indicate their nature (for example, for sync preview folder adds, the Task Name field will say "*** Sync Preview ***").

Available report columns are:

- **Log Time**: Date and time the entry was logged
- **Scheduled Time**: Date and time the entry's associated task run was scheduled to run
- **Node**: MOVEit Central failover node number
- **Task Name**: Name of the entry's associated task
- **Task ID**: Numeric ID of the entry's associated task
- **Log ID**: Log entry's unique, numeric ID
- **Status**: Whether or not the attempt succeeded
- **Action**: What command, change, etc. action was attempted
- **S.Host**: Source host
- **S.Path**: Source path
- **S.File**: Source file
- **S.FileID**: Source file ID
- **S.Bytes**: Source byte count
- **S.Duration**: Source duration (seconds)
- **S.Rate**: Source rate (bytes per second)
- **S.ASxID**: Source AS1/AS2/AS3 message ID
- **S.ASxMDN**: Source AS1/AS2/AS3 MDN
- **S.Stamp**: Source date/time stamp (usually modified stamp)
- **D.Host**: Destination host
- **D.Path**: Destination path
- **D.File**: Destination file
- **D.FileID**: Destination file ID
- **D.Bytes**: Destination byte count
- **D.Duration**: Destination duration (seconds)
- **D.Rate**: Destination rate (bytes per second)
- **D.ASxID**: Destination AS1/AS2/AS3 message ID
- **D.ASxMDN**: Destination AS1/AS2/AS3 MDN
- **Status Code**: Numeric error code (or 0 if no error)
- **Status Message**: Error or status message

Audit

Audit reports include information about commands and configuration changes executed against MOVEit Central.

Available report columns are:

- **Log Time**: Date and time the entry was logged
- **Node**: MOVEit Central failover node number
- **S.Ver**: MOVEit Central server version
- **C.Name**: Client agent name
- **C.Ver**: Client agent version
- **Action**: What command, change, etc. action was attempted
- **Target Type**: Type of entity (e.g., task, host, etc.) affected (may be none)
- **Target ID**: Numeric ID of entity affected (may be none)
- **Target Name**: Name of entity affected (may be none)
- **Log ID**: Log entry's unique, numeric ID
- **Status**: Whether or not the attempt succeeded
- **User**: Name of user who initiated command, change, etc.
- **IP Address**: Location from which command, change, etc. was initiated
- **Status Code**: Numeric error code (or 0 if no error)
- **Status Message**: Error or status message
- **Additional Info**: "Yes" if additional info about this entry is available

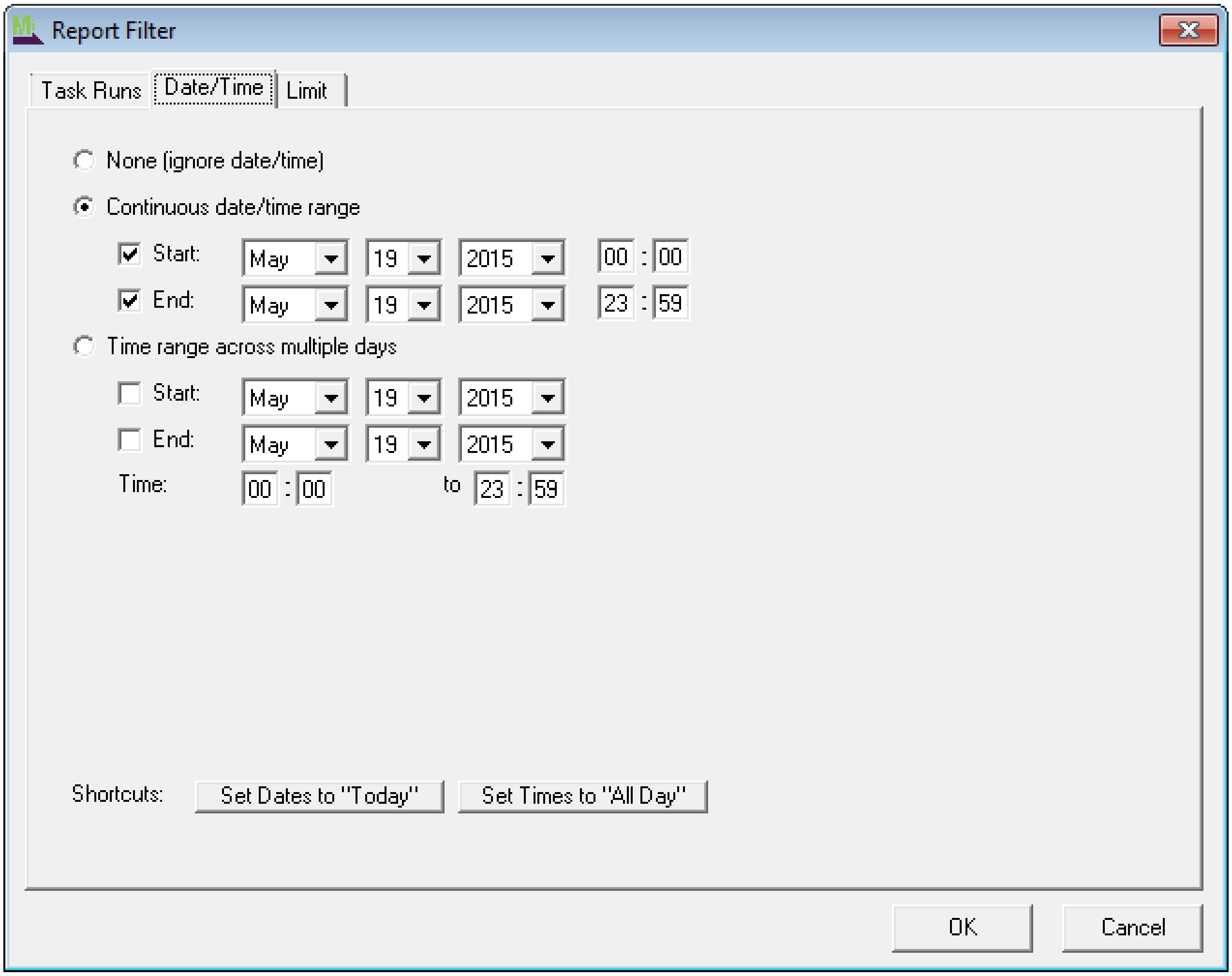
Report Filter

Report data can be filtered many different ways in order to return the exact data a user is looking for. In addition to applying the current task filter in use on the main MOVEit Central Admin window, the report filters may be edited and applied by clicking on the Edit Filter button next to the report filter descriptions.

Generic Filters

The following filters are available for all report types.

Date/Time



Report Filter

Task Runs | Date/Time | Limit

○ None (ignore date/time)

● Continuous date/time range

☑ Start: May 19 2015 00 : 00

☑ End: May 19 2015 23 : 59

○ Time range across multiple days

□ Start: May 19 2015

□ End: May 19 2015

Time: 00 : 00 to 23 : 59

Shortcuts: Set Dates to "Today" | Set Times to "All Day"

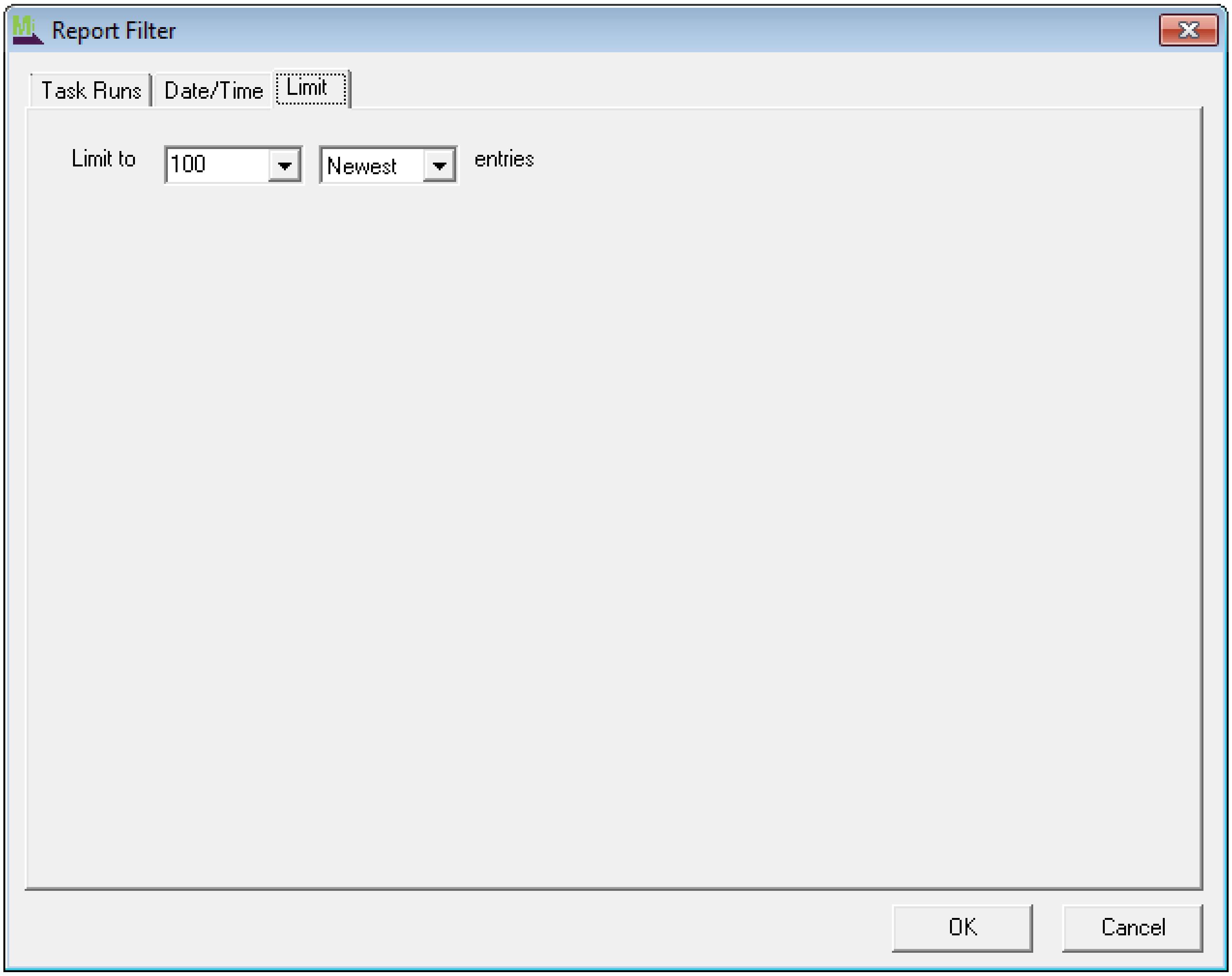
OK | Cancel

The Date/Time filter limits report data to those entries whose Log Time field value matches the selected filter option. (Note that some report types have several date and time fields. The Date/Time filter only applies to the Log Time field value.) The available Date/Time filter options are:

- **None**: Disables the Date/Time filter
- **Continuous date/time range**: Limits report data to those entries that fall between the start and end date/time stamps. The start and end stamps can be applied by checking the associated checkbox for each stamp. Otherwise, that stamp will not be used.
- **Time range across multiple days**: Limits report data to those entries whose date falls between the start and end dates, and whose time falls between the start and end times. The start and end dates can be applied by checking the associated checkbox for each date. Otherwise, that date will not be used. The start and end times are applied regardless of the date selections.

There are also two shortcut buttons available to make changing the date/time filter options easier. The Set Dates to "Today" button changes all date selectors to the current date. The Set Times to "All Day" button changes all start times to midnight, and all end times to 11:59 PM (23:59 in 24-hour time).

Limit



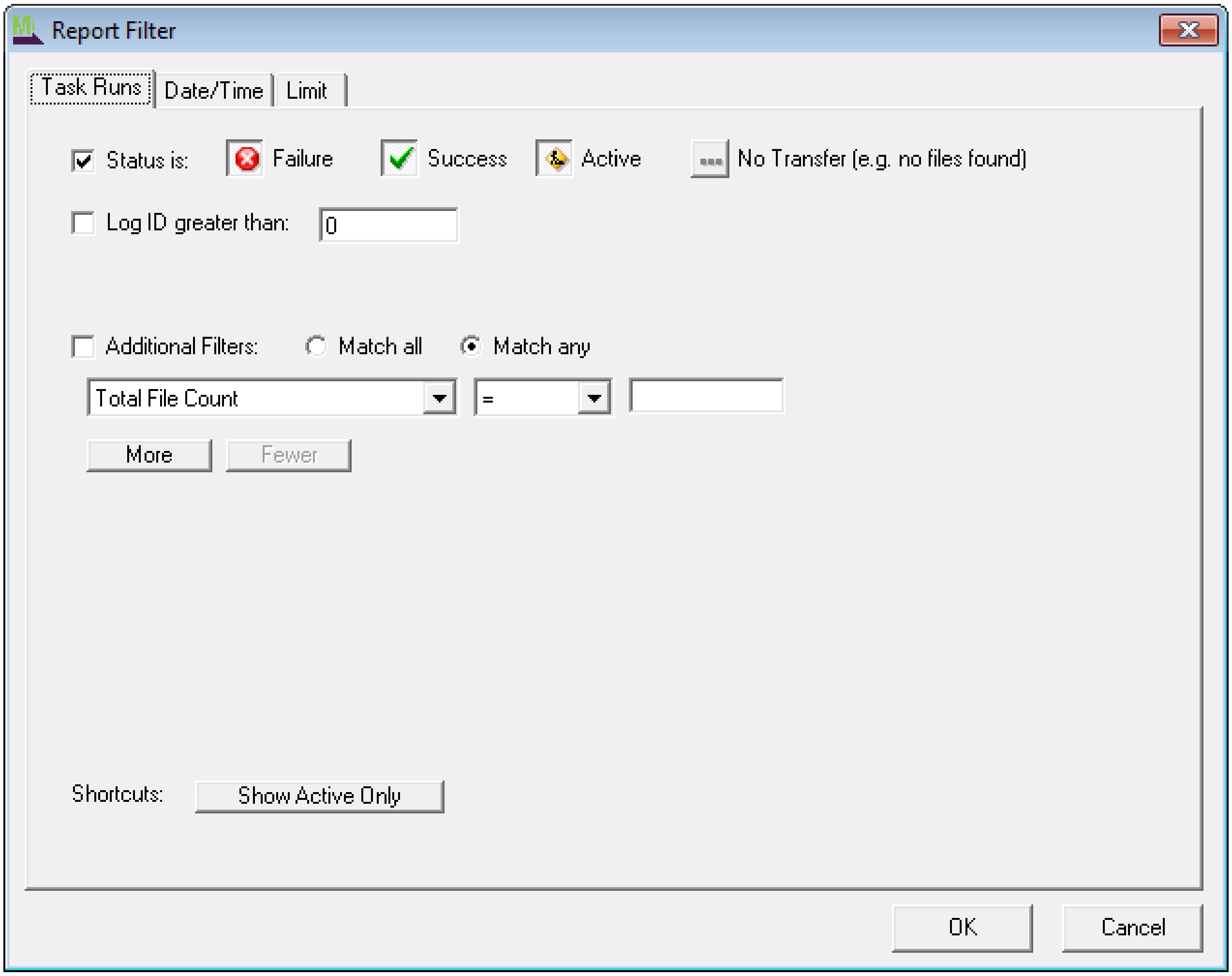
Limit to 100 Newest entries

The Limit filter limits how many entries will be returned. The maximum number of entries that can be returned is 10,000, but any number between 1 and 10,000 may be entered as a limit. Some typical limit values may also be selected. The only other limit option is whether the newest or oldest entries will be returned.

Specific Filters

In addition to the generic filters, each report type has its own specific filter options.

Task Runs



☑ Status is: Failure Success Active No Transfer (e.g. no files found)

□ Log ID greater than: 0

□ Additional Filters: ○ Match all ● Match any

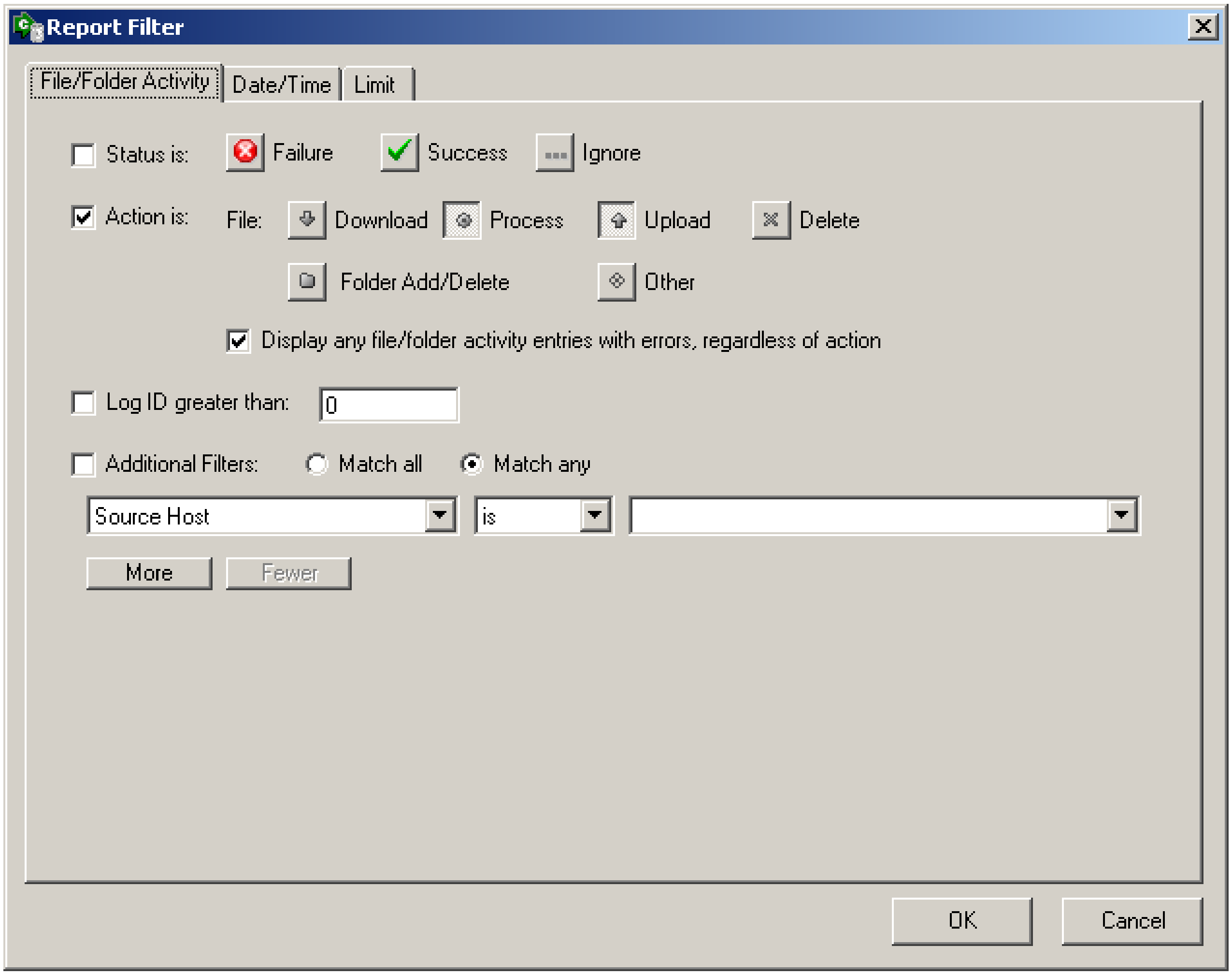
Total File Count =

Available Task Runs report filters are:

- **Status**: When enabled, limits report data to entries whose status matches the selected status options.
- **Log ID**: When enabled, limits report data to entries whose Log ID is greater than the specified value.
- **Hide Cleared Entries**: When the Hide Cleared Task Runs option is enabled, this filter option will be visible. When enabled, omits report entries marked as "cleared".
- **Additional Filters**: When enabled, applies the specified additional filters. More filters (up to three total) can be added by clicking the More button. If the Match Any option is selected, report data will be returned if it matches any of the specified filters. If the Match All option is selected, report data will only be returned if it matches all of the specified filters. Available additional filters are:
  - **Total File Count**: Matches report data whose total file count value returns true against the specified test and test value. Available test options are Equals (=), Greater Than (>), Greater Than or Equal To (>=), Less Than (<), or Less Than or Equal To (<=).
  - **Total File Size**: Matches report data whose total file size value returns true against the specified test and test bytecount. Available test options are Equals (=), Greater Than (>), Greater Than or Equal To (>=), Less Than (<), or Less Than or Equal To (<=).
  - **Status Message**: Matches report data whose status message value returns true against the specified test and test value. Available test options are Is and Contains.
  - **Task ID**: Matches report data whose task ID value returns true against the specified test and test value. Available test options are Is and Contains.
  - **Scheduled Time**: Matches report data whose scheduled time value returns true against the specified test and test date/time. Available test options are Equals (=), Greater Than (>), Greater Than or Equal To (>=), Less Than (<), or Less Than or Equal To (<=).

There is also one shortcut button available to make changing the task runs filter options easier. The Show Active Only button resets all filter options, then selects only the Status selector to only show active tasks. Use this shortcut button when you only want to see the currently active task runs.

File/Folder Activity



Report Filter

File/Folder Activity | Date/Time | Limit

☐ Status is: Failure Success Ignore

☑ Action is: File: Download Process Upload Delete Folder Add/Delete Other

☑ Display any file/folder activity entries with errors, regardless of action

☐ Log ID greater than: 0

☐ Additional Filters: ○ Match all ● Match any

Source Host | is |

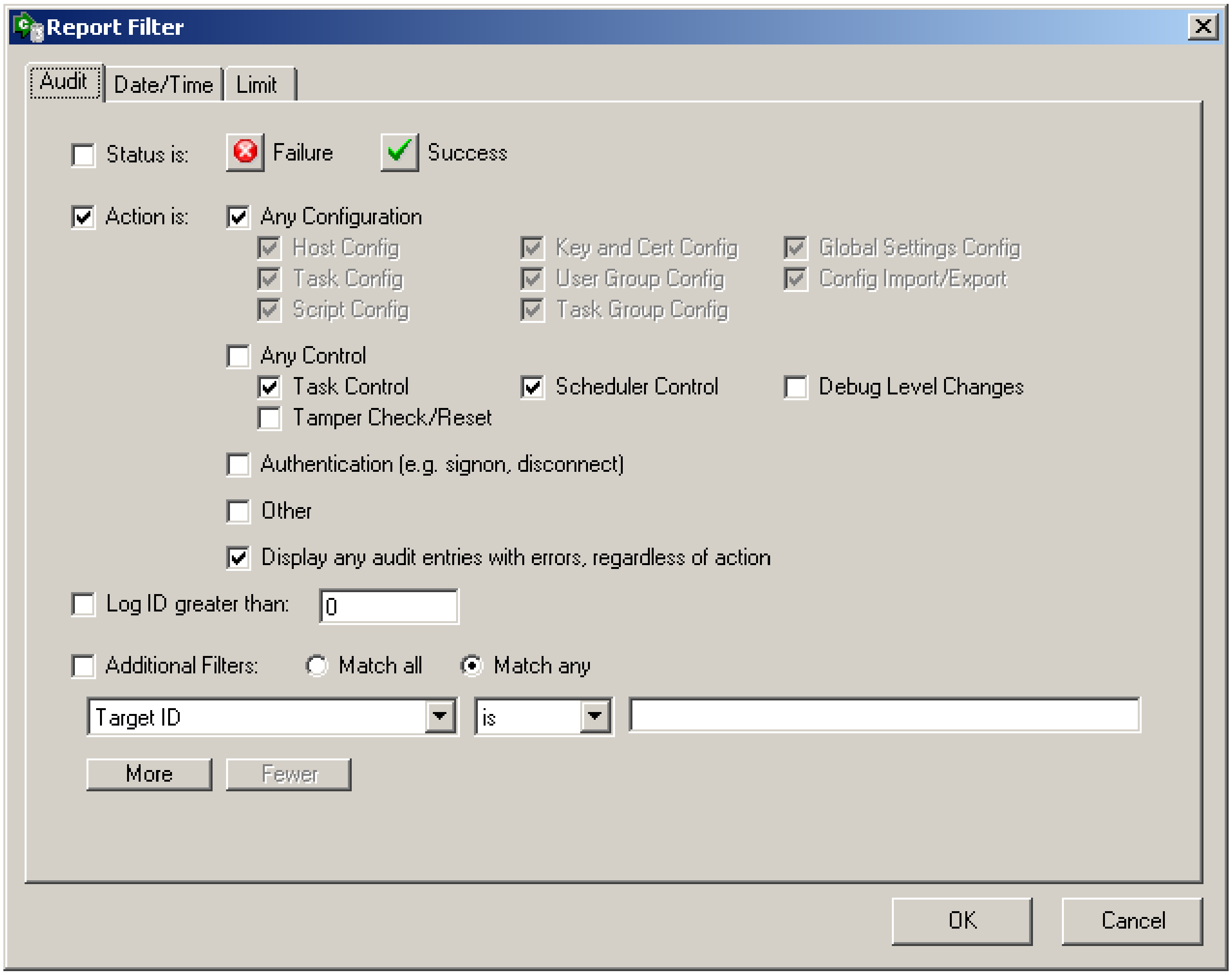
Available File/Folder Activity report filters are:

- **Status**: When enabled, limits report data to entries whose status matches the selected status options.
- **Action**: When enabled, limits report data to entries whose action matches the selected action options.
  - **Display any file/folder activity entries with errors, regardless of action**: When enabled, file/folder activity entries whose status is Failure will be shown, even if that entry's action is not selected in the Action filter.

- **Log ID**: When enabled, limits report data to entries whose Log ID is greater than the specified value.
- **Additional Filters**: When enabled, applies the specified additional filters. More filters (up to six total) can be added by clicking the More button. If the Match Any option is selected, report data will be returned if it matches any of the specified filters. If the Match All option is selected, report data will only be returned if it matches all of the specified filters. Available additional filters are:
    - **Source Host**: Matches report data whose source host value returns true against the specified test and test host value (source hosts can be selected from the drop down, or manually entered). Available test options are Is and Contains.
    - **Destination Host**: Matches report data whose destination host value returns true against the specified test and test host value (source hosts can be selected from the drop down, or manually entered). Available test options are Is and Contains.
    - **Any Host**: Matches report data whose source or destination host value returns true against the specified test and test host value (source hosts can be selected from the drop down, or manually entered). Available test options are Is and Contains.
    - **Source Path**: Matches report data whose source path value returns true against the specified test and test value. Available test options are Is and Contains.
    - **Destination Path**: Matches report data whose destination path value returns true against the specified test and test value. Available test options are Is and Contains.
    - **Any Path**: Matches report data whose source or destination path value returns true against the specified test and test value. Available test options are Is and Contains.
    - **Source File**: Matches report data whose source file value returns true against the specified test and test value. Available test options are Is and Contains.
    - **Destination File**: Matches report data whose destination file value returns true against the specified test and test value. Available test options are Is and Contains.
    - **Any File**: Matches report data whose source or destination file value returns true against the specified test and test value. Available test options are Is and Contains.
    - **Source FileSize**: Matches report data whose source file size value returns true against the specified test and test bytecount. Available test options are Equals (=), Greater Than (>), Greater Than or Equal To (>=), Less Than (<), or Less Than or Equal To (<=).
    - **Destination FileSize**: Matches report data whose destination file size value returns true against the specified test and test bytecount. Available test options are Equals (=), Greater Than (>), Greater Than or Equal To (>=), Less Than (<), or Less Than or Equal To (<=).
    - **Any FileSize**: Matches report data whose source or destination file size value returns true against the specified test and test bytecount. Available test options are Equals (=), Greater Than (>), Greater Than or Equal To (>=), Less Than (<), or Less Than or Equal To (<=).
    - **Source MOVEit DMZ FileID**: Matches report data whose source file ID value returns true against the specified test and test value. Available test options are Is and Contains.
    - **Destination MOVEit DMZ FileID**: Matches report data whose destination file ID value returns true against the specified test and test value. Available test options are Is and Contains.

- **Any MOVEit DMZ FileID**: Matches report data whose source or destination file ID value returns true against the specified test and test value. Available test options are Is and Contains.
- **Source AS1/AS2/AS3 MsgID**: Matches report data whose source ASx Message ID value returns true against the specified test and test value. Available test options are Is and Contains.
- **Destination AS1/AS2/AS3 MsgID**: Matches report data whose destination ASx Message ID value returns true against the specified test and test value. Available test options are Is and Contains.
- **Any AS1/AS2/AS3 MsgID**: Matches report data whose source or destination ASx Message ID value returns true against the specified test and test value. Available test options are Is and Contains.
- **Status Message**: Matches report data whose status message value returns true against the specified test and test value. Available test options are Is and Contains.
- **Task ID**: Matches report data whose task ID value returns true against the specified test and test value. Available test options are Is and Contains.
- **Scheduled Time**: Matches report data whose scheduled time value returns true against the specified test and test date/time. Available test options are Equals (=), Greater Than (>), Greater Than or Equal To (>=), Less Than (<), or Less Than or Equal To (<=).

Audit



□ Status is: Failure Success

☑ Action is: ☑ Any Configuration

☑ Host Config ☑ Key and Cert Config ☑ Global Settings Config

☑ Task Config ☑ User Group Config ☑ Config Import/Export

☑ Script Config ☑ Task Group Config

□ Any Control

☑ Task Control ☑ Scheduler Control □ Debug Level Changes

□ Tamper Check/Reset

□ Authentication (e.g. signon, disconnect)

□ Other

☑ Display any audit entries with errors, regardless of action

□ Log ID greater than: 0

□ Additional Filters: ○ Match all ● Match any

Target ID is

Available Audit report filters are:

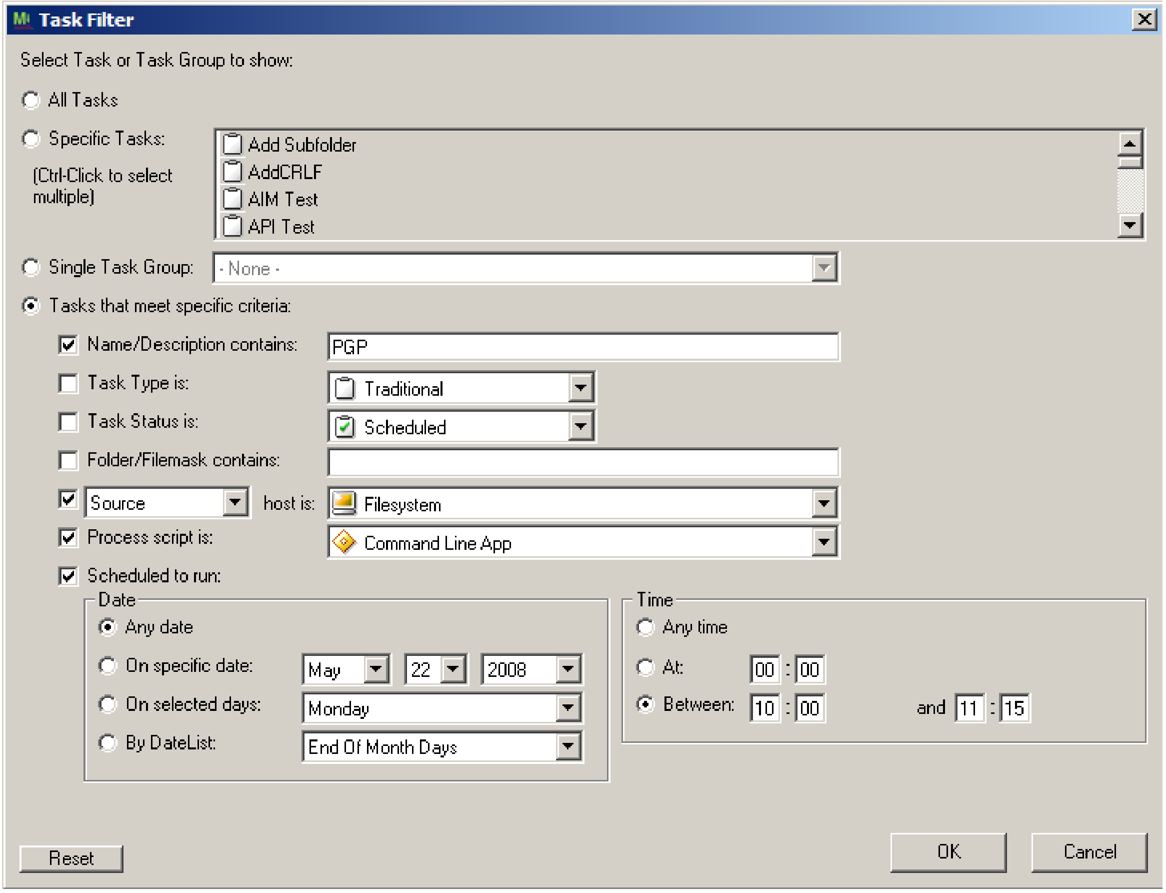
- **Status**: When enabled, limits report data to entries whose status matches the selected status options.
- **Action**: When enabled, limits report data to entries whose action matches the selected action options.
    - **Any Configuration**: Matches audit entries describing a configuration change of any kind. If not selected, the following configuration-specific options are available.

        - **Host Config**: Matches host configuration changes.
        - **Task Config**: Matches task configuration changes.
        - **Script Config**: Matches script configuration changes.
        - **Key and Cert Config**: Matches SSH key and SSL cert configuration changes.
        - **User Group Config**: Matches user group configuration changes.
        - **Task Group Config**: Matches task group configuration changes.
        - **Global Settings Config**: Matches global settings changes.
        - **Config Import/Export**: Matches configuration import and export actions.
    - **Any Control**: Matches audit entries describing a control action of any kind. If not selected, the following control-specific options are available.
        - **Task Control**: Matches task control commands.
        - **Scheduler Control**: Matches scheduler thread control commands.
        - **Debug Level Changes**: Matches debug level changes.
        - **Tamper Check/Reset**: Matches tamper check actions.
    - **Authentication**: Matches signon/signoff audit entries.
    - **Other**: Matches any audit entry not covered by the above selections.
    - **Display any audit entries with errors, regardless of action**: When enabled, audit entries whose status is Failure will be shown, even if that entry's action is not selected in the Action filter.
- **Log ID**: When enabled, limits report data to entries whose Log ID is greater than the specified value.
- **Additional Filters**: When enabled, applies the specified additional filters. More filters (up to two total) can be added by clicking the More button. If the Match Any option is selected, report data will be returned if it matches any of the specified filters. If the Match All option is selected, report data will only be returned if it matches all of the specified filters. Available additional filters are:
    - **Target ID:** Matches report data whose target ID value returns true against the specified test and test value. Available test options are Is and Contains.
    - **Target Type**: Matches report data whose target type value returns true against the specified test and test target type value (target types can be selected from the drop down, or manually entered). Available test options are Is and Contains.
    - **Target Name**: Matches report data whose target name value returns true against the specified test and test value. Available test options are Is and Contains.
    - **User**: Matches report data whose username value returns true against the specified test and test value. Available test options are Is and Contains.
    - **IP Address**: Matches report data whose IP address value returns true against the specified test and test value. Available test options are Is and Contains.

- **Status Message or Additional Info**: Matches report data whose status message or additional info value returns true against the specified test and test value. Available test options are Is and Contains.

Task Filter

To allow easier trouble-shooting of problem tasks, MOVEit Central Admin provides a task filtering option, to narrow down the list of tasks displayed on the Tasks tab, the Status tab, and also potentially in the Reports window. It also filters the information displayed on the Debug Log tab to only that information pertaining to the selected task or tasks (system log events can also be displayed if desired).



Task Filter

Select Task or Task Group to show:

○ All Tasks

○ Specific Tasks: (Ctrl-Click to select multiple)
Add Subfolder
AddCRLF
AIM Test
API Test

○ Single Task Group: - None -

● Tasks that meet specific criteria:

☑ Name/Description contains: PGP

☐ Task Type is: Traditional

☐ Task Status is: Scheduled

☐ Folder/Filemask contains:

☑ Source host is: Filesystem

☑ Process script is: Command Line App

☑ Scheduled to run:

Date
● Any date
○ On specific date: May 22 2008
○ On selected days: Monday
○ By DateList: End Of Month Days

Time
○ Any time
○ At: 00 : 00
● Between: 10 : 00 and 11 : 15

To set the task filter, click on the Edit Filter button in the lower right-hand corner of the application. This will open the Task Filter dialog. Here, the user has several choices of how to set the filter:

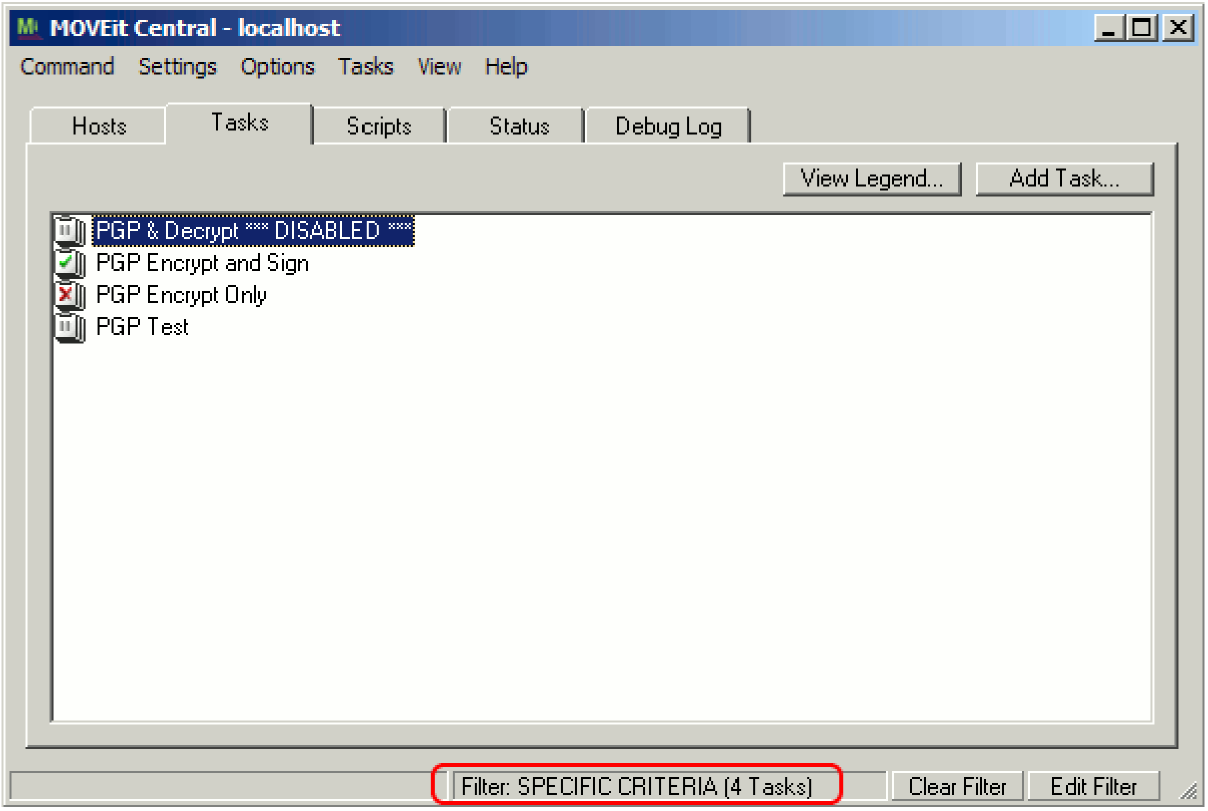
- **All Tasks** - All tasks will be shown (effectively turns off the filter).
- **Specific Tasks** - Sets the filter to one or more selected tasks. Hold down the Ctrl key to select multiple tasks.
- **Single Task Group** - Sets the filter to all the tasks in a single selected task group.
- **Tasks that meet specific criteria** - Allows the user to set one or more sets of criteria to filter the list of tasks based on. Only those tasks that match all the selected criteria will be displayed. Available criteria are:
  - **Name/Description contains** - Selects tasks whose name or description contains the entered text.
  - **Task Type is** - Selects tasks that are of the selected type. Options include "Traditional", "Synchronization", and "Advanced".
  - **Task Status is** - Selects tasks whose status matches the selected status. Options include "Scheduled", "Disabled or Unscheduled", and "Incomplete".
  - **Folder/Filemask contains** - Selects tasks whose sources and/or destinations contain the entered text in the folder and/or filemask fields.
  - **Source/Destination/Src or Dest/Next Action/Any host is** - Selects tasks which contain a source, destination, source or destination, next action, or any step which uses the selected host.
  - **Process script is** - Selects tasks which contain a process that calls the selected script.
  - **Scheduled to run** - Selects tasks which have schedules that cause the task to run on the selected day or days, and the selected time or within the selected time period. Available date criteria are:
    - **On specific date** - Selects tasks that are scheduled to run on the specified exact date. This option will check all scheduled tasks to see if their schedules match the provided date. For example, if a task is scheduled to run on all Wednesdays, a specific date of April 19, 2006 would match that task.
    - **On selected days** - Selects tasks that run on the selected day of the week or month.
    - **By DateList** - Selects tasks which run according to the selected DateList.

    Available time criteria are:

- **Any Time** - Selects tasks that run at any time of day.
- **At** - Selects tasks that run at the specified exact time of day.
- **Between** - Selects tasks that run between the two specified times of day.

Additionally, a Reset button is available which will return all selections to the default, which is to show all tasks.

The current filter setting will always be visible in the information panel at the bottom of the application. The currently selected filter and a count of tasks that are selected by that filter are displayed here.



PGP & Decrypt *** DISABLED ***
PGP Encrypt and Sign
PGP Encrypt Only
PGP Test

Filter: SPECIFIC CRITERIA (4 Tasks)

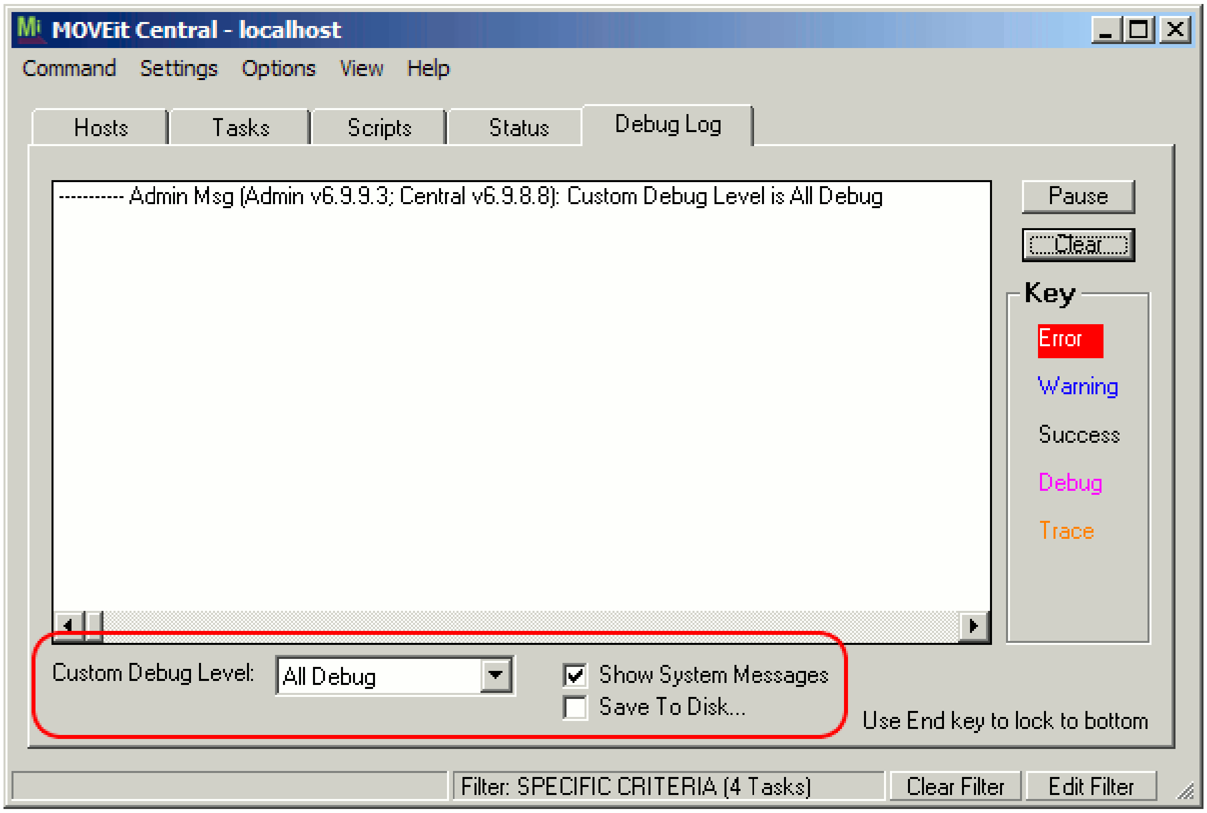
In addition to setting the filter manually using the Task Filter dialog, the user can automatically set the task filter by right-clicking a task, host, or script and selecting the Set Filter to This option. This will set the filter to display only the specific task selected, or only tasks the use the selected host or script. Since many users will use this feature to aid in the debugging of a task, this option will also automatically set the per-task debug option for the selected tasks to More Debug.

Per-Task Debugging

When a set of tasks is selected using the task filter, the Custom Debug Level option becomes available on the Log tab. This allows the user to select a custom debug level to be temporarily applied to the currently selected tasks, which will override the current system debug level. The selected tasks will output debug information at that higher level, while the rest of the system will use the system level. This helps facilitate the debugging of problem tasks without the need to raise the entire system debug level, which can cause performance problems on heavily used systems. If the task filter is changed at any point, the custom debug level will be reset automatically.

The Show System Messages option is also available here. When enabled, the Log tab will display system-level messages in addition to messages from the tasks selected by the filter.

Finally, an option to write the log output to a local disk file is available. Check the Save To Disk option to begin using this feature. You will be prompted for a filename to save the log information to. Once a filename has been specified, log information will be written to the file as long as the option is checked. Clicking the checkbox off, or changing the task filter, will cause MOVEit Central Admin to stop writing to the log file and close it.



```
---------- Admin Msg (Admin v6.9.9.3; Central v6.9.8.8): Custom Debug Level is All Debug
```

Custom Debug Level: All Debug

☑ Show System Messages

□ Save To Disk...

Use End key to lock to bottom

Filter: SPECIFIC CRITERIA (4 Tasks)

...Without Admin

This section describes monitoring options available without the Admin Console.

Event Log

MOVEit Central can be configured to write file transfer and other events into the Windows Event Log. This is often handy in enterprise environments because many enterprises ***use third party applications to boost event logs into various central management/monitoring systems*** (see "***SysLog and SNMP***" on page 407).

Writing Events to the Event Log

To configure MOVEit Central to write events to the Windows Event Log:

1. From MOVEit Central Admin's main menu, select "Settings | System Settings".
2. Select a log level for event logs.

3 To monitor individual file transfers through the event log, set the log level value to "File Completions."

Event Log Messages

Depending on the event log messages level that is configured in the ***System Settings*** (on page 229) dialog, there may be many different types of messages being sent to the event log by MOVEit Central.

Error Messages

Default settings will typically include only errors. These messages will generally be sent with a type of "Error". Here are some examples of possible Central error messages:

```
Error watching directory C:/BC4/BGI: The specified path is invalid. .
See http://support.microsoft.com/kb/810886
```

```
Error processing cmd DONEWTASK: Running this task would exceed the
maximum simultaneous tasks specified in the command.
```

```
AS2 Polling thread could not list AS2 files for Common Sync MOVEit DMZ:
Error 12029: Could not access URL 'https://localhost:443/machine.aspx':
HttpSendRequestEx failed: The attempt to connect to the server failed.
```

Task Run Messages

If the event log setting is set to Task Completions or higher, MOVEit Central will send task run messages indicating that tasks have successfully or unsuccessfully completed. Failure messages will be sent with a type of "Error", while success messages will be sent with a type of "Information". Here are some examples of possible Central task completion messages:

```
Task "Download from HP FTP site using ad hoc host (1 of 5)": (ID 98245241)
Completed successfully.
```

```
Task "Intro to MOVEit - Automatically PGP Files": (ID 559830296)
Completed with no actions taken.
```

```
Task "SatSync2 - HQ": Encountered 2 errors
```

File Completion Messages

If the event log setting is set to File Completions, MOVEit Central will send individual messages for each processed file indicating that they have been successfully or unsuccessfully processed or sent to their destination. Failure messages will be sent with a type of "Error", while success messages with be sent with a type of "Information". Here are some examples of possible Central file completion messages:

```
Task "Very Simple Task": Saved
'd:/temp/33strings/strings/ButtonText-fr.sts' to
d:/temp/deletethistoo/ButtonText-fr.sts
```

```
Task "Test MD5Sum - Create MD5": Saved 'md5sum_20071015.txt' from script
'md5sum' to d:/temp/md5sum2/out/md5sum_20071015.txt
```

Failover Messages

Information and Error type messages may also be sent by MOVEit Central regarding Failover events. These messages will be prefixed with the string "FO:", indicating they are Failover messages. Problems will be sent with a type of "Warning" or "Error", while informational events will be sent with a type of "Information". Here is an example of a possible Central Failover message:

```
FO: Saved PGP keyrings
```

Email Notification

MOVEit Central can be configured to send certain people email messages if certain tasks succeed (e.g. transfer files OK), fail or find they have nothing to do. These types of conditional messages are configured by attaching a "Next Action" to specific tasks.

To attach an email alert Next Action to a particular task, open MOVEit Central Admin, go to the "Tasks" tab, and select an interesting task. Right-click on the task and select "Add Next Action..." from the pop-up menu. Select under what conditions you want to send email alerts in the "Execute on" section, check the "Send Email" action, enter an email address, a message subject and the message body.

Note that the email address, message subject and message body can be completely or partially populated with macros, including task parameters. For example, you may want the message to send you the specific name of a file which failed to transfer. (You can get a list of files this task has attempted to transfer if you use the "OrigNames" script included with MOVEit Central Admin installations.)

Direct Access

You can securely read MOVEit Central's tamper-evident task run, transfer and audit database directly with SQL commands issued through an SSL connection established by MOVEit Central API. If you have local access to MOVEit Central or the security of the connection to the database is not an issue, ODBC access can also be used instead of MOVEit Central API.

Please also see the ***"Database - Schema" documentation*** (see "***Schema***" on page 438).

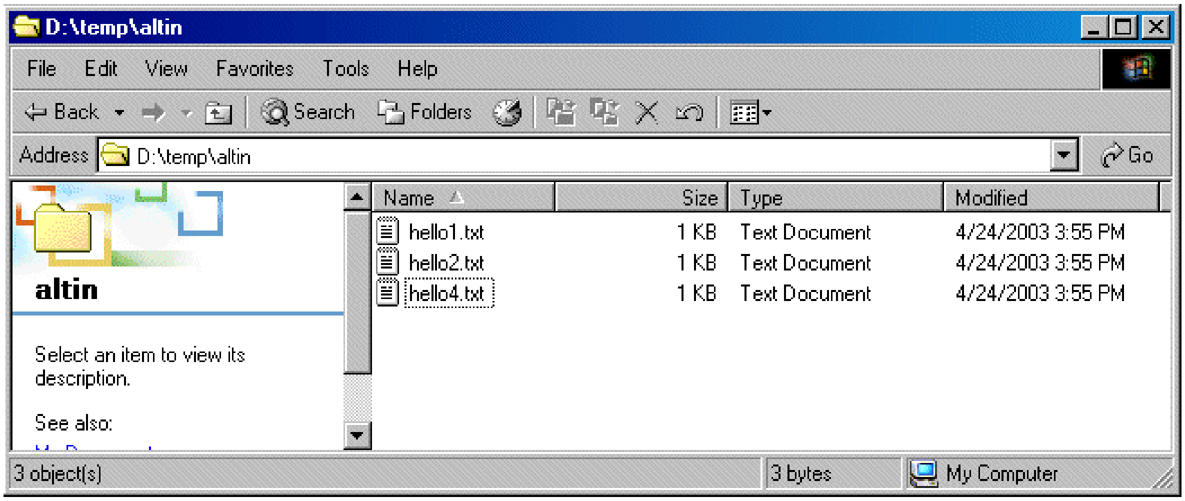
You can also "tail" the MOVEit Central log file, usually written to the same folder into which MOVEit Central is installed. Configuration options for the log file are found in the System Settings dialog through MOVEit Central Admin. The amount of detail written into the log is controlled by the "Global Debug Level" on the same dialog.

Common Applications

Trigger Files

Using its scripting abilities, MOVEit Central can be configured to use a "trigger" file to force the upload of a second "data" file of the same name from a local folder. This is a situation often encountered with mainframe file transfers, where a mainframe determines which files are to be transferred by using trigger files such as these.

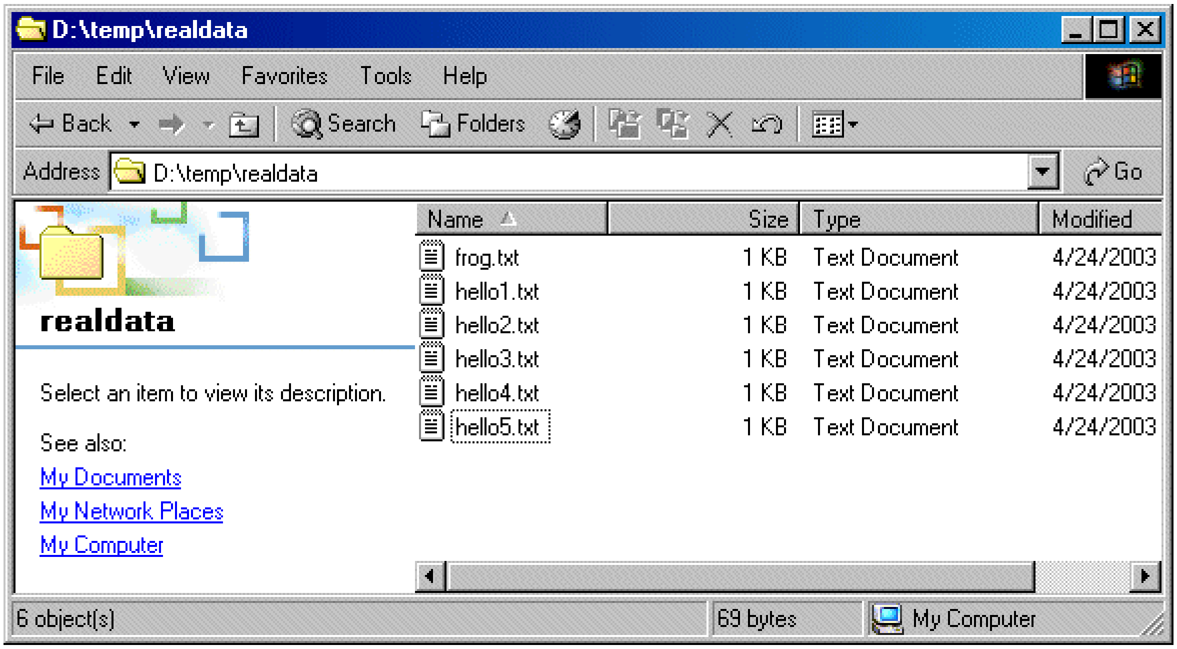
In this example, we have a "trigger" folder named "d:\temp\altin". This folder contains three very small text files. (The contents of these files can be anything, but it is the names of the files which are important.)



Select an item to view its description.

Name	Size	Type	Modified
hello1.txt	1 KB	Text Document	4/24/2003 3:55 PM
hello2.txt	1 KB	Text Document	4/24/2003 3:55 PM
hello4.txt	1 KB	Text Document	4/24/2003 3:55 PM

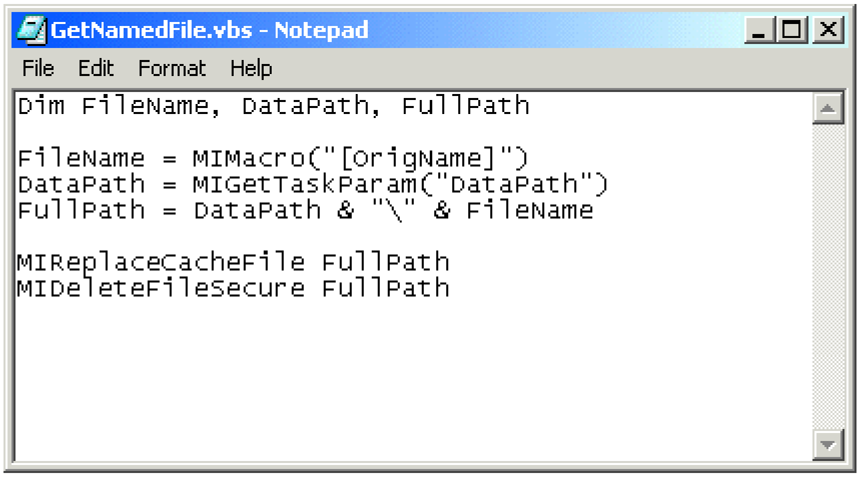
We also have a "data" folder named "d:\temp\realdata". This folder contains 6 data files, but we only want to move a few of these files up to our selected destination.



Name	Size	Type	Modified
frog.txt	1 KB	Text Document	4/24/2003
hello1.txt	1 KB	Text Document	4/24/2003
hello2.txt	1 KB	Text Document	4/24/2003
hello3.txt	1 KB	Text Document	4/24/2003
hello4.txt	1 KB	Text Document	4/24/2003
hello5.txt	1 KB	Text Document	4/24/2003

We create a new script called "GetNamedFile.vbs" and import it into MOVEit Central as as process named "GetNamedFile". This process does three things:

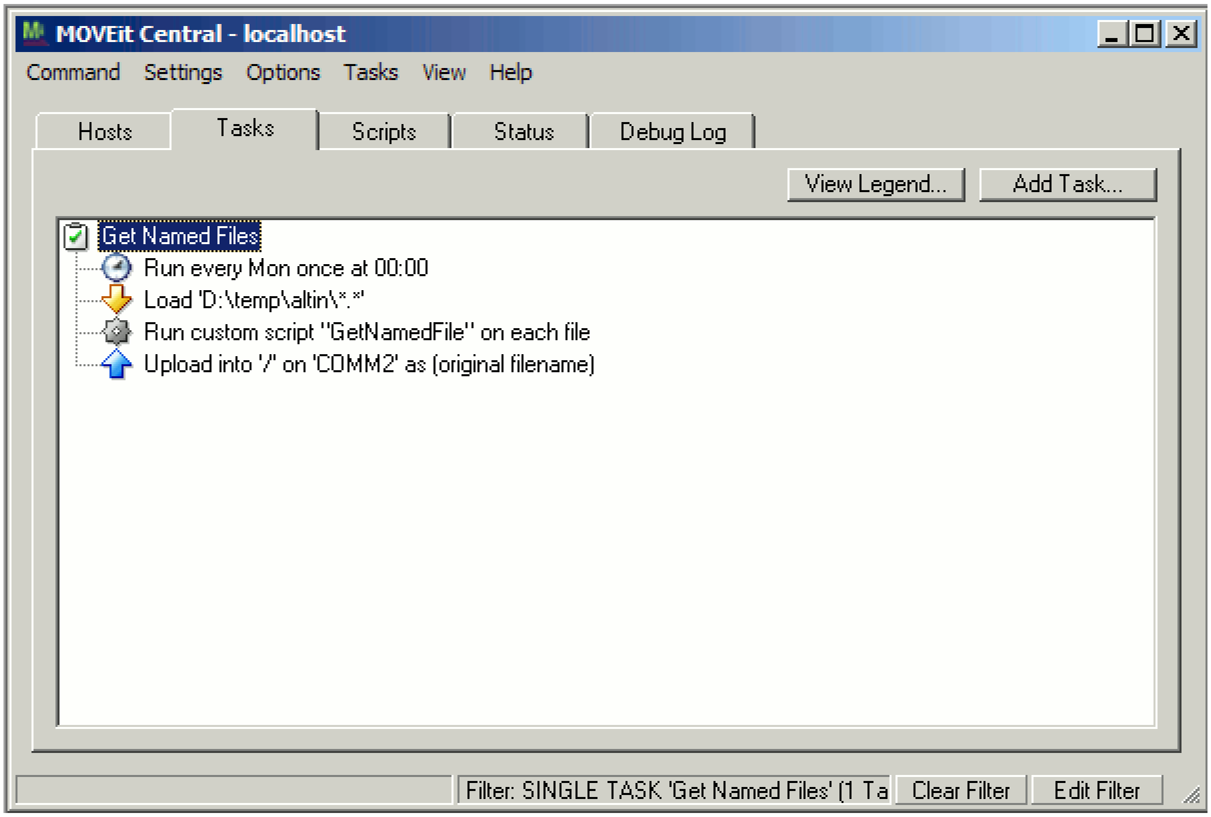
- Builds up the full path of the real data file given the name of a trigger file and a path specified as a task parameter.
- Replaces the contents of the working cache with the contents of the data file.
- Deletes (and scrubs) the original data file.



```
Dim FileName, DataPath, FullPath

FileName = MIMacro("[origName]")
DataPath = MIGetTaskParam("DataPath")
FullPath = DataPath & "\" & FileName

MIReplaceCacheFile FullPath
MIDeleteFileSecure FullPath
```

Next, we build a new task to download the trigger file, run the process and upload the data file.

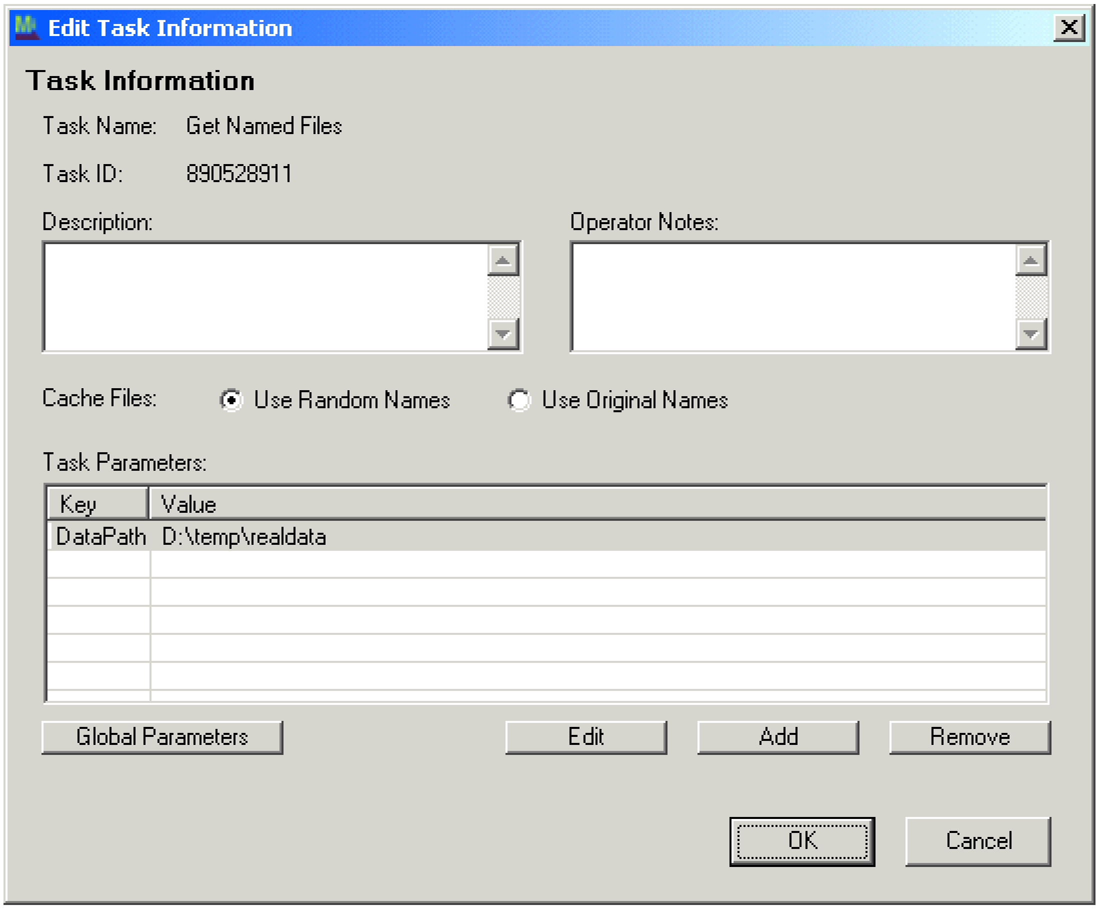
- Either the source of the trigger file or destination of the data file can be a remote machine (FTP, SSH, MOVEit)
- However, the original data file must be on a local drive.
- Check the "Delete Original" flag on the source; trigger files should be destroyed as soon as they force an upload.
- Also, be sure to leave the "Use Original Filename" checkbox checked on the destination.



Get Named Files
- Run every Mon once at 00:00
- Load 'D:\temp\altin\*.*'
- Run custom script "GetNamedFile" on each file
- Upload into '/' on 'COMM2' as (original filename)

Filter: SINGLE TASK 'Get Named Files' (1 Ta

A critical addition to the task is the use of a Task Parameter to indicate where to find the data files. Be sure to add a Task Parameter called "DataPath" to your task with the full path of your data folder.



Edit Task Information

Task Information

Task Name: Get Named Files

Task ID: 890528911

Description:

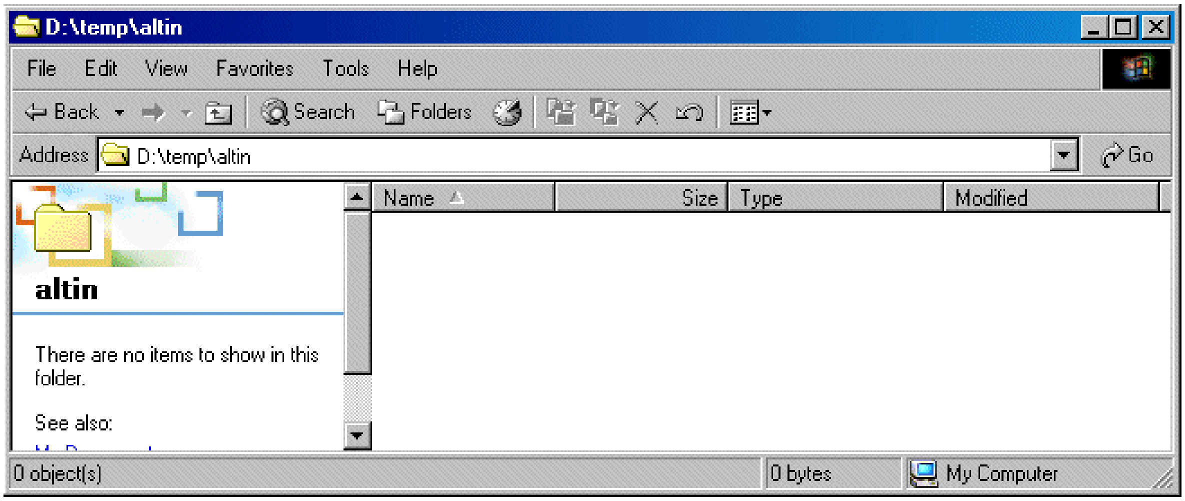
Operator Notes:

Cache Files: ● Use Random Names ○ Use Original Names

Task Parameters:

Key	Value
DataPath	D:\temp\realdata

Now, run the task, and notice that the trigger files disappear.



D:\temp\altin

Address D:\temp\altin

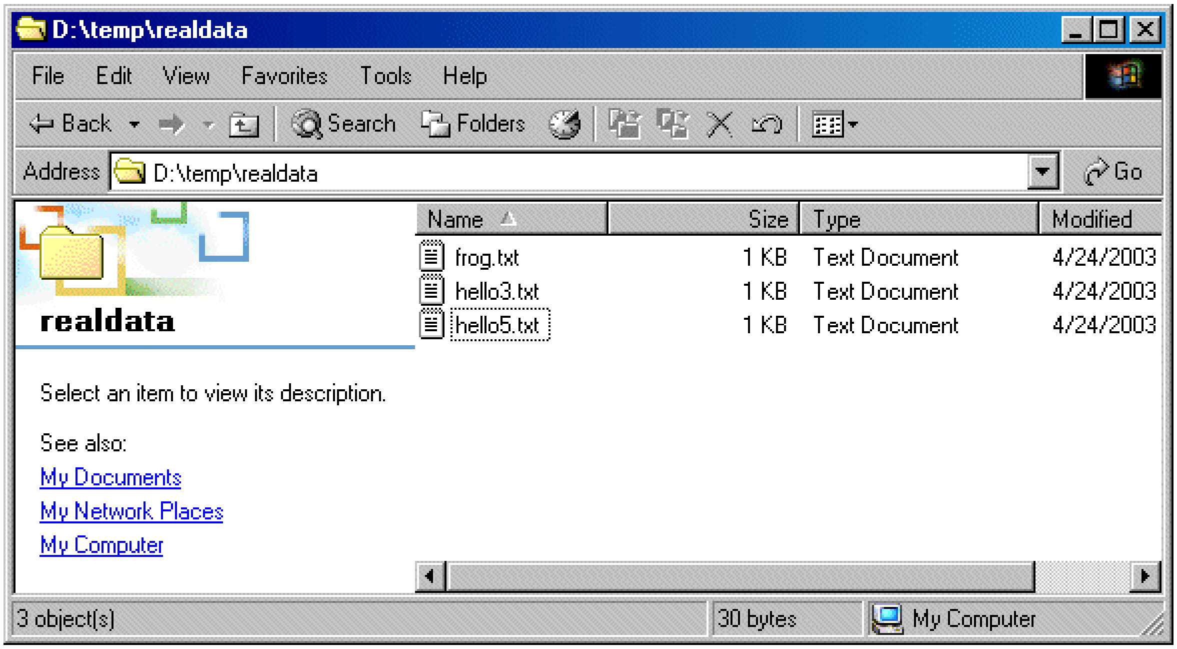
altin

There are no items to show in this folder.

See also:

0 object(s) 0 bytes My Computer

Also notice that only the three selected data files are gone.



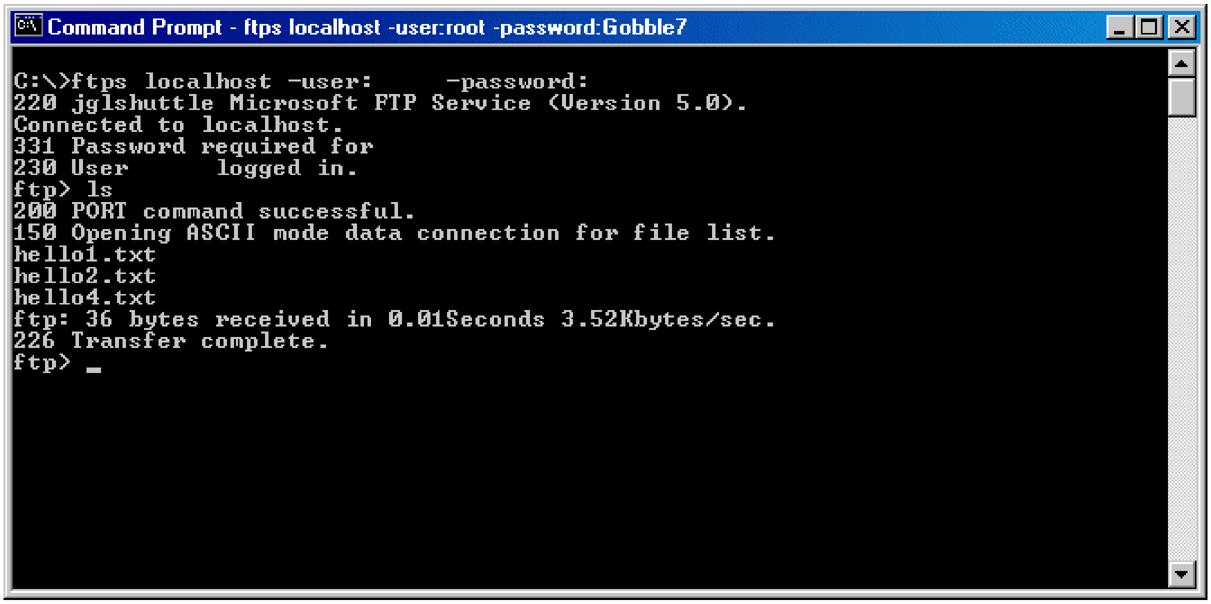
Name	Size	Type	Modified
frog.txt	1 KB	Text Document	4/24/2003
hello3.txt	1 KB	Text Document	4/24/2003
hello5.txt	1 KB	Text Document	4/24/2003

Select an item to view its description.

See also:
My Documents
My Network Places
My Computer

3 object(s) | 30 bytes | My Computer

Finally, notice that the data files are where they are supposed to be on the destination. (Download one or two manually to make sure!)


Command Prompt - ftps localhost -user:root -password:Gobble7

```
C:\>ftps localhost -user:      -password:
220 jglshuttle Microsoft FTP Service (Version 5.0).
Connected to localhost.
331 Password required for
230 User       logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
hello1.txt
hello2.txt
hello4.txt
ftp: 36 bytes received in 0.01Seconds 3.52Kbytes/sec.
226 Transfer complete.
ftp> _
```

GetNamedFile.vbs

```
Dim FileName, FilePath, FullPath



FileName = MIMacro("[OrigName]")

DataPath = MIGetTaskParam("DataPath")

FullPath = DataPath & "\" & FileName



MIReplaceCacheFile(FullPath) MIDeleteFileSecure(FullPath)
```

"Last Day Of Month" Schedules

While MOVEit Central does not directly support scheduling task runs on the last day of the month, the ***Date Lists*** (on page 144) feature can be used to provide equivalent functionality. A date list can be set up containing all "end-of-the-month" dates for a period of some years, and used as the date schedule for a task. A list of all "end-of-the-month" days for the period of March, 2012 through December, 2020, is included below. To use it, create a new date list in MOVEit Central Admin, and then copy the list below and paste it into the Entries text box.

Another way to provide end-of-month date lists is to use the wildcard character *, instead of specifying dates for each year. This will allow the use of a 12-line date list, instead of 12 lines for each year. The drawback to this method, however, is that the date list will need to be modified for leap years. An example wildcard datelist is supplied below.

For information about creating and managing date lists, see the ***Date Lists*** (on page 144) page in this manual. For information about using date lists, see the ***Schedules*** (see "***Schedule***" on page 130) page in this manual.

"End-Of-The-Month" Days for March, 2012 through December, 2020

2012-03-31
2012-04-30
2012-05-31
2012-06-30
2012-07-31
2012-08-31
2012-09-30
2012-10-31
2012-11-30

```
2012-12-31
2013-01-31
2013-02-28
2013-03-31
2013-04-30
2013-05-31
2013-06-30
2013-07-31
2013-08-31
2013-09-30
2013-10-31
2013-11-30
2013-12-31
2014-01-31
2014-02-28
2014-03-31
2014-04-30
2014-05-31
2014-06-30
2014-07-31
2014-08-31
2014-09-30
2014-10-31
2014-11-30
2014-12-31
2015-01-31
2015-02-28
2015-03-31
2015-04-30
2015-05-31
2015-06-30
2015-07-31
2015-08-31
2015-09-30
2015-10-31
2015-11-30
2015-12-31
2016-01-31
2016-02-29
2016-03-31
2016-04-30
2016-05-31
```

2016-06-30
2016-07-31
2016-08-31
2016-09-30
2016-10-31
2016-11-30
2016-12-31
2017-01-31
2017-02-28
2017-03-31
2017-04-30
2017-05-31
2017-06-30
2017-07-31
2017-08-31
2017-09-30
2017-10-31
2017-11-30
2017-12-31
2018-01-31
2018-02-28
2018-03-31
2018-04-30
2018-05-31
2018-06-30
2018-07-31
2018-08-31
2018-09-30
2018-10-31
2018-11-30
2018-12-31
2019-01-31
2019-02-28
2019-03-31
2019-04-30
2019-05-31
2019-06-30
2019-07-31
2019-08-31
2019-09-30
2019-10-31
2019-11-30

2019-12-31
2020-01-31
2020-02-29
2020-03-31
2020-04-30
2020-05-31
2020-06-30
2020-07-31
2020-08-31
2020-09-30
2020-10-31
2020-11-30
2020-12-31

Wildcard "End-Of-The-Month" Days for Non-Leap Years

*-01-31
*-02-28
*-03-31
*-04-30
*-05-31
*-06-30
*-07-31
*-08-31
*-09-30
*-10-31
*-11-30
*-12-31

Wildcard "End-Of-The-Month" Days for Leap Years

*-01-31
*-02-29
*-03-31
*-04-30
*-05-31
*-06-30
*-07-31
*-08-31
*-09-30
*-10-31
*-11-30
*-12-31

Converting Unisys Print Backup Files to Text

Unisys mainframe applications often use a file format commonly known as "print backup file". A normal MOVEit Central task can download and move these files, frequently via non-secure FTP (binary transfer mode) or a mapped drive. However, MOVEit Central is also asked to "crack" or "convert" these files from their native print backup file format into an ASCII text format that many non-Unisys mainframe applications can use.

To convert Unisys mainframe print backup files to ASCII using MOVEit Central:

1. Sign on to the ***MOVEit support site*** (see https://moveitsupport.ipswitch.com/moveit - ***https://moveitsupport.ipswitch.com/moveit***) and download "ConvertPBA.exe" from the "Distribution / MOVEit / Central / Extras" folder into your "C:\Program Files\MOVEit" folder (or other appropriate local folder).
2. Set up a file transfer task (one source and one destination) to download and save the Unisys print backup file without converting it. If your source is an FTP source, you will need to specify "BINARY" mode and you may also need to specify additional "QUOTE" commands to complete the transfer.
3. Once you have the basic file transfer task working, add a "Command Line App" built-in process.
4. Configure "Command Line App" with the following parameters:
   - **CommandLineApp_AppPath** = C:\Program Files\MOVEit\ConvertPBA.exe *(or the actual location of this file)*
   - **CommandLineApp_AppParms** = [InputFile] [OutputFile]
   - **CommandLineApp_OutputFile** = Yes
5. Save these parameters and test. When checked, the file at the destination should be readable using any ASCII text reader (such as notepad.exe).

Please note that NULL characters encountered by this utility are converted to spaces.

Converting EBCDIC Text to ASCII Text

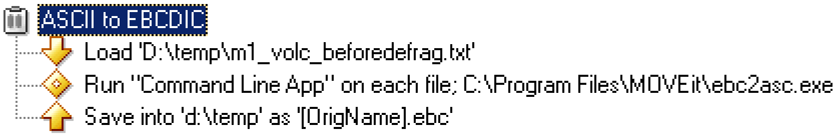
Mainframes often use a 256-bit character set called EBCDIC rather than the 128-bit ASCII character set most often used on Windows, Mac and Unix platforms. MOVEit Central can be used to convert text files from ASCII to EBCDIC or from EBCDIC to ASCII using the "CommandLineApp" built-in script and a command-line utility called "ebc2asc".

To convert EBCDIC text files to ASCII (or ASCII to EBCDIC) using MOVEit Central:

1. Sign on to the ***MOVEit support site*** (see https://moveitsupport.ipswitch.com/moveit - ***https://moveitsupport.ipswitch.com/moveit***) and download "ebc2asc.exe" from the "Distribution / MOVEit / Central / Extras" folder into your "C:\Program Files\MOVEit" folder *(or other appropriate local folder)*.
2. Set up a file transfer task (one source and one destination) to download and save our original text file without converting it. If your source is a mainframe accessible via FTP, you may need to specify "BINARY" mode and you may also need to specify additional "QUOTE" commands to complete the transfer.
3. Once you have the basic file transfer task working, add a "Command Line App" built-in process.
4. Configure "Command Line App" with the following parameters:
   - **CommandLineApp_AppPath** = C:\Program Files\MOVEit\ebc2asc.exe (or the actual location of this file)
   - **CommandLineApp_OutputFile** = Yes
   - EBCDIC to ASCII only: **CommandLineApp_AppParms** = <"[InputFile]" >"[OutputFile]"
   - ASCII to EBCDIC only: **CommandLineApp_AppParms** = -a <"[InputFile]" >"[OutputFile]"
5. Save these parameters and test. When checked, EBCDIC files should be unreadable using Notepad.exe, but ASCII files should be readable using Notepad.exe.

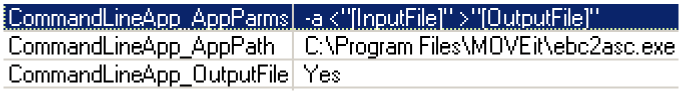
Sample Task - ASCII to EBCDIC

This task loads a local ASCII file (output from a defrag check) and converts it to an EBCDIC file.



ASCII to EBCDIC
Load 'D:\temp\m1_volc_beforedefrag.txt'
Run "Command Line App" on each file; C:\Program Files\MOVEit\ebc2asc.exe
Save into 'd:\temp' as '[OrigName].ebc'

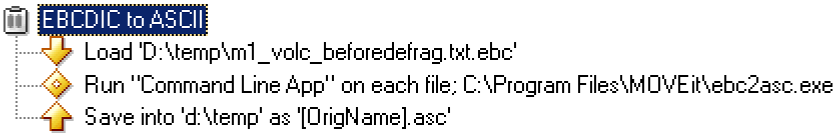
These are the CommandLineApp parameters. Notice the "-a" argument.



CommandLineApp_AppParms	-a <"[InputFile]" >"[OutputFile]"
CommandLineApp_AppPath	C:\Program Files\MOVEit\ebc2asc.exe
CommandLineApp_OutputFile	Yes

Sample Task - EBCDIC to ASCII

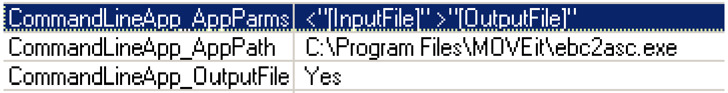
This task loads a local EBCDIC file (the EBCDIC file created in the previous step) and converts it back to an ASCII file.



EBCDIC to ASCII

- Load 'D:\temp\m1_volc_beforedefrag.txt.ebc'
- Run "Command Line App" on each file; C:\Program Files\MOVEit\ebc2asc.exe
- Save into 'd:\temp' as '[OrigName].asc'

These are the CommandLineApp parameters. Notice there is no "-a" argument.



CommandLineApp_AppParms	<"[InputFile]" >"[OutputFile]"
CommandLineApp_AppPath	C:\Program Files\MOVEit\ebc2asc.exe
CommandLineApp_OutputFile	Yes

HTTP Uploads and Downloads

MOVEit Central supports uploading to and downloading from webservers using the HTTP and HTTPS protocol. This is in addition to the support for MOVEit DMZ hosts, which also use the HTTP and HTTPS protocols, but require a specific upload/download format.

Support for this capability comes in the form of built-in scripts:

- ***HTTP Get*** (on page 183) - downloads a file from a webserver using the HTTP GET verb.
- ***HTTP Post*** (on page 184) - uploads a file to a webserver using the HTTP POST verb.
- ***HTTP Put*** (on page 185) - uploads a file to a webserver using the HTTP PUT verb. This mechanism is not available on many websites, but it is preferable to POST because it is easier to configure.
- ***HTTP SharePoint Get*** (on page 186) - downloads a file from a Microsoft SharePoint Server webserver.
- ***HTTP SharePoint Put*** (on page 186) - Uploads a file to a Microsoft SharePoint Server webserver.

When configuring a task to access a webserver, use one of the above scripts as a Process step instead of adding a Source or Destination.

Not all webservers can be successfully accessed via these scripts. Some websites require complex, human-oriented navigation which is beyond the scope of these scripts.

MessageWay Translation

If your organization sends documents in EDI (Electronic Data Interchange) format, you may also need to transform the data in these documents to match a format used by a trading partner. In EDI terms, this is known as a translation. If you use MessageWay and the MessageWay Translator from Ipswitch to do these translations, then you can incorporate the translation workflow into a MOVEit Central task.

Using the built-in script "MessageWay Translation", you can set up a task that gets files from a source location, sends them to the MessageWay Translator, and puts the translated files in a destination. This topic provides an example of how you set up a task using the built-in script.

For more information about the script itself, see the topic "Configuring Tasks - Processes/Scripts - Built-In - MessageWay Translation." For more information about configuring MessageWay, see "MessageWay User's Guide and Reference." For more information about configuring and testing a translation, see "MW Translator Workbench User's Guide and Reference" and "MW Translator Workbench Tutorial."

Basic Instructions

This example shows how to set up a task that runs a translation. It translates a test document X12 850 (Purchase Order) to a proprietary fixed format document and generates an acknowledgement (X12 997). This example uses files installed with the MessageWay installation.

The example assumes that a MessageWay environment, including the MessageWay Translator, is already configured and has the following user and location information:

- user name and password: **micentral**
- location name for the MWTranslator service: **translate**
- location name for pickup mailbox: **moveit**

To translate an EDI document using MOVEit Central and MessageWay, in our example, we do the following in MOVEit Central:

1. Set up a file transfer Advanced Task (one source and one destination) to download and save the X850TEST file without translating it.
2. Once you have the basic file transfer task working, add a "MessageWay Translation" built-in process.
3. Configure "MessageWay Translation" with the following parameters:
   - MWayConn_Host: the IP address or host name of the MessageWay server
   - MWayConn_User: **micentral** (a MessageWay user)
   - MWayConn_Password: password associated with the **micentral** MessageWay user
   - MWayConn_Recipient: translate:**moveit** (a compound address that represents the default MessageWay service location plus the MessageWay pickup mailbox)
   - MWayConn_Sender: X850Test

4 Run the task to test the translation.

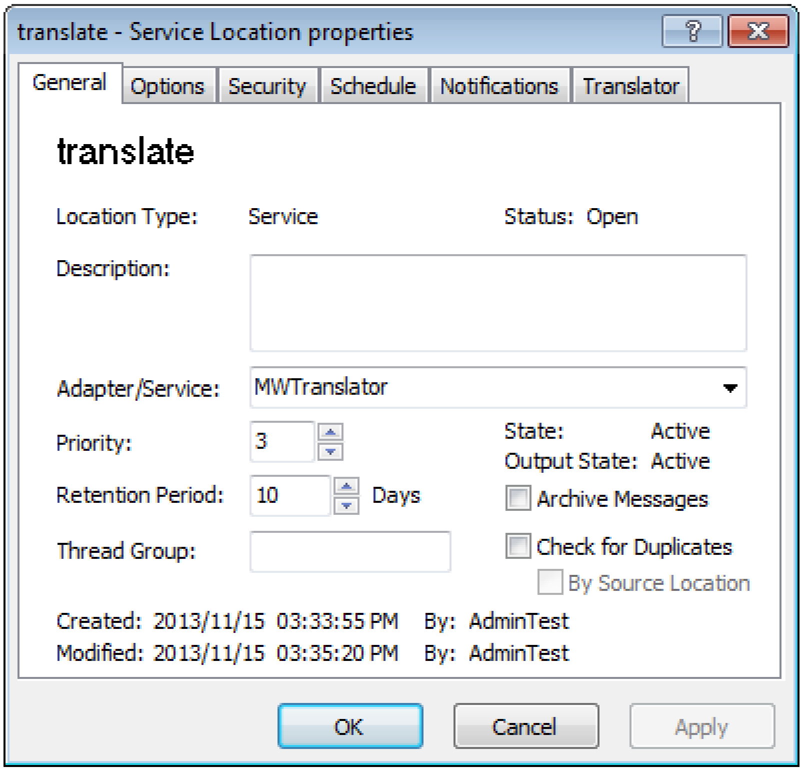
Sample Task

This sample task shows our example using the X850TEST files that are installed with MessageWay, and are described in the "MessageWay Installation Guide." Translation of EDI documents require an associated trading partner and map to be configured in the MessageWay Translation Workbench. This configuration is already present for the X850TEST, but needs to be done for each type of document to be translated. See the "MessageWay Translator Workbench User's Guide and Reference" for more information about configuring the environment.

MessageWay Setup

Before we create the task in MOVEit Central, we configure the following items in our MessageWay environment:

- A default Service location for the MWTranslator service named translate. The Security tab must show the Administrator group.



translate

Location Type: Service

Status: Open

Description:

Adapter/Service: MWTranslator

Priority: 3

State: Active

Output State: Active

Retention Period: 10 Days

□ Archive Messages

Thread Group:

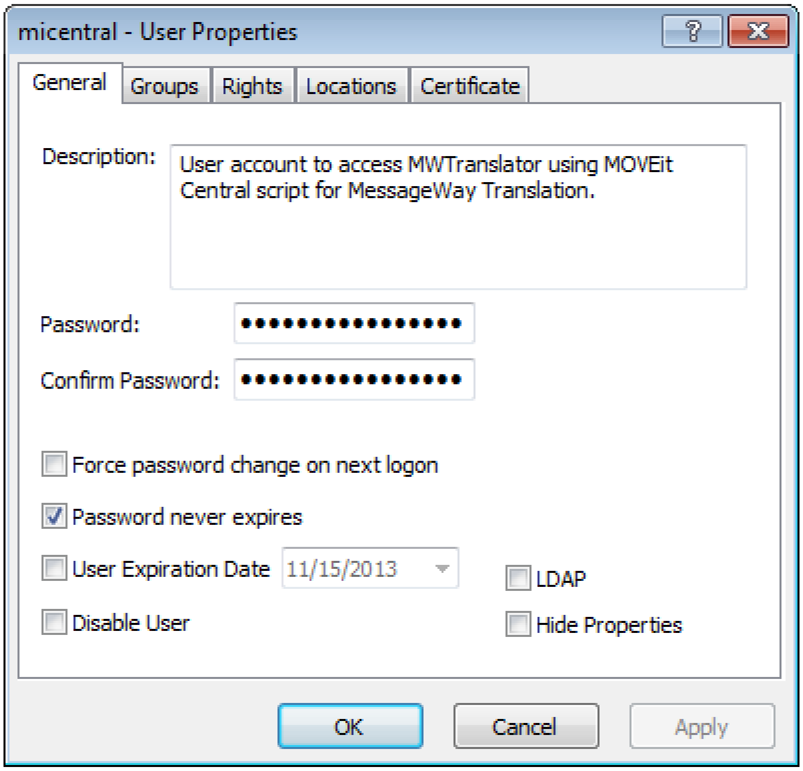
□ Check for Duplicates

□ By Source Location

Created: 2013/11/15 03:33:55 PM By: AdminTest

Modified: 2013/11/15 03:35:20 PM By: AdminTest

- A MessageWay user named **micentral** and associated password, which the MOVEit Central script will use to log in to MessageWay. The user should have appropriate rights. For information about assigning rights to remote users, refer to the "MessageWay User's Guide and Reference." The Locations tab for this user should have an entry for **translate**, the default Service location.



Description: User account to access MWTranslator using MOVEit Central script for MessageWay Translation.

Password: ••••••••••••••••

Confirm Password: ••••••••••••••••

□ Force password change on next logon

☑ Password never expires

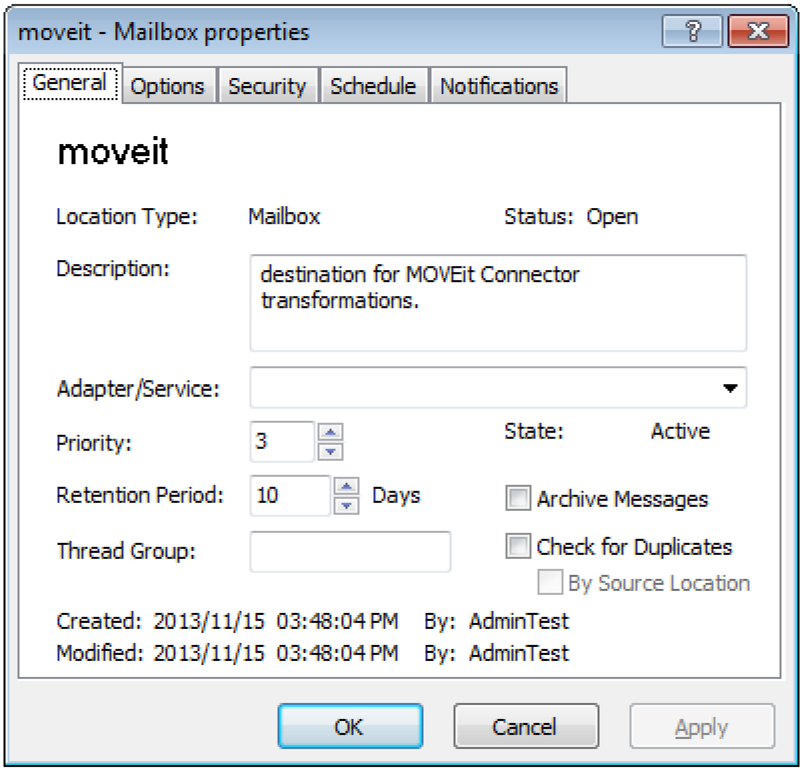
□ User Expiration Date 11/15/2013

□ LDAP

□ Disable User

□ Hide Properties

- A pickup mailbox named **moveit**. The Security tab must show the Administrator group.



moveit

Location Type: Mailbox Status: Open

Description: destination for MOVEit Connector transformations.

Adapter/Service:

Priority: 3 State: Active

Retention Period: 10 Days

□ Archive Messages

Thread Group:

□ Check for Duplicates

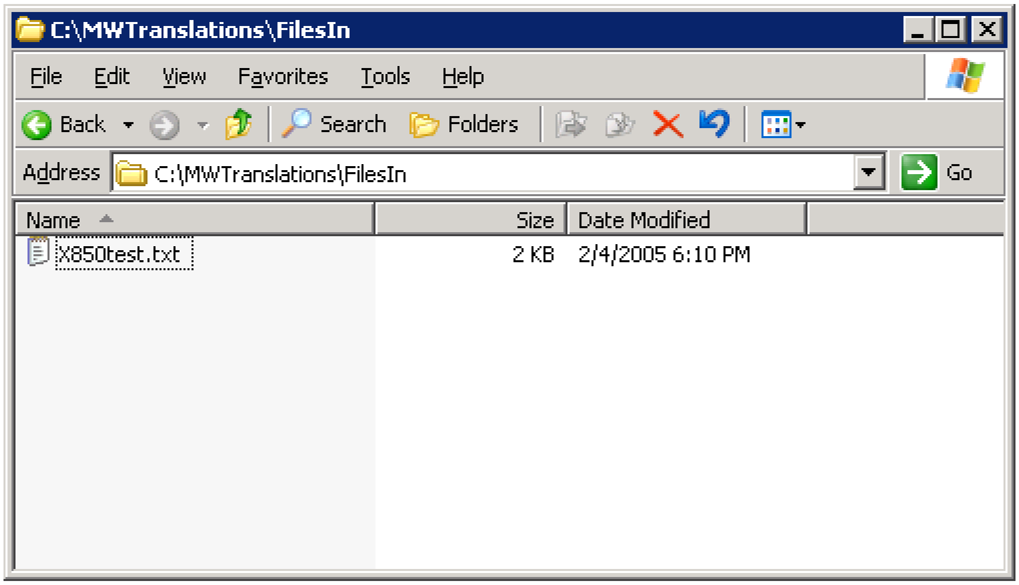
□ By Source Location

Created: 2013/11/15 03:48:04 PM By: AdminTest

Modified: 2013/11/15 03:48:04 PM By: AdminTest

MOVEit Central Setup

Next, we will create an Advanced Task in MOVEit Central to send the X850TEST.txt file for translation. The source location will be: "c:\MWTranslations\FilesIn\X850Test.txt"

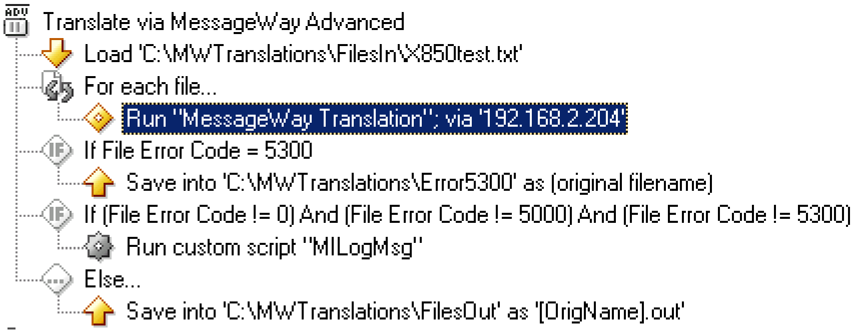


Address: C:\MWTranslations\FilesIn

Name	Size	Date Modified
X850test.txt	2 KB	2/4/2005 6:10 PM

Note: The X850TEST.txt file can be found on the host where you installed MessageWay, in the folder: "c:\MessageWay\Server\MWTranslator"

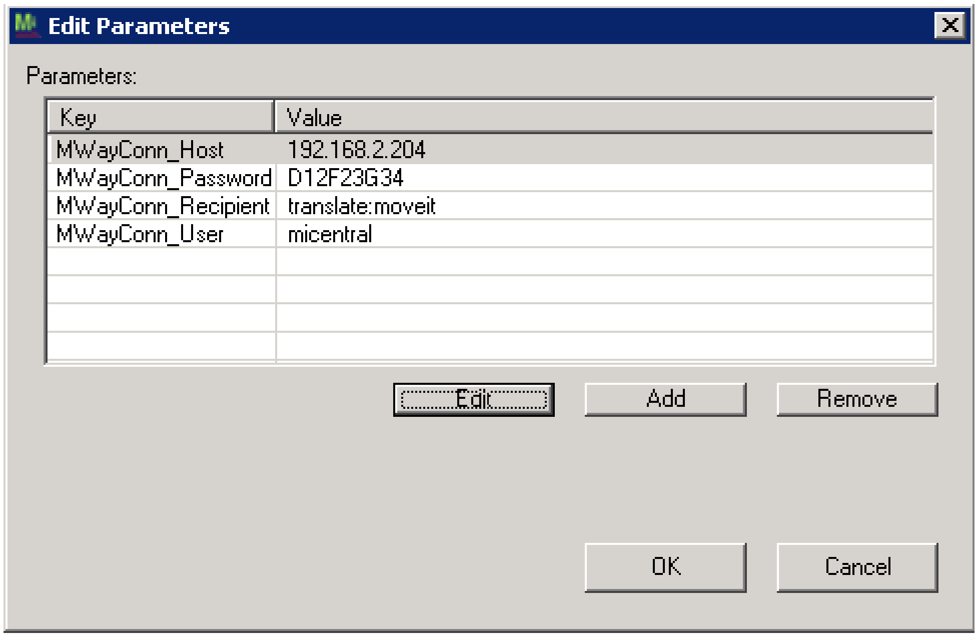
We create an Advanced Task named Translate Via MessageWay. The complete task is shown here:



```
Translate via MessageWay Advanced
    Load 'C:\MWTranslations\FilesIn\X850test.txt'
    For each file...
        Run "MessageWay Translation"; via '192.168.2.204'
    If File Error Code = 5300
        Save into 'C:\MWTranslations\Error5300' as (original filename)
    If (File Error Code != 0) And (File Error Code != 5000) And (File Error Code != 5300)
        Run custom script "MILogMsg"
    Else...
        Save into 'C:\MWTranslations\FilesOut' as '[OrigName].out'
```

We have a source file named "c:\MWTranslations\FilesIn\X850Test.txt". In the Advanced Task, this file is defined as the source.

The FOR file loop runs the MessageWay Translation process, selected from the list of built-in scripts. The parameters needed for MessageWay are defined in the built-in script. Our example shows the required parameters. For a description of all parameters, see the topic "***Configuring Tasks - Processes/Scripts - Built-In - MessageWay Translation*** (see "***MessageWay Translation***" on page 195)."

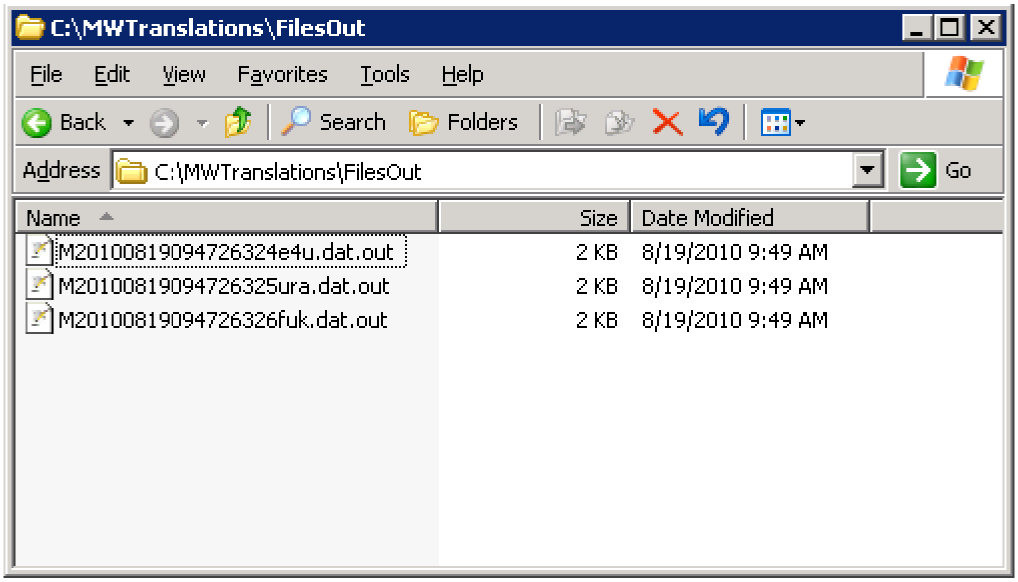


Edit Parameters

Parameters:

Key	Value
MWayConn_Host	192.168.2.204
MWayConn_Password	D12F23G34
MWayConn_Recipient	translate:moveit
MWayConn_User	micentral

The MessageWay Translation process sends the source file(s) to the MessageWay Translator. If an error does not occur, the translated files are received back and placed in the destination: "c:\MWTranslations\FilesOut"



Address C:\MWTranslations\FilesOut

Name	Size	Date Modified
M20100819094726324e4u.dat.out	2 KB	8/19/2010 9:49 AM
M20100819094726325ura.dat.out	2 KB	8/19/2010 9:49 AM
M20100819094726326fuk.dat.out	2 KB	8/19/2010 9:49 AM

If a translation error (error code 5300) occurs, this means that some, but not all, the files were successfully translated. In this case, the resulting files are sent to the destination: "c:\MWTranslations\Error5300". Note that the MessageWay Translation script differs from other tasks in allowing a partially successful outcome. You can set up the task to accept partially successful translation, or to reject the translation and receive a report. For more information, see the description of the MWayConn_ExceptionsInsteadofData parameter in the MessageWay Translation built-in script.

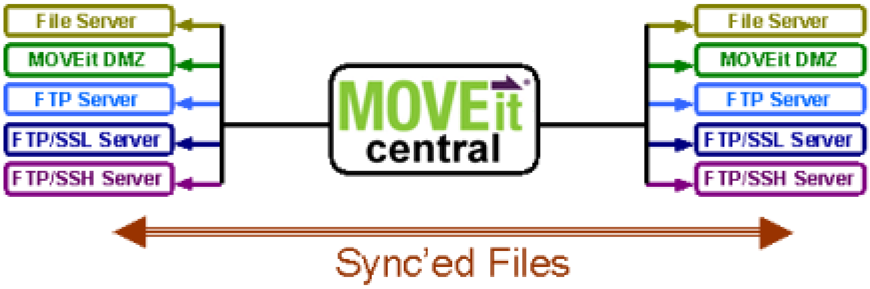
If an error other than code 5000 or 5003 occurs, it is logged in the location specified by the custom script "MILogMsg."

See also ***"Advanced Topics - MessageWay CLI."*** (on page 431)

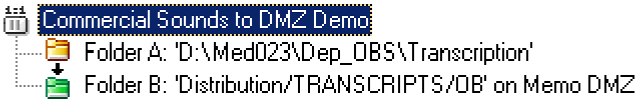
Synchronization

Overview

MOVEit Central can replicate the contents of two folders to ensure the files and folder structures remain in sync. Any two folders on MOVEit Central's local hard drive, other Windows servers/shares, FTP servers, FTPS servers, SFTP servers and/or MOVEit DMZ servers may be involved in a single synchronization task.



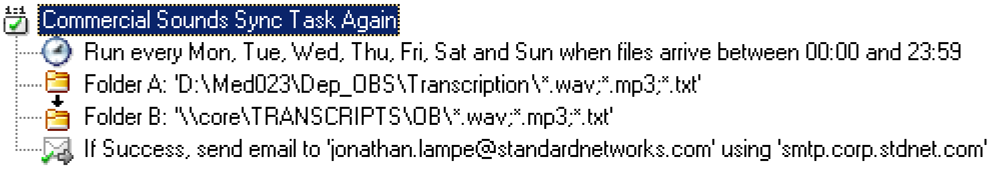
Folder sync operations are configured in special "synchronization tasks". Instead of the sources and destinations found in a traditional task, a synchronization task consists of "Folder A", "Folder B" and a "sync direction" arrow. Possible sync directions include "one-way" and "two-way", and there are additional options that control whether or not certain deletions or extra files are permitted.



Commercial Sounds to DMZ Demo
Folder A: 'D:\Med023\Dep_OBS\Transcription'
Folder B: 'Distribution/TRANSCRIPTS/OB' on Memo DMZ

Synchronization tasks are scheduled like traditional tasks and may be event-driven if their folders are on hosts that permit file notifications. Next actions elements are also permitted and a special "[SyncReport()]" macro is available to quickly summarize actions taken by synchronization tasks.

Synchronization tasks may also be configured to only transfer (and/or exclude) particular folders and files based on name, extension or size.



Commercial Sounds Sync Task Again
Run every Mon, Tue, Wed, Thu, Fri, Sat and Sun when files arrive between 00:00 and 23:59
Folder A: 'D:\Med023\Dep_OBS\Transcription\*.wav;*.mp3;*.txt'
Folder B: '\\core\TRANSCRIPTS\OB\*.wav;*.mp3;*.txt'
If Success, send email to 'jonathan.lampe@standardnetworks.com' using 'smtp.corp.stdnet.com'

What Synchronization Tasks Do That Traditional Tasks Do Not

Synchronization tasks can:

- Delete files and folders from one folder if MOVEit Central notices they have been deleted from another folder.
- Replicate (add and trim) empty folder structures. (Traditional tasks only create folder structures, and only do so if files are present in them.)
- Respond to file and folder create, delete and rename events. (Traditional tasks only react to file create or rename events.)

What Traditional Tasks Do That Synchronization Tasks Do Not

Traditional tasks can:

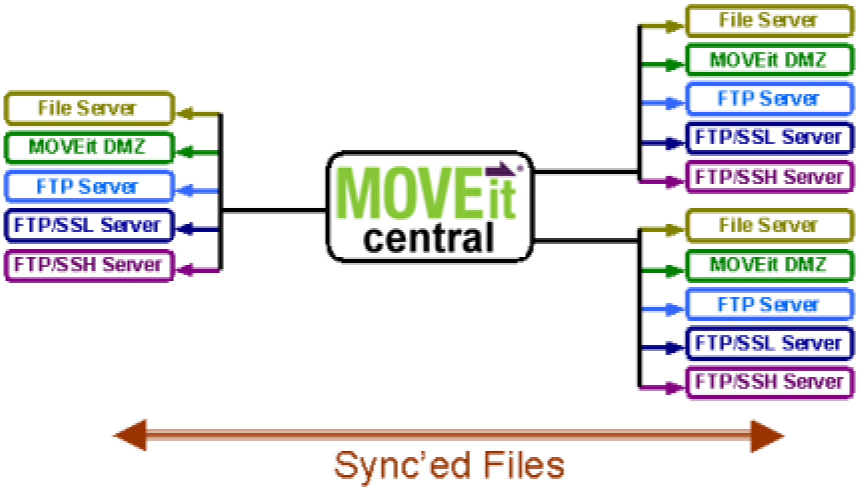
- Run processes.
- Delete/rename/move files on sources after copying them to destinations.
- Rename downloaded files and folders before writing or creating them on destinations.
- Pull from multiple destinations in a single task.
- Push to multiple destinations in a single task.
- Work with AS1, AS2, AS3 and SMTP/POP3 (email) sources and destinations.
- Select source files based on specific date criteria (such as "older than 60 days").
- Handle "blind" downloads (typically through FTP servers that do not provide directory listings).
- Zip or unzip simple files.
- Issue per-file FTP commands.
- *(perform several other rarely-used options)*

Synchronization tasks also automatically deal with concepts such as "new files" and "creation of 'destination' subfolders if necessary" so many of the settings that deal with such things on traditional task sources and destinations will not be found on synchronization task folder A and folder B configurations.

Advanced Synchronization Architecture

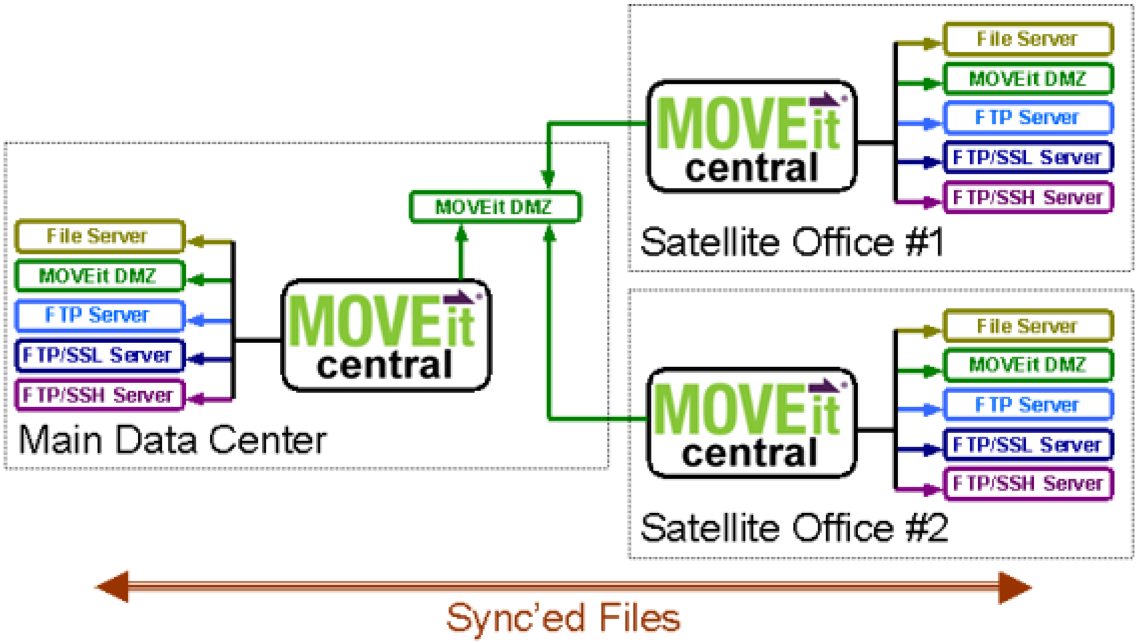
Synchronizing Content To or Between Multiple Folders

MOVEit Central can synchronize content to or between more than two folders. To achieve this, pick one particular folder to serve as a "master" folder and then set up one task for each remote folder with which you wish to synchronize your master folder. (Every related task will have the master folder as "Folder A", regardless of synchronization direction or other options.)



Synchronizing Content To or Between Multiple Remote Sites

MOVEit Central can synchronize content to or between multiple remote sites across the Internet, even if the remote sites have no secure server of their own. To achieve this, MOVEit Central software can be installed at each remote site and a single MOVEit DMZ server can be used as a common, secure and shared repository.



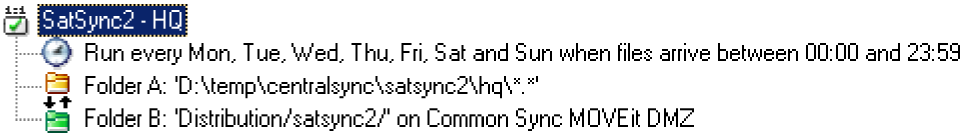
MOVEit DMZ Configuration

If each remote site contains unique content, then a different folder should be set up for each remote site. Otherwise, a single folder containing shared content for all remote sites should be set up. All folders should be set up to ALLOW overwrites and any related user-folder permissions should grant Read, List, Write, Delete and Subs access.

Each remote site should have its own end user account or FileAdmin account. The main data center should also have a FileAdmin account.

Main Data Center MOVEit Central Configuration

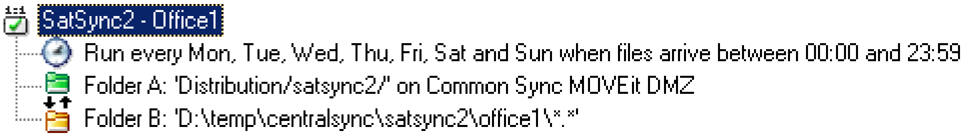
If each remote site contains unique content, then a different sync task should be set up for each remote site's folder on MOVEit DMZ. Otherwise, a single sync task to move shared content for all remote sites should be set up. (Every related task will have a MOVEit DMZ folder as "Folder B", regardless of synchronization direction or other options.)



SatSync2 - HQ
Run every Mon, Tue, Wed, Thu, Fri, Sat and Sun when files arrive between 00:00 and 23:59
Folder A: 'D:\temp\centralsync\satsync2\hq\*.*'
Folder B: 'Distribution/satsync2/' on Common Sync MOVEit DMZ

Remote Site MOVEit Central Configuration

Regardless of whether or not each remote site has its own unique content, each remote site only needs a single sync task to sync from either the remote site's unique content MOVEit DMZ folder or a shared MOVEit DMZ folder. (Every related task will have a MOVEit DMZ folder as "Folder A", regardless of synchronization direction or other options.)



SatSync2 - Office1
Run every Mon, Tue, Wed, Thu, Fri, Sat and Sun when files arrive between 00:00 and 23:59
Folder A: 'Distribution/satsync2/' on Common Sync MOVEit DMZ
Folder B: 'D:\temp\centralsync\satsync2\office1\*.*'

Synchronization Icons

Synchronization tasks use slightly different icons than traditional tasks. Where traditional tasks use a "clipboard" icon (□), synchronization tasks use a "1=1" icon (□). However, both types of tasks use "status modifiers" such as green checkmarks in the same way.

☑	☑	**Scheduled** sync task
□	□	**Disabled or unscheduled** sync task
☒	☒	**Incomplete** sync task

Instead of large colored-by-type-of-host arrows to indicate sources and destinations, synchronization tasks use colored-by-type-of-host folders. There are always two (and only two) folders listed in a synchronization task. Synchronization tasks also use small black arrows between the two folders to clearly indicate the sync direction.

🟨	**Windows File System or Share** sync folder
🟩	**MOVEit DMZ** sync folder
🟦	**FTP** or **FTPS** sync folder
🟪	**SFTP** sync folder
↓	**One-way** sync direction (from "Folder A" to "Folder B")
↓↑	**Two-way** sync direction

Options

The "Sync Options" dialog is displayed during new sync task creation and is also available as a "right-click" option on existing sync tasks. It provides two important options that control how synchronization is performed between Folder A and Folder B.

Sync Direction

Possible sync directions include "one-way" and "two-way".

- One-way sync tasks (a.k.a., "--->" or ⬇) always replicate content from Folder A to Folder B.
- Two-way sync tasks (a.k.a., "<-->" or ⬇⬆) always replicate content from Folder A to Folder B and from Folder B and A.

Sync Deletes

Possible sync delete options include "ignore deletes", "sync deletes" and "sync deletes and delete extra files on Folder B".

- The **ignore deletes** option causes the task to ignore any files or folders deleted from Folder A in a one-way sync task or ignore any files or folders deleted from either Folder A or Folder B in a two-way sync task. New files, updated files and renamed files and folders are still replicated.
- The **sync deletes** option causes the task to delete from Folder B any files or folders deleted from Folder A in a one-way sync task or delete from the other folder any files or folders deleted from either Folder A or Folder B in a two-way sync task. New files, updated files and renamed files and folders are also replicated. This option is the default for new two-way sync tasks.
- The **sync deletes and delete extra files on Folder B** option is only available to one-way tasks. This option behaves like "sync deletes" with one exception: any "extra" files or folders created or renamed on Folder B by anything other than this sync task will automatically be deleted. This option is the default for new one-way sync tasks.

Best Option Scenarios

This section describes the best option for the following scenarios:

- One-Way "Master Folder" Scenarios
- Two-Way Scenarios

One-Way "Master Folder" Scenarios

Some "replication" scenarios call for one or more copies of a single "master" folder. A sync direction of "one-way" should normally be selected in these situations. The "master folder" should always be configured as Folder A.

One-Way "Master Folder", Exact Replica

To ensure that all Folder B's only contain files and folder structures that are present in the "master" Folder A, use the "**sync deletes and delete extra files on Folder B**" sync delete option.

Folder A Action	Folder B Action	Sync Task Reaction
Add, update or rename file or folder	-	Add, update or rename file or folder to/on Folder B
Delete file or folder	-	Delete file or folder from Folder B
-	Add file or folder	Delete related file or folder from Folder B
-	Rename file or folder	Delete renamed file or folder from Folder B and copy file or folder from Folder A
-	Update file	Overwrite updated file on Folder B with file from Folder A
-	Delete file or folder	Replace file or folder on Folder B with copy from Folder A

One-Way "Master Folder", Extra Files on Folder B Are OK

If "extra" files and folders on Folder B that do not exist in the "master" Folder A are acceptable, use the "**sync deletes**" sync delete option.

Folder A Action	Folder B Action	Sync Task Reaction
Add, update or rename file or folder	-	Add, update or rename file or folder to/on Folder B
Delete file or folder	-	Delete file or folder from Folder B
-	Add or update file or folder	*(nothing)*
-	Rename file or folder	Copy original file or folder from Folder A
-	Delete file or folder	Replace file or folder on Folder B with copy from Folder A

One-Way "Master Folder", Keep Content on Folder B After It's Been Deleted from Folder A

If you want content and folders replicated to Folder B from Folder A to remain on Folder B after the originals have been deleted from Folder A, use the "**ignore deletes**" sync delete option.

Folder A Action	Folder B Action	Sync Task Reaction
Add, update or rename file or folder	-	Add, update or rename file or folder to/on Folder B
Delete file or folder	-	*(nothing)*
-	Add, update or rename file or folder	*(nothing)*
-	Delete file or folder	Replace file or folder on Folder B with copy from Folder A

Two-Way Scenarios

Some replication scenarios require that changes made to either of two folders be replicated to the other. A sync direction of "two-way" should normally be selected in these situations. Either folder in these relationships may be configured as Folder A, but it is usually more intuitive to replicate content if the "more populated" of the two folders is selected as Folder A.

Two-Way, Exact Replica

To ensure that file and folder additions, updates, deletions and renames are replicated between two folders, use the "**sync deletes**" sync delete option.

Folder A Action	Folder B Action	Sync Task Reaction
Add, update or rename file or folder	-	Add, update or rename file or folder to/on Folder B
Delete file or folder	-	Delete file or folder from Folder B
-	Add, update or rename file or folder	Add, update or rename file or folder to/on Folder A
-	Delete file or folder	Delete file or folder from Folder A

Two-Way, Preserve Copy If Original Is Deleted

If you want content and folders replicated between folders to remain on the "copied to" folder after the original files and/or folders have been deleted from the "copied from" folder, use the "**ignore deletes**" sync delete option.

Folder A Action	Folder B Action	Sync Task Reaction
Add, update or rename file or folder	-	Add, update or rename file or folder to/on Folder B
Delete file or folder	-	*(nothing)*
-	Add, update or rename file or folder	Add, update or rename file or folder to/on Folder A

Folder A Action	Folder B Action	Sync Task Reaction
-	Delete file or folder	*(nothing)*

Hosts

MOVEit Central can synchronize files and folders on Windows servers/shares, FTP servers, FTPS servers, SFTP servers and MOVEit DMZ servers. Each "Folder A" and "Folder B" definition is tied to one of these types of MOVEit Central Hosts. Related Host definitions can and often are shared among traditional and synchronization tasks.

There are no special Host-level configuration options that are unique to synchronization tasks. See the "***Configuring Tasks - Hosts*** (see "***Overview***" on page 148)" section of this documentation for more information about Hosts.

File Notifications

Both Windows servers/shares and MOVEit DMZ Hosts can use the "File Notification" option to feed file and folder add, delete and rename events to interested synchronization tasks. Note that interested synchronization tasks still require a schedule that permits them to run when receiving events. (Traditional tasks work the same way, but do not receive folder events or file delete events.)

MOVEit DMZ Host Considerations

Delete and Rename Notifications (Requires v4.5+)

To receive file/folder delete and rename notifications from MOVEit DMZ hosts, those MOVEit DMZ hosts must be running MOVEit DMZ version 4.5 or greater. Otherwise, new file notifications will be seen by MOVEit Central, but file/folder delete and rename operations will not be noticed until the next time a sync task runs (either on a scheduled interval or as a result of a related file notification).

Folders

Every synchronization task replicates files and folders between two folders. MOVEit Central refers to these two folders as "Folder A" and "Folder B" in its configuration dialogs, previews and logs.

One-way sync tasks always replicate content from Folder A to Folder B. Two-way sync tasks always replicate content from Folder A to Folder B and from Folder B to A. Task-level replication options control this behavior; see the "***Synchronization - Options*** (see "***Options***" on page 288)" for more information.

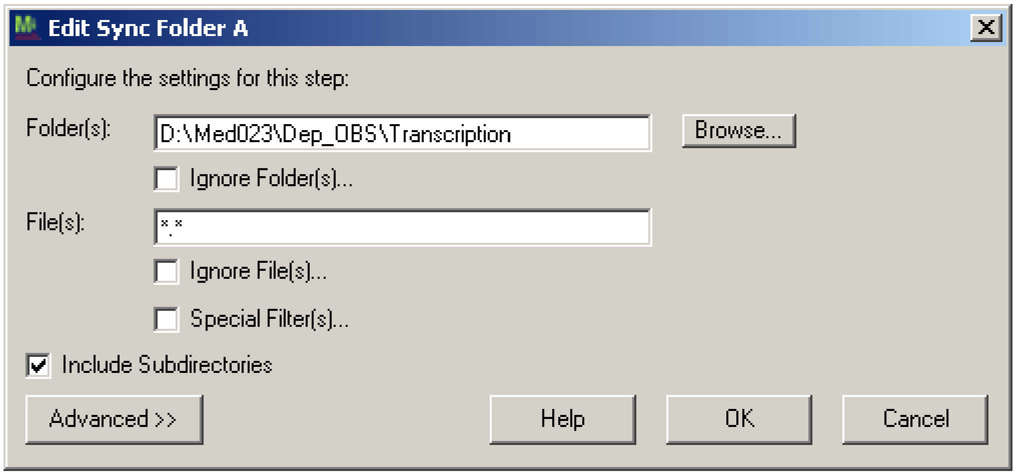
Folder Permissions and Settings

In almost all cases, the account MOVEit Central uses to authenticate to folders used in sync tasks should enjoy the following permissions:

- Read, write, list and delete files
- Overwrite existing files (this is a separate folder-level option on MOVEit DMZ folders)
- Create and remove subfolders files (this is "Subs" permission in MOVEit DMZ)

Folder A

Synchronization task Folder A configuration dialogs feel similar to traditional task Source dialogs, but have far fewer options.



Edit Sync Folder A

Configure the settings for this step:

Folder(s): D:\Med023\Dep_OBS\Transcription

☐ Ignore Folder(s)...

File(s): *.*

☐ Ignore File(s)...

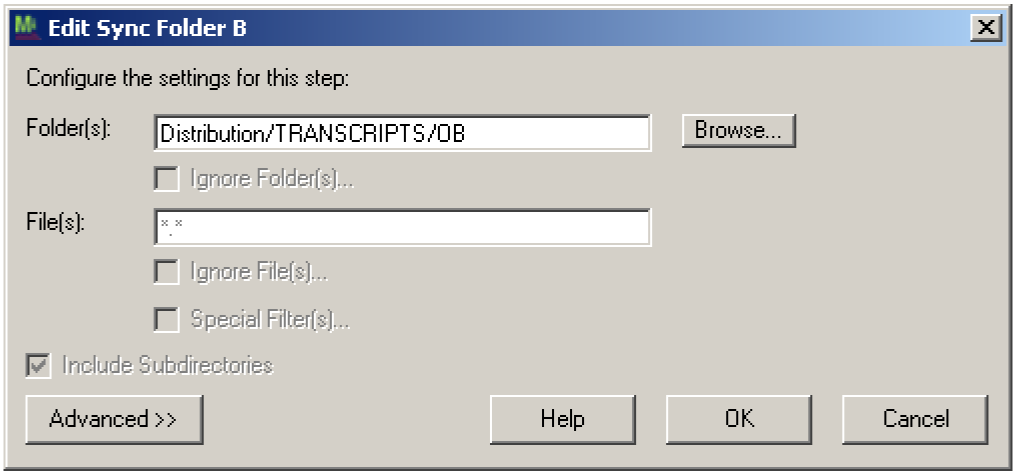
☐ Special Filter(s)...

☑ Include Subdirectories

See the "***Configuring Tasks - Task Elements - Source*** (see "***Source***" on page 120)" documentation for more information about these fields. Note that sync tasks do not permit files to be selected by age; this information is part of what MOVEit Central uses internally to determine which files have changed.

Folder B

Folder B configuration dialogs have fewer active options than ***Folder A configuration dialogs*** (on page 293). This is because many options, including file and folder masks, are simply copied from the Folder A configuration.



Configure the settings for this step:

Folder(s): Distribution/TRANSCRIPTS/OB

□ Ignore Folder(s)...

File(s): *.*

□ Ignore File(s)...

□ Special Filter(s)...

☑ Include Subdirectories

See the "***Configuring Tasks - Task Elements - Source*** (see "***Source***" on page 120)" documentation for more information about these fields. Normally the only fields that can be changed on this dialog are the "Folder" path, retry options and rescan options - all other Folder B settings mirror Folder A settings.

Next Actions

Synchronization tasks may use the same types of ***Next Actions*** (on page 136) as traditional tasks.

Special Macro(s)

Synchronization tasks offer a special "**[SyncReport()]**" macro that allows a complete report of all synchronization actions to be sent in a Next Action email notification. The format of this report is shown below.

- Folder A: (folder path and host of Folder A)
  - X files were copied from Folder B
    - (Specific list of files, if any)
  - X empty folders were created in Folder A
    - (Specific list of folders, if any)
  - X files were deleted from Folder A
    - (Specific list of files, if any)

  - X folders were deleted from Folder A
    - (Specific list of folders, if any)
- Folder B: (folder path and host of Folder B)
  - X files were copied from Folder A
    - (Specific list of files, if any)
  - X empty folders were created in Folder B
    - (Specific list of folders, if any)
  - X files were deleted from Folder B
    - (Specific list of files, if any)
  - X folders were deleted from Folder B
    - (Specific list of folders, if any)

Individual file listings are indented four spaces, start with a path and include last modified date/time and size in parenthesis. For example:

```
    Reports/C13543/urlscan_unattend.txt (2007-03-28 12:55:45, 32 bytes)
```

Individual folder listings are indented four spaces and only include a path. For example:

```
    Reports/D20130
```

Preview

The "Preview" dialog is displayed during new sync task creation and can also be invoked at any time through a "right-click" option on existing sync tasks. This dialog provides an easy way to see what will happen to files and folders on Folder A and Folder B the next time your configured synchronization task runs.

NOTE: It can take several minutes or longer for MOVEit Central to compile a list of changes that the sync task will make, depending on how many files and folders are present in the sources. For performance reasons, a maximum of 1,000 entries will be displayed in the Preview dialog. If more than 1,000 entries are received, an alert message will be displayed indicating how many total entries there were.

Preview Columns

The following columns will be visible (and sortable) in a sync preview:

- **Folder A (or B) File/Folder** - The relative path of an existing file or folder in Folder A (or B). For example, a file named "fileb.txt" in the "twofiles" folder of "Folder A" (or "Folder B") will be listed as "twofiles/filea.txt" in this column.
- **Size** - The size (in bytes) of an existing file or folder in Folder A (or B). Folders will have a value of "<DIR>" in this column.
- **TimeStamp** - The time and date an existing file or folder in Folder A (or B) was last modified.
- **Action** - The action MOVEit Central will take on the listed file or folder the next time the task runs. Specific actions include:
  - **copy ->** : MOVEit Central will copy this file from Folder A to Folder B. Any existing file with the same relative path on Folder B will be overwritten.
  - **<- copy** : MOVEit Central will copy this file from Folder B to Folder A. Any existing file with the same relative path on Folder A will be overwritten.
  - **create ->** : MOVEit Central will create a folder with this relative path on Folder B.
  - **<- create** : MOVEit Central will create a folder with this relative path on Folder A.
  - **delete** : MOVEit Central will delete this file or folder.
  - **- none -** : MOVEit Central will take no action on these files or folders. Entries with these actions will only be visible when the "Show 'no action' entries" box in the lower left corner of the Preview dialog is checked.

Preview Controls

The following controls are available at the bottom of the Preview dialog.

- **OK** button - Saves your initial run options, asks if you want to start the task (usually, "Yes") and asks if you want to enable the task to allow the scheduler to run it automatically.
- **Change Initial Run Options** button - Allows you to change your initial run options to include/exclude more files from the initial copy step. This button will be visible on the Preview page only until you run the task for the first time. See the "***Initial Run Options" section in the "Synchronization - Add New..." documentation*** (on page 304) for more information about sync task initial run options.
- **Refresh** button - Refreshes the preview page with more recent information.
- **Cancel** button - Closes the preview window and leaves your new synchronization task disabled. Before enabling or running your new task, you should use the "preview" option to make sure all connectivity is in place and that synchronization will be occurring the way you intend it to happen.
- **Show "no action" entries"** checkbox - Shows or hides any entries marked with an action of "- none -".

Sync Preview Example

The following example shows how the sync preview represents an initial two-way synchronization between two folders with some existing files and folders.

Given these two folders...

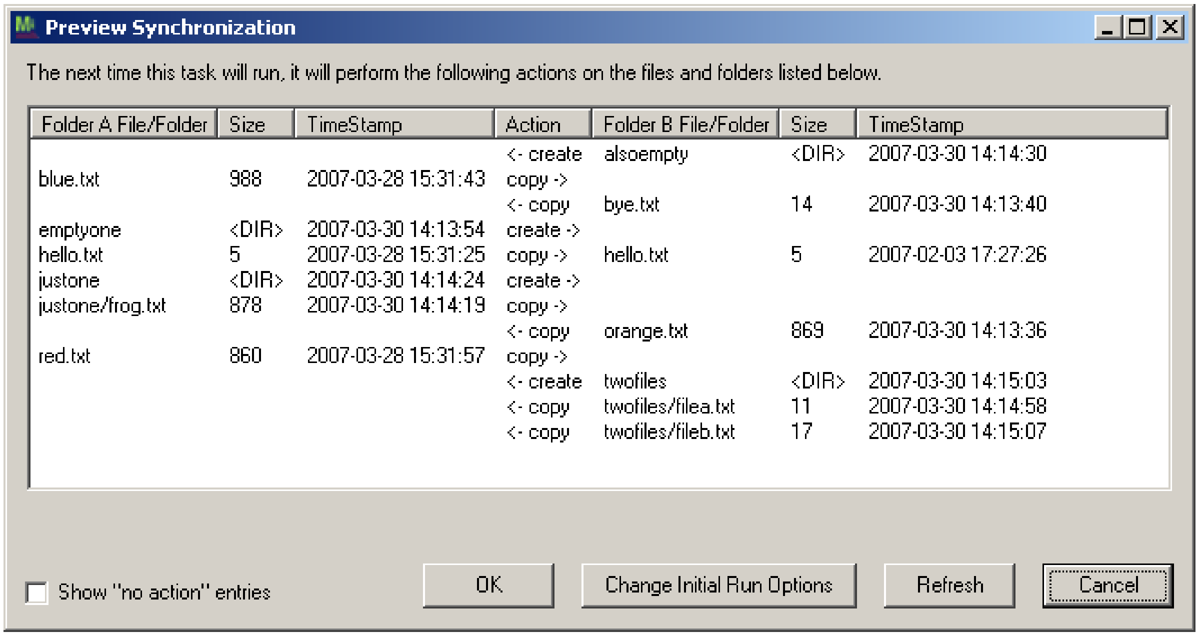
Folder A

```
blue.txt          988     03/28/2007     03:31 PM
hello.txt           5     03/28/2007     03:31 PM
onboth.txt          8     03/30/2007     02:17 PM
red.txt           860     03/28/2007     03:31 PM
\alsoonboth\     (dir)
  elroy.txt        23     03/30/2007     02:17 PM
  point.txt        92     03/30/2007     02:18 PM
  sparta.txt       46     03/30/2007     02:18 PM
\emptyone\       (dir)
\justone\        (dir)
  frog.txt        878     03/30/2007     02:14 PM
```

Folder B

```
bye.txt            14     03/30/2007     02:13 PM

hello.txt           5     02/03/2007     05:27 PM

onboth.txt          8     03/30/2007     02:17 PM

orange.txt        869     03/30/2007     02:13 PM

\alsoempty\      (dir)

\alsoonboth\     (dir)

  elroy.txt        23     03/30/2007     02:17 PM

  point.txt        92     03/30/2007     02:18 PM

  sparta.txt       46     03/30/2007     02:18 PM

\twofiles\       (dir)

  filea.txt        11     03/30/2007     02:14 PM

  fileb.txt        17     03/30/2007     02:15 PM
```

...MOVEit Central will display the following preview in a two-way sync situation (assuming the related sync task has not yet run).

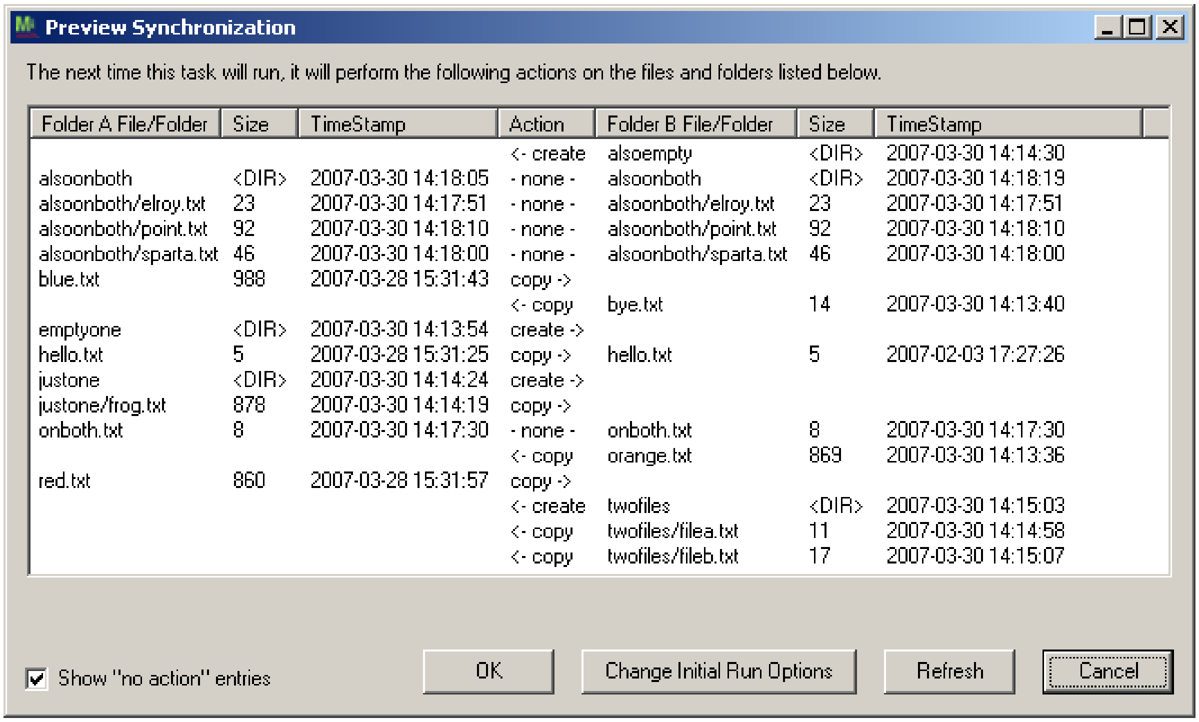


The next time this task will run, it will perform the following actions on the files and folders listed below.

Folder A File/Folder	Size	TimeStamp	Action	Folder B File/Folder	Size	TimeStamp
			<- create	alsoempty	<DIR>	2007-03-30 14:14:30
blue.txt	988	2007-03-28 15:31:43	copy ->			
			<- copy	bye.txt	14	2007-03-30 14:13:40
emptyone	<DIR>	2007-03-30 14:13:54	create ->			
hello.txt	5	2007-03-28 15:31:25	copy ->	hello.txt	5	2007-02-03 17:27:26
justone	<DIR>	2007-03-30 14:14:24	create ->			
justone/frog.txt	878	2007-03-30 14:14:19	copy ->			
			<- copy	orange.txt	869	2007-03-30 14:13:36
red.txt	860	2007-03-28 15:31:57	copy ->			
			<- create	twofiles	<DIR>	2007-03-30 14:15:03
			<- copy	twofiles/filea.txt	11	2007-03-30 14:14:58
			<- copy	twofiles/fileb.txt	17	2007-03-30 14:15:07

□ Show "no action" entries

To see the rest of the files and folder in Folder A and Folder B (the ones with "both" in their names in this example), check the "Show 'no action' entries" box in the lower left corner of the Preview dialog.



The next time this task will run, it will perform the following actions on the files and folders listed below.

Folder A File/Folder	Size	TimeStamp	Action	Folder B File/Folder	Size	TimeStamp
			<- create	alsoempty	<DIR>	2007-03-30 14:14:30
alsoonboth	<DIR>	2007-03-30 14:18:05	- none -	alsoonboth	<DIR>	2007-03-30 14:18:19
alsoonboth/elroy.txt	23	2007-03-30 14:17:51	- none -	alsoonboth/elroy.txt	23	2007-03-30 14:17:51
alsoonboth/point.txt	92	2007-03-30 14:18:10	- none -	alsoonboth/point.txt	92	2007-03-30 14:18:10
alsoonboth/sparta.txt	46	2007-03-30 14:18:00	- none -	alsoonboth/sparta.txt	46	2007-03-30 14:18:00
blue.txt	988	2007-03-28 15:31:43	copy ->			
			<- copy	bye.txt	14	2007-03-30 14:13:40
emptyone	<DIR>	2007-03-30 14:13:54	create ->			
hello.txt	5	2007-03-28 15:31:25	copy ->	hello.txt	5	2007-02-03 17:27:26
justone	<DIR>	2007-03-30 14:14:24	create ->			
justone/frog.txt	878	2007-03-30 14:14:19	copy ->			
onboth.txt	8	2007-03-30 14:17:30	- none -	onboth.txt	8	2007-03-30 14:17:30
			<- copy	orange.txt	869	2007-03-30 14:13:36
red.txt	860	2007-03-28 15:31:57	copy ->			
			<- create	twofiles	<DIR>	2007-03-30 14:15:03
			<- copy	twofiles/filea.txt	11	2007-03-30 14:14:58
			<- copy	twofiles/fileb.txt	17	2007-03-30 14:15:07

☑ Show "no action" entries

Task Actions

Synchronization "task actions" are available from the pop-up menu that appears when you right-click the name of a synchronization task on the ***Tasks Tab*** (on page 109).

Edit Sync Options...

This option simply opens the ***Synchronization Task Options*** (see "***Options***" on page 288) dialog.

Swap Sync Folders

This will cause MOVEit Central to swap Folder A and Folder B. In a one-way sync task this action will swap the identity of the master folder. In a two-way sync task this action will have much less effect. In both cases the saved directory listings MOVEit Central uses to figure out which files and folders need to be ignored, moved, created, etc. are also swapped to avoid incurring an immediate "re-transfer everything" situation.

Clear Sync Listings

Clearing a task's sync listings will cause MOVEit Central to treat this task like a new sync task and may cause MOVEit Central to re-transfer files and folders it already moved.

The selected task will be marked Disabled, and you will need to run a Sync Preview before re-enabling it.

Clearing sync listings is typically useful only if you want to "start over" with this sync task without rebuilding it from scratch. This task's Sync Preview will regain access to "Initial Run" parameters after sync listings are clear. If this task is old or has been busy over its lifetime, MOVEit Central may decide to rebuild or delete many files and folders once the sync listings have been cleared.

View Sync Preview...

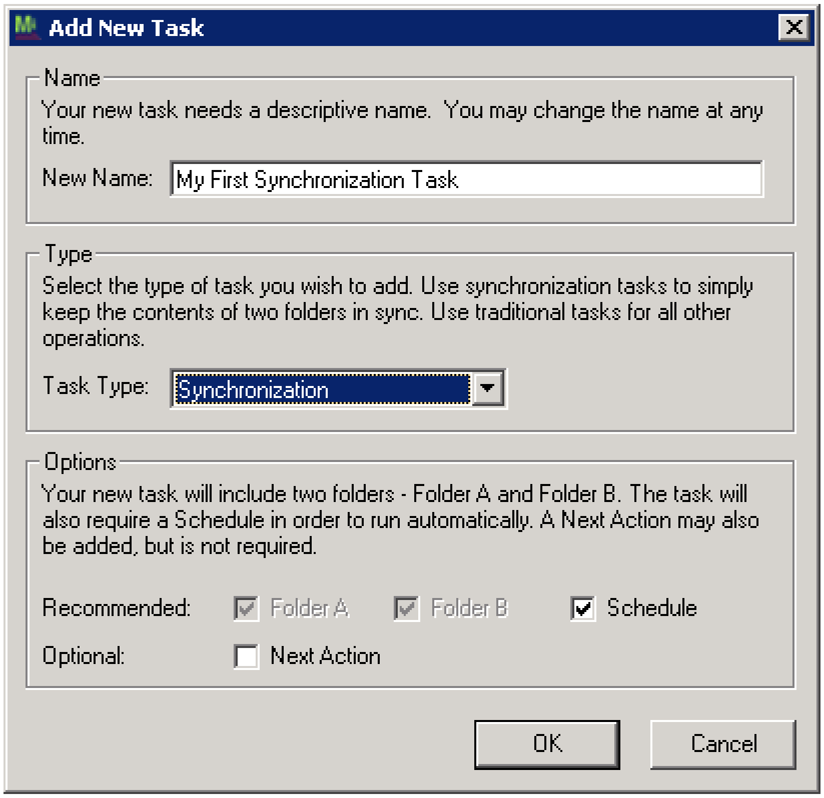
This option simply opens the ***Synchronization Preview*** (see "***Preview***" on page 295) dialog.

Adding a New Synchronization Task

Before you begin, make sure the account MOVEit Central will use to authenticate to your sync folders enjoys the permissions described in the "***Folder Permissions and Settings" section of the "Synchronization - Folders*** (on page 293)" documentation. Also make sure that related hosts are not using "blind downloads" or other traditional-task oriented features that could get in the way of synchronization.

"Add New Task" Dialog

To add a new synchronization task, go to the "Tasks" tab and click the "Add New..." button. Choose "synchronization" (not "traditional") from the "Task Type" option. You will notice that the list of possible task elements will shift when you make this change. Check "Schedule" if you know when you want this synchronization to take place. Check "Next Action" only if you know what action you want to take every time this task completes.



Add New Task

Name

Your new task needs a descriptive name. You may change the name at any time.

New Name: My First Synchronization Task

Type

Select the type of task you wish to add. Use synchronization tasks to simply keep the contents of two folders in sync. Use traditional tasks for all other operations.

Task Type: Synchronization

Options

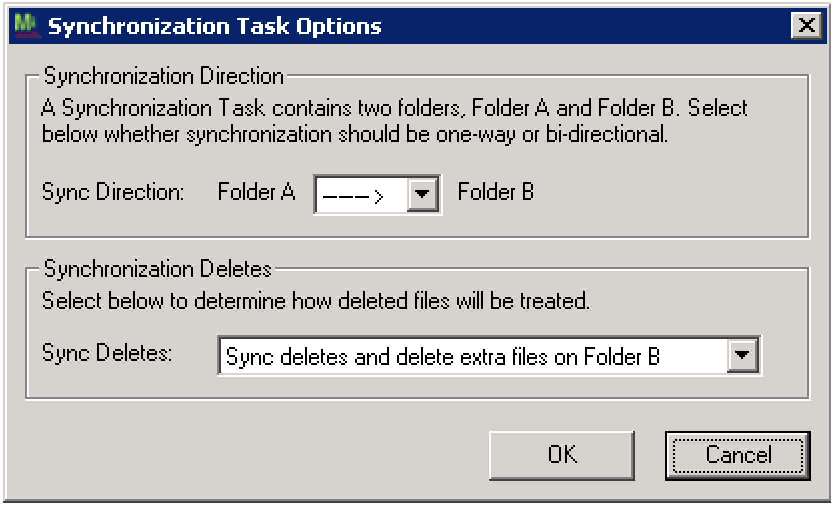
Your new task will include two folders - Folder A and Folder B. The task will also require a Schedule in order to run automatically. A Next Action may also be added, but is not required.

Recommended: ☑ Folder A ☑ Folder B ☑ Schedule

Optional: □ Next Action

"Synchronization Options" Dialog

The next screen will ask you about ***sync options*** (see "***Options***" on page 288). Various combinations of "sync direction" and "sync delete" options can make a large difference in how MOVEit Central treats files and folders, but if you really just want MOVEit Central to make sure two folders contain identical folders and files, use the default options for either one-way ("--->") or two-way ("<-->") synchronization.



Synchronization Direction

A Synchronization Task contains two folders, Folder A and Folder B. Select below whether synchronization should be one-way or bi-directional.

Sync Direction: Folder A ---> Folder B

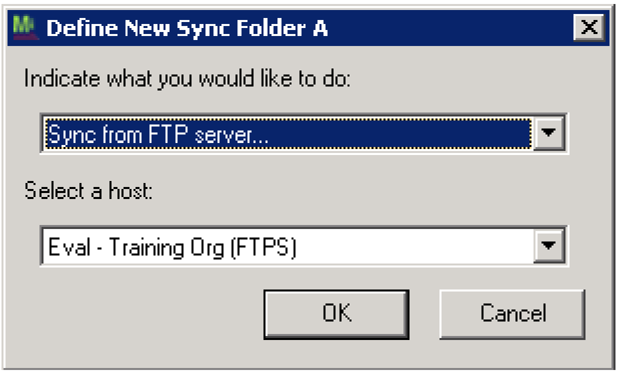
Synchronization Deletes

Select below to determine how deleted files will be treated.

Sync Deletes: Sync deletes and delete extra files on Folder B

Folder A Dialogs

Next, you will be asked to select which host Folder A is found on...



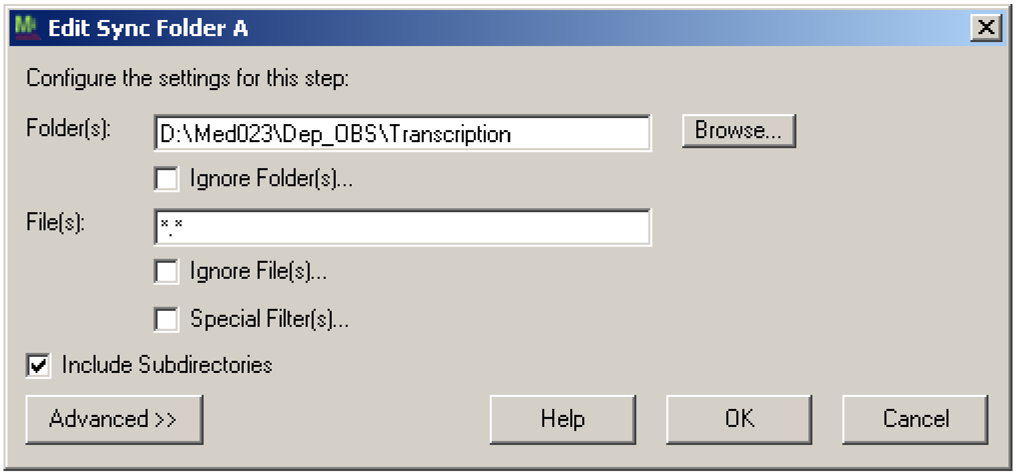
Indicate what you would like to do:

Sync from FTP server...

Select a host:

Eval - Training Org (FTPS)

...and will be asked to provide the exact path of Folder A on that host. You will also be allowed to define specific file and folder name masks (and/or exclusions) and file size restrictions.



Configure the settings for this step:

Folder(s): D:\Med023\Dep_OBS\Transcription

□ Ignore Folder(s)...

File(s): *.*

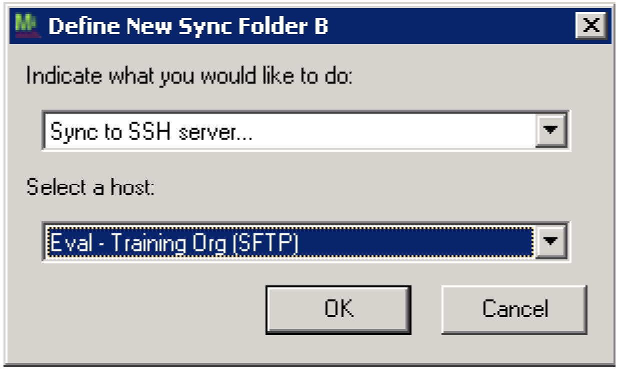
□ Ignore File(s)...

□ Special Filter(s)...

☑ Include Subdirectories

Folder B Dialogs

Next, you will be asked to select which host Folder B is found on...



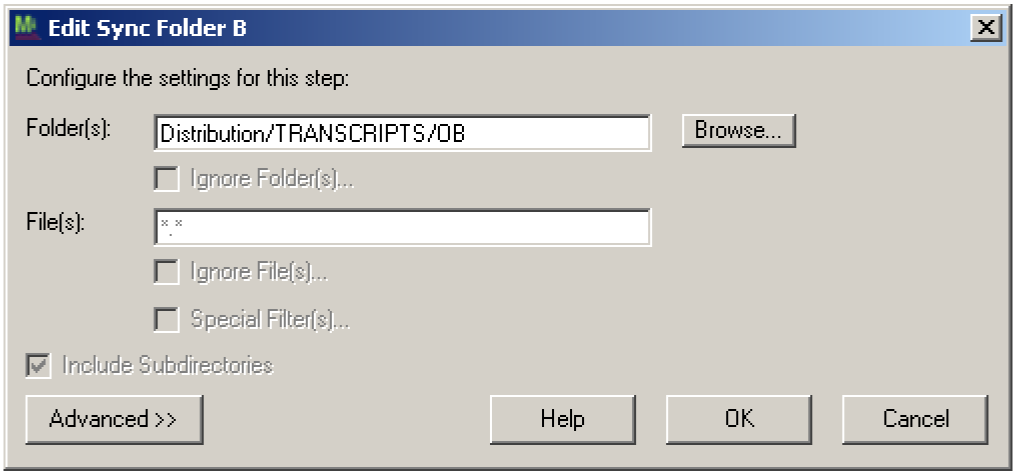
Indicate what you would like to do:

Sync to SSH server...

Select a host:

Eval - Training Org (SFTP)

...and will be asked to provide the exact path of Folder B on that host. (Other options will mostly be mirrored from your Folder A definition, so there will be little else to configure here.)



Configure the settings for this step:

Folder(s): Distribution/TRANSCRIPTS/OB

□ Ignore Folder(s)...

File(s): *.*

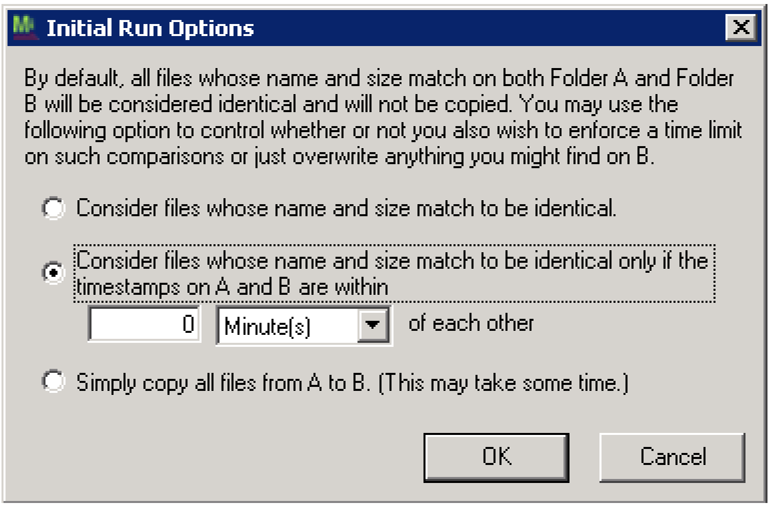
□ Ignore File(s)...

□ Special Filter(s)...

☑ Include Subdirectories

"Initial Run Options" Dialog

The "Initial Run Options" dialog that appears next is there to try to save you time by avoiding recopying files that may already exist on both Folder A and Folder B but have different date/times.



By default, all files whose name and size match on both Folder A and Folder B will be considered identical and will not be copied. You may use the following option to control whether or not you also wish to enforce a time limit on such comparisons or just overwrite anything you might find on B.

○ Consider files whose name and size match to be identical.

● Consider files whose name and size match to be identical only if the timestamps on A and B are within 0 Minute(s) of each other

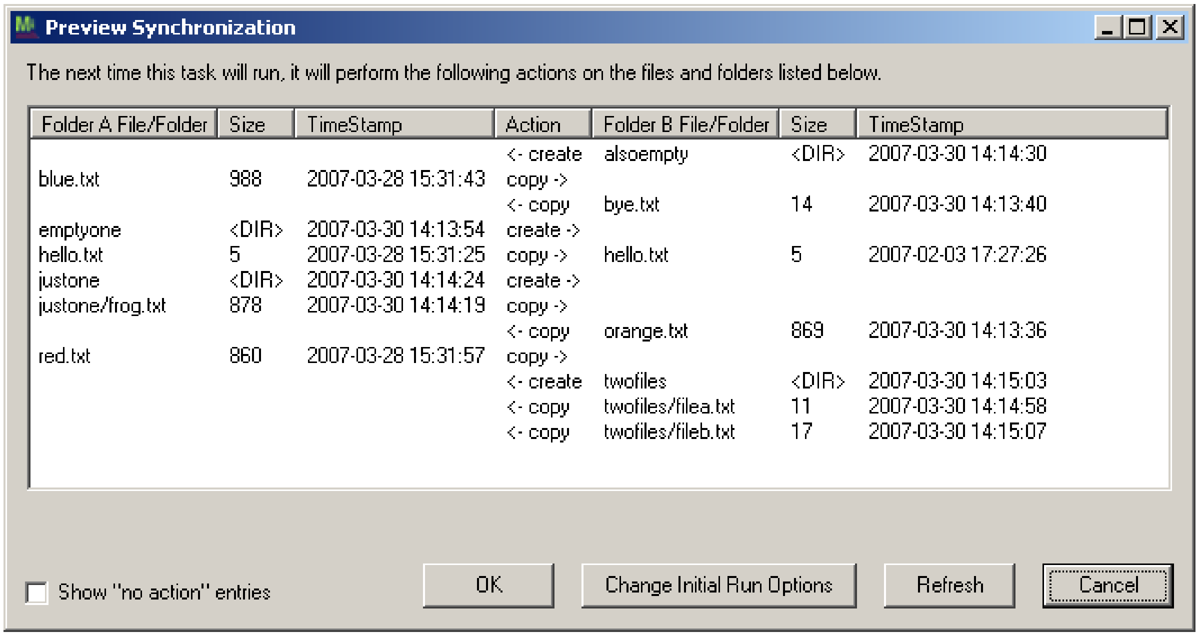
○ Simply copy all files from A to B. (This may take some time.)

- **Consider files whose name and size match to be identical** - You may want to use this option if there are existing files on both Folder A and Folder B that you know are the same but whose last modified date may differ by months or years. (This is the default option.)
- **Consider files whose name and size match to be identical only if the timestamps on A and B are within X (units) of each other** - This option resembles the previous "Consider..." option except it gives to the ability to say that files older than a particular age need to be copied even if they have the same name and size. (A setting of "0 minutes" really make this option behave like "Simply copy...")
- **Simply copy all files from A to B** - This replaces all files on Folder B with fresh copies of files from Folder A. As the label suggests, this option takes the longest of any of the three options.

If Folder A or Folder B is empty, your selection will have no effect. Files with the same name on Folder A and Folder B but having different sizes will always be overwritten, regardless of your selection. (Your selection only affects existing files with the same name and the same size.)

"Preview" Dialog

Once you have selected your initial run options, a preview of the actual synchronization will be displayed. Pay special attention to files that you think ought not to be "recopied"; their sizes on Folder A and Folder B could be different or their modification date/times could be different by more than the value you allowed in the previous "initial run options" dialog.



The next time this task will run, it will perform the following actions on the files and folders listed below.

Folder A File/Folder	Size	TimeStamp	Action	Folder B File/Folder	Size	TimeStamp
			<- create	alsoempty	<DIR>	2007-03-30 14:14:30
blue.txt	988	2007-03-28 15:31:43	copy ->			
			<- copy	bye.txt	14	2007-03-30 14:13:40
emptyone	<DIR>	2007-03-30 14:13:54	create ->			
hello.txt	5	2007-03-28 15:31:25	copy ->	hello.txt	5	2007-02-03 17:27:26
justone	<DIR>	2007-03-30 14:14:24	create ->			
justone/frog.txt	878	2007-03-30 14:14:19	copy ->			
			<- copy	orange.txt	869	2007-03-30 14:13:36
red.txt	860	2007-03-28 15:31:57	copy ->			
			<- create	twofiles	<DIR>	2007-03-30 14:15:03
			<- copy	twofiles/filea.txt	11	2007-03-30 14:14:58
			<- copy	twofiles/fileb.txt	17	2007-03-30 14:15:07

□ Show "no action" entries

What happens next depends on which button you click.

- **OK** - Saves your initial run options, asks if you want to start the task (usually, "Yes") and asks if you want to enable the task to allow the scheduler to run it automatically.
- **Change Initial Run Options** - Allows you to change your initial run options to include/exclude more files from the initial copy step. This button will be visible on the Preview page only until you run the task for the first time.
- **Refresh** - Refreshes the preview page with more recent information.
- **Cancel** - Closes the preview window and leaves your new synchronization task disabled. Before enabling or running your new task, you should use the "preview" option to make sure all connectivity is in place and that synchronization will be occurring the way you intend it to happen.

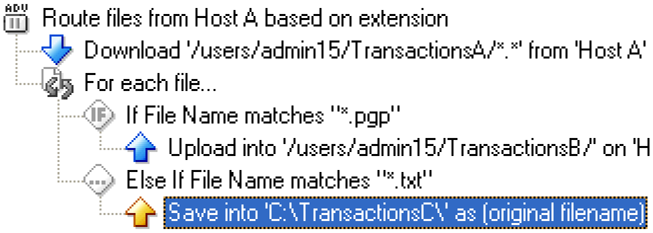
More information about the preview dialog can be found in the "***Synchronization Preview*** (see "***Preview***" on page 295)" section of this documentation.

Advanced Tasks (Enterprise Only)

Overview

An Advanced Task can have many of the elements (source, destination, schedule, process) available to a Traditional Task. In addition, an Advanced Task can use the two conditional elements (If blocks) and (File loops) to determine if and when the other elements are run. The conditional elements provide powerful job flow control without requiring programming or chained tasks.

For example, the following Advanced Task routes files to different destinations based on the file extension.



```
Route files from Host A based on extension
    Download '/users/admin15/TransactionsA/*.*' from 'Host A'
    For each file...
        If File Name matches "*.pgp"
            Upload into '/users/admin15/TransactionsB/' on 'Host B' as (original filename)
        Else If File Name matches "*.txt"
            Save into 'C:\TransactionsC\' as (original filename)
```

You can create an Advanced Task by opening the Tasks tab, clicking Add Task, and then selecting the Advanced Task type.

Note that when you create an Advanced Task, your new task will be created as an empty task. This is different than the behavior of the Traditional Task, which has a wizard that steps you through creating a complete task. Add elements to an Advanced Task using the right-mouse menu. Most Advanced Tasks use a source, a File Loop, and a destination within the File Loop.

The placement of elements within an Advanced Task determines the processing flow of the task, and is thus key to setting up the task. Note the following differences from Traditional Tasks:

- Elements are processed from top to bottom
- Elements that are inline (left justified, rather than indented) are considered independent elements, which means processing is completed for one before moving on to the next.
- When an element is indented under a File Loop, the element is processed for each file in the list of source files.
- When an element is indented under an If Block, the element is executed only if the specified conditions are met.
- You can move elements within an Advanced Task without needing to create or delete elements.

What Advanced Tasks Can Do:

- Test that a specified condition is met, then run a process or transfer a file. For example, transfer a file to a folder based on the file extension: you can use the If block to check if a file name has a .pgp extension; if the file is a .pgp, them move it to a folder. The If Block is used to take an action one time, if the condition is met.
- Test for a specified condition, and while it exists, run a process or transfer files. For example, download a set of encrypted files, and for each encrypted file, save the file to a folder, then decrypt the file, and save it to another folder. The File Loop is used to loop though multiple files until the specified condition no longer applies.
- Simplify task sequences by combining multiple Traditional Tasks into one Advanced Task.
- Create tasks that more clearly correspond to business workflows.

For a step-by-step procedure on how to configure an Advanced Task, see:

- ***Advanced Tasks - Getting Started - If Block*** (see "***If Block***" on page 312)
- ***Advanced Tasks - Getting Started - File Loop*** (see "***File Loop***" on page 309)
- ***Advanced Tasks - Adding a New Advanced Task*** (see "***Adding a New Advanced Task***" on page 320)

Getting Started

This section describes how to create File Loop tasks and If Block tasks.

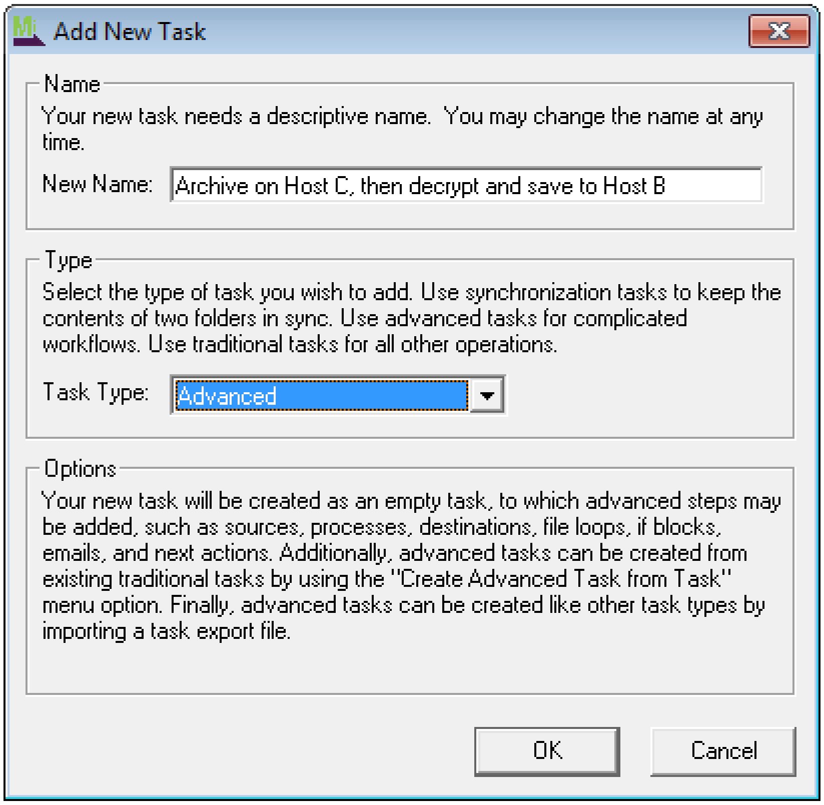
File Loop

The following example shows how an Advanced Task can be used to create a single task to download encrypted files, archive them, then decrypt and save the decrypted version of the file to file server.

In this example, the goal is to archive encrypted files that are initially stored on a host in a branch office that is remote to the MOVEit Central host, and to also do some processing on the downloaded files.

We will create a task that downloads encrypted files from the EncryptionsA folder on Host A at the branch, archives the files to the EncryptionsC folder on your local Host C (the MOVEit Central host), then decrypts each file, and sends the decrypted file to the EncryptionsB folder on Host B.

1 In the Tasks tab, click **Add Task**. The Add New Task dialog opens.



Add New Task

Name

Your new task needs a descriptive name. You may change the name at any time.

New Name: Archive on Host C, then decrypt and save to Host B

Type

Select the type of task you wish to add. Use synchronization tasks to keep the contents of two folders in sync. Use advanced tasks for complicated workflows. Use traditional tasks for all other operations.

Task Type: Advanced

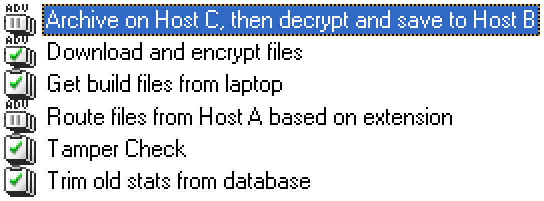
Options

Your new task will be created as an empty task, to which advanced steps may be added, such as sources, processes, destinations, file loops, if blocks, emails, and next actions. Additionally, advanced tasks can be created from existing traditional tasks by using the "Create Advanced Task from Task" menu option. Finally, advanced tasks can be created like other task types by importing a task export file.

2 In the New Name box, enter a descriptive name for the task: "Archive on Host C, then decrypt and save to Host B".

3 For Task Type, select **Advanced**.

4 Click **OK**.



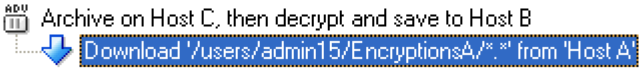
Archive on Host C, then decrypt and save to Host B
Download and encrypt files
Get build files from laptop
Route files from Host A based on extension
Tamper Check
Trim old stats from database

The task is added to the list of tasks. This task is marked with a red X to indicate that it cannot yet be run. This differs from a Traditional Task in that we do not complete a wizard before the task is added to the task list. We will right-click the task name to select the task elements to be added to this task.

5 Right-click the task, and select **Add source**. The Define New Source dialog opens.

a) In the Define New Source dialog, select **Download from FTP server**, then select Host A, then click **OK**. The FTP Source - Host A dialog opens.

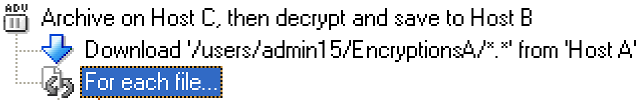
b) Browse for and select the EncryptionsA folder. This is the folder that holds the encrypted (.pgp) files. We want to select all files in this folder, so we'll keep the default File(s) selection (*.*), then click **OK**. The source is now added to the task.



Archive on Host C, then decrypt and save to Host B
Download '/users/admin15/EncryptionsA/*.*' from 'Host A'

When you add a source to an Advanced Task, MOVEit Central displays a message asking whether you want to add a File Loop. In most cases, you will want to use a File Loop so you can apply elements to all files in the source list.

6 Click **Yes** to add a File Loop. (If the message does not appear, then right-click the source definition and select **Add File Loop**.) The File Loop is added to the task. The "For each file ..." statement indicates for each file downloaded from the source, any task element that we put in this file loop will be run on that file.

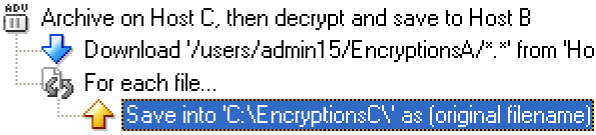


Archive on Host C, then decrypt and save to Host B
Download '/users/admin15/EncryptionsA/*.*' from 'Host A'
For each file...

7 Right-click the File Loop (**For each file ...**) and select **Add Destination**.

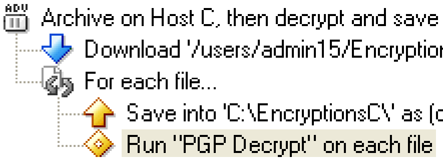
a) In the Define New Destination dialog, select **Save to local folder**, then click **OK**. The Edit Local Folder Destination dialog opens.

b) Browse for and select the EncryptionsC folder, then click **OK**. This is the destination for the .pgp files. The destination is now added to the task.



Archive on Host C, then decrypt and save to Host B
Download '/users/admin15/EncryptionsA/*.*' from 'Host A'
For each file...
Save into 'C:\EncryptionsC\' as [original filename]

8 Right-click the Destination (**Save into...**) and select **Add Process**. The Add Process dialog opens. Under Scripts, select "PGP Decrypt" and click **OK**. The process is added to the task. This will take a .pgp file in the EncryptionsC folder, and decrypt it.

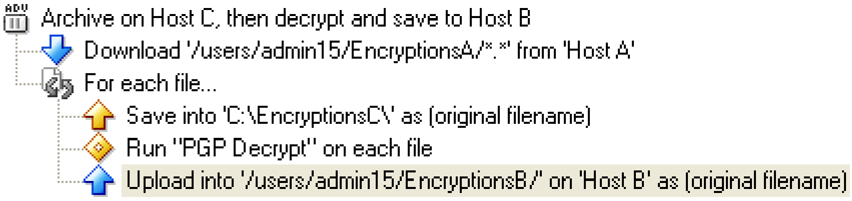


Archive on Host C, then decrypt and save to Host B
Download '/users/admin15/EncryptionsA/*.*' from 'Host A'
For each file...
Save into 'C:\EncryptionsC\' as (original filename)
Run "PGP Decrypt" on each file

9 Right-click the **Run PGP Decrypt Process**, and select **Add Destination**. The Define New Destination dialog opens.

a) In the Define New Destination dialog, select **Upload into FTP server**, then select **Host B**, then click **OK**. The FTP Destination - Host B dialog opens.

b) Browse for and select the EncryptionsB folder. This is the archive destination for the decrypted files. The destination is now added to the task.



Archive on Host C, then decrypt and save to Host B
Download '/users/admin15/EncryptionsA/*.*' from 'Host A'
For each file...
Save into 'C:\EncryptionsC\' as (original filename)
Run "PGP Decrypt" on each file
Upload into '/users/admin15/EncryptionsB/' on 'Host B' as (original filename)

We now have the completed task. When run, this task will download .pgp files from Host A and archive the files on local host (Host C), then decrypt each .pgp file and push the decrypted files to Host B.

You can add a schedule, or other sources, destinations, file loops, if blocks, or emails.

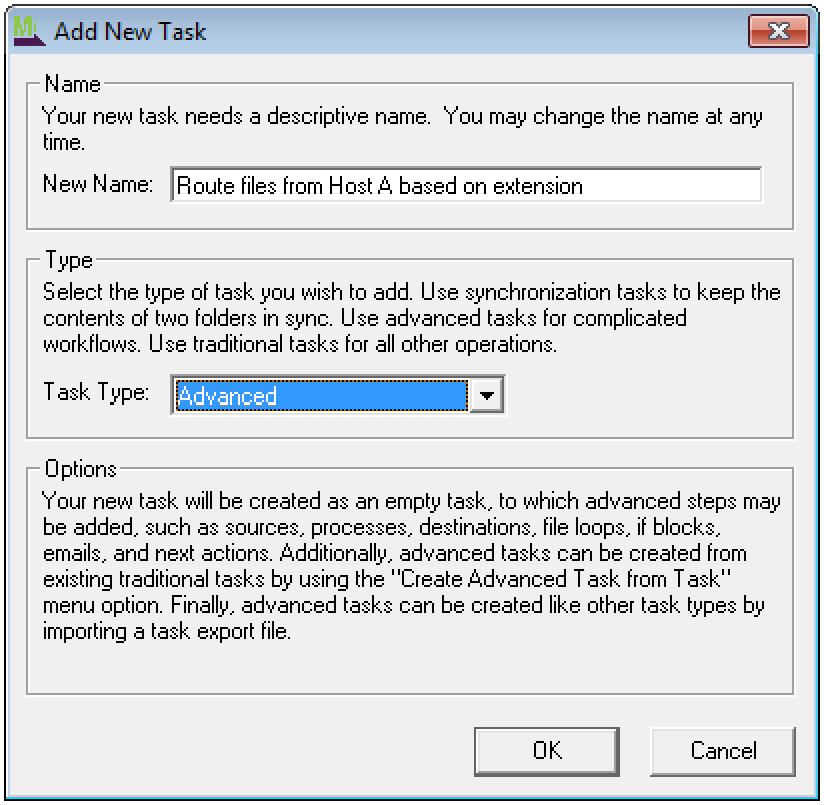
If Block

The following example shows how an Advanced Task can be used to process and route source files based on file extension.

In this example, the goal is to archive and secure records of customer transactions for a financial company. Multiple branch offices record the transactions and send them to a central host, which is remote to the MOVEit Central host. Two types of files (.pgp, .txt) are placed on the remote host.

We will create an Advanced Task that pulls files from the TransactionsA folder on remote Host A, and based on the file extension, pushes the file to the appropriate host. The .pgp files go to the TransactionsB folder on Host B and the .txt files go to the TransactionsC folder on your localhost (Host C).

1 In the Tasks tab, click **Add Task**. The Add New Task dialog opens.



Add New Task

Name

Your new task needs a descriptive name. You may change the name at any time.

New Name: Route files from Host A based on extension

Type

Select the type of task you wish to add. Use synchronization tasks to keep the contents of two folders in sync. Use advanced tasks for complicated workflows. Use traditional tasks for all other operations.

Task Type: Advanced

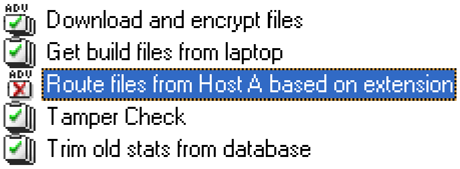
Options

Your new task will be created as an empty task, to which advanced steps may be added, such as sources, processes, destinations, file loops, if blocks, emails, and next actions. Additionally, advanced tasks can be created from existing traditional tasks by using the "Create Advanced Task from Task" menu option. Finally, advanced tasks can be created like other task types by importing a task export file.

2 In the New Name box, enter a descriptive name for the task: "Route files from Host A based on extension."

3 For Task Type, select **Advanced**.

4 Click **OK**.



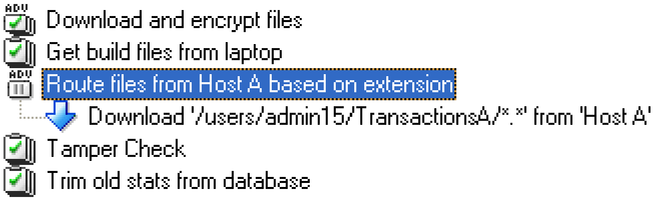
Download and encrypt files
Get build files from laptop
Route files from Host A based on extension
Tamper Check
Trim old stats from database

The task is added to the list of tasks. This task is marked with a red X to indicate that it cannot yet be run. This differs from a Traditional Task in that we do not complete a wizard before the task is added to the task list. We will right-click on the task name to select the task elements to be added to this task.

5 Right-click the task, and select **Add source**. The Define New Source dialog opens.

a) In the Define New Source dialog, select **Download from FTP server**, then select **Host A**, then click **OK**. The FTP Source - Host A dialog opens.

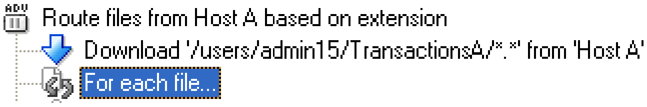
b) Browse for and select the TransactionsA folder. This is the folder that holds the customer transactions (.pgp and .txt files). We want to select all files in this folder, so we'll keep the default File(s) selection (*.*), then click **OK**. The source is now added to the task.



Download and encrypt files
Get build files from laptop
Route files from Host A based on extension
Download '/users/admin15/TransactionsA/*.*' from 'Host A'
Tamper Check
Trim old stats from database

When you add a source to an Advanced Task, MOVEit Central displays a message asking whether you want to add a File Loop. In most cases, you will want to use a File Loop so you can apply elements to all files in the source list.

6 Click **Yes** to add a File Loop. (If the message does not appear, then right-click on the source definition and select **Add File Loop**.) The File Loop is added to the task. The "For each file ..." statement indicates for each file downloaded from the source, any task element that we put in this file loop will be run on that file. We use the loop so that we can run the If block against all the source files.

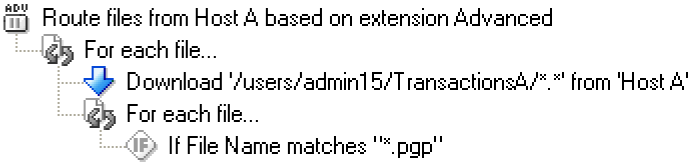


Route files from Host A based on extension
Download '/users/admin15/TransactionsA/*.*' from 'Host A'
For each file...

7 Right-click the File Loop (**For each file...**) and select **Add If block**. The Edit If Branch dialog opens. First, we will look for all files with the .pgp extension. Select the following parameters:

Match all File Name matches *.pgp

The If Block is added to the task, below the source definition.

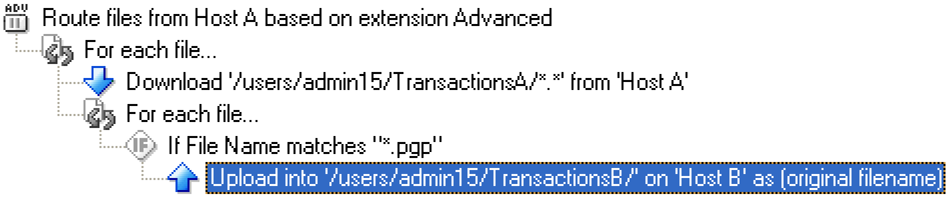


Route files from Host A based on extension Advanced
For each file...
Download '/users/admin15/TransactionsA/*.*' from 'Host A'
For each file...
If File Name matches "*.pgp"

8 Right-click the If Block and select **Add Destination**. The Define New Destination dialog opens.

a) In the Define New Destination dialog, select **Upload into FTP server**, then select **Host B**, then click **OK**. The FTP Destination - Host B dialog opens.

b) Browse for and select the TransactionsB folder. This is the destination for the .pgp files. The destination is now added to the task.

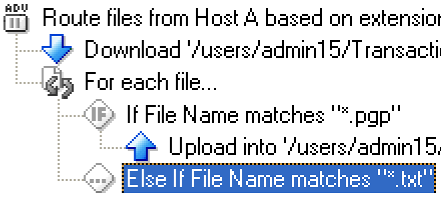


```
Route files from Host A based on extension Advanced
    For each file...
        Download '/users/admin15/TransactionsA/*.*' from 'Host A'
        For each file...
            If File Name matches "*.pgp"
                Upload into '/users/admin15/TransactionsB/' on 'Host B' as [original filename]
```

9 Right-click the If Block and select **Add Else If Branch**. The Edit If Branch dialog opens. We now look for all files with the .txt extension. Select the following parameters:

- Match all File Name matches *.txt

The Else If Block is added to the task, below the destination definition.

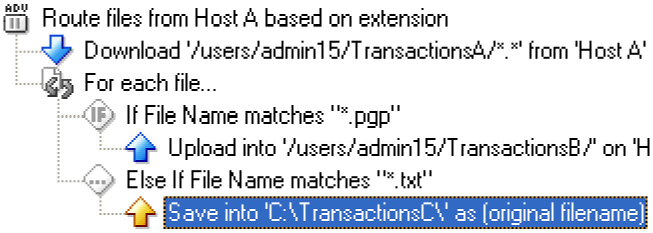


```
Route files from Host A based on extension
    Download '/users/admin15/TransactionsA/*.*' from 'Host A'
    For each file...
        If File Name matches "*.pgp"
            Upload into '/users/admin15/TransactionsB/' on 'Host B' as [original filename]
        Else If File Name matches "*.txt"
```

10 Right-click the Else If block and select **Add Destination**. The Define New Destination dialog opens.

a) In the Define New Destination dialog, select **Add to local folder**, then click OK. The Edit Local Folder Destination dialog opens.

b) Browse for and select the TransactionsC folder. This is the destination for the .txt files. The destination is now added to the task.



```
Route files from Host A based on extension
    Download '/users/admin15/TransactionsA/*.*' from 'Host A'
    For each file...
        If File Name matches "*.pgp"
            Upload into '/users/admin15/TransactionsB/' on 'Host B' as [original filename]
        Else If File Name matches "*.txt"
            Save into 'C:\TransactionsC\' as [original filename]
```

We now have the completed task. When run, this task will filter the folder on Host A and send any .pgp files to Host B, and any .txt files to Host B.

You can add a schedule, or other sources, destinations, file loops, if blocks, or emails.

Task Elements

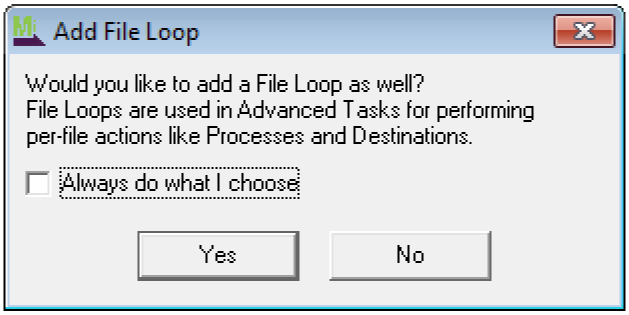
This section describes various task elements.

File Loop

A File Loop causes a set of jobsteps to be performed once for each file that has been downloaded or created so far in the task. An unlimited number of jobsteps can appear inside a loop. Any task element, except a schedule, can be inside a loop. File Loops are particularly powerful when one or more If Blocks appear inside the loop; this allows processing to be customized on a per-file basis.

Because File Loops operate on the current list of files, a File Loop must be preceded by at least one source element, or, less commonly, by at least one process that adds to the list of files.

When you add a source to an Advanced Task, MOVEit Central displays a message asking whether you want to add a File Loop. In most cases, you will want to use a File Loop so you can apply elements to all files in the source list.


Add File Loop

Would you like to add a File Loop as well?
File Loops are used in Advanced Tasks for performing per-file actions like Processes and Destinations.

□ Always do what I choose

Selecting **Always do what I choose** will apply your choice, without showing this dialog, whenever you add a source to an Advanced Task.

To return to the original settings (and show prompts), from the Options menu, select **Reset Advanced Task Prompts**.

Note: There is a known issue that occurs if you use multiple File Loops within an Advanced Task. When files are processed by multiple File Loops which do a rename in the first and a delete in the second, the rename does not work because MOVEit Central is still searching for the original file name on the source. In the Debug log, you will see a (blue) WARNING that says the original file cannot be deleted.

If Block

An If Block defines a condition, and the set of actions to be performed if that condition is true. Any task element, except a schedule, can appear inside an If Block.

An If Block can be used within a File Loop when you want to test each file, for example, when the If Block is intended to act on source files. However, an If Block can be used to test more than just files; for instance, you can test the values of task parameters.

There are at least two elements required: the condition to be tested (for example "File Name matches *.txt") and the action to be taken if the file meets the condition. Actions include pulling files from a specified source, pushing files to a specified destination, or running a process.

An If block can be configured anywhere within an Advanced Task.

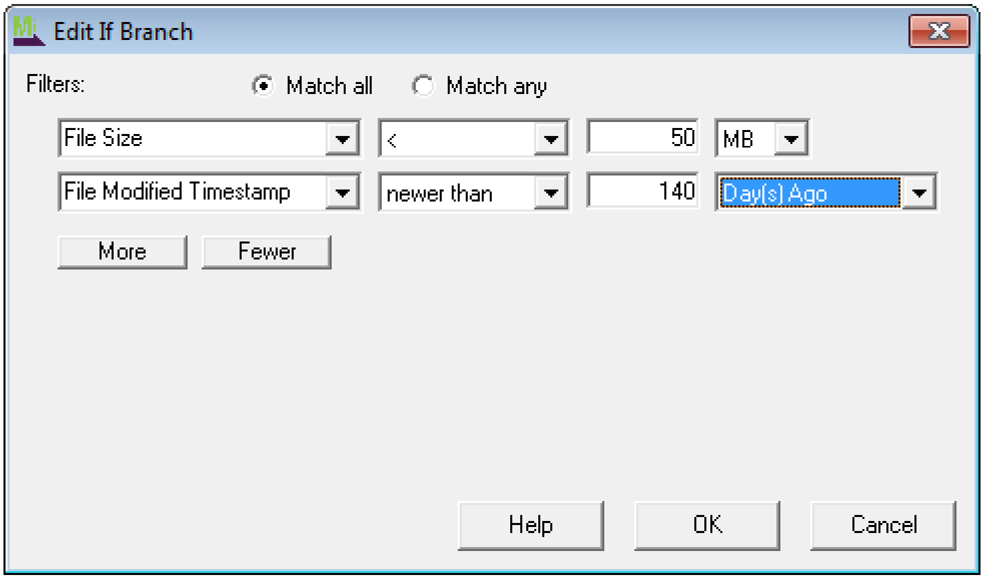
When adding an If Block, there are two settings to configure:

- **Filters** - When you add an If block, the Edit If Branch dialog opens. Within this dialog you can build a filter to select the files or parameters that you want to test. See the section below for more information on using filters. Note that you can use up to 6 filters.
- **Actions** - the action (destination, process, email, etc) you want to take when the condition specified in the filter is true.

Within an If Block, you can do further conditional processing by using these two elements:

- **Else If Branch** - This element lets you set a different test of a condition, followed by a different action for the files that do not meet the condition specified in the initial If element.
- **Else Branch** - This element lets you set a different action (destination, process, email, etc) for those files that do not meet the condition specified in the If element.

Using Filters



Filters: ● Match all ○ Match any

File Size | < | 50 | MB

File Modified Timestamp | newer than | 140 | Day(s) Ago

Note: You can use up to 6 filters. A "match all/any" selection controls whether files must match all or just one of the filter criteria.

- **File Name** - When "matches" is selected, specifies the file name (i.e. "readme.txt") or file mask (i.e. "*.txt") MOVEit Central should use to select files on the remote host. You may use Macros in this field. When "does not match" is selected, MOVEit Central selects the files that do not match the file name or file mask.
- **Note**: You cannot use the "=" operator to match file names (string values). You must use "matches" or "does not match."

  There are two special wildcard characters:

  *, which matches zero or more characters at that position in the filename

  ?, which matches exactly one character at that position in the filename

  You may use multiple wildcard characters in a single mask.

  For example, a*.rpt matches a.rpt, a1.rpt, and apple.rpt, but not apple.rp or lemon.rpt.
  a?.rpt matches a1.rpt and aQ.rpt, but not a.rpt, a12.rpt, or a1.rp

  You may also use multiple filenames or filemasks, separated by semi-colons (";"). The semi-colons act as an "Or" operator. For instance, the filemask "fred*.*;*.zip" will match fred7.txt and will also match sally.zip.
- **File Size** - Select files based on their size. Supported size filters are expressed in your choice of bytes, KB, MB or GB. A "match all/any" selection controls whether files must match all or just one of the filter criteria.
- **File Modified Timestamp** - Select files based on their date/time of last modification. Supported date/time filters are expressed the difference between now and some other date in hours, days, months or years.
- **Task Error Code** - Test the value of an error code returned from the task.
- **Custom macro** - Select any ***MOVEit Central macros*** (see "***Macro***" on page 137), or custom macros you have created. For example, to take action based on the value returned from a previous Look Up process, enter "[Parm:Lookup_Value]".

Run Task

You can use the Run Task element to run a second task anywhere within an Advanced Task. When you add a Run Task element, you can set the following options:

- **Run Task** - Select the task to run; this can be any existing task.
- **Wait until this task is complete before continuing** - Select this option to stop the Advanced Task processing until the task selected above has completed.
- **Parameters** - As you can with Traditional Tasks, you can add task parameters that can be accessed by scripts and macros. See the ***Task Information*** (on page 105) page for more information.

Email

An Email action sends an email message to a specified recipient or list of recipients. It is different from a Next Action in that it can run regardless of task results, so can be used anywhere in a task.

An Email action can be configured to run anywhere within a task.

When sending an email, there are four settings to configure:

- **SMTP Host** - The SMTP host to use for sending email. At least one SMTP host must be configured in the Hosts section in order to send an email.
- **AddressTo** - A single email address or a comma-separated list of email addresses to send an email to. You may use ***Macros*** (see "***Macro***" on page 137) in this field.
- **Subject** - Subject of the email message. You may use Macros in this field.
- **Message** - Main body of the email message. You may use Macros in this field.

Delete/Rename Original

In an Advanced Task, you can use the Delete/Rename Original element to either delete the source files, or rename the source files. If you select the Rename option, you can enter a file mask and/or macros to use when renaming the files.

Note: When using the Delete/Rename Originals element, we recommend that you first check that the transfer was successful, as the outcome is not tracked by an Advanced Task. You can add this type of check by adding an If Block and checking for a file error. If there are no file errors, then run the Delete/Rename.

When you add a Delete/Rename Originals element, you can select the following options:

- **Delete original(s)** - Select this option to delete the source files.
- **Rename original(s)** - Select this option and then enter a file name or file mask to use for the rename operation. You can use macros in the file mask. If you select the option to overwrite existing files, if a file of the same name already exists, it will be overwritten. If you do not select this option, and a file of the same name already exists, the original file will be maintained.

Move Commands

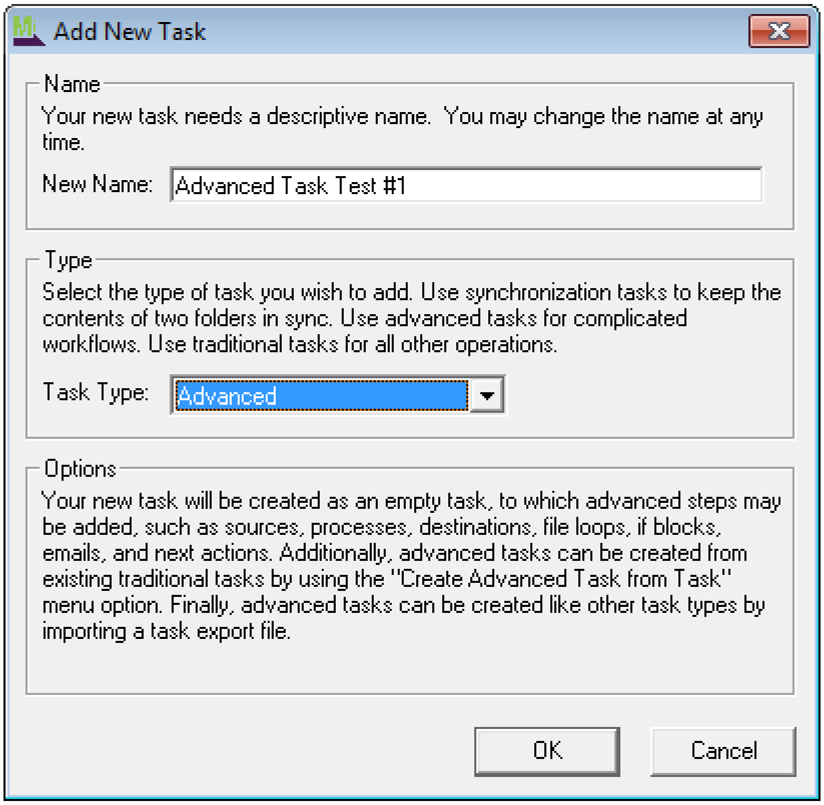
The Move commands provide an easy way to change the location of an element within the task.

- **Move Up** - Moves the selected element up one line. Note that when the preceding element is a File Loop or If Block, using Move Up will place the element within the File Loop or If Block.
- **Move Down** - Moves the selected element down one line. Note that when the following element is a File Loop or If Block, using Move Down will place the element within the File Loop or If Block.
- **Move Top** - Moves the selected element to the top of the task.
- **Move Bottom** - Moves the selected element to the bottom of the task
- **Move to Previous Block** - Moves the selected element to the previous File Loop or If Block.
- **Move to Next Block** - Moves the selected element to the next File Loop or If Block.

Adding a New Advanced Task

This topic describes how to add a new Advanced Task from scratch. There are many possible configurations of an Advanced Task, so this topic presents the general procedure for adding a new Advanced Task. A second way to create an Advanced Task is by ***converting a traditional task*** (on page 322).

1 To add a new advanced task, go to the "Tasks" Tab and click the "Add Task ..." button. The Add New Task dialog opens.



Add New Task

Name

Your new task needs a descriptive name. You may change the name at any time.

New Name: Advanced Task Test #1

Type

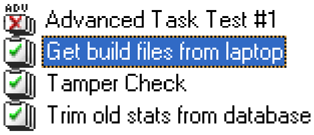
Select the type of task you wish to add. Use synchronization tasks to keep the contents of two folders in sync. Use advanced tasks for complicated workflows. Use traditional tasks for all other operations.

Task Type: Advanced

Options

Your new task will be created as an empty task, to which advanced steps may be added, such as sources, processes, destinations, file loops, if blocks, emails, and next actions. Additionally, advanced tasks can be created from existing traditional tasks by using the "Create Advanced Task from Task" menu option. Finally, advanced tasks can be created like other task types by importing a task export file.

2 Enter a name for the task, select the Advanced Task type, then click OK. The new task is added to the list of tasks (Task tab). This task is marked with a red X to indicate that it cannot yet be run.

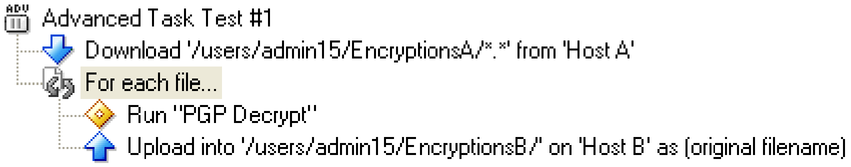


Advanced Task Test #1
Get build files from laptop
Tamper Check
Trim old stats from database

3 To build out the advanced task, right-click the task name and select an element. For more information about the elements used in an advanced task, see the "Right-click menu options" section below.

Note that the order and placement of a task element determines when it is processed. If you use a File Loop, the element needs to be within the File loop, if it is to be processed as part of the loop. The same is true for an If Block. To place an element in a loop or block, you can right-click the loop or block, then add the element. You can also use the various Move commands to move an element within the task.

In the example below, the process and the destination are within the File Loop (shown by indenting the process and destination.



- Advanced Task Test #1
  - Download '/users/admin15/EncryptionsA/*.*' from 'Host A'
  - For each file...
    - Run "PGP Decrypt"
    - Upload into '/users/admin15/EncryptionsB/' on 'Host B' as (original filename)

4 When you have the task structure in place, you can run the task to check that it is working the way you want. We suggest using test data for the first run, then checking the logs to see that the task is working as expected.

Right-click menu options

- **Add Schedule** - A schedule works the same as with a Traditional Task.
- **Add Source** - You can add a source in the same way that you would add it to a Traditional Task. Most of the time, after you add a source, you will add a File Loop to perform actions on each file in the list of source files.
- **Add Process** - A process works much the same as with a Traditional Task. The difference being that a process in an Advanced Task will run where it is located in the task. You will likely place a process within a File Loop to run the process for each source file. The Traditional Task options of "Run Per File" and "Run Once After All Downloads" are not available.
- **Add Destination** - Again, you add a Destination just as you would for a Traditional Task. However, you must put the destination in a File Loop so that it will process all of the files.
- **Add File Loop** - File Loops are used in Advanced Tasks for performing per-file actions like Processes and Destinations. The File Loop will run elements within it on each file in the existing list of source files.
- **Add If Block** - An If Block tests for one or more conditions, for example, for whether any source files exist, or for files of a specified type. In order for an If Block to process each file in a source list, the If Block needs to be within a File Loop.
  - **Add Else If Branch** - Within an If block, you can use an Else If branch to specify a second condition to be applied. For files in the source list that did not meet the preceding If condition, you can test for a different condition, then add a second process and/or destination for these files.
  - **Add Else Branch** - Within an If block, you can use an Else Branch to specify a second action to be run for any files (from the source list) that do not match the preceding If condition. For example, an Else Branch can contain a second process and/or destination.

- **Add Delete/Rename Original** - You can use the Delete/Rename Original element to either delete the source files, or rename the source files. If you select the Rename option, you can enter a file mask and/or macros to use when renaming the files.
- **Add Email** - The Email element can be placed anywhere in the task, including within a File Loop or If Block.
- **Add Run Task** - The Run Task element can run a second task anywhere within an Advanced Task. As with next Actions in Traditional Tasks, you can add task parameters that can be accessed by scripts and macros. See the ***Task Information*** (on page 105) page for more information.
- **Edit commands** - The various Edit commands will open a dialog that lets you make changes to the selected element.
- **Remove commands** - The Remove commands will remove the selected element, deleting it from the task. The Remove File Loop and Remove Entire If Block commands also remove any elements within the loop or block.
- **Move commands** - The ***Move commands*** (on page 319) provide an easy way to change the location of an element within the task.

Converting a Traditional Task

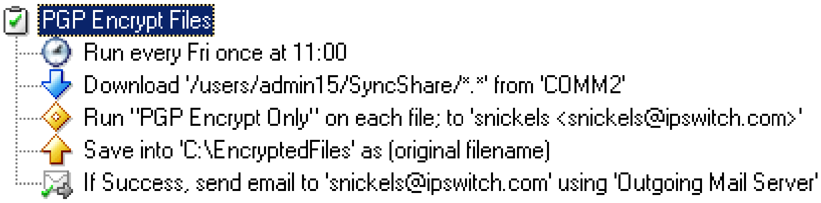
This topic describes how to create an Advanced Task by converting an existing Traditional Task. There are many possible configurations of an Advanced Task, so this topic presents the general procedure for converting to an Advanced Task, and shows an example. You can also ***create a new Advanced Task*** (see "***Adding a New Advanced Task***" on page 320) from scratch.

1. To convert a Traditional Task, go to the "Tasks" Tab, right-click the Traditional Task, then select Create Advanced Task from Traditional. MOVEit Central creates a copy of the Traditional Task and adds it to the Tasks tab. The copy is renamed with the text "Advanced" appended to the original name. This Advanced Task is also disabled. In creating the advanced task, MOVEit Central adds any File Loops and/or If Blocks where appropriate.

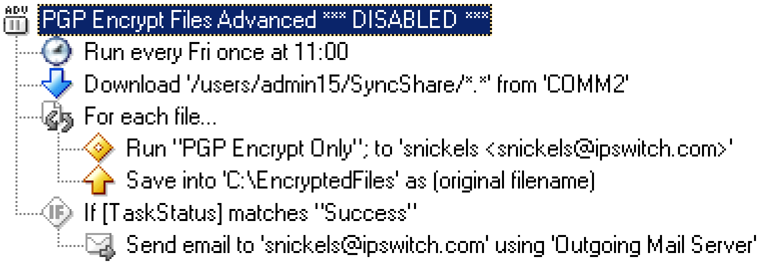
   The converted task should be tested using test data before you use it in production.
2. Use the right-mouse menu to add or remove elements, or to move elements within the task.
3. To enable the task, right-click and select Enable Task.
4. When you have the task structure in place, you can run the task to check that it is working the way you want. We suggest using test data for the first run, then checking the logs to see that the task is working as expected.

Example: Converting a Traditional Task

In the example below, the first image shows a Traditional Task that downloads files from an FTP server, encrypts them using PGP, then saves them to a local directory. Finally, the task sends an email if successful. The second image shows the Advanced Task that results from converting the first task.



```
PGP Encrypt Files
    Run every Fri once at 11:00
    Download '/users/admin15/SyncShare/*.*' from 'COMM2'
    Run "PGP Encrypt Only" on each file; to 'snickels <snickels@ipswitch.com>'
    Save into 'C:\EncryptedFiles' as (original filename)
    If Success, send email to 'snickels@ipswitch.com' using 'Outgoing Mail Server'
```



```
PGP Encrypt Files Advanced *** DISABLED ***
    Run every Fri once at 11:00
    Download '/users/admin15/SyncShare/*.*' from 'COMM2'
    For each file...
        Run "PGP Encrypt Only"; to 'snickels <snickels@ipswitch.com>'
        Save into 'C:\EncryptedFiles' as (original filename)
    If [TaskStatus] matches "Success"
        Send email to 'snickels@ipswitch.com' using 'Outgoing Mail Server'
```

As can be seen, the PGP encryption process and destination are now in a File Loop, and the email Next Action has been converted to an Email element inside an If block which tests for a task status of "Success".

Note: A Traditional Task will track whether a process (such as encryption or decryption) succeeds or fails, and will not complete the transfer if the process fails. When you convert a Traditional Task to an Advanced Task, you need to track the success or failure of a process by adding an If Block that checks for a file error.

PGP Encryption

Overview

PGP ("Pretty Good Privacy") encryption is a popular form of public key file encryption invented by Phil Zimmerman in 1991. Although traditionally associated with email messages, this technology is also used to encrypt files for transfer over public networks like the Internet. Because the term "PGP" has recently become the trademark of a specific PGP vendor, the vendor-neutral term "OpenPGP" is used herein to refer to the original, published, interoperable PGP standard.

Starting with version 3.2.5, MOVEit Central contains a built-in, fully integrated, OpenPGP software module with comprehensive encryption and key management capabilities. These can enable the creation and deletion of public and private keys, the import and export of private keys with other OpenPGP applications, and automatic file encryption, encryption and signing, decryption, and signature-checking by new and existing MOVEit Central tasks.

The OpenPGP software in MOVEit Central has been commercially licensed from ***Didisoft http://www.didisoft.com/net-openpgp/***, which warrants that it is fully interoperable with all other OpenPGP applications, including PGP Command-Line[TM] by PGP Corporation.

Use of the MOVEit Central OpenPGP capabilities is strictly optional. Activation requires a special license key, and commercial use requires payment of a one-time license fee and an annual maintenance fee.

Please use the following links to read more about...

- ***Managing PGP Keys*** (on page 219)
- ***Encrypting PGP Files*** (see "***Encrypting***" on page 326)
- ***Decrypting PGP Files*** (see "***Decrypting***" on page 330)

MOVEit Central is also often used to automate other third-party command-line PGP clients. In a separate document titled "PGPOtherVendors" is complete documentation and a library of pre-tested scripts to automate command-line utilities from GnuPG, Network Associates Command Line and PGP Corp. (Similar command-line clients have also been configured to work with MOVEit Central.) Contact ***MOVEit support*** (***http://www.ipswitchft.com/company/contactsupport.aspx***) for complete details.

(Terminology note: PGP Corporation holds a registered trademark on the term "PGP" and sells OpenPGP products under the name "PGP" so all uses of "PGP" in MOVEit Central and this documentation are to be treated as the common abbreviation of *"OpenPGP" rather than references to PGP Corporation's software except where noted.)*

How Does PGP Work?

When you first install/config a piece of PGP software, the first thing you always do is create a new key pair. This is YOUR key pair (or your company's) and it consists of 1 private key and 1 public key. The private key is immediately password-protected and locked away on your machine. The public key is meant to be distributed to anyone else who needs to exchange PGP-encrypted files with you. (Normally, this key is "exported" to a small "ASCII" file and is often emailed to potential partners as an attachment.)

The second thing you generally do with a piece of PGP software is to import the keys of those people, partners and customers you want to exchange PGP-encrypted files with. Using PGP terminology, keys imported this way are said to be "on your keyring."

Finally, people generally practice exchanging files with PGP a few times before "going into production." To make this happen, the sender encrypts the file with the recipient's public key. (Remember, both sides already have the other's public key.) In addition, the sender may also "sign" the file with the sender's private key. (This provides an element of non-repudiation in a system which has no other method to authenticate the sender, such as email.) The recipient receives the file and decrypts it using the recipient's private key, and may verify the authenticity of the contents using the sender's public key.

Between large organizations where many people are sending files in this manner, PGP key management can quickly get out of hand. (In fact, many customers have opted to use MOVEit DMZ/Central to get out of the "key management business.") However, when used in small doses, PGP can be a useful tool, and MOVEit Central's built-in PGP capabilities help make day-to-day transport of PGP-encrypted files easy.

For a discussion of MOVEit Central's built-in features to generate, import, export, and delete PGP keys, see ***Managing PGP Keys*** (on page 219).

Encrypting

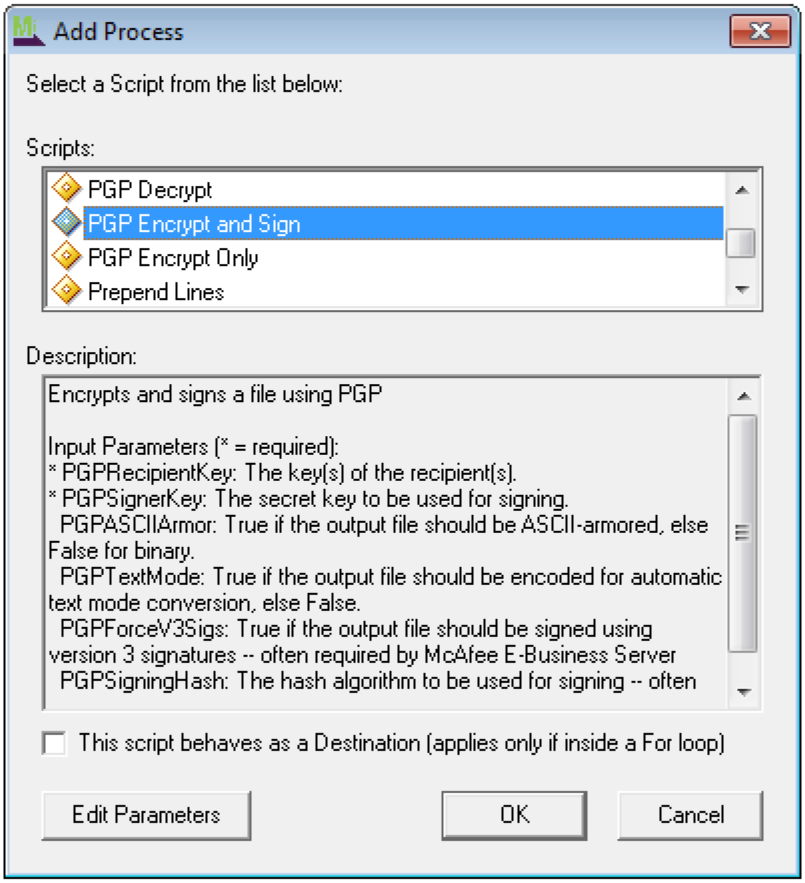
Files are encrypted in MOVEit Central by using Process steps that refer to one of two built-in PGP encryption scripts. To encrypt and digitally sign a file, use the ***"PGP Encrypt and Sign"*** (on page 199) script. To only encrypt a file, use the ***"PGP Encrypt Only"*** (on page 200) script. Though slightly more processor-intensive, it is generally recommended that you use encrypt-and-sign, rather than just encrypt. This allows the recipient to ensure that you really are the sender of the message.

Configuring the Process

To add a process step that encrypts a file before sending it to its destination, proceed as follows:

1 Right-click the task name and choose Add Process...

2 Choose one of the two built-in processes mentioned previously. (In this example, "PGP Encrypt and Sign" is used.)



Select a Script from the list below:

Scripts:

- PGP Decrypt
- PGP Encrypt and Sign
- PGP Encrypt Only
- Prepend Lines

Description:

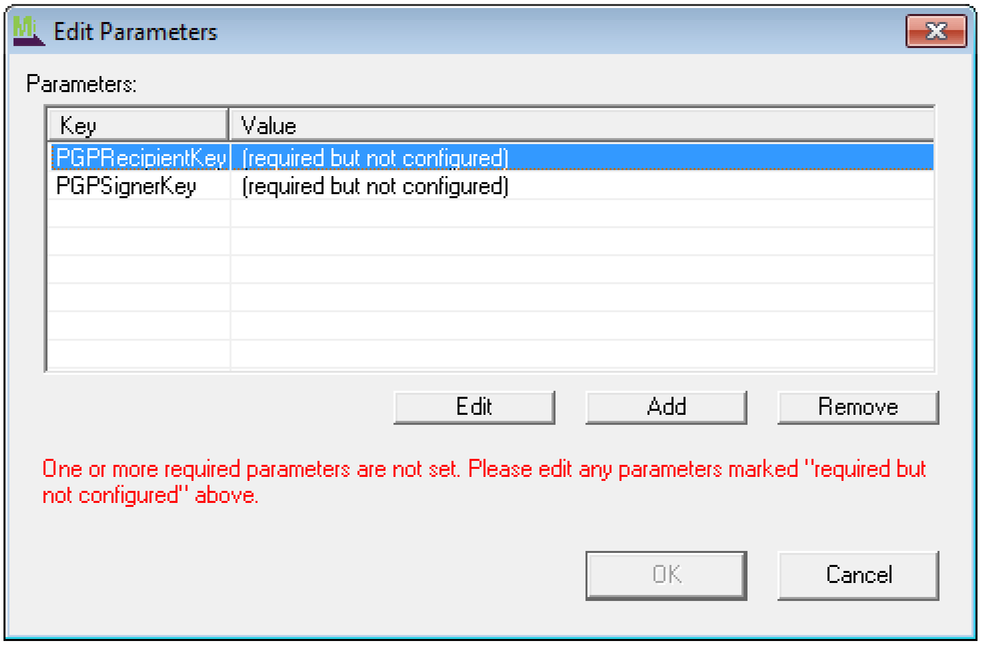
Encrypts and signs a file using PGP

Input Parameters (* = required):
* PGPRecipientKey: The key(s) of the recipient(s).
* PGPSignerKey: The secret key to be used for signing.
  PGPASCIIArmor: True if the output file should be ASCII-armored, else False for binary.
  PGPTextMode: True if the output file should be encoded for automatic text mode conversion, else False.
  PGPForceV3Sigs: True if the output file should be signed using version 3 signatures -- often required by McAfee E-Business Server
  PGPSigningHash: The hash algorithm to be used for signing -- often

□ This script behaves as a Destination (applies only if inside a For loop)

3 Click **OK.**

MOVEit Central Admin will see that the recipient and sender keys are required parameters, so it will bring up the Edit Parameters dialog to prompt for these keys:



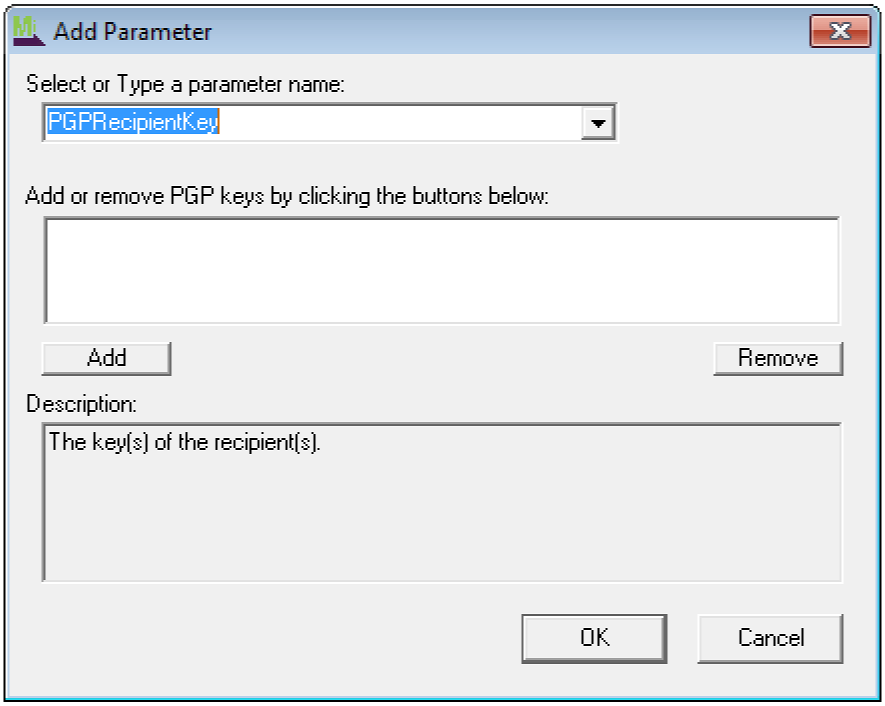
Edit Parameters

Parameters:

Key	Value
PGPRecipientKey	(required but not configured)
PGPSignerKey	(required but not configured)

One or more required parameters are not set. Please edit any parameters marked "required but not configured" above.

4 Double-click the PGP recipient name parameter to get the Add Parameter dialog:



Add Parameter

Select or Type a parameter name: PGPRecipientKey

Add or remove PGP keys by clicking the buttons below:

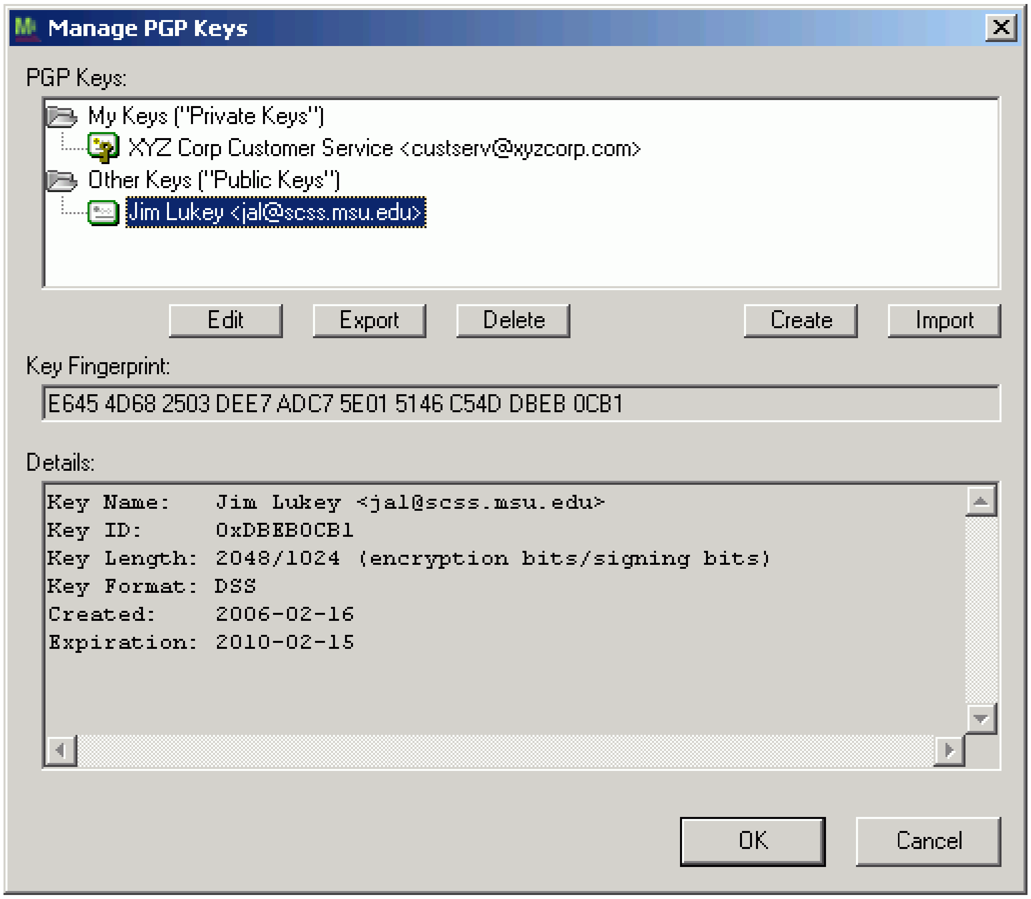
Description: The key(s) of the recipient(s).

5 To add a recipient key, click the "Add" button to get the Select PGP Key dialog.

6 Select a key for the recipient, and click **OK**.

More keys may be added and removed using the buttons.

7 When finished, click **OK** to close the Add Parameter dialog. Recipient key can be selected from either My Keys (if you want to send a file to yourself) or Other Keys.



E645 4D68 2503 DEE7 ADC7 5E01 5146 C54D DBEB 0CB1

```
Key Name:   Jim Lukey <jal@scss.msu.edu>
Key ID:     0xDBEB0CB1
Key Length: 2048/1024 (encryption bits/signing bits)
Key Format: DSS
Created:    2006-02-16
Expiration: 2010-02-15
```

8 Double-click the signer key parameter to select a key to be used to sign the encrypted file. Because only private keys can be used to sign files, you may select only from My Keys.

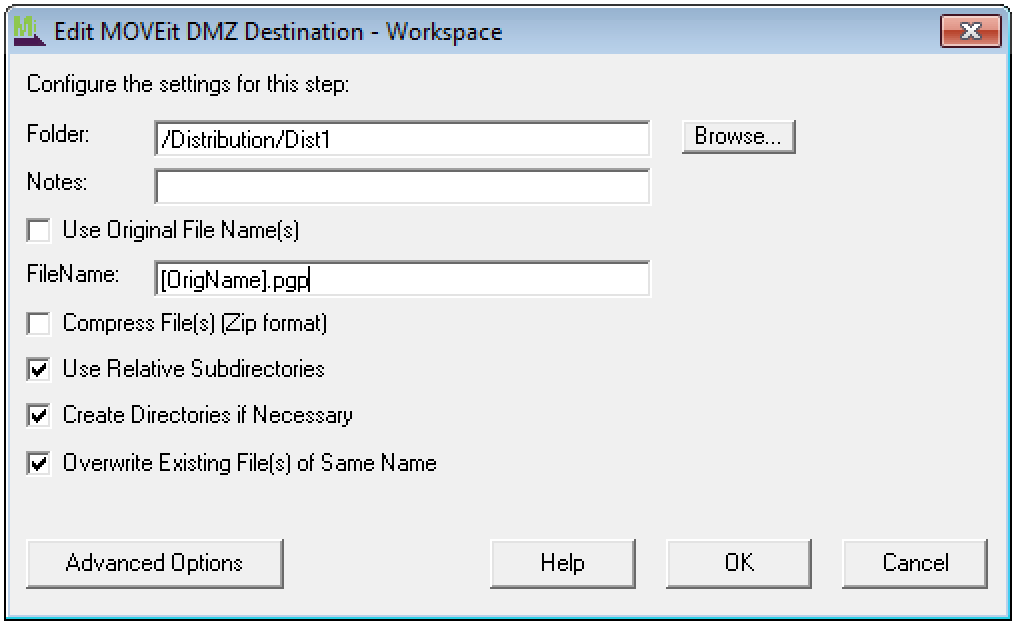
The optional PGPASCIIArmor can be set to True if you want to convert the encrypted file to ASCII format. This increases the size of the file. This option is designed to accommodate file transfer mechanisms that cannot send binary files. However, all of MOVEit Central's transfer protocols properly handle binary files, so there is little reason to select ASCII armoring in MOVEit Central.

Configuring the Destination

By default, MOVEit Central sends files under their original name. You may wish to indicate to your recipient that the file you are sending is PGP-encrypted by appending a ".pgp" suffix to the filename. To do this, edit the task's destination.

1 Uncheck "Use Original File Name(s)."

2 Change the FileName to "[OrigName].pgp".



Edit MOVEit DMZ Destination - Workspace

Configure the settings for this step:

Folder: /Distribution/Dist1

Notes:

□ Use Original File Name(s)

FileName: [OrigName].pgp

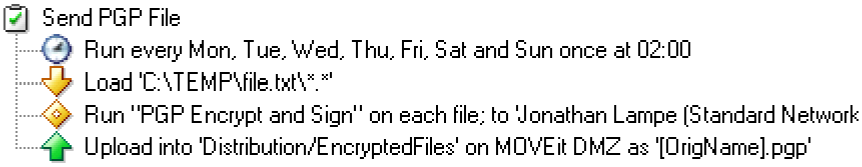
□ Compress File(s) (Zip format)

☑ Use Relative Subdirectories

☑ Create Directories if Necessary

☑ Overwrite Existing File(s) of Same Name

When your task is complete, it should look something like this:



Send PGP File
Run every Mon, Tue, Wed, Thu, Fri, Sat and Sun once at 02:00
Load 'C:\TEMP\file.txt\*.*'
Run "PGP Encrypt and Sign" on each file; to 'Jonathan Lampe (Standard Network
Upload into 'Distribution/EncryptedFiles' on MOVEit DMZ as '[OrigName].pgp'

Using Global Parameters for Keys

It is common for a given site to sign most or all of its outgoing files with the same key. Thus, you may wish to set a global parameter named PGPSignerKey. If you do so, you will not need to set the PGPSignerKey in the Process step of each task that does PGP encryption and signing. You may override the global signer key by specifying it in an individual Process step if desired.

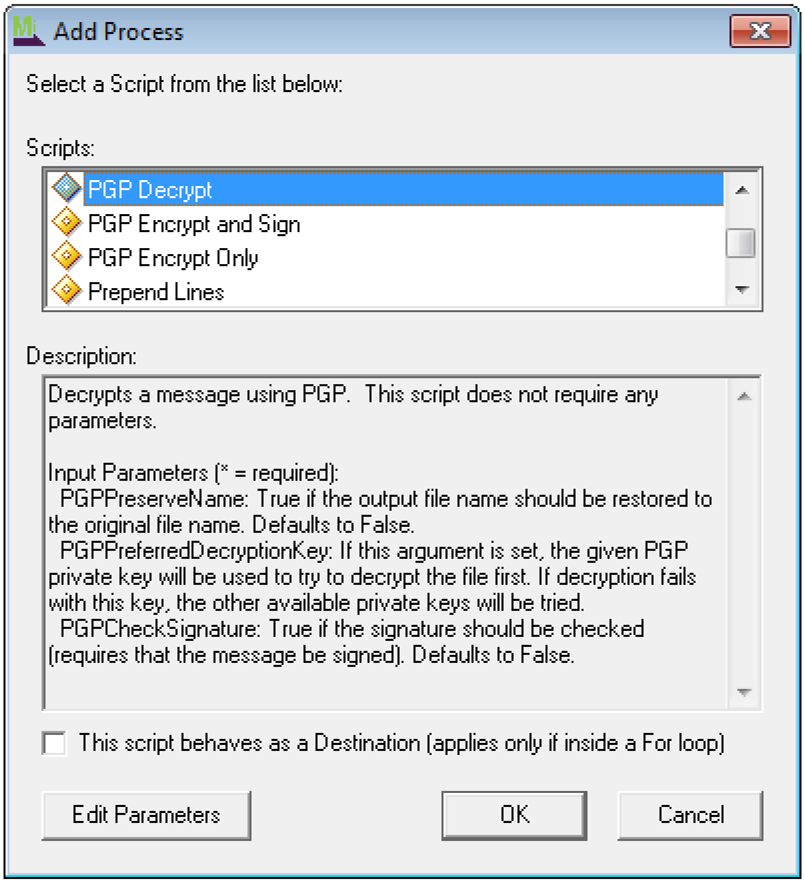
Decrypting

Files are decrypted in MOVEit Central by using Process steps that refer to built-in script "PGP Decrypt". This script does not require any parameters, so configuring the Process step is straightforward.

Configuring the Process

1 To add a process step that decrypts a file before sending it to its destination, right-click the task name and choose Add Process...

2 Choose "PGP Decrypt."



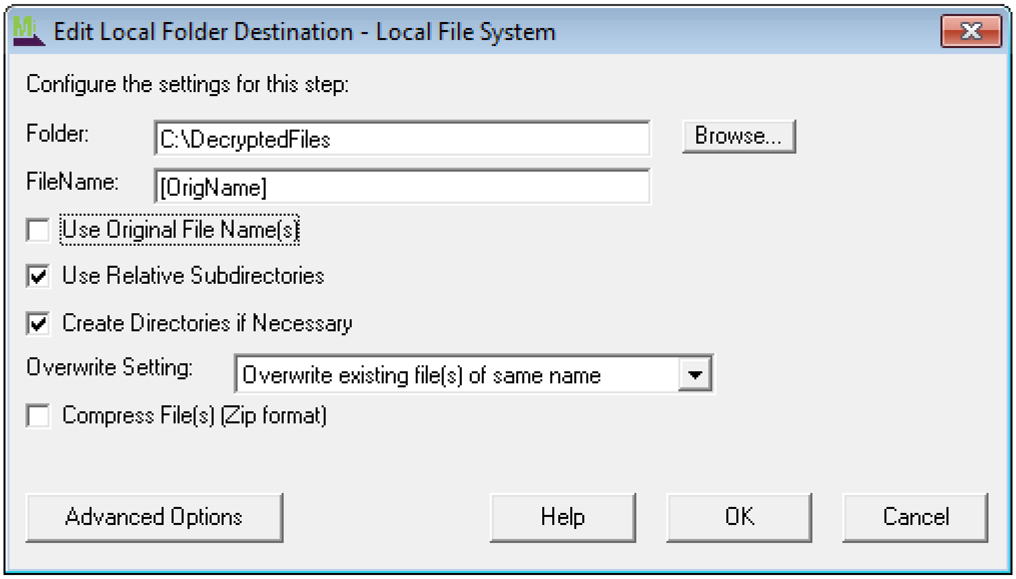
Decrypts a message using PGP. This script does not require any parameters.

Input Parameters (* = required):
PGPPreserveName: True if the output file name should be restored to the original file name. Defaults to False.
PGPPreferredDecryptionKey: If this argument is set, the given PGP private key will be used to try to decrypt the file first. If decryption fails with this key, the other available private keys will be tried.
PGPCheckSignature: True if the signature should be checked (requires that the message be signed). Defaults to False.

☐ This script behaves as a Destination (applies only if inside a For loop)

To decrypt a file, you must have a private key corresponding to the public key that was used to encrypt the file. MOVEit Central will automatically search for a matching key in your PGP keyring. If there is no matching key, the process will fail with an appropriate error message.

3 If the original files had a file extension such as ".pgp" to indicate that they were encrypted, you may wish to save the decrypted version of the file under a name without that extension. You can do this by configuring the destination. Uncheck "Use Original File Name(s)" and enter [OnlyName] as the FileName.



Edit Local Folder Destination - Local File System

Configure the settings for this step:

Folder: C:\DecryptedFiles

FileName: [OrigName]

□ Use Original File Name(s)

☑ Use Relative Subdirectories

☑ Create Directories if Necessary

Overwrite Setting: Overwrite existing file(s) of same name

□ Compress File(s) (Zip format)

S/MIME Email

Overview

S/MIME Email is a standards-based method for sending and receiving secure, verified email messages. It involves using public/private-key based certificates to encrypt and/or sign an email message, so that only the recipient of the email can open it (if encrypted), and the recipient knows with a high degree of certainty who sent the message (if signed).

MOVEit Central ships with S/MIME support, but the actual S/MIME operations occur in one or two pre-qualified scripts. Likewise, S/MIME parameters are expressed as task-level parameters which control qualified scripts rather than source or destination options.

How Does S/MIME Work?

Encrypting, signing, and decrypting S/MIME email messages requires the use of certificates. Certificates are simply public and/or private keys wrapped up in a specific format, so that they can be used together and understood by various programs. The Email Architect tools rely on Microsoft Windows Certificate Stores to contain and manage the various certificates that may be used to create and receive S/MIME emails.

An S/MIME email message can be signed, encrypted, or both. Encrypting a message is done using the public key certificate of the recipient of the message. This ensures that only the recipient can decrypt the message, as the encryption is done so that only the recipient's private key certificate can reverse the encryption. Signing the message is done with the sender's private key certificate, and ensures to the recipient that the sender of the message is who they say they are. A hash of the message is also created by the signing process so that the recipient of the message knows that the message has not been changed since it was written.

As with PGP encryption/decryption, some amount of key exchange is required. In order to encrypt a message to a given recipient, the sender must have a copy of the recipient's public key certificate. This is generally accomplished by having the recipient send the sender a signed S/MIME email message. S/MIME signatures are done in such a way that the sender's public key certificate can be extracted and stored for later use. Most modern email clients, including Microsoft Outlook Express and Mozilla Email Client will automatically recognize a signed message, extract the public key certificate, and store it for examination and later use.

Configuring Certificates

Before MOVEit Central can be used to exchange S/MIME email, the certificates of both the sender and the recipient must be obtained and stored correctly.

Personal Certificate

The personal certificate is used to sign outgoing messages and decrypt incoming messages. Personal certificates can be obtained from most Certificate Authority companies, such as ***Thawte*** (see http://www.thawte.com/html/COMMUNITY/personal/index.html - ***http://www.thawte.com/html/COMMUNITY/personal/index.html***). The personal certificate contains both a private and public key, and is generally given out based on email address.

A personal certificate should be obtained in a PKCS12 format, which allows both the public and private keys to reside in the same password-protected file. This file will usually have an extension of either .pfx, or .p12.

The certificate should be stored in the Personal certificate store of the local user that MOVEit Central is running under. To import the certificate, use the ***SSL Client Certificates*** (on page 217) menu option in MOVEit Central Admin.

Other Certificates

Other certificates are used to encrypt outgoing messages to a specific user. Other certificates are simply the public-key half of the other party's personal certificate, and can obtained from the other party, usually by having the other party send a signed S/MIME message to the current user.

The public-key certificate should be obtained as an X.509 certificate, which may be encoded in a binary format (DER) or a text format (base-64). Both encoding formats are usually stored in a file with an extension of .cer. The certificate should then be stored in the Other People certificate store of the local user that MOVEit Central is running under.

To import the certificate into Windows, use the ***SSL Client Certificates*** (on page 217) menu option in MOVEit Central Admin.

Sending and Receiving

This area describes how to use the built-in S/MIME scripts to send or receive encrypted and/or signed S/MIME email messages with source files as attachments. Before proceeding, you should already have configured the current user's personal certificate, as well as any other party certificates, and set MOVEit Central to run under the proper user code that has access to those certificates.

To send, create a new task and add a source to load the file(s) you wish to send in S/MIME signed and/or encrypted emails. Add a process to your task that references the built-in SMIME Send script, and configure the task parameters accordingly. See the ***SMIME Send*** (on page 205) script for details.

To receive, create a new task and add a destination to process the file(s) that will be received as attachments to incoming S/MIME emails. Add a process to your task that references the built-in SMIME Receive script, and configure the task parameters accordingly. See the ***SMIME Receive*** (on page 204) script for details.

AS1, AS2, AS3 (Enterprise Only)

Overview

Approaching the AS1, AS2 and AS3 protocols (collectively referred to as "ASx" herein) can be a daunting experience for someone without any file transfer experience. On the other hand, someone with an understanding of the transport protocols (SMTP, POP3, HTTP, FTP and SSL/TLS) and/or public-key/private-key encryption (such as SMIME or PGP) should find some familiar ground.

ASx Protocols Provide Similar File Encryption to PGP, SMIME or Other Encrypted File Methods

The ASx protocols use a subset of SMIME ("Secure MIME") to sign and encrypt files. SMIME is a public/private-key encryption technology based on SSL certificates. Many email clients implement SMIME to encrypt and decrypt email messages and attachments, but the ASx implementation of SMIME is specific enough to consider ASx clients and SMIME-enabled email clients incompatible.

Similar public/private-key technology can be found in OpenPGP (which uses simple keys rather than SSL certs to sign and encrypt) and many lesser-known technologies such as "strongly authenticated, encrypted zip files". However, any public/private-key implementation which does not carry an AS1, AS2 or AS3 mark should be considered incompatible with ASx technology because the ASx protocols are quite strict.

ASx Protocols Provide Superior Receipts to PGP, SMIME or Other Encrypted File Methods

The primary advantage of ASx over other public/private key file encryption schemes is that the ASx protocol includes an "MDN" receipt mechanism that proves to the sender that the designated recipient of an ASx message actually received and decrypted the message and verified the identity of the sender.

An MDN ("message disposition notification") receipt is a direct extension of the "delivery receipts" you may have seen or used in your favorite email client. Under AS1 MDNs may be returned via email like any other delivery receipt, but under AS2 and AS3, MDNs may be returned via the HTTP and FTP protocols, respectively.

Regardless of the actual ASx protocol used, each MDN can be cryptographically signed by the recipient of an ASx message and lets the original ASx message sender know the recipient performed three important actions:

- Received the message
- Decrypted the message (if the ASx message was encrypted)
- Validated the sender's signature (if the ASx message was signed)

MDNs also provide cryptographic hash information about the file sent so the sender can verify that the recipient actually received the file the sender thought they sent.

ASx Protocols Provide Standards-Based "Non-Repudiation", "Pedigrees", etc.

In the file transfer arena, "non-repudiation" is a term that means someone can prove who sent a file, who received a file and that the contents of the file were not changed between sender and recipient. In practice, "who sent" and "who received" are questions answered by authentication credentials ranging from usernames and passwords to certificates and keys. The "not changed" question is almost always answered by a cryptographic-quality hash.

However, there is really a fourth piece to the "non-repudiation" puzzle: the record of the "who sent", "who received" and "not changed" itself. When this information is retained in traditional logs, those logs must be made tamper-evident through cryptographic technology (such as that included in MOVEit products). ASx provides an alternate "non-repudiation" technology through standards-based MDNs: each MDN is a "non-repudiation" receipt for a single file.

In MOVEit Central, MDNs are retained in MOVEit Central's tamper-evident audit database from which they may be examined and exported at any time.

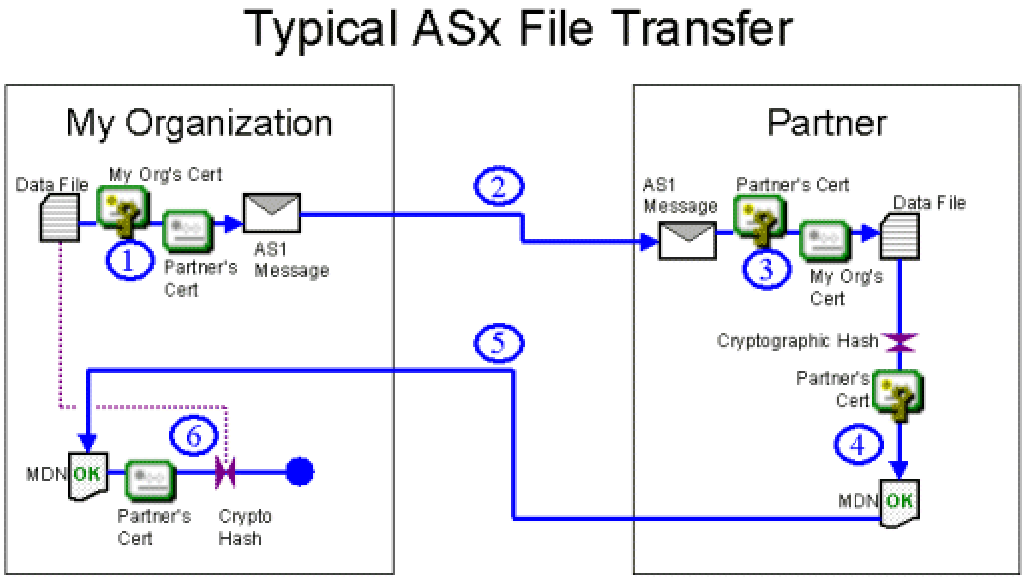
Again, in the file transfer arena, if a series of file transfers all had characteristics of non-repudiation, it used to be common to refer to this situation as "end-to-end file non-repudiation" or an "unbroken chain of non-repudiation." More recently (and thanks largely to new regulatory requirements) this same concept has been described as a "file pedigree".

In either case the end result is the same: if you can prove who sent a file over each hop, who received that file over each hop and that the contents of the file were not changed between original sender and final recipient, you have all the necessary elements to satisfy "end-to-end file non-repudiation", "file pedigree", etc.

Proper implementation of MOVEit's ASx protocols will give you "end-to-end file non-repudiation", "file pedigree", etc.

(Notice that "encryption" is NOT an element of file non-repudiation. Many operational requirements ask for encryption on only part of a file delivery chain because some internal process needs to examine and possible modify a file along the way; MOVEit Central is often involved in this kind of processing step.)

AS1, AS2 and AS3



All of the ASx protocols can:

1. Encrypt a file using a recipient's public SSL certificate and sign the file using the sender's private SSL certificate
2. Specify the type and manner of MDN that the recipient should return
3. Deliver the file to a partner
4. Decrypt a file using a recipient's private SSL certificate and confirm the signature of the sender using the sender's public SSL certificate
5. Create an MDN delivery receipt signed with the recipient's private SSL certificate and containing a cryptographic hash of the file contents in order to prove that the recipient got the unaltered file
6. Return the MDN to the sender
7. Verify the MDN (against the recipient's public SSL certificate and the cryptographic hash) to absolutely prove that the recipient got the file

See also (on their respective "AS1, AS2 and AS3 - The ASx Protocol" pages):

- ***How an AS1 File Transfer Works*** (on page 344)
- ***How an AS2 File Transfer Works*** (on page 350)
- ***How an AS3 File Transfer Works*** (on page 361)

In addition, all of the ASx protocols treat a single file as a single message. Unless you explicitly zip or otherwise bundle multiple files together before an ASx operation, each file will be sent individually and each will be paired up with its own MDN later.

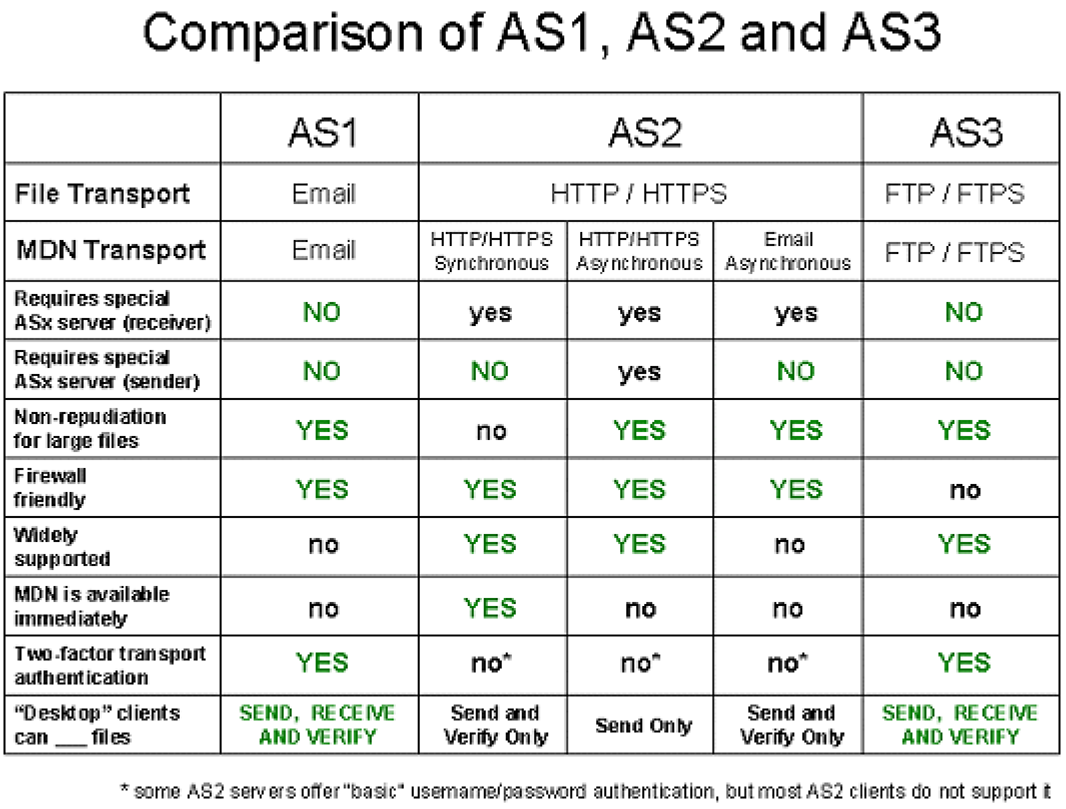
The difference between the AS1, AS2 and AS3 protocols is really the different TRANSPORT protocol each one uses to send messages and receive MDNs.

- AS1: Email
- AS2: HTTP(S)
- AS3: FTP(S)

The MDNs for AS2 transfers come in three varieties. In the synchronous HTTP(S) type, MDNs are transmitted using the same connection as the original file upload. In the asynchronous HTTP(S) type, MDNs are transmitted using a different web upload session. In the asynchronous email type, MDNs are transmitted via email, just as in AS1 MDN transmissions.

AS1 was developed first, followed by AS2 and AS3. AS2 did not completely detach itself from AS1 in one respect: asynchronous email MDNs. Remember that the file sender always controls how its MDN is returned from the recipient.

Some of the primary attributes, advantages and disadvantages of the three ASx protocols are summarized in the table below.



Comparison of AS1, AS2 and AS3

	AS1	AS2			AS3
File Transport	Email	HTTP / HTTPS			FTP / FTPS
MDN Transport	Email	HTTP/HTTPS Synchronous	HTTP/HTTPS Asynchronous	Email Asynchronous	FTP / FTPS
Requires special ASx server (receiver)	NO	yes	yes	yes	NO
Requires special ASx server (sender)	NO	NO	yes	NO	NO
Non-repudiation for large files	YES	no	YES	YES	YES
Firewall friendly	YES	YES	YES	YES	no
Widely supported	no	YES	YES	no	YES
MDN is available immediately	no	YES	no	no	no
Two-factor transport authentication	YES	no*	no*	no*	YES
"Desktop" clients can ___ files	SEND, RECEIVE AND VERIFY	Send and Verify Only	Send Only	Send and Verify Only	SEND, RECEIVE AND VERIFY

* some AS2 servers offer "basic" username/password authentication, but most AS2 clients do not support it

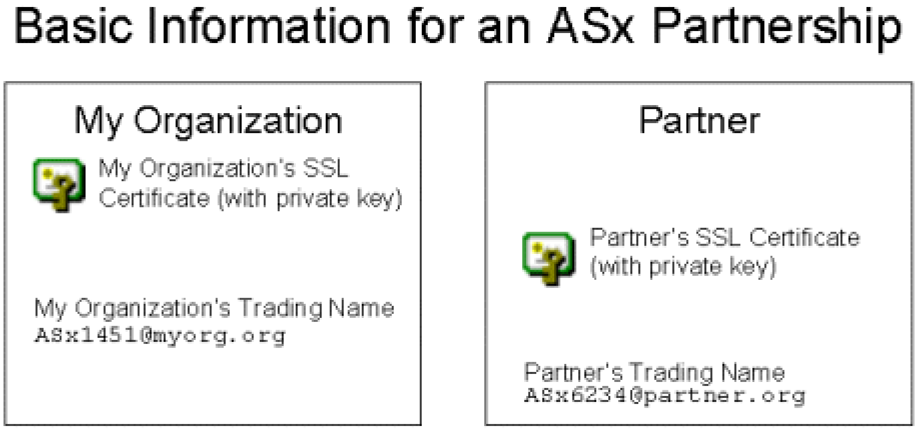
See also (on their respective "AS1, AS2 and AS3 - The ASx Protocol" pages):

- ***Advantages/Disadvantages of AS1*** (on page 349)
- ***Advantages/Disadvantages of AS2*** (on page 360)
- ***Advantages/Disadvantages of AS3*** (on page 367)

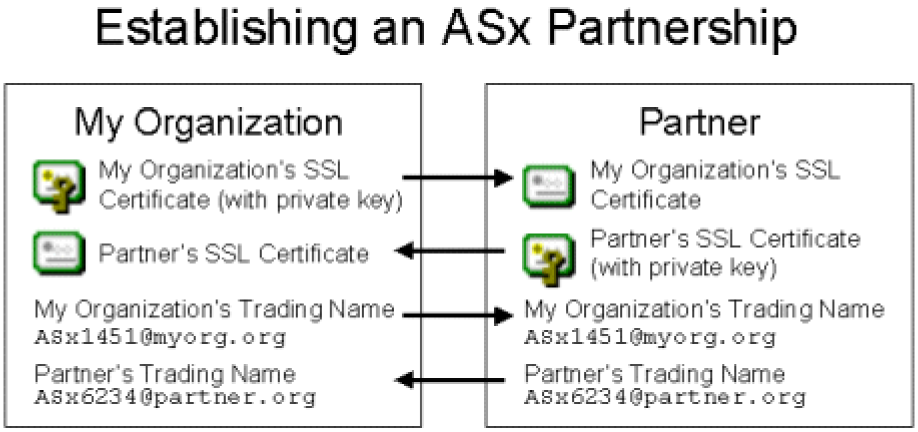
Identifying My Organization and a Partner

ASx transfers are "1-sender, 1-recipient" affairs. Although support for multiple recipients is common in similar encryption schemes such as PGP and SMIME, ASx transfers do not support this concept.

Most ASx products define the two sides in a file exchanges as "my organization" (i.e., you) and "your partner" (i.e., anyone else). Both sides are responsible for coming up with at least two pieces of information: an SSL certificate and their trading partner name. (In practice, one side may provide all of this information.)


Basic Information for an ASx Partnership
My Organization
My Organization's SSL Certificate (with private key)
My Organization's Trading Name
ASx1451@myorg.org
Partner
Partner's SSL Certificate (with private key)
Partner's Trading Name
ASx6234@partner.org

The two sides must exchange their information (minus the private keys on their own SSL certificates) and agree on which certificates and trading names before any ASx file transfers may take place.


Establishing an ASx Partnership
My Organization
My Organization's SSL Certificate (with private key)
Partner's SSL Certificate
My Organization's Trading Name
ASx1451@myorg.org
Partner's Trading Name
ASx6234@partner.org
Partner
My Organization's SSL Certificate
Partner's SSL Certificate (with private key)
My Organization's Trading Name
ASx1451@myorg.org
Partner's Trading Name
ASx6234@partner.org

Each AS1, AS2 or AS3 protocol will also require each side to agree on additional protocol-specific items such as which server to send files too, what credentials to use to authenticate to the server and what flavors of MDNs are supported. Additional information about these specifics is covered in each ASx protocol's discussion.

Optional Elements

If everyone always signed and encrypted their ASx messages, requested signed MDNs and used SSL encryption when transporting ASx messages there would still be plenty of options to configure. However, almost every element discussed so far is really an optional element. Specifically, the following configuration items are among those considered optional in the ASx specifications. (You can probably guess - hint: "Y" - what the best practice values are.)

- Sign message? (Y/N)
- Encrypt message? (Y/N)
- Request MDN? (Y/N)
- If requested, request a signed MDN? (Y/N)
- Use SSL transport encryption while sending the message? (Y/N)
- Use SSL transport encryption while sending the MDN? (Y/N)

Limitations of the ASx Protocols

When used properly, ASx protocols solve a number of traditionally vexing secure file transfer issues, but they do not solve all problems. Some of the cases that require additional thought and planning are described below.

ASx's "Two-Way Handshake" Does Not Let Receiver Know Sender Got MDN

As described above, properly configured MDNs provide a high degree of non-repudiation. The sender knows that the recipient got his/her file, and the recipient knows that he/she is looking at an exact copy of the original content. However, the recipient never knows for sure whether the sender received or verified a requested MDN.

TCP networking uses a "three-way" handshake to avoid a similar problem. The three handshakes in TCP are:

1. Client sends a "SYN" to the server to ask for a connection.
2. Server sends an "ACK" packet back to the client to confirm the connection and also sends an "ACK" to the client to confirm opening the connection.
3. Client sends an "ACK" back to the server to confirm that the client knows the connection is open.

The ASx protocols specify only two of three possible "handshakes": an ASx file recipient never finds out what the file sender thinks of the MDN the file recipient created. This limitation can lead to several issues:

- ASx file recipients must retain MDNs of any ASx message that requested one unless the recipient can absolutely not deliver the MDN.
- "Duplicate posts" are possible if an ASx sender is set to resend files until a valid MDN is received and an ASx recipient believes that it has successfully posted a valid MDN back to a sender's server.

ASx MDNs Represent Handoffs of Responsibility, Not Fitness

The ASx protocols require that MDNs get sent as soon as an ASx message recipient can decrypt, validate the signature of and verify the contents of a data file.

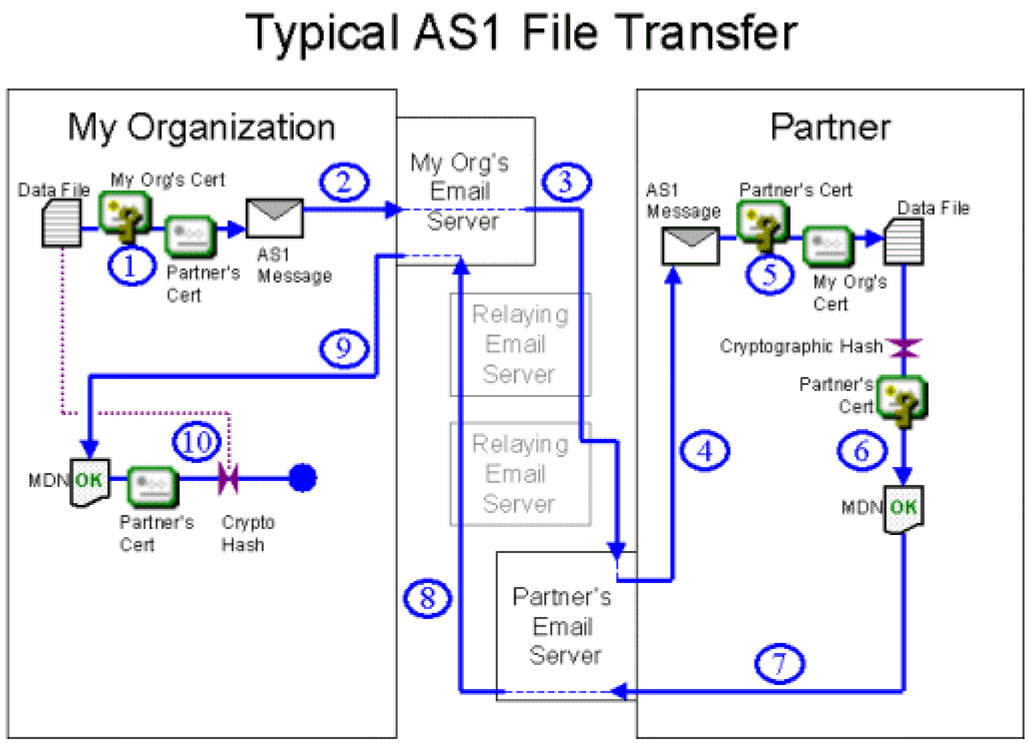
In other words, after an MDN has been successfully sent, it is now the recipient's sole responsibility to not lose the decrypted file (or at least retain and be able to decrypt the original file at will). If internal processing or delivery errors crop up, they are the file recipient's sole responsibility and MDN technology can not be used to notify the sender about any data file format or content problems.

The AS1 Protocol

The AS1 protocol relies wholly on email. It was the first ASx protocol developed and established the signing, encryption and MDN conventions used in later AS2 and AS3 protocols. It is probably the easiest ASx protocol to set up and work with, but it is rarely used.

How an AS1 File Transfer Works

Like any other ASx file transfer, AS1 file transfers typically require both sides of the exchange to trade SSL certificates and specific "trading partner" names before any transfers can take place. AS1 trading partner names must really be email addresses. (AS1 is the only ASx protocol that contains this requirement.)



1 You encrypt a data file with the public key on your partner's SSL certificate and sign it with the private key of your organization's SSL certificate as you bundle everything into an AS1 message. *(Both the encryption and signing steps are optional, but should be used when possible.)*

2 You send the AS1 message to an email server via SMTP. Often, this will be your local email server. *(Credentials and cleartext message headers may be protected with SSL transport in this step.)*

3 If the AS1 message was sent to your local email server, it will now deliver it to your partner's email server using the SMTP protocol. Along the way your AS1 message may traverse several intermediate email servers as it is relayed across the Internet or corporate email infrastructure. *(Cleartext message headers are rarely protected with SSL transport if relay servers are involved.)* This step will be skipped if the AS1 message was delivered directly to your partner's email server in step #2.

4 Your partner will retrieve your AS1 message off your partner's local email server using the POP3 protocol. *(Credentials and cleartext message headers may be protected with SSL transport in this step.)*

5 If the message is encrypted, your partner will decrypt it using the private key on his/her SSL certificate. If the message is signed, your partner will validate your signature using the public key on your SSL certificate. Your partner will also use the contents of the AS1 message to verify that the data file they now have is identical to the data file you sent them.

6 If you requested an MDN delivery receipt for your data file, your partner will calculate a cryptographic hash from the data file they received, sign the hash (and some other information) with the private key on their SSL certificate and create an MDN delivery receipt message. *(The signing step is optional and controlled by the original message sender.)*

7 Your partner will send his/her MDN delivery receipt message to an email server via SMTP. Often, this will be your partner's local email server. *(Credentials and the cleartext MDN delivery receipt message may be protected with SSL transport in this step.)*

8 If the MDN delivery receipt message were sent to your partner's local email server, it will now deliver it to your email server using the SMTP protocol. Along the way your partner's MDN delivery receipt message may traverse several intermediate email servers as it is relayed across the Internet or corporate email infrastructure. *(The cleartext MDN delivery receipt message is rarely protected with SSL transport if relay servers are involved.)* This step will be skipped if the MDN delivery receipt message was delivered directly to your email server in step #7.

9 You will retrieve your partner's MDN delivery receipt message off your local email server using the POP3 protocol. *(Credentials and the cleartext MDN delivery receipt message may be protected with SSL transport in this step.)*

10 You will inspect your partner's MDN delivery receipt message, making sure that you can verify his/her signature using the public key on your partner's SSL certificate and that the cryptographic hash calculated from your partner's copy of your data file matches the same hash calculation from your original data file.

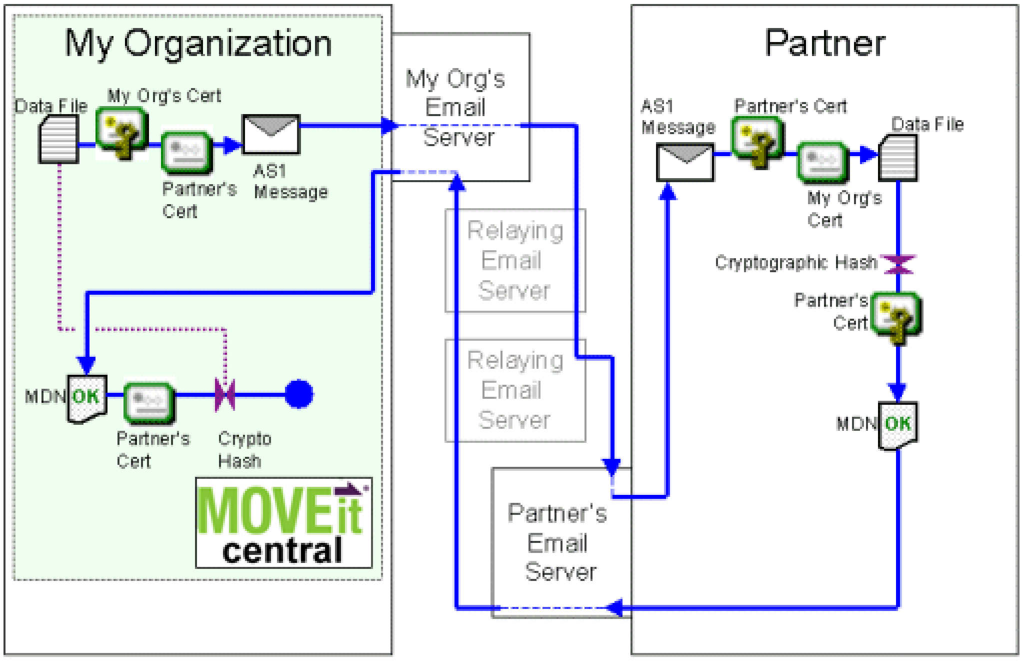
Variations

Direct connections to each mail server - AS1 clients can usually be configured to connect directly to your partner's email server rather than your local email server. Doing so avoids multiple "relay hops" but usually involves some additional firewall configuration.

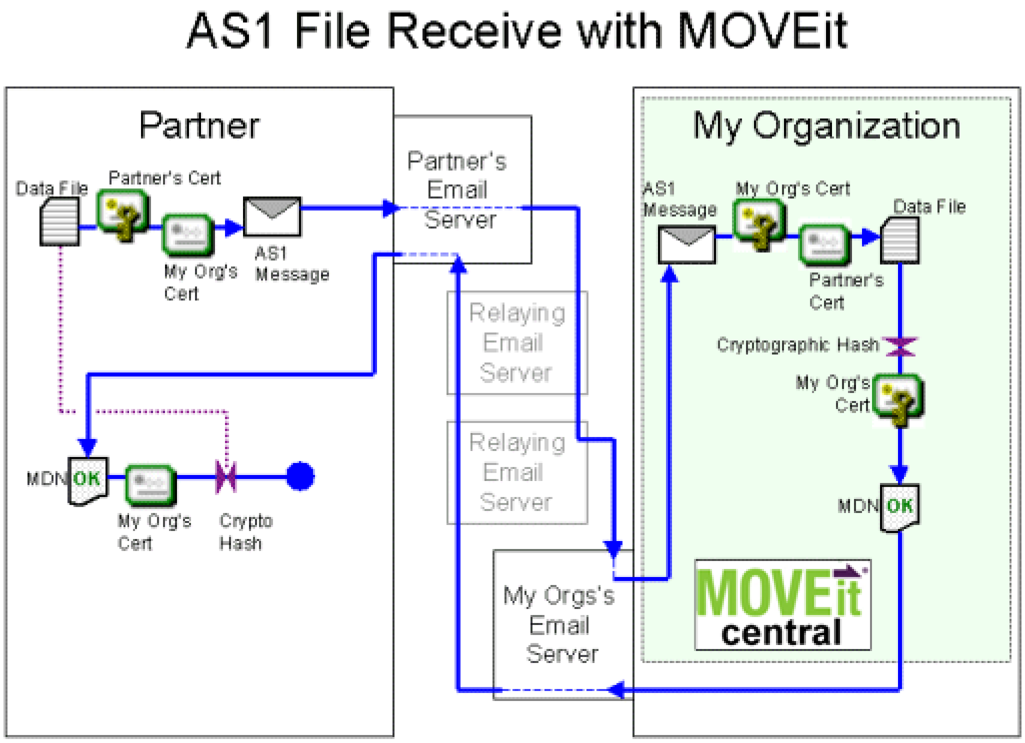
Shared mail server - Your organization and your partner could agree to use different email accounts on the same physical email server, hosted at your data center, your partner's data center, or any other email server in the world. Doing so avoids multiple "relay hops" but usually involves some additional firewall configuration.

MOVEit Implementation of AS1

MOVEit Central is the only MOVEit product required to send or receive files using AS1. In either case files and MDNs are sent through email servers. Because virtually all organizations already have access to an email server, there are no email servers bundled with MOVEit products.



AS1 File Send with MOVEit



See also:

- ***AS1, AS2 and AS3 - Hosts - AS1*** (see "***AS1***" on page 376)
- ***AS1, AS2 and AS3 - Tasks - AS1 - Source*** (on page 389)
- ***AS1, AS2 and AS3 - Tasks - AS1 - Destination*** (on page 390)

Advantages/Disadvantages of AS1 (Compared to AS2 and AS3)

AS1 is the original ASx protocol. All of the file encryption and signing elements of ASx are present in this protocol, so the following discussion really concentrates on the SMTP/POP3 email protocol used to transport AS1 messages and MDNs receipts.

- **Advantage: If you have an AS1 client and access to a email server, you can send and receive AS1 transmissions.** Nearly everyone connected to the Internet these days has access to an email server (you don't need to control or host the email server participating in an AS1 transmission), so AS1 is arguably the easiest of the ASx protocols to install and configure.
- **Advantage: Conceptually, "SMIME messages" and "MDN receipts" fit well with AS1's email-based model.** If you have previously sent encrypted messages (with SMIME or PGP) and/or used delivery receipts, you already have a pretty good feel for the way AS1 works.
- **Advantage: AS1 is firewall-friendly.** If you can send and receive email messages to and from the Internet , you can perform AS1 transfers (even if your only access is to a local email server). However, firewall issues will likely appear if you decide to perform "direct-to-remote-server" AS1 transmissions because most modern firewall rule sets only permit designated email servers to send messages to and from the internal network.
- **Disadvantage: Very few people use AS1.** The ASx protocols really did not gain wide acceptance until AS2 was introduced; most people today use AS2 or AS3 instead of AS1.
- **Disadvantage: Loss of control over email relay hops.** Typically, to send email, you send a message to a local email server. This server turns around and sends your message to another email server. Eventually, your message arrives at the receiver's email server, from which the message receiver can pull your message down and read it. Three common problems with this system of multiple email hops are 1) that transmission time is increased, 2) SSL enforcement is only possible on the first (usually internal) hop and 3) your AS1 encrypted messages and signed MDNs can be copied and retained by any intermediate server. To avoid these problems some people have implemented direct-to-remote-server AS1 transmissions, but these configurations usually require firewall setups that lead them to consider other ASx protocols.
- **Disadvantage: AS1 messages are lumped in with regular email.** In most situations AS1 messages are passed through traditional email servers, which means they are subject to attachment filters, size limits, spam filters, anti-virus filters, server downtime, message queues, spam surges and other email issues that people often do not want to involve in file transfers with their partners. ("Getting our file transmissions off the mail server" is why many companies set up a dedicated secure file transfer infrastructure in the first place.)

See also: ***Comparison of AS1, AS2 and AS3*** (on page 339) on the "AS1, AS2 and AS3 - Overview" page.

The AS2 Protocol

The AS2 protocol is based on HTTP. It was the second ASx protocol developed and uses the same signing, encryption and MDN conventions used in the original AS1 protocol. AS2 is the most popular of the ASx protocols but usually requires more work to set up than AS1 or AS3.

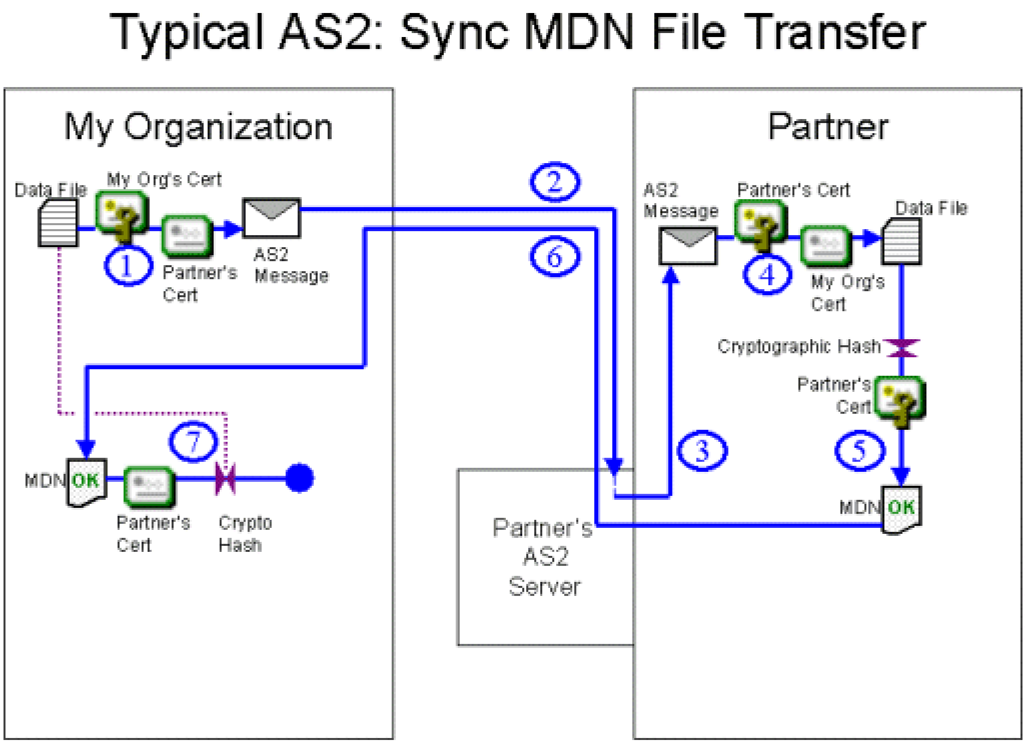
How an AS2 File Transfer Works

Like any other ASx file transfer, AS2 file transfers typically require both sides of the exchange to trade SSL certificates and specific "trading partner" names before any transfers can take place. AS2 trading partner names can be any valid phrase.

Unlike any other ASx file transfer, AS2 file transfers offer several "MDN return" options instead of the traditional options of "yes" or "no". Specifically, the choices are:

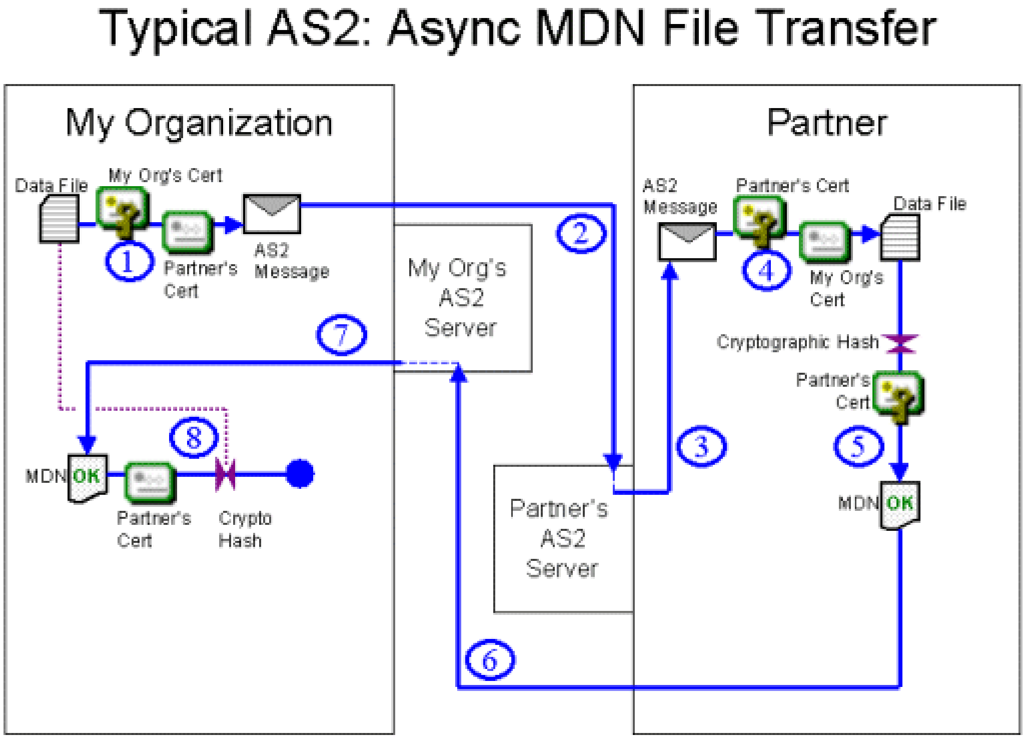
- Return Synchronous MDN via HTTP(S) (a.k.a. "AS2 Sync") - This popular option allows AS2 MDNs to be returned to AS2 message sender clients over the same HTTP connection they used to send the original message. This "MDN while you wait" capability makes "AS2 Sync" transfers the fastest of any type of ASx file transfer, but it also keeps this flavor of MDN request from being used with large files (which may time out in low bandwidth situations).
- Return Asynchronous MDN via HTTP(S) (a.k.a. "AS2 Async") - This popular option allows AS2 MDNs to be returned to the AS2 message sender's server later over a different HTTP connection. This flavor of MDN request is usually used if large files are involved.
- Return (Asynchronous) MDN via Email - This rarely-used option allows AS2 MDNs to be returned to AS2 message senders via email rather than HTTP. Otherwise, it is similar to "AS2 Async (HTTP)".
- Do not return MDN - This option works like it does in any other ASx protocol: the receiver of an AS2 message with this option set simply does not try to return an MDN to the AS2 message sender.

AS2 with Synchronous MDN via HTTP(S)



1. You encrypt a data file with the public key on your partner's SSL certificate and sign it with the private key of your organization's SSL certificate as you bundle everything into an AS2 message. *(Both the encryption and signing steps are optional, but should be used when possible.)*
2. You send the AS2 message to your partner's AS2 server AND WAIT UNTIL YOUR PARTNER RETURNS AN "MDN" RESPONSE. *(Credentials and cleartext message headers may be protected with SSL transport in this step.)*
3. Your partner will retrieve your AS2 message off his/her AS2 server. *(Credentials and cleartext message headers may be protected with SSL transport in this step.)*
4. If the message is encrypted, your partner will decrypt it using the private key on his/her SSL certificate. If the message is signed, your partner will validate your signature using the public key on your SSL certificate. Your partner will also use the contents of the AS2 message to verify that the data file they now have is identical to the data file you sent them.
5. If you requested an MDN delivery receipt for your data file, your partner will calculate a cryptographic hash from the data file they received, sign the hash (and some other information) with the private key on their SSL certificate and create an MDN delivery receipt message. *(The signing step is optional and controlled by the original message sender.)*
6. Your partner will send his/her MDN delivery receipt message back as a response to your still-waiting AS2 "send message and get MDN" request. Once you receive this response (or time out while waiting) you will close your connection. *(Credentials and the cleartext MDN delivery receipt message may be protected with SSL transport in this step.)*
7. You will inspect your partner's MDN delivery receipt message, making sure that you can verify his/her signature using the public key on your partner's SSL certificate and that the cryptographic hash calculated from your partner's copy of your data file matches the same hash calculation from your original data file.

AS2 with Asynchronous MDN via HTTP(S)



1 You encrypt a data file with the public key on your partner's SSL certificate and sign it with the private key of your organization's SSL certificate as you bundle everything into an AS2 message. *(Both the encryption and signing steps are optional, but should be used when possible.)*

2 You send the AS2 message to your partner's AS2 server and close the connection. *(Credentials and cleartext message headers may be protected with SSL transport in this step.)*

3 Your partner will retrieve your AS2 message off his/her AS2 server. *(Credentials and cleartext message headers may be protected with SSL transport in this step.)*

4 If the message is encrypted, your partner will decrypt it using the private key on his/her SSL certificate. If the message is signed, your partner will validate your signature using the public key on your SSL certificate. Your partner will also use the contents of the AS2 message to verify that the data file they now have is identical to the data file you sent them.

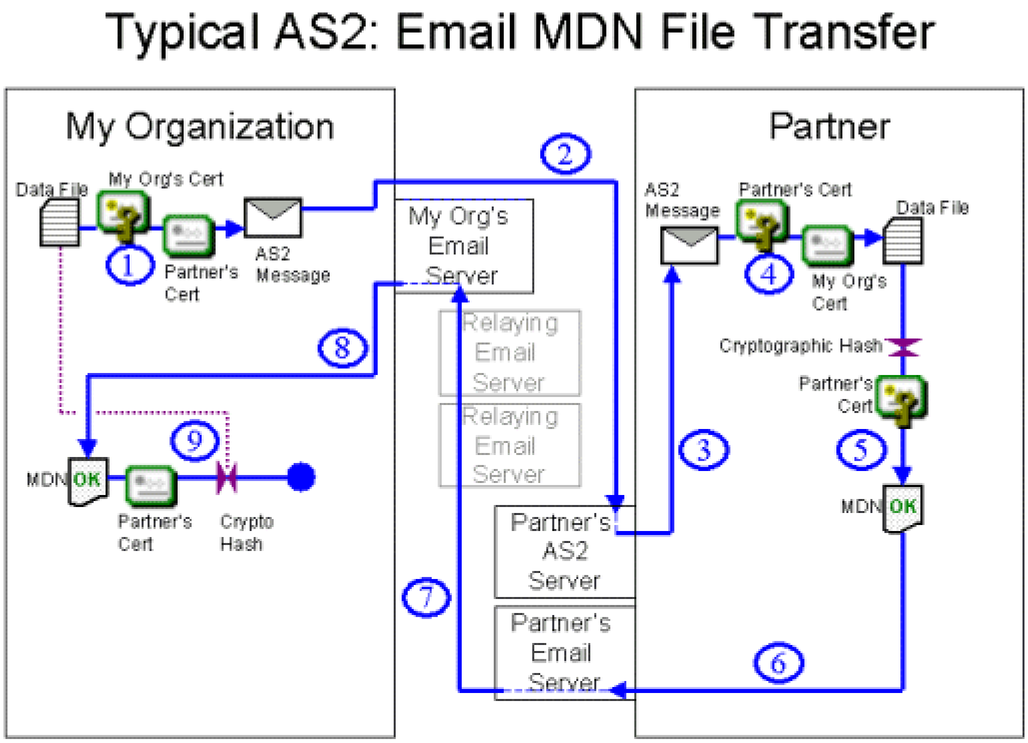
5 If you requested an MDN delivery receipt for your data file, your partner will calculate a cryptographic hash from the data file they received, sign the hash (and some other information) with the private key on their SSL certificate and create an MDN delivery receipt message. *(The signing step is optional and controlled by the original message sender.)*

6 Your partner will send his/her MDN delivery receipt message back by posting it to your AS2 server. *(Credentials and the cleartext MDN delivery receipt message may be protected with SSL transport in this step.)*

7 You will retrieve your partner's MDN delivery receipt message off your AS2 server. *(Credentials and the cleartext MDN delivery receipt message may be protected with SSL transport in this step.)*

8 You will inspect your partner's MDN delivery receipt message, making sure that you can verify his/her signature using the public key on your partner's SSL certificate and that the cryptographic hash calculated from your partner's copy of your data file matches the same hash calculation from your original data file.

AS2 with (Asynchronous) MDN via Email



1 You encrypt a data file with the public key on your partner's SSL certificate and sign it with the private key of your organization's SSL certificate as you bundle everything into an AS2 message. *(Both the encryption and signing steps are optional, but should be used when possible.)*

2 You send the AS2 message to your partner's AS2 server and close the connection. *(Credentials and cleartext message headers may be protected with SSL transport in this step.)*

3 Your partner will retrieve your AS2 message off his/her AS2 server. *(Credentials and cleartext message headers may be protected with SSL transport in this step.)*

4 If the message is encrypted, your partner will decrypt it using the private key on his/her SSL certificate. If the message is signed, your partner will validate your signature using the public key on your SSL certificate. Your partner will also use the contents of the AS2 message to verify that the data file they now have is identical to the data file you sent them.

5 If you requested an MDN delivery receipt for your data file, your partner will calculate a cryptographic hash from the data file they received, sign the hash (and some other information) with the private key on their SSL certificate and create an MDN delivery receipt message. *(The signing step is optional and controlled by the original message sender.)*

6 Your partner will send his/her MDN delivery receipt message to an email server via SMTP. Often, this will be your partner's local email server. *(Credentials and the cleartext MDN delivery receipt message may be protected with SSL transport in this step.)*

7 If the MDN delivery receipt message were sent to your partner's local email server, it will now deliver it to your email server using the SMTP protocol. Along the way your partner's MDN delivery receipt message may traverse several intermediate email servers as it is relayed across the Internet or corporate email infrastructure. *(The cleartext MDN delivery receipt message is rarely protected with SSL transport if relay servers are involved.)* This step will be skipped if the MDN delivery receipt message was delivered directly to your email server in step #6.

8 You will retrieve your partner's MDN delivery receipt message off your local email server using the POP3 protocol. *(Credentials and the cleartext MDN delivery receipt message may be protected with SSL transport in this step.)*

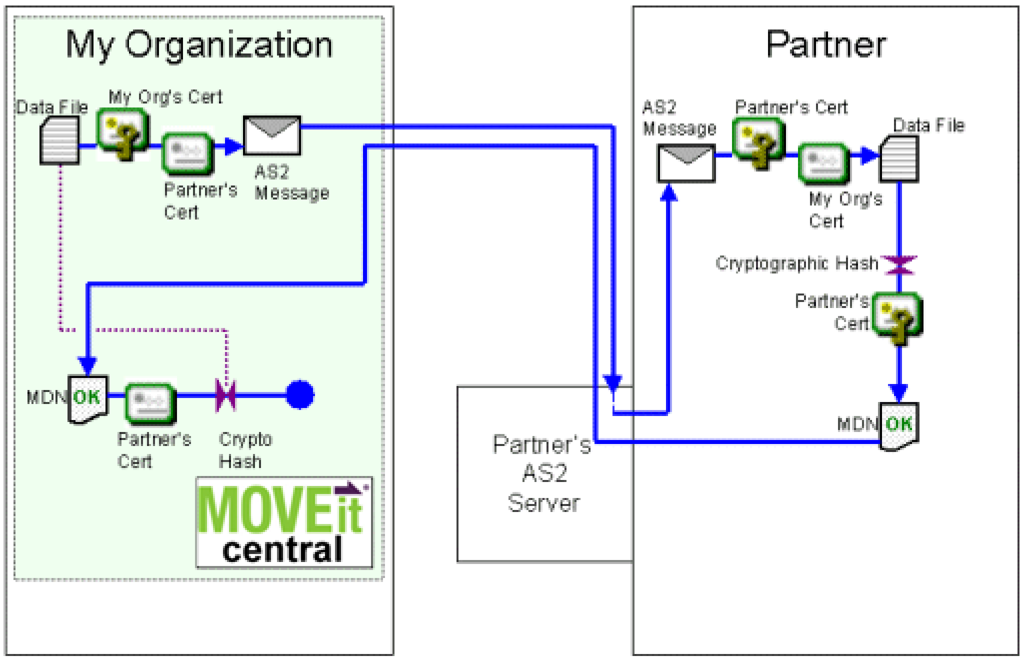
9 You will inspect your partner's MDN delivery receipt message, making sure that you can verify his/her signature using the public key on your partner's SSL certificate and that the cryptographic hash calculated from your partner's copy of your data file matches the same hash calculation from your original data file.

MOVEit Implementation of AS2

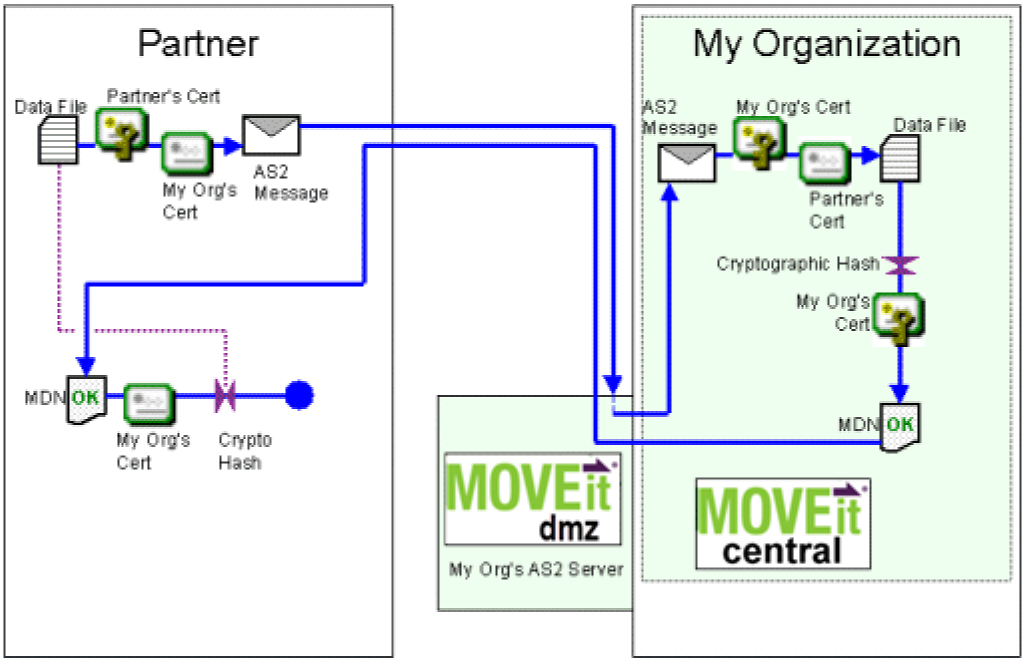
To support AS2 most sites will typically need to deploy both MOVEit Central and MOVEit DMZ. MOVEit Central performs all AS2 encryption, decryption, signing, verification and sending steps, but MOVEit DMZ is required to receive AS2 files or AS2 HTTP-based asynchronous MDNs.

AS2 with Synchronous MDN via HTTP(S)

“AS2: Sync MDN” File Send with MOVEit

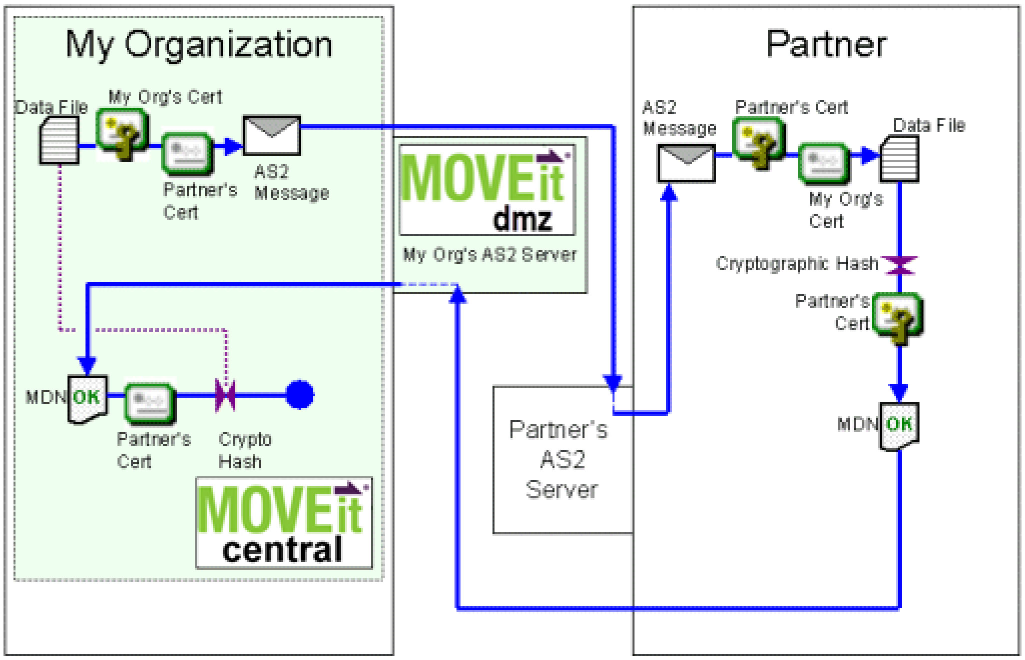


“AS2: Sync MDN” File Receive with MOVEit

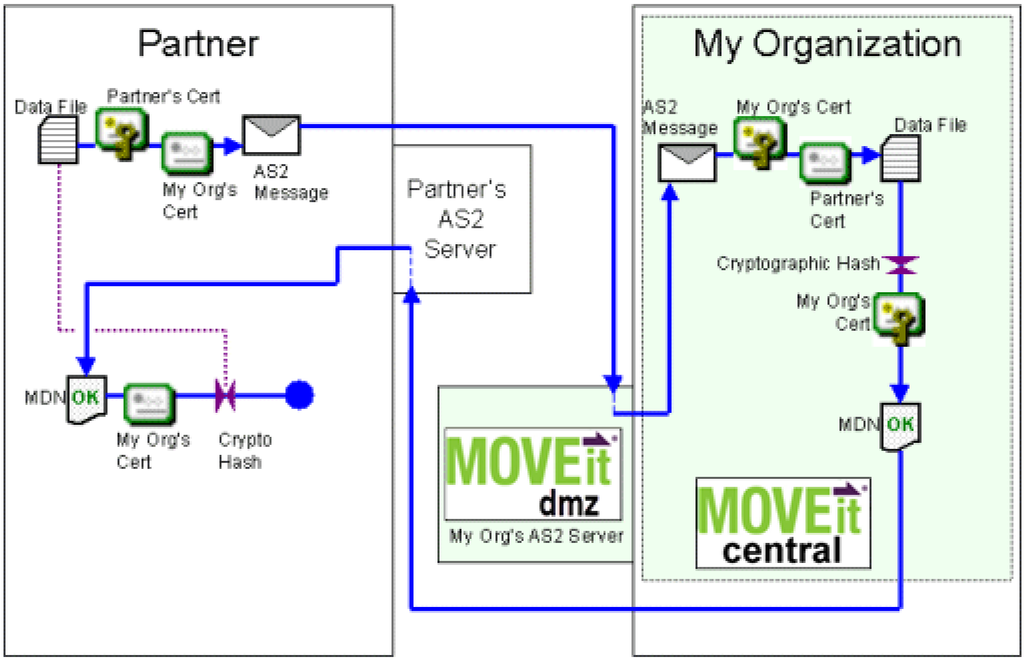


AS2 with Asynchronous MDN via HTTP(S)

"AS2: Async MDN" File Send with MOVEit

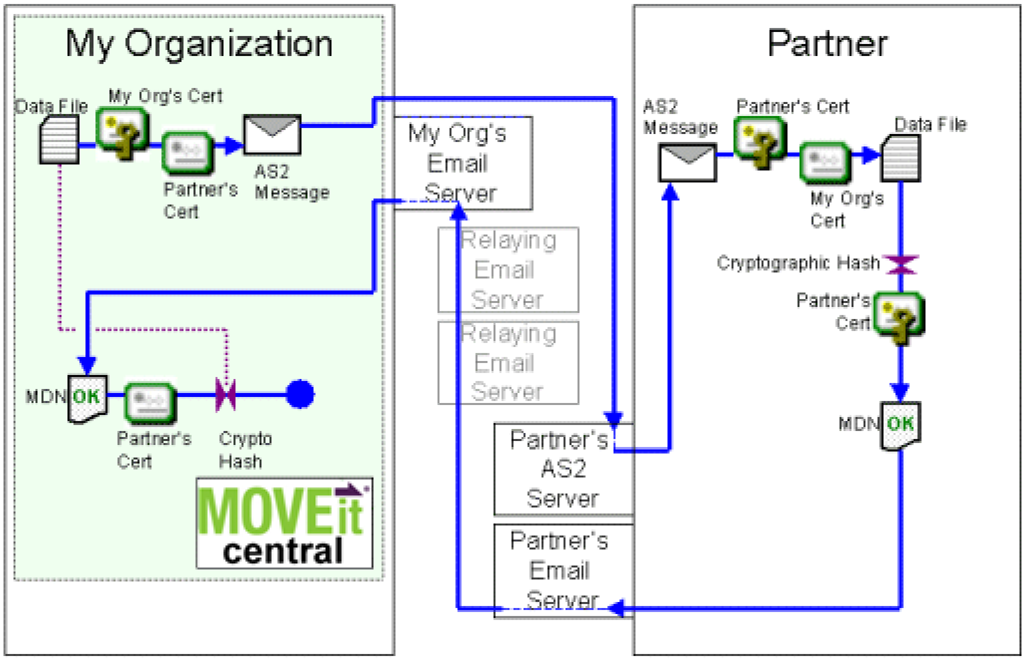


"AS2: Async MDN" File Receive with MOVEit

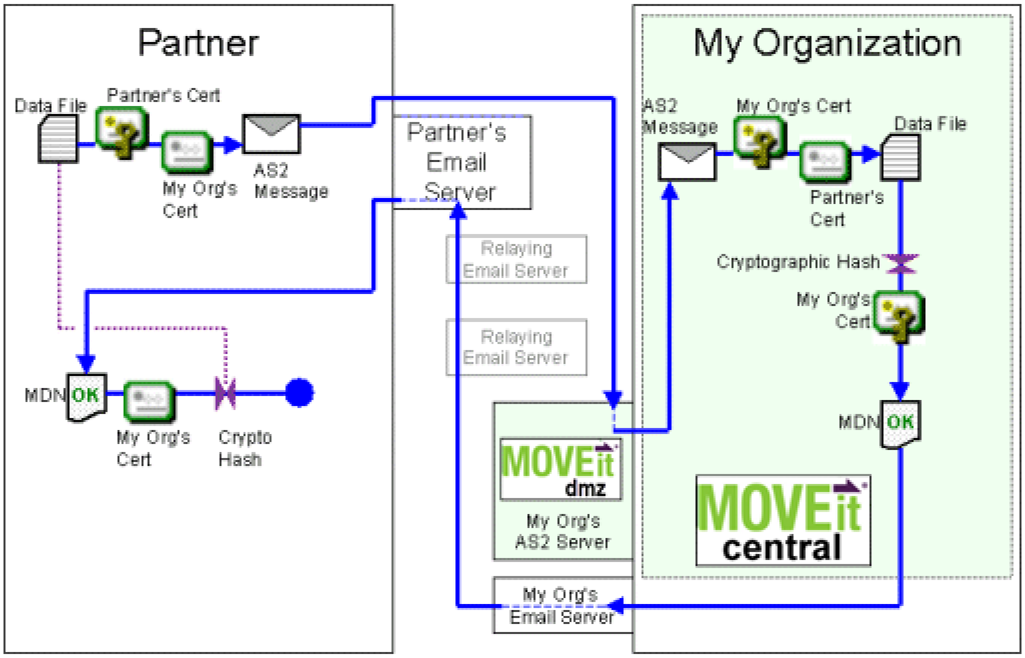


AS2 with (Asynchronous) MDN via Email

“AS2: Email MDN” File Send with MOVEit



“AS2: Email MDN” File Receive with MOVEit



See also:

- ***AS1, AS2 and AS3 - Hosts - AS2*** (see "***AS2***" on page 379)
- ***AS1, AS2 and AS3 - Tasks - AS2 - Source*** (on page 392)
- ***AS1, AS2 and AS3 - Tasks - AS2 - Destination*** (on page 393)

Advantages/Disadvantages of AS2 (Compared to AS1 and AS3)

To an outside observer, AS2 is a strange protocol. ("Why would you want to try sending SMIME-encrypted messages and picking up SMIME-signed delivery receipts over HTTP? Isn't that what email is for?") Its appeal lies largely in the fact that its "sync MDNs" make AS2 the fastest and most discrete of any of the ASx protocols because only one "external" connection between your organization and your partner is required to complete these transactions. (Any other ASx "transfer file and return MDN" operation requires at least two external connections.)

- **Advantage: AS2 is the most popular of the ASx protocols.** Most people who support any one or two of the ASx protocols support AS2. It is a de facto standard in many industries, and an explicit standard in others (e.g., some pharmaceutical file transfer "pedigrees").
- **Advantage: AS2 is firewall-friendly when sending files.** If you can connect to Internet-based web sites from your desktop, you can probably send AS2 files of any size and receive (synchronous-mode) AS2 MDNs for small to medium sized files.
- **Advantage: AS2 is the only ASx protocol that allows the sender to ask for an "immediate" (synchronous) MDN response.** AS2 allows senders to request immediate, "synchronous" MDN's as part of their HTTP file transmission. Synchronous MDN responses are calculated on the fly as soon as the entire file is received and returned as the response to the file transmission over the same HTTP connection. All AS1, AS3 and "asynchronous" AS2 MDNs are expressed as files to be picked up after the original transmission is complete and closed rather than as an immediate response to the current transmission.
- **Disadvantage: Synchronous ("immediate") MDN responses are only appropriate for small files.** Both sides must usually set up an AS2 server if large files are to transferred. AS2 transmissions involving large files can "time out" (with no "I'll get back to you" recourse) if the files sent are large. (The actual value of "large" depends on available bandwidth and timers in AS2 client, AS2 server and any intervening HTTP proxy server.) To handle large files, AS2 asynchronous MDNs may be requested instead, but these may only be requested if the file sender also owns an AS2 server on which the file receiver can post asynchronous MDNs. (In other words, "desktop AS2 clients" can 1) either send and verify small files with a synchronous MDN or 2) send large files without any MDN or verification.)
- **Disadvantage: AS2 requires firewall configuration and deployment of a designated AS2 server when receiving files.** To receive AS2 files, you must set up your own AS2 server (usually in a DMZ network segment) and open up firewall rules that allow remote AS2 clients to connect to your AS2 server. (MOVEit DMZ fills the role of an AS2 server in the MOVEit family.) Neither AS1 nor AS3 require you to host your own server to receive ASx files.

- **Disadvantage: AS2 messages may be subject to HTTP proxy rules.** In most situations AS2 messages are passed through traditional HTTP proxies, which means they are subject to content filters, size limits, server downtime, banned sites, "header" restrictions and other HTTP proxy issues that people may do not want to involve in file transfers with their partners. (In practice, AS2 HTTP proxy issues tend to be less of a hassle than AS1 email server issues, but "header" restrictions are probably an area to keep an eye on because AS2 depends heavily on special headers.)
- **Disadvantage: AS2 has no standard concept of "username" or "password" when posting files.** ("Two-factor authentication" is not standard.) Both AS1 and AS3 support the traditional file transfer concept of providing a username and password before you are allowed to upload files to the server. AS2 does not. (Some AS2 servers may have implemented "basic authentication", but it is not supported in most AS2 clients.)

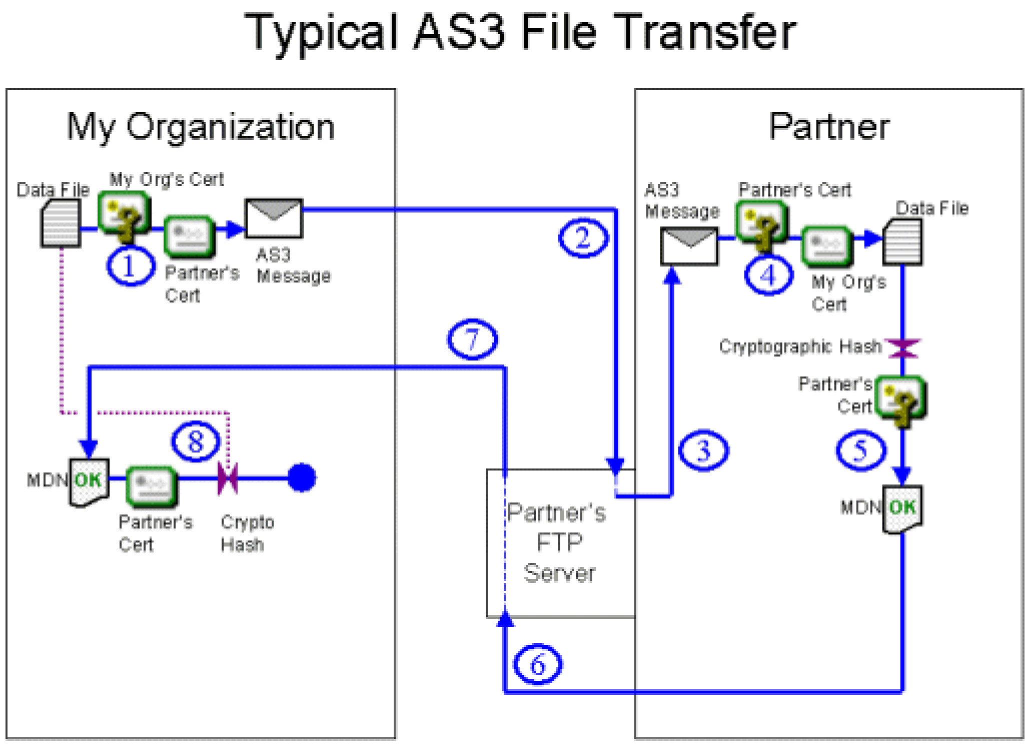
See also: ***Comparison of AS1, AS2 and AS3*** (on page 339) on the "AS1, AS2 and AS3 - Overview" page.

The AS3 Protocol

The AS3 protocol is based on FTP. It is the latest ASx protocol developed and uses the same signing, encryption and MDN conventions used in the original AS1 protocol. After AS1, AS3 is probably the easiest ASx protocol to set up and work with (if firewall issues do not crop up), but AS3 still trails AS2 in terms of general acceptance.

How an AS3 File Transfer Works

Like any other ASx file transfer, AS3 file transfers typically require both sides of the exchange to trade SSL certificates and specific "trading partner" names before any transfers can take place. AS3 trading partner names can be any valid phrase.



1 You encrypt a data file with the public key on your partner's SSL certificate and sign it with the private key of your organization's SSL certificate as you bundle everything into an AS3 message. *(Both the encryption and signing steps are optional, but should be used when possible.)*

2 You send the AS3 message to an FTP server. This could be your FTP server, your partner's FTP server or a hosted FTP server somewhere else. *(Credentials and cleartext message headers may be protected with SSL transport in this step.)*

3 Your partner will retrieve your AS3 message off the same FTP server. *(Credentials and cleartext message headers may be protected with SSL transport in this step.)*

4 If the message is encrypted, your partner will decrypt it using the private key on his/her SSL certificate. If the message is signed, your partner will validate your signature using the public key on your SSL certificate. Your partner will also use the contents of the AS3 message to verify that the data file they now have is identical to the data file you sent them.

5 If you requested an MDN delivery receipt for your data file, your partner will calculate a cryptographic hash from the data file they received, sign the hash (and some other information) with the private key on their SSL certificate and create an MDN delivery receipt message. *(The signing step is optional and controlled by the original message sender.)*

6. Your partner will send his/her MDN delivery receipt message back to the same FTP server the original AS3 message traveled through, though perhaps in a different folder or bearing a different file name. *(Credentials and the cleartext MDN delivery receipt message may be protected with SSL transport in this step.)*
7. You will retrieve your partner's MDN delivery receipt message off the same FTP server. *(Credentials and the cleartext MDN delivery receipt message may be protected with SSL transport in this step.)*
8. You will inspect your partner's MDN delivery receipt message, making sure that you can verify his/her signature using the public key on your partner's SSL certificate and that the cryptographic hash calculated from your partner's copy of your data file matches the same hash calculation from your original data file.

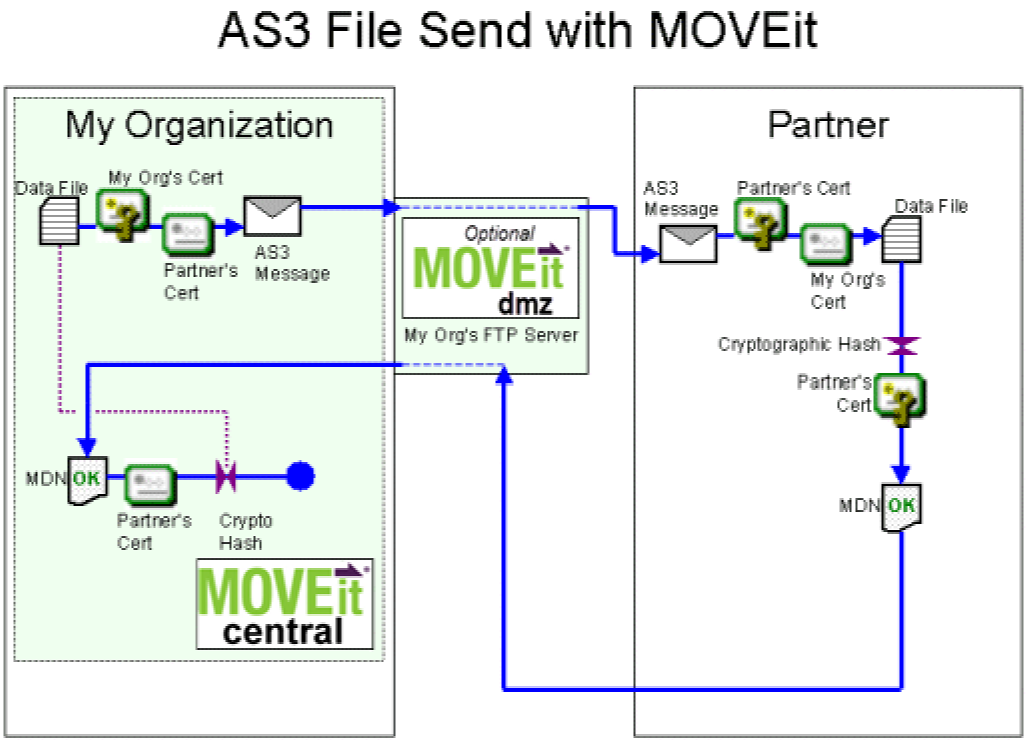
Variations

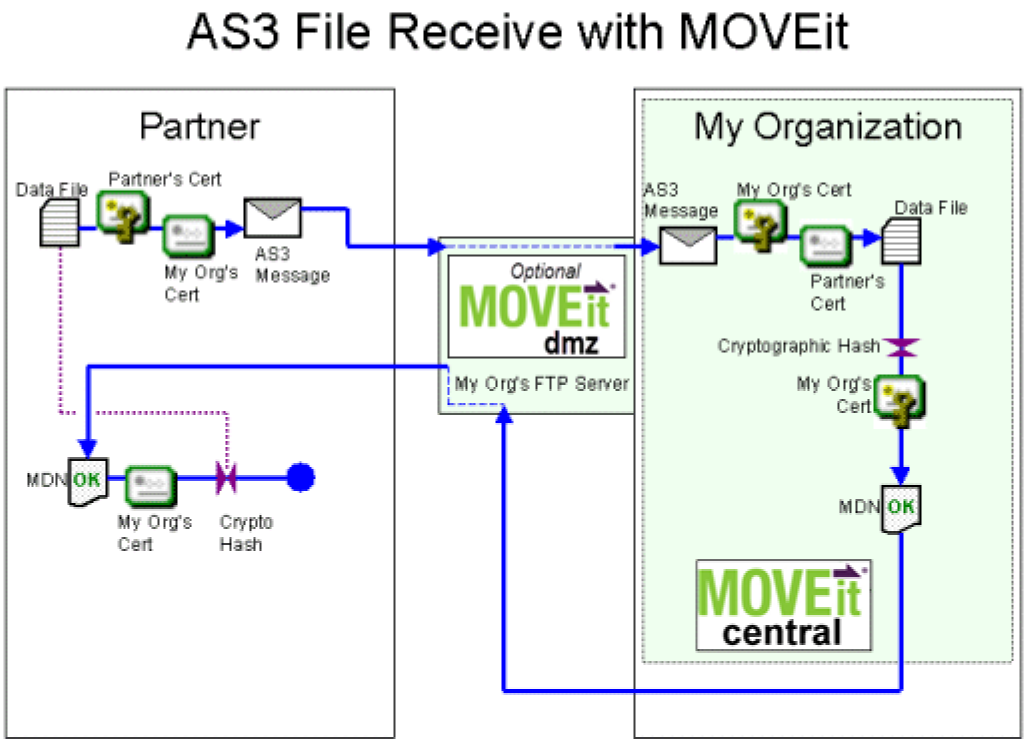
FTP Server Location - The FTP server used in an AS3 transfer could be your FTP server, your partner's FTP server or a hosted FTP server somewhere else. If you have control over the FTP server, we recommend deploying/using a ***MOVEit DMZ FTP server*** (on page 368).

MOVEit Implementation of AS3

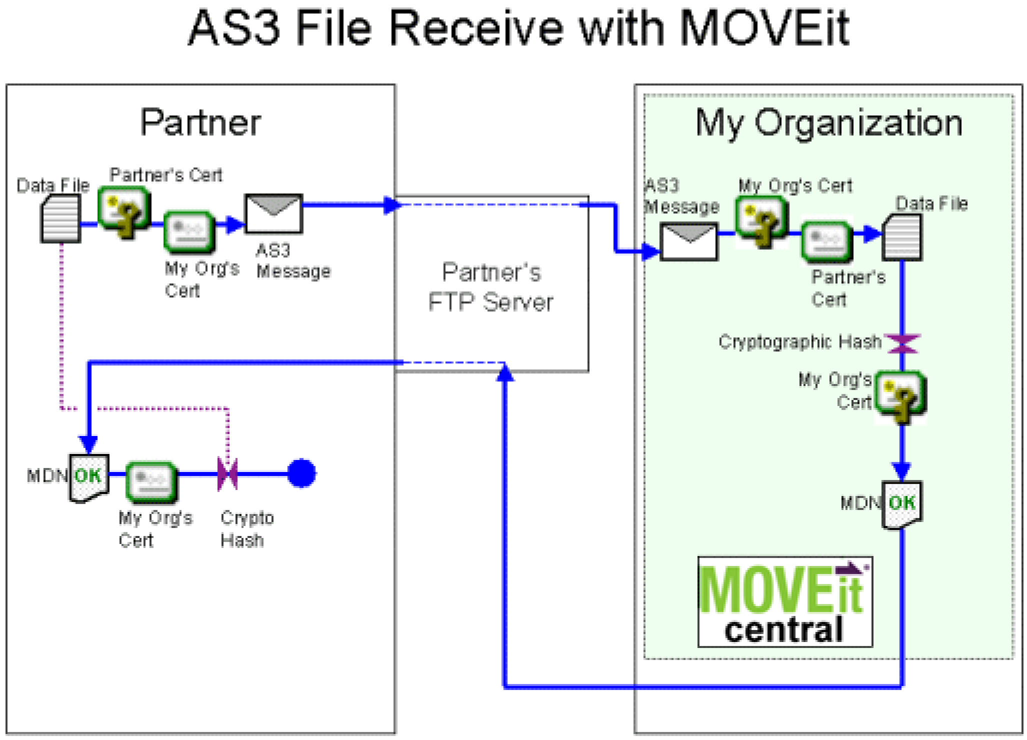
MOVEit Central is the only MOVEit product required to send or receive files using AS1. In either case files and MDNs are sent through FTP servers, and we recommend deploying/using a ***MOVEit DMZ FTP server*** (on page 368) when possible.

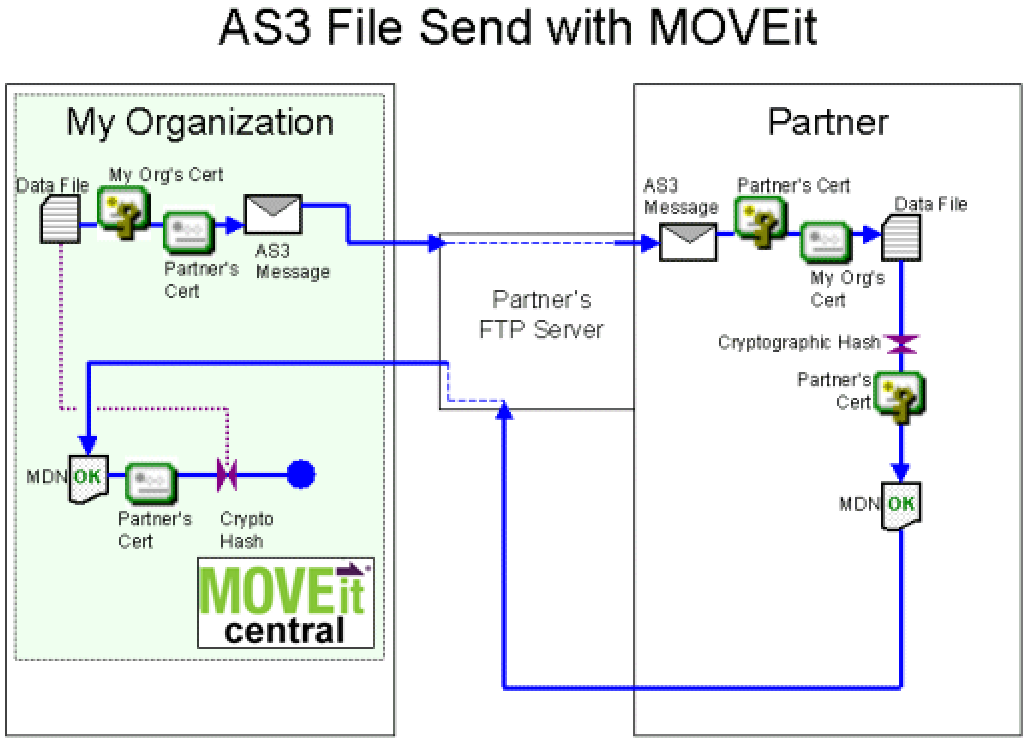
...Using Your FTP Server




AS3 File Receive with MOVEit
Partner
Data File
Partner's Cert
My Org's Cert
AS3 Message
MDN
OK
My Org's Cert
Crypto Hash
Optional
MOVEit
dmz
My Org's FTP Server
My Organization
AS3 Message
My Org's Cert
Data File
Partner's Cert
Cryptographic Hash
My Org's Cert
MDN
OK
MOVEit
central

...Using Your Partner's FTP Server (Or a Hosted FTP Server)





See also:

- ***AS1, AS2 and AS3 - Hosts - AS3*** (see "***AS3***" on page 387)
- ***AS1, AS2 and AS3 - Tasks - AS3 - Source*** (on page 395)
- ***AS1, AS2 and AS3 - Tasks - AS3 - Destination*** (on page 397)

Advantages/Disadvantages of AS3 (Compared to AS1 and AS2)

AS3 was developed to add ASx file transfer capabilities to the well-established FTP/SSL ("FTPS") protocol. Also, using FTP as a transport rather than HTTP seemed to address the "no standard regarding username/password" limitation of AS2: most FTP servers already require username/password. The AS3 protocol is generally recognized by various industries as the "next" ASx protocol, but movement toward AS3 from established AS2 users has not been rapid.

- **Advantage: If you have an AS3 client and access to an FTP server, you can send and receive AS3 transmissions.** You do not need to control or host the FTP server participating in an AS3 transmission, so AS3 ranks just behind AS1 in terms of easiest ASx protocols to install and configure as long as firewall issues are not much of a concern.
- **Disadvantage: AS3 has frequent firewall issues.** AS3 is built on the FTP/SSL protocol, one of the most firewall-unfriendly protocols in use today. Some of the common issues involving FTP/SSL involve NAT translation, multiple data ports and improper translation of FTP commands by intervening firewalls. (Some people look for SSH and/or HTTP file transfer solutions specifically to avoid reoccurring FTP/SSL firewall issues; MOVEit products offer several tactical solutions for various FTP/SSL issues in terms of features and support.)
- **Disadvantage: No AS3 transmission mode is as fast as AS2 "synchronous MDN" transfers.** This is likely the issue that keeps established many ASx players from moving from AS2 to AS3. When AS2 senders request on-the-fly "synchronous MDNs" for their small file transfers (such as part orders), AS2 is by far the fastest ASx protocol. The AS3 protocol does not support similar MDN-on-the-fly capabilities.

See also: ***Comparison of AS1, AS2 and AS3*** (on page 339) on the "AS1, AS2 and AS3 - Overview" page.

MOVEit Implementation

The MOVEit product family implements a complete AS1, AS2 and AS3 file transfer solution. MOVEit products can be used to send and receive files using any of these three protocols.

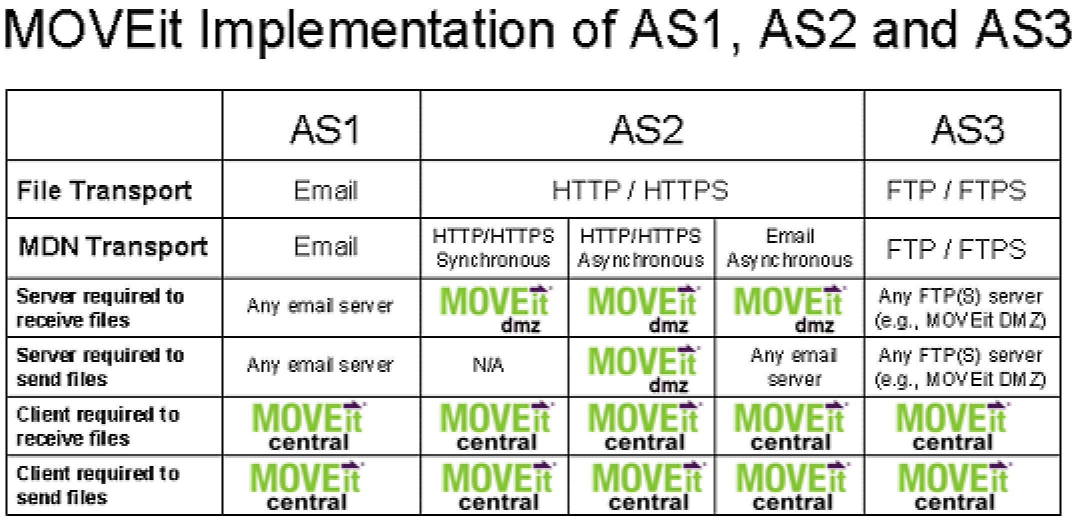
Different combinations of MOVEit products are required to implement the different protocols:

- AS1: MOVEit Central is the only MOVEit product required to implement AS1. (However, access to an email server must also be available.)
- AS2: MOVEit Central and MOVEit DMZ are both required to implement AS2. (MOVEit DMZ is MOVEit Central's AS2 server for purposes of receiving AS2 messages and MDNs.)
- AS3: MOVEit Central is the only MOVEit product required to implement AS3. (Access to an FTP(S) server must also be available; for security or operational reasons you may want to make this server a MOVEit DMZ FTPS server.)

There are a few unusual exceptions to these rules:

- You can use MOVEit DMZ without MOVEit Central to house AS3 messages and AS3 MDNs. However, MOVEit DMZ cannot encrypt, sign or verify MDN files; it simply stores, protects access to and logs access to them securely.
- You can use MOVEit Central without MOVEit DMZ to send files as AS2 messages if synchronous MDNs and email MDNs are the only types of MDNs ever requested. (MOVEit Central cannot receive AS2 files or HTTP-based asynchronous MDNs without MOVEit DMZ.)

The following table summarizes the roles MOVEit products play in providing AS1, AS2 and AS3 services.



MOVEit Implementation of AS1, AS2 and AS3

	AS1	AS2			AS3
File Transport	Email	HTTP / HTTPS			FTP / FTPS
MDN Transport	Email	HTTP/HTTPS Synchronous	HTTP/HTTPS Asynchronous	Email Asynchronous	FTP / FTPS
Server required to receive files	Any email server	MOVEit dmz	MOVEit dmz	MOVEit dmz	Any FTP(S) server (e.g., MOVEit DMZ)
Server required to send files	Any email server	N/A	MOVEit dmz	Any email server	Any FTP(S) server (e.g., MOVEit DMZ)
Client required to receive files	MOVEit central	MOVEit central	MOVEit central	MOVEit central	MOVEit central
Client required to send files	MOVEit central	MOVEit central	MOVEit central	MOVEit central	MOVEit central

See also (on their respective "AS1, AS2 and AS3 - The ASx Protocol" pages):

- ***MOVEit Implementation of AS1*** (on page 347)
- ***MOVEit Implementation of AS2*** (on page 356)
- ***MOVEit Implementation of AS3*** (on page 364)

Drummond "eBusinessReady" Certification

MOVEit DMZ supports any AS2 client that has been "Drummond" or "eBusinessReady" certified; the software MOVEit DMZ uses to handle incoming AS2 files and MDNs has itself been certified "eBusinessReady" under a program now managed by Drummond.

Why MOVEit DMZ is best choice for AS3

MOVEit DMZ has been able to participate in AS3 transmissions as a secure FTP server for years. Traditionally, people have thought that any FTP server with basic security features such as SSL with client certificate authentication could be used in AS3 transmissions. However, operational experience and security best practices have led many to higher expectations of their AS3 FTP server.

The MDN response files returned to AS3 file senders and used for non-repudiation can be signed, but are never encrypted. To protect these important files from tampering or unauthorized view, MOVEit DMZ offers its own built-in FIPS-validated encryption and cryptographic file integrity checks while at rest and in transit.

The FTP protocol can be tricky to implement across firewalls and NAT when SSL is introduced. To deal with these challenges, MOVEit DMZ offers comprehensive, remote-readable protocol logs and features that handle almost every possible FTP over SSL or NAT configuration. Three of the technologies MOVEit DMZ uses to avoid FTP firewall problems include a configuration of limited passive server port ranges (that has been widely copied in the industry since it was introduced in MOVEit DMZ), explicit configuration of NAT and a recent technology called "Clear Command Channel" (CCC).

Finally, the auditing facility in MOVEit DMZ can be used to help complete AS3 non-repudiation chains. In order for both sides in an AS3 exchange to agree that both parties have the same file, both sides must possess the same MDN. However, if the MDN is downloaded by the original file sender but there is a later dispute about whether or not this action actually took place, MOVEit DMZ tamper-evident audit logs can be used to show that the original file sender's MDN was made available and downloaded at a specific time by a specific user connected from a specific IP address.

Advantages of MOVEit's Implementation

MOVEit Central calculates and stores an MDN for every ASx message it processes whether or not an MDN was requested. This feature allow operations to temporarily disable automatic MDNs and send them later using another channel if the MDN delivery channel has been temporarily disrupted. This will not work for synchronous MDNs, for obvious reasons.

All file transfers, including ASx message operations (and their MDNs), are logged in a tamper-evident audit log.

There are configurable, automatic retries on file transfers and MDN transfers.

Time-saving configuration prevents you from having to completely redefine each new file transfer with the same partner and to save steps with new partners.

Limitations of MOVEit's Implementation

MOVEit does not support the "RC4" encryption algorithm, although this algorithm could be supported in a future version if necessary. (Contact Ipswitch if you need to support this non-FIPS algorithm.)

MOVEit does not support GET-method AS2 messages. Some AS2 clients support these type of messages, but POST-method submissions are the industry standard (and generally regarded as more secure and less work for operations).

Certificates

As covered in the ***Overview*** (on page 337) documentation, the AS protocols depend heavily on digital certificates to sign and encrypt files. Digital certificates are also known as "X.509 certificates", "SSL certificates", "web certificates" and "client certificates" in various contexts, but all of these are just terms for digital certificates.

What Are "Certificates"?

All digital certificates are made up a public key, a private key and some additional information like "common name" ("CN"). They may be distributed with or without their private key: as the name suggests, in most situations you should NOT distribute certs containing your private key.

Many digital certificates are "signed" by other "certificate authority" ("CA") certificates. This allows people and computers that trust the certificate authorities to trust, use and allow certificates signed by the certificate authorities.

More information can be found in the "***Configuring Tasks - Keys and Certs - SSL Client Certificates*** (see "***SSL Client Certificates***" on page 217)" documentation.

Where Do You Get a Certificate?

Certificates without private keys will generally be delivered to you by your trading partners. These certificates need only to be imported into MOVEit Central (through the "***SSL Certificates*** (see "***SSL Client Certificates***" on page 217)" dialog) to be used as "Partner" certificates in AS Hosts.

There are several ways to obtain a certificate with a private key to be used as "My Organization" certificates in AS Hosts:

- **Purchase a commercial "client certificate"** from Thawte, Verisign or one of the many other commercial CA vendors. If there is any chance that your AS partners will be requiring trusted CAs as well as specific certificates in AS transactions, this option may be the safest route. (Sometimes these certificates are also known as "email certificates" because they may also be used with SMIME-encrypted email.)
- **Get a new certificate from your corporate CA**. If your company is already issuing client certificates and acting as its own CA, your certificate group should be able to provide you with a certificate and instructions on how to use it.
- **Obtain a certificate (with private key) from your partner**. Some partners will simply deliver a *.pfx (or other format) certificate-with-private-key file before you start trading. In this case you will need to import this certificate (with the proper password) through MOVEit Central's "***SSL Certificates*** (see "***SSL Client Certificates***" on page 217)" dialog.
- **Create your own certificate**.

In any case, you can import a certificate, or create a new one, using MOVEit Central's ***Cert/Key Manager*** (see "***Key/Cert Manager***" on page 212).

Once you have imported your own certificate with private key (MOVEit Central calls these "My Certs" or "Private Certs"), the good news is that you can usually use the same cert to sign and encrypt traffic for multiple partners. In other words, you will generally only have one or a few certs with private keys, no matter how many partner certs (without private keys) you may collect.

Where Might You Configure AS Certificates in MOVEit Central

The two most common uses of certificates in AS transfers are to sign/verify messages and encrypt/decrypt messages. MOVEit Central requires these two different certificates for any AS transport: one is defined in the "Partner - Certificate" section of each AS host and the other is defined in the "My Organization - Certificate" section of each AS host. (See "***AS1*** (on page 376), ***AS2*** (on page 379) or ***AS3*** (on page 387) Host" documentation for more information.)

However, there may be as many as 8 different certificates (plus any number of CA certificates) involved in any AS2 transfer. The following list breaks down the possible certificate uses and where they are configured in MOVEit Central. Certificate uses #1-5 draw on certificates from the "***SSL Certificates*** (see "***SSL Client Certificates***" on page 217)" dialog. The "require partner to use a client cert to authenticate to AS server" (#6) and the two server certificate uses (#7-8) involve importing and configuring certificates through other means.

1. **Cert (w/ private key) you use to sign messages for your partner and your partner normally uses to encrypt files for you. (REQUIRED)** - This is configured on the main page of your AS Host definition in the "My Organization" pane.
2. **Cert (w/ private key) you use to decrypt messages and MDNs from your partner** - Normally this is the same certificate used to sign messages for your partner (i.e., #1), but an alternate certificate can be used for this purpose. To define an alternate "decryption" certificate, see the "SSL Certs" tab on your AS Host's "Advanced Options" dialog.
3. **Partner's cert (no private key) you use to encrypt messages for your partner and your partner will use to sign his/her messages (REQUIRED)** - This is configured on the main page of your AS Host definition in the "Partner" pane.
4. **Partner's cert (no private key) your partner will use to sign MDNs** - Normally this is the same cert you use to encrypt messages for your partner, but an alternate certificate can be used for this purpose. To define an alternate "signature verification" certificate, use the related option on AS destinations. (This is a task-level, not a host-level option.)
5. **Optional SSL client cert (w/ private key) you use to authenticate to your partners AS server** - This is an optional authentication credential you may need to provide before your partner's AS server will permit you to post a message or MDN. To designate this kind of certificate, use the "SSL Client Cert" option in the "Partner" pane on the main page of your AS Host definition.
6. **Optional SSL client cert (no private key) you require your partners to provide to your AS server** - This is an optional authentication credential your partner may need to provide before your partner will be permitted to post a message or MDN to your AS server. To set this up on your MOVEit DMZ server when acting as an AS2 server, you may need to set up an additional IIS site and enable IIS certificate mapping after requiring certificates through IIS. (MOVEit DMZ's AS2 facility does not currently allow you to require client certificates through the software.) To set this up on your MOVEit DMZ server when acting as an AS3 server, simply perform the same actions as you would to require client certificates on MOVEit DMZ's FTP interface.

7 **Optional (but common) SSL server cert (w/ private key) you use to provide SSL transport security on your AS server** - All SSL-protected servers require a digital certificate, and SSL-protected AS servers protected by SSL are no exception. Although this use of digital certificates is technically optional under the AS protocol standards, SSL server certificates are commonly found protecting AS2 and AS3 servers, including MOVEit DMZ servers (which act as your AS2 servers and can also be AS3 servers). If you are running a MOVEit DMZ server, an SSL server certificate will automatically have been set up for you during installation, and existing procedures to renew/replace your SSL server certificates through IIS and/or MOVEit DMZ FTP are all that are required.

8 **Optional (but common) SSL server cert (w/ private key) your partner uses to provide SSL transport security on their AS server** - All SSL-protected servers require a digital certificate, and AS servers protected by SSL are no exception. Although this certificate is optional, it is commonly found protecting AS2 and AS3 servers. If your partner's server SSL cert is not signed by a trusted CA, you may use the "Ignore Cert Errors" option to avoid the need to import your partner's SSL server certificate.

Hosts

This section describes configuration options for the various types of AS hosts.

Overview

AS1, AS2, and AS3 hosts define the parameters for transferring files to and from a partner using the AS1, AS2, and AS3 protocols. While the methods of transport are different for each of the three protocols, most of the rest of the file transfer process is shared. As a result, there are many configuration options which are common to the three host types.

For details about the specific options available to the individual host types, see the following pages:

- ***AS1, AS2, AS3 - Hosts - AS1*** (see "***AS1***" on page 376)
- ***AS1, AS2, AS3 - Hosts - AS2*** (see "***AS2***" on page 379)
- ***AS1, AS2, AS3 - Hosts - AS3*** (see "***AS3***" on page 387)

My Organization

The My Organization section is where options that define your side of the file transfer process are configured.

Common Options:

- **Name/Email Address** - The name your organization will be known by. This identifies your organization in the course of the file transfer process. For AS1 hosts, this identifier must be an email address, and will be the address by which files are sent and received.
- **Certificate** - The SSL certificate used by your organization for message signing and decryption. It must be a full public/private certificate. The public portion of the certificate is given to the file transfer partner so that they can encrypt files to your organization and verify messages signed by your organization.

Partner

The Partner section is where options that define your partner's side of the file transfer process are configured.

Common Options:

- **Name/Email Address** - The name which the partner will be known by. This identifies the partner in the course of the file transfer process. For AS1 hosts, this identifier must be an email address, and will be the address to which files are sent.
- **Certificate** - The public portion of the SSL certificate used by the partner. This certificate is used to encrypt files to the partner and verify messages signed by the partner.
- **Encryption Algorithm** - The symmetric encryption algorithm used for encrypting files. This algorithm should be agreed upon by both sides of the file transfer process. Supported algorithms are 3DES, DES, and RC2. Choosing None will disable encryption of files.
- **Compression Format** - The compression format used to automatically compress files. This format should be agreed upon by both sides of the file transfer process. The only supported format is ZLib. Choosing None will disable compression of files.
- **EDI Data Type** - The tag used to describe the format of the data. This tag is placed in the outbound message and applies to sending only. In most cases, the default of application/edi-x12 should be used. However, some recipients prefer the more generic application/octet-stream. This tag does not affect the actual data bytes that are sent.

Miscellaneous

The Miscellaneous section contains MOVEit Central-specific miscellaneous options.

Common Options:

- **Host ID** - The automatically-generated unique ID for the host. This value is not editable.
- **Description** - A description field for the host. This field does not affect the operation of the host and is used simply to provide operators with information about the host.

Advanced Options

Each AS1, AS2, and AS3 host has an Advanced Options button which opens up the Advanced Host Options dialog for that host. This dialog contains host options which are typically not used but are available for advanced environments.

Firewall

Common Options:

- **Type** - The type of firewall which MOVEit Central needs to communicate with. Available firewall types are Tunnel, SOCKS4, and SOCKS5. The default value is None.
- **Hostname/IP** - The hostname or IP address of the firewall.
- **Port** - The TCP port of the firewall.
- **Username** - The username which MOVEit Central should use to authenticate to the firewall.
- **Password** - The password which MOVEit Central should use to authenticate to the firewall.

SSL Certs

Common Options:

- **Decrypting certificate is different from signing certificate** - When this option is checked, MOVEit Central will use the certificate indicated by the **Decrypting Certificate** field in order to decrypt files received from the partner. The main certificate configured in the My Organization section of the host will continue to be used to sign outgoing messages to the partner.

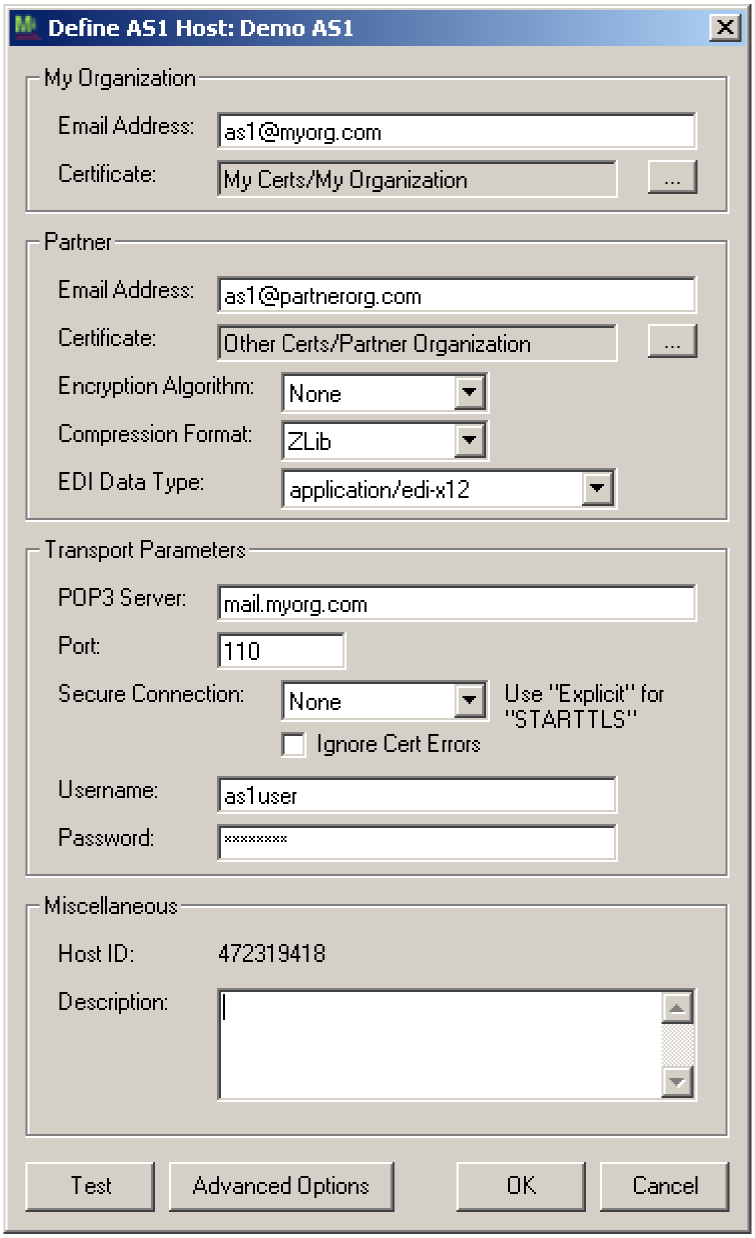
Retry

Common Options:

- **Default Retry Count** - The default number of extra times that a transfer (get or put) should be retried before MOVEit Central gives up. A value of 0 means MOVEit Central should not retry the transfer after a failure. The default value is 3, and the value can be overridden by individual tasks.
- **Default Retry Timeout** - The number of seconds between retries. The default value is 30 seconds, and can be overridden by individual tasks.

AS1

An AS1 host defines the parameters for transferring files to and from a partner via the AS1 protocol. For more information about AS1, please see "***AS1, AS2 and AS3 - The AS1 Protocol*** (on page 344)".



Define AS1 Host: Demo AS1

My Organization

Email Address: as1@myorg.com

Certificate: My Certs/My Organization

Partner

Email Address: as1@partnerorg.com

Certificate: Other Certs/Partner Organization

Encryption Algorithm: None

Compression Format: ZLib

EDI Data Type: application/edi-x12

Transport Parameters

POP3 Server: mail.myorg.com

Port: 110

Secure Connection: None

Use "Explicit" for "STARTTLS"

☐ Ignore Cert Errors

Username: as1user

Password: ********

Miscellaneous

Host ID: 472319418

Description:

AS1-Specific Host Options

The following options are specific to the AS1 Host.

Transport

- **POP3 Server** - The hostname or IP address of the POP3 email server from which AS1 messages will be retrieved.
- **Secure Connection** - The SSL connection type to use when connecting to the POP3 server. Selecting the None option will cause MOVEit Central to connect insecurely to the server. Selecting Explicit will cause MOVEit Central to connect insecurely to the server and then request that a secure connection be negotiated before continuing. Selecting Implicit will cause MOVEit Central to connect securely to the server.
- **Ignore Cert Errors** - When this option is checked, problems with the POP3 server's SSL certificate, such as a lack of trust or a name that does not match the host name, will be ignored.
- **SSL Client Cert** - The SSL client certificate that should be used when establishing a secure connection to the POP3 server. If "- None -" is selected, no client certificate will be used.
- **Username** - The username that MOVEit Central should use to authenticate to the POP3 server with.
- **Password** - The password that MOVEit Central should use to authenticate to the POP3 server with.
- **Delete messages older than X days** - Causes MOVEit Central to delete messages on the POP3 server that are older than the indicated number of days. The default value is 7.

Advances AS1-Specific Host Options

The following are advanced options that are specific to the AS1 host.

SMTP

- **SMTP server is different from POP3 server** - When this option is checked, MOVEit Central will use the SMTP server information configured here for sending email messages to the partner. Otherwise, MOVEit Central will use the POP3 server configured in the Transport section of the host as the SMTP server as well.
- **SMTP Server** - The hostname or IP address of the SMTP server.
- **SMTP Port** - The TCP port of the SMTP server.
- **SMTP Auth Method** - The authentication method MOVEit Central should use to authenticate to the SMTP server. Supported authentication methods are Auth and CRAM-MD5. If None is selected, no authentication will be attempted.
- **SMTP Username** - The username MOVEit Central should use to authenticate to the SMTP server.
- **SMTP Password** - The password MOVEit Central should use to authenticate to the SMTP server.

Transport

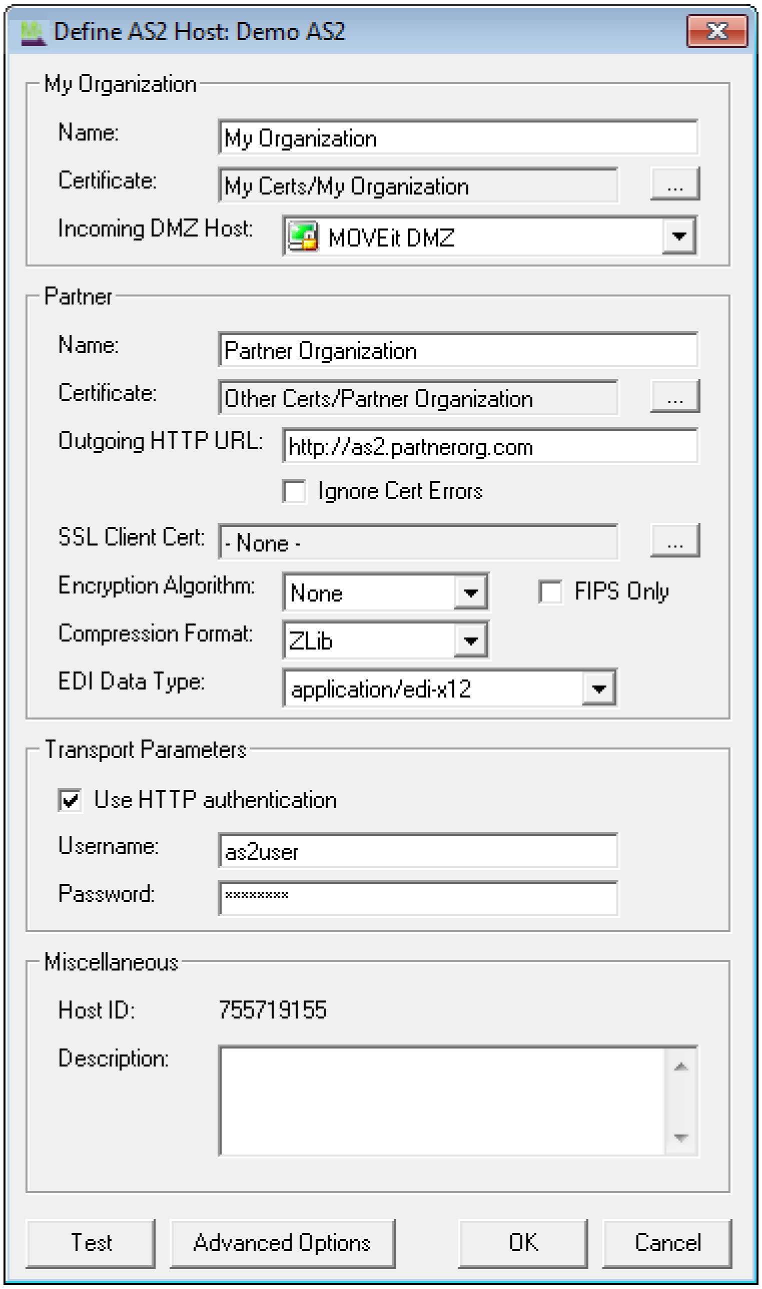
- **MDN Poll Count** - The number of times MOVEit Central will poll the POP3 server for an MDN message from the partner after an EDI data message has been sent to the partner. The default value is 10.
- **MDN Poll Timeout** - The number of seconds MOVEit Central should wait between MDN polls. The default value is 30 seconds.

Retry

- **Pause X seconds before rerunning successful task** - Since AS1, AS2, and AS3 file transfers operate one file at a time, MOVEit Central repeats the task after a successful file transfer in order to catch any other files that also need to be processed. This value causes MOVEit Central to delay for the indicated number of seconds before running the task again after a successful transfer.

AS2

An AS2 host defines the parameters for transferring files to and from a partner via the AS2 protocol. For more information about AS2, please see "***AS1, AS2 and AS3 - The AS2 Protocol*** (on page 350)".



My Organization

Name: My Organization

Certificate: My Certs/My Organization

Incoming DMZ Host: MOVEit DMZ

Partner

Name: Partner Organization

Certificate: Other Certs/Partner Organization

Outgoing HTTP URL: http://as2.partnerorg.com

□ Ignore Cert Errors

SSL Client Cert: - None -

Encryption Algorithm: None □ FIPS Only

Compression Format: ZLib

EDI Data Type: application/edi-x12

Transport Parameters

☑ Use HTTP authentication

Username: as2user

Password: ********

Miscellaneous

Host ID: 755719155

Description:

AS2-Specific Host Options

The following options are specific to the AS2 host.

My Organization

- **Incoming DMZ Host** - The MOVEit DMZ host which should receive AS2 messages from the partner.

Partner

- **Outgoing HTTP URL** - The partner's HTTP server URL which MOVEit Central should post AS2 messages to.
- **Ignore Cert Errors** - When this option is checked, problems with the partner HTTP server's SSL certificate, such as a lack of trust or a name that does not match the host name, will be ignored.
- **SSL Client Cert** - The SSL client certificate that should be used when establishing a secure connection to the partner's HTTP server. If "- None -" is selected, no client certificate will be used.

Transport

- **Use HTTP Authentication** - If checked, HTTP authentication with the specified username and password will be attempted when sending files via this AS2 host.
- **Username** - The username that MOVEit Central should use when attempting HTTP authentication.
- **Password** - The password that MOVEit Central should use when attempting HTTP authentication.

Advanced AS2-Specific Host Options

The following are advanced options specific to the AS2 host.

Proxy

- **Type** - The type of proxy server which MOVEit Central needs to communicate with. Available proxy types are Default and Specific. The default value is None.
- **Hostname/IP** - The hostname or IP address of the proxy server.
- **Port** - The TCP port of the proxy server.
- **Username** - The username which MOVEit Central should use to authenticate to the proxy server.
- **Password** - The password which MOVEit Central should use to authenticate to the proxy server.
- **SSL** - Indicates whether MOVEit Central should use SSL to communicate with the proxy server. Available options are Auto, Always, Never, and Tunnel. The default value is Auto.

Email MDN

- **AS1 Host to be used for receiving email MDNs** - In order to request asynchronous email MDNs, this option must be set to an existing AS1 host. This host's configuration options will be used to determine the parameters sent in the MDN request.
- **SMTP Server to be used for sending email MDNs** - The SMTP server which email MDNs will be sent through when such MDNs are requested by the partner.
- **From Address to be used for sending email MDNs** - The email address which will be listed as the From address when email MDNs are sent to the partner.

MOVEit DMZ's Role in AS2 File Transfers

MOVEit DMZ can accept and store AS2 messages and asynchronous AS2 MDNs that will be processed later (and often immediately) by MOVEit Central. MOVEit DMZ, rather than MOVEit Central, is used in the role of an "AS2 server" because MOVEit DMZ already serves the function of a secure, Internet-exposed HTTP(S) server and MOVEit Central already has an interface to MOVEit DMZ.

No additional license is required to accept and store AS2 messages and asynchronous AS2 MDNs on MOVEit DMZ because this feature is only useful when a separate AS1, AS2 and AS3 license has been purchased for MOVEit Central.

AS2 messages and asynchronous AS2 MDNs are uploaded and downloaded through HTTP(S) but are not part of the "normal" MOVEit DMZ file system. More specifically, all AS2 messages and AS2 MDNs will be found in special "/AS/[partner-name]" folders, created as needed (where "[partner-name]" is your partner's official trading name.) For example, if your partner "John Smith" sends you an AS2 message, it will be found in the "/AS2/John Smith" folder. Nonetheless, MOVEit DMZ administrators can view and delete AS2 message files through their usual web interface.

AS2 Server URL and MOVEit DMZ File Specifics

MOVEit DMZ receives AS2 messages and asynchronous AS2 MDNs though its built-in "as2receiver.aspx" component. When your AS2 trading partners ask for the URL they should use to post AS2 messages for you, you will need to give them a URL containing "as2receiver.aspx" and the name of your host. An example of such a URL is "https://as2.moveitdmz.com/as2receiver.aspx".

The same URL value is also used when requesting AS2 asynchronous MDNs as an AS2 destination step in MOVEit Central, but MOVEit Central lets you specify a macro of "[AS2ReceiverURL]" (in the "MDN URL" field) and figures out the exact URL at run time (because each AS2 Host can be linked to a specific MOVEit DMZ Host).

AS2 messages are normally stored as files bearing a name of "AS2Data". If you want different MOVEit Central tasks to process different AS2 messages from the same partner, you may want to "tag" each type of AS2 message transmission separately so MOVEit Central tasks can rapidly distinguish between them. The way to tag different types of AS2 transmissions is to include a "?Tag=[some-as2-filename]" argument on the URLs you hand out to your partners. For example, a modified URL of "https://as2.moveitdmz.com/as2receiver.aspx?Tag=Blue" would force MOVEit DMZ to save AS2 messages from partners using that URL as files named "Blue" rather than "AS2Data".

Asynchronous AS2 MDNs are stored as files bearing a name of "MDN=[AS2-ID]" where "[AS2-ID]" is the ID of the original AS2 message. An example of an AS2 MDN filename is "MDN=373c55dc-f4b6-4c1b-81a1-e39f3a1c22d7@9b751ee7-d32e-4138-8124-1c107f2cd5d2". Like AS2 messages, AS2 MDNs will be stored in folders named after the partners who sent them; MOVEit Central automatically knows where to look (because it uses the values configured for "partner name" in its AS2 Host definitions).

If your MOVEit DMZ hosts multiple Organizations and you want each to use its own store of AS2 messages and MDNs, you will also need to include an "OrgID=[OrgID]" tag (such as "OrgID=8011") in the URLs you give to your partners and configure in your requests for asynchronous HTTP MDNs. For example, you would need to give partners URLs such as "https://as2.moveitdmz.com/as2receiver.aspx?OrgID=8011" or "https://as2.moveitdmz.com/as2receiver.aspx?Tag=Blue&OrgID=8011" and would need to configure a URL of "[AS2ReceiverURL]?OrgID=8011" in your asynchronous HTTP MDN field if you wanted related AS2 messages and MDNs to go to a particular organization in a multiorganization configuration.

Both AS2 messages and asynchronous AS2 MDNs are deleted from MOVEit DMZ as soon as MOVEit Central successfully decrypts and/or validates them, determines that they are unfit or gives up after (re)trying to deliver any requested MDNs. AS2 messages that have requested synchronous MDNs will also be automatically deleted from MOVEit DMZ folders if MOVEit DMZ cannot deliver their respective MDNs. Additional automated clean up rules can also be applied to AS2 folders and files using the usual "folder settings" web interface in MOVEit DMZ.

Troubleshooting

Troubleshooting AS2 transmissions can be challenging because of all the different elements involved in a single AS2 transfer. However, the following methodologies should help you tackle transfer issues.

Troubleshooting Tasks with AS2 Destinations

Tasks with AS2 destinations are used to ***send files*** (on page 356) to your partners.

1. **Double-check that you and your partner agree on the following items** and that they are configured identically on both sides of the transmission.
   - The URL of your partner's remote AS2 server
   - Your organization's name and your partner's name
   - Your organization's client certificate and your partner's client certificate
   - The type of encryption to be used
   - What sort of MDN you should receive from your partner (usually "none", "synchronous" or "asynchronous"; your partner doesn't need to configure this but should probably know about your choice or will have an opinion of their own)
2. **Make sure MOVEit Central can connect to your partner's AS2 server.** You test this when you run your transfer task - pay attention to "host not defined", "cannot connect", "404" errors and the like. If you are having problems here, your partner's URL is likely incorrect or inaccessible. (It's generally worth asking if you are the first one to try this particular connection.)
3. **Make sure MOVEit Central thinks it has sent the file successfully.** You will know this is the case if MOVEit Central shows a working status of "X bytes sent" for your AS2 task and X is both "large" (sometimes larger than the original file size) and constant. If this is as far as MOVEit Central gets (because it it waiting for an MDN), the task will usually fail with an "AS2 Post Error: Timeout" error after one minute.
4. **Make sure the remote AS2 server thinks it has sent the MDN successfully.** If MOVEit Central is getting past this step successfully, the task will simply complete successfully. If the task does not complete successfully, failure could be due to a number of things:
   - Remote AS2 server told MOVEit Central it received the file but then never processed it or failed to process it and silently through it away. You will need an administrator on the remote AS2 server to help you if this is the case.
   - Remote AS2 server does not support the requested MDN and takes the file anyway - another type of "silent" failure. You may want to switch your MDN type between sync/async, but you may need to get the remote AS2 server administrator involved in here too.
   - Remote AS2 server processes your file but fails to get you a synchronous MDN back in time. If this is the case, the remote AS2 server may log that it created an MDN for your file, but it should also log the fact that you never got it.

- Remote AS2 server processes your file but cannot send you an asynchronous MDN. As long as you have taken care to leave a value of "[AS2ReceiverURL]" in your Destination's "MDN URL" this error is likely due to an unresolvable DNS, proxy server or other connection problem on the remote AS2 server's side.

Troubleshooting Tasks with AS2 Sources

Tasks with AS2 sources are used to ***receive files*** (on page 356) from your partners.

1. **Double-check that you and your partner agree on the following items** and that they are configured identically on both sides of the transmission.
   - The URL of your (MOVEit DMZ) AS2 server. This will be something like "https://myserver.moveitdmz.com/as2receiver.aspx"
   - Your organization's name and your partner's name
   - Your organization's client certificate and your partner's client certificate
   - The type of encryption to be used
   - (You can ask about what sort of MDN your partner expects, but there is nothing to configure in MOVEit Central regarding this information because AS2 file senders configure this value and AS2 file receivers - MOVEit Central in this case - are expected to pull it off incoming AS2 messages.)
2. **Make sure your partner's AS2 client can connect to your MOVEit DMZ server.** You can start with basic connectivity and DNS tests by simply asking your partner to connect to your MOVEit DMZ using the URL you use for normal, interactive web access. Then have your partner try to send an AS2 file with the client and look/listen for "cannot connect", "404" and other errors that suggest that the remote AS2 client cannot connect to the AS2 interface of your MOVEit DMZ server.
3. **Make sure your partner is successfully posting files to MOVEit DMZ.** sign on to your MOVEit DMZ server as an Admin or FileAdmin to see if you suspect your partner is not posting AS2 files successfully. If your partner is posting files successfully, you will see a folder named "/AS2/[PartnerName]" where "[PartnerName]" is the exact name of your partner (as configured in your AS2 host configuration). As your partner posts AS2 files, you will also see files named "AS2Data" (or something else if URLs with the "Tag=" attribute are used) show up in this folder and in the audit log.
4. **Make sure MOVEit Central is automatically kicking off the task associated with this transfer correctly.** There are several reasons why this could not be happening - see the "Tasks Configured to Receive AS2 Files Do Not Run Automatically" section below for details.
5. **Make sure your MOVEit Central task is correctly processing your partner's AS2 file and returning a valid MDN.** Fortunately, this is mostly internal processing at this point: MOVEit Central will provide you information about any problems occurring here. If your partner has requested an asynchronous MDN for its AS2 file, it is possible that the URL he/she provided in the AS2 message is invalid or unreachable, but this is almost the only error caused by external conditions that could be encountered at this stage.

Error Messages Encountered During AS2 File Transfer

"cannot connect to MIAS2: Access is denied"

This message usually indicates that MOVEit Central's "MIAS2.exe" AS2 helper application has not been started. This application should be started and have its own "Task Manager - Processes" entry when the MOVEit Central service starts. First try restarting the MOVEit Central service. If this does not fix the problem, use the "Run MOVEit Central manually" option from the "Start | Programs | MOVEit Central" program group to run MOVEit Central in the foreground and watch for other clues from the MOVEit Central or MIAS2 windows in the foreground.

"Host default partner cert not found"

This message often means that a partner's client certificate was imported and selected in an AS2 Host configuration, but that the underlying certificate has since been deleted. The best way to correct this situation is to reimport your partner's client certificate and reselect it in the AS2 Host configuration.

"405 Method Not Supported"

This message means you got to a web server (all AS2 servers are web servers) but that the web server doesn't understand or allow your request. If you copied an "Outgoing HTTP URL" from an AS2 Host configuration into a web browser, this message is perfectly normal (especially if your partner's server is an MOVEit DMZ AS2 server). However, if you see this message during an AS2 file transfer it more likely indicates one or more of the following problems:

- The "Outgoing HTTP URL" you typed in is incorrect.
- A proxy server between your MOVEit Central and your partner's AS2 server does not allow AS2 traffic.
- URLScan or some other host-based intrusion engine does not allow AS2 transactions.

"The requested name is valid, but no data of the requested type was found"

This error typically indicates that a DNS entry for a configured hostname could not found. If you see this error you should recheck any hostnames configured as part of this transfer. In a specific case, if this error starts with a "AS2SendMDN error: " prefix then the value of the "SMTP Server to be used for sending email MDNs" field in your AS2 host's Advanced settings ("Email MDN" tab) is probably not correct or not reachable.

"304 Could not write to file"

This message may mean that the transfer has exceeded the file size limit for AS2 Receive. The limit for a single file is 1 GB. If you are attaching files to a message (sent via ASx), the limit for a single message and attached files is 200 MB.

Tasks Configured to Receive AS2 Files Do Not Run Automatically

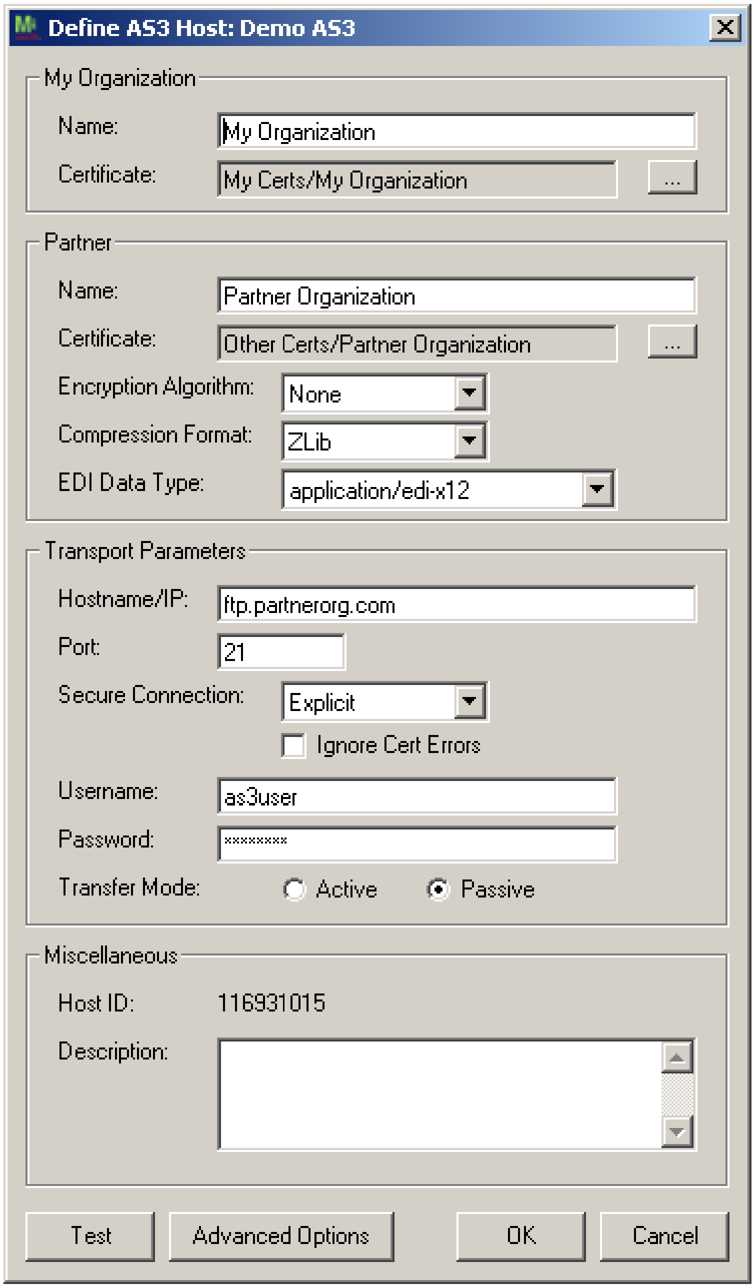
If you are receiving AS2 files from partners, you must set up tasks with AS2 Sources for each partner that will be sending you AS2 files. Partners post AS2 files to a MOVEit DMZ server and MOVEit Central normally learns about posted files and acts on them within seconds of their completion.

There are several reasons why tasks configured to receive AS2 files will not start automatically.

- **Your partner isn't really posting AS2 files successfully** - Your partner will post AS2 files to your MOVEit DMZ server so you must sign on to your MOVEit DMZ server as an Admin or FileAdmin to see if you suspect your partner is not posting AS2 files successfully. If your partner is posting files successfully, you will see a folder named "/AS2/[PartnerName]" where "[PartnerName]" is the exact name of your partner (as configured in your AS2 host configuration). As your partner posts AS2 files, you will also see files named "AS2Data" (or something else if URLs with the "Tag=" attribute are used) show up in this folder and in the audit log. If AS2 file posts are not making it this far, please consult the "405 Method Not Supported" advice above.
- **AS2 poller is not running** - If you watch the MOVEit Central debug log at the All Debug level with no task filter set, you should see orange messages like "AS poller found X files on..." and "AS2 poller polled X hosts, saw Y files, started Z tasks" scroll by every few seconds. If you do not see these messages, the AS2 poller (that looks for AS2 file postings on MOVEit DMZ) is probably not running. Normally, restarting the MOVEit Central service will fix this.
- **AS2 poller is finding files, but your task isn't scheduled to run at the time the files are found** - At the All Debug level, orange messages like "Considering new file AS2/.../... for task X" will scroll by whenever new AS2 files are posted to your MOVEit DMZ server. If the task you would expect to act on the posted files is not one of the ones listed, it is probably because your task is missing a schedule that would allow it to run when files arrive during a particular window of time. The easiest way to correct this situation is to add a "always on" schedule to your task that runs on "All Days", "Repeated" between "00:00" and "23:59".
- **AS2 poller is finding files and your task is scheduled to run when the files are found but the related "receive" task still isn't getting called.** - If this is your situation, make sure your AS2 source's "File Tag(s)" match (or include) the filenames of AS2 files being posted to your MOVEit DMZ server. When in doubt, use a wildcard File Tag of "*" to download everything from that particular partner.

AS3

An AS3 host defines the parameters for transferring files to and from a partner via the AS3 protocol. For more information about AS3, please see "***AS1, AS2 and AS3 - The AS3 Protocol*** (on page 361)".



Define AS3 Host: Demo AS3

My Organization

Name: My Organization

Certificate: My Certs/My Organization

Partner

Name: Partner Organization

Certificate: Other Certs/Partner Organization

Encryption Algorithm: None

Compression Format: ZLib

EDI Data Type: application/edi-x12

Transport Parameters

Hostname/IP: ftp.partnerorg.com

Port: 21

Secure Connection: Explicit

□ Ignore Cert Errors

Username: as3user

Password: ********

Transfer Mode: ○ Active ● Passive

Miscellaneous

Host ID: 116931015

Description:

AS3-Specific Host Options

The following options are specific to the AS3 host.

Transport

- **Hostname/IP** - The hostname or IP address of the FTP server used for AS3 messages uploads or downloads.
- **Port** - The FTP server's command channel port. The default value is 21 when using no security or an explicit secure connection and 990 when using an implicit secure connection.
- **Secure Connection** - The SSL connection type to use when connecting to the FTP server. Selecting the None option will cause MOVEit Central to connect insecurely to the server. Selecting Explicit will cause MOVEit Central to connect insecurely to the server and then request that a secure connection be negotiated before continuing. Selecting Implicit will cause MOVEit Central to connect securely to the server.
- **Ignore Cert Errors** - When this option is checked, problems with the FTP server's SSL certificate, such as a lack of trust or a name that does not match the host name, will be ignored.
- **SSL Client Cert** - The SSL client certificate that should be used when establishing a secure connection to the FTP server. If "- None -" is selected, no client certificate will be used.
- **Username** - The username that MOVEit Central should use to authenticate to the FTP server with.
- **Password** - The password that MOVEit Central should use to authenticate to the FTP server with.
- **Transfer Mode** - The FTP transfer mode to use for uploading and downloading files. When Active mode is selected, the FTP server will initiate a data channel connection to MOVEit Central for data transfers. When Passive mode is selected, MOVEit Central will initiate a data channel connection to the FTP server for data transfers. The default value is Passive.

Advanced AS3-Specific Host Options

The following are advanced options specific to the AS3 host.

Transport

- **MDN Poll Count** - The number of times MOVEit Central will poll the FTP server for an MDN message from the partner after an EDI data message has been sent to the partner. The default value is 10.
- **MDN Poll Timeout** - The number of seconds MOVEit Central should wait between MDN polls. The default value is 30 seconds.

Retry

- **Pause X seconds before rerunning successful task** - Since AS1, AS2, and AS3 file transfers operate one file at a time, MOVEit Central repeats the task after a successful file transfer in order to catch any other files that also need to be processed. This value causes MOVEit Central to delay for the indicated number of seconds before running the task again after a successful transfer.

MOVEit DMZ's Role in AS3 File Transfers

MOVEit DMZ can accept and store AS3 messages and AS3 MDNs that will be processed later by MOVEit Central or any other AS3 client. MOVEit DMZ, rather than MOVEit Central, is used in the role of an "AS3 server" because MOVEit DMZ already serves the function of a secure, Internet-exposed FTP(S) server.

No additional license is required to accept and store AS3 messages and AS3 MDNs on MOVEit DMZ because, according to the AS3 specification, any FTP server can function as an AS3 server. (That is, if you have licensed a MOVEit DMZ server, you already have an AS3 server.)

AS3 messages and AS3 MDNs are uploaded and downloaded through FTP and are thus part of the "normal" MOVEit DMZ file system. More specifically, all AS3 messages and AS3 MDNs will be found in the "/Home/..." or "/Distribution/..." folders and are otherwise treated as "normal" files.

Tasks

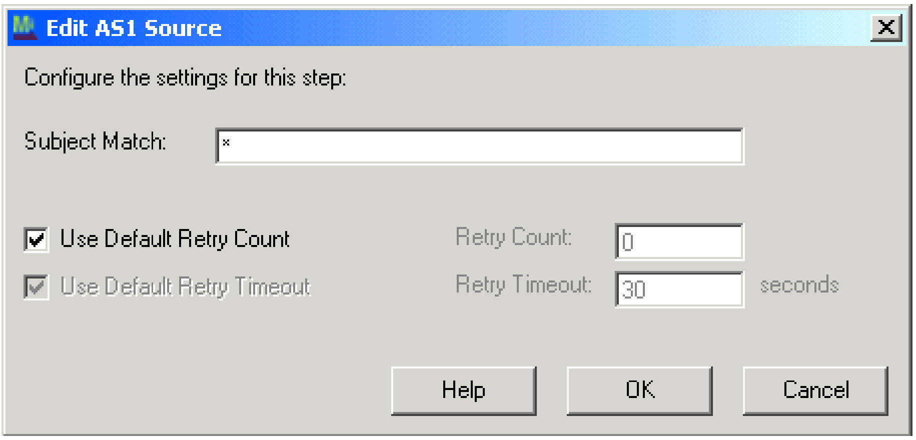
This section describes tasks available for the various types of AS protocols.

AS1

This section describes tasks available for AS1 transfers based on the source or destination configurations.

Source

An AS1 source is a reference to an AS1 host which defines a single ruleset for a file from a partner's EDI data message for use in a task. Partner credentials, encryption method and other "partnership-level" details are configured at the Host level; see "***AS1, AS2 and AS3 - Hosts - AS1*** (see "***AS1***" on page 376)" for more information.


Edit AS1 Source

Configure the settings for this step:

Subject Match: *

☑ Use Default Retry Count   Retry Count: 0

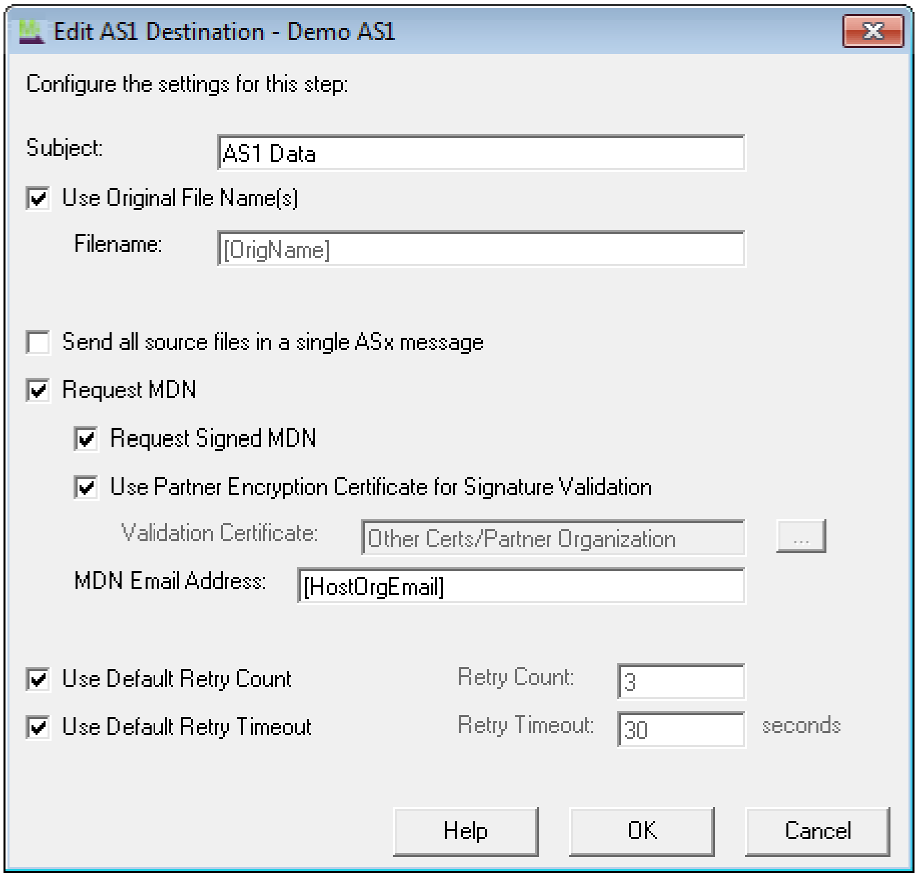
☑ Use Default Retry Timeout   Retry Timeout: 30 seconds

AS1 Source Options:

- **Subject Match** - Indicates which messages should be downloaded from the AS1 POP3 server. You may use ***Macros*** (see "***Macro***" on page 137) in this field, as well as * and ? wildcard characters.

Destination

An AS1 destination is a reference to an AS1 host which defines a single ruleset for sending a file as an EDI data message to a partner and requesting an MDN to confirm receipt of the file. Partner credentials, encryption method and other "partnership-level" details are configured at the Host level; see "***AS1, AS2 and AS3 - Hosts - AS1*** (see "***AS1***" on page 376)" for more information.



Edit AS1 Destination - Demo AS1

Configure the settings for this step:

Subject: AS1 Data

☑ Use Original File Name(s)

Filename: [OrigName]

☐ Send all source files in a single ASx message

☑ Request MDN

☑ Request Signed MDN

☑ Use Partner Encryption Certificate for Signature Validation

Validation Certificate: Other Certs/Partner Organization

MDN Email Address: [HostOrgEmail]

☑ Use Default Retry Count — Retry Count: 3

☑ Use Default Retry Timeout — Retry Timeout: 30 seconds

AS1 Destination Options:

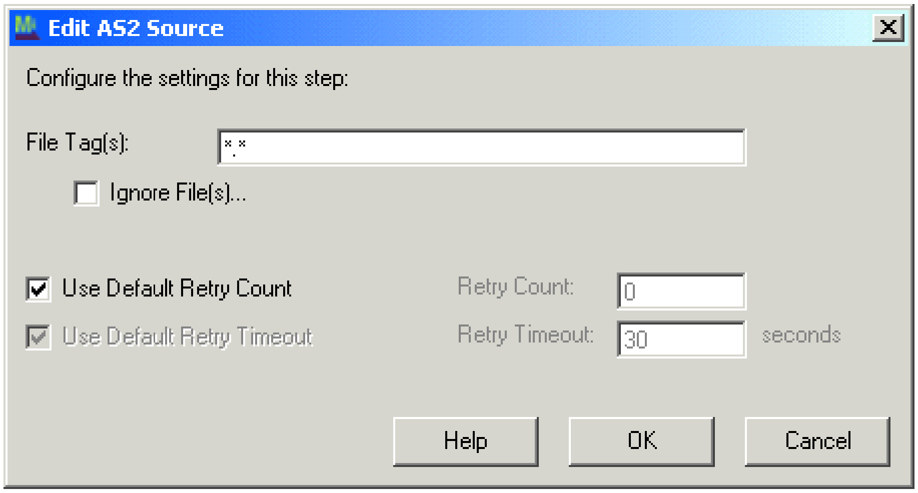
- **Subject** - The subject of the email message which will be sent to the partner. You may use ***Macros*** (see "***Macro***" on page 137) in this field
- **Use Original File Name(s)** - Indicates whether or not MOVEit Central should send the file with the name under which it was saved on the source. If this option is not checked, MOVEit Central will use the name defined in the **Filename** field. This name may contain macros.
- **Send all source files in a single ASx message** – When this option is checked, instead of an individual ASx message for each of the source files, this destination will send a single ASx message with multiple attachments.
- **Request MDN** - When this option is checked, MOVEit Central will request an MDN from the destination partner to verify that the data arrived, and will not consider the task complete until it has received one.
- **Request Signed MDN** - When this option is checked, MOVEit Central will request that the MDN sent by the destination partner be signed by the partner's SSL certificate, to verify the origin of the MDN message.
- **Use Partner Encryption Certificate for Signature Validation** - When this option is checked, MOVEit Central will use the Partner Certificate configured in the referenced AS1 host to validate the signature on the MDN received from the partner. If this option is not checked, a different SSL certificate may be configured for signature validation in the **Validation Certificate** field.
- **MDN Email Address** - The email address to which the destination partner should send MDNs. By default, this is set to the "[HostOrgEmail]" macro, which represents by the My Organization - Email Address field value of the referenced AS1 host.

AS2

This section describes tasks available for AS2 transfers based on the source or destination configurations.

Source

An AS2 source is a reference to an AS2 host which defines a single ruleset for a file from a partner's EDI data message for use in a task. Partner credentials, encryption method and other "partnership-level" details are configured at the Host level; see "***AS1, AS2 and AS3 - Hosts - AS2*** (see "***AS2***" on page 379)" for more information.



Edit AS2 Source

Configure the settings for this step:

File Tag(s): *.*

□ Ignore File(s)...

☑ Use Default Retry Count — Retry Count: 0

☑ Use Default Retry Timeout — Retry Timeout: 30 seconds

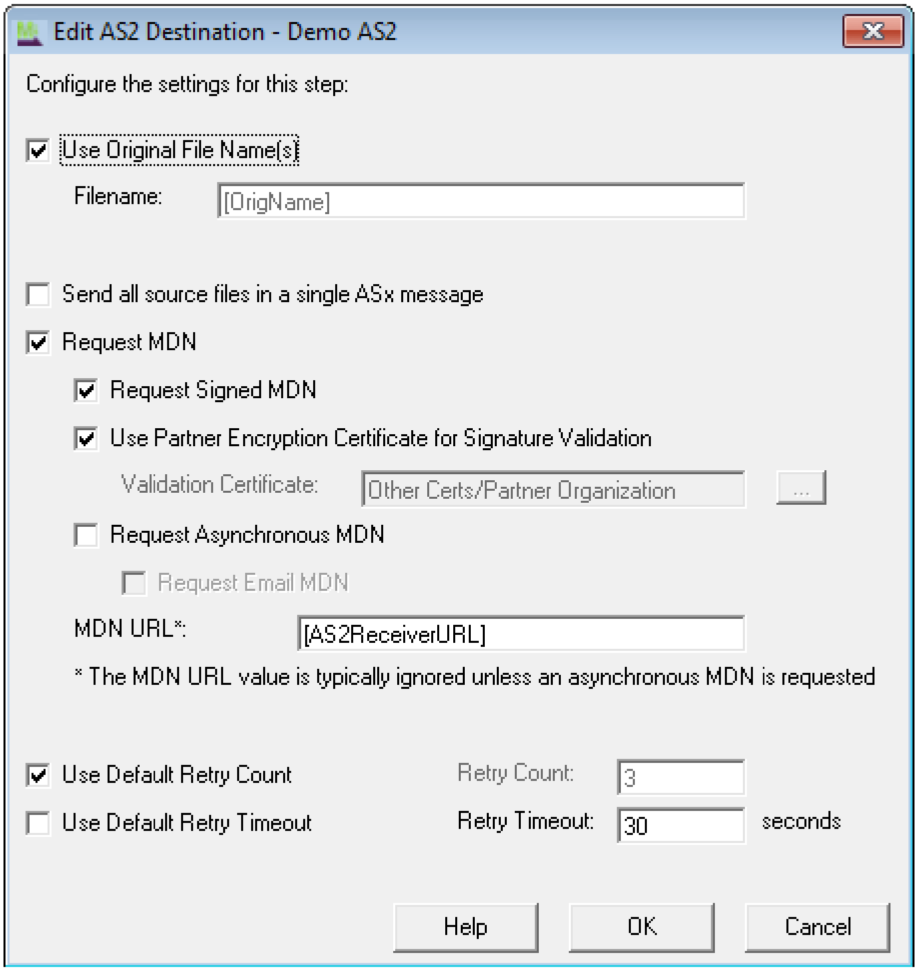
AS2 Source Options:

- **File Tag(s)** - Indicates which files should be downloaded from the AS2 MOVEit DMZ server. You may use ***Macros*** (see "***Macro***" on page 137) in this field, as well as * and ? wildcard characters. As with other mask fields, multiple masks may be entered, separated by semicolons (";").
- **Ignore File(s)** - When this option is checked, one or more file masks may be entered. When MOVEit Central finds a file that matches one of the entered masks, it will be ignored. You may use Macros in this field. As with other mask fields, multiple masks may be entered, separated by semicolons (";").

Note: For an AS2 Receive, the file size limit for a single file is 1 GB. If you are attaching files to a message (sent via ASx), the limit for a single message and attached files is 200 MB.

Destination

An AS2 destination is a reference to an AS2 host which defines a single ruleset for sending a file as an EDI data message to a partner and requesting an MDN to confirm receipt of the file. Partner credentials, encryption method and other "partnership-level" details are configured at the Host level; see "***AS1, AS2 and AS3 - Hosts - AS2*** (see "***AS2***" on page 379)" for more information. For asynchronous HTTP(S) MDN requests, you must have an incoming DMZ host already defined. For asynchronous email MDN requests, you must have an AS1 host already defined



Edit AS2 Destination - Demo AS2

Configure the settings for this step:

☑ Use Original File Name(s)

Filename: [OrigName]

☐ Send all source files in a single ASx message

☑ Request MDN

☑ Request Signed MDN

☑ Use Partner Encryption Certificate for Signature Validation

Validation Certificate: Other Certs/Partner Organization

☐ Request Asynchronous MDN

☐ Request Email MDN

MDN URL*: [AS2ReceiverURL]

* The MDN URL value is typically ignored unless an asynchronous MDN is requested

☑ Use Default Retry Count — Retry Count: 3

☐ Use Default Retry Timeout — Retry Timeout: 30 seconds

AS2 Destination Options:

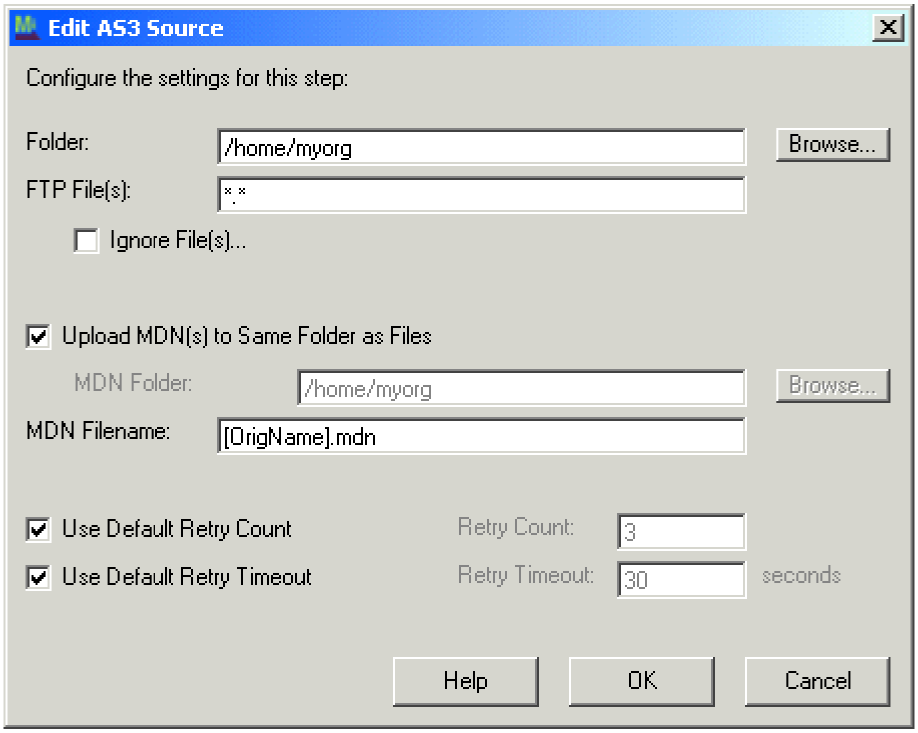
- **Use Original File Name(s)** - Indicates whether or not MOVEit Central should send the file with the name under which it was saved on the source. If this option is not checked, MOVEit Central will use the name defined in the **Filename** field. This name may contain ***Macros*** (see "***Macro***" on page 137).
- **Request MDN** - When this option is checked, MOVEit Central will request an MDN from the destination partner to verify that the data arrived, and will not consider the task complete until it has received one.
- **Send all source files in a single ASx message** – When this option is checked, instead of an individual ASx message for each of the source files, this destination will send a single ASx message with multiple attachments.
- **Request Signed MDN** - When this option is checked, MOVEit Central will request that the MDN sent by the destination partner be signed by the partner's SSL certificate, to verify the origin of the MDN message.
- **Use Partner Encryption Certificate for Signature Validation** - When this option is checked, MOVEit Central will use the Partner Certificate configured in the referenced AS1 host to validate the signature on the MDN received from the partner. If this option is not checked, a different SSL certificate may be configured for signature validation in the **Validation Certificate** field.
- **Request Asynchronous MDN** - When this option is checked, MOVEit Central will request that the MDN be sent after the file transfer connection has been closed, instead of at the end of the file transfer before the connection closes. An asynchronous MDN can be sent either to an HTTP server, or by email. If this option is not checked, a synchronous MDN will be requested.
- **Request Email MDN** - When this option is checked, MOVEit Central will request that the MDN be sent via email to the email address indicated by the **MDN Email Address** field.
- **MDN URL** - The URL to which HTTP MDNs should be sent by the destination partner. For synchronous MDN requests, this value (while required by the AS2 specification) is typically ignored since the MDN is sent in response to the file transfer via the same connection. For asynchronous HTTP(S) MDN requests, however, this value is necessary in order to tell the destination partner where to send the MDN. By default, this is set to the "[AS2ReceiverURL]" macro, which represents a properly formatted URL based on the linked MOVEit DMZ host of the referenced AS2 host. Note that this field will not be available if the Request Asynchronous MDN and Request Email MDN options are checked.
- **MDN Email Address** - The email address to which the destination partner should send MDNs. By default, this is set to the "[AS1OrgEmail]" macro, which represents the My Organization - Email Address field value of the AS1 host configured in the referenced AS2 host. Note that this field will only be available if the Request Asynchronous MDN and Request Email MDN options are checked.

AS3

This section describes tasks available for AS3 transfers based on the source or destination configurations.

Source

An AS3 source is a reference to an AS3 host which defines a single ruleset for obtaining a file from a partner's EDI data message for use in a task. Partner credentials, encryption method and other "partnership-level" details are configured at the Host level; see "***AS1, AS2 and AS3 - Hosts - AS3*** (see "***AS3***" on page 387)" for more information.



Edit AS3 Source

Configure the settings for this step:

Folder: /home/myorg

FTP File(s): *.*

☐ Ignore File(s)...

☑ Upload MDN(s) to Same Folder as Files

MDN Folder: /home/myorg

MDN Filename: [OrigName].mdn

☑ Use Default Retry Count — Retry Count: 3

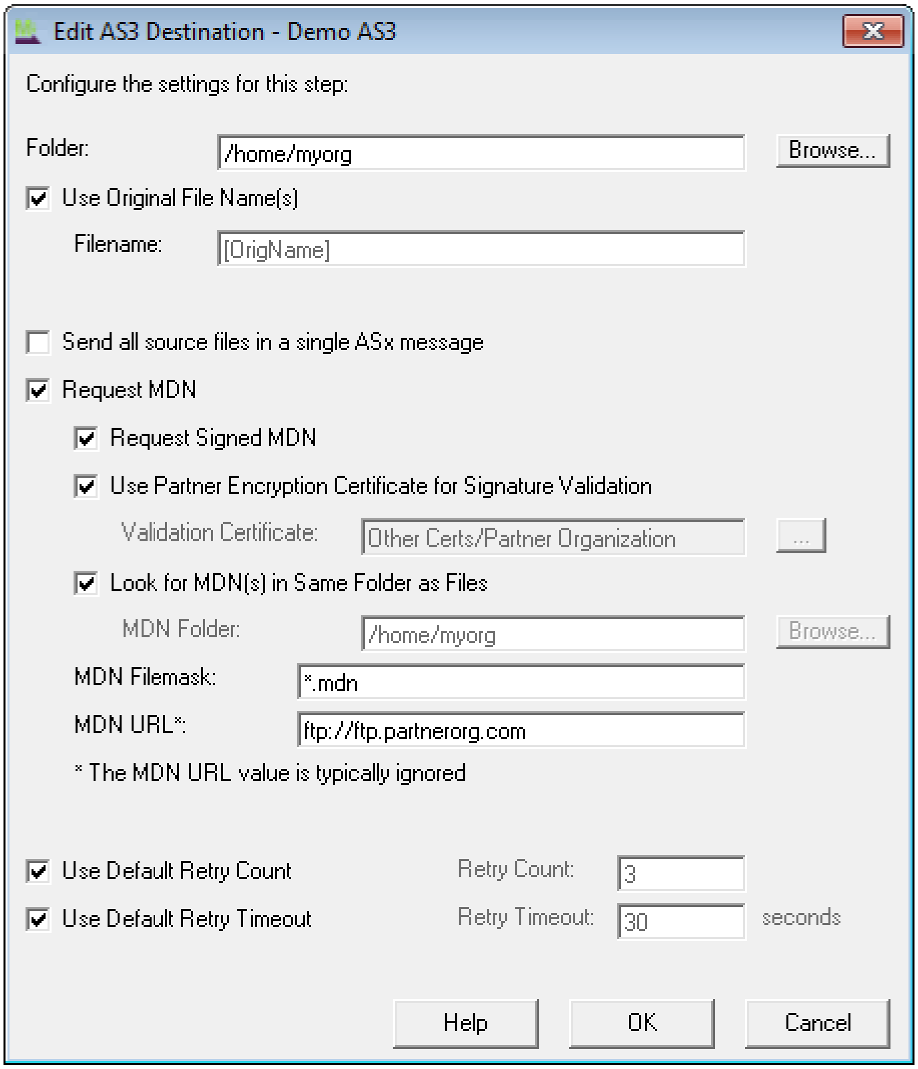
☑ Use Default Retry Timeout — Retry Timeout: 30 seconds

AS3 Source Options:

- **Folder** - The folder on the AS3 FTP server to search for EDI data message files. The Browse button may be used to easily select a folder on the remote host. You may use ***Macros*** (see "***Macro***" on page 137) in this field.
- **FTP File(s)** - Indicates which files should be downloaded from the AS3 FTP server. You may use Macros in this field, as well as * and ? wildcard characters. As with other mask fields, multiple masks may be entered, separated by semicolons (";").
- **Ignore File(s)** - When this option is checked, one or more file masks may be entered. When MOVEit Central finds a file that matches one of the entered masks, it will be ignored. You may use Macros in this field. As with other mask fields, multiple masks may be entered, separated by semicolons (";").
- **Upload MDN(s) to Same Folder as Files** - When this option is checked, MDNs will be written to the same FTP folder that we found the original EDI data message file in. If this option is not checked, a different MDN folder may be entered in the **MDN Folder** field. The Browse button next to this field may be used to easily select a folder on the remote host. You may use Macros in the MDN Folder field.
- **MDN Filename** - The name of the file which MOVEit Central will write the MDN to if an MDN is requested by the sending partner. You may use Macros in this field.

Destination

An AS3 destination is a reference to an AS3 host which defines a single ruleset for sending a file as an EDI data message to a partner and requesting an MDN to confirm receipt of the file. Partner credentials, encryption method and other "partnership-level" details are configured at the Host level; see "***AS1, AS2 and AS3 - Hosts - AS3*** (see "***AS3***" on page 387)" for more information.



Edit AS3 Destination - Demo AS3

Configure the settings for this step:

Folder: /home/myorg

☑ Use Original File Name(s)

Filename: [OrigName]

□ Send all source files in a single ASx message

☑ Request MDN

☑ Request Signed MDN

☑ Use Partner Encryption Certificate for Signature Validation

Validation Certificate: Other Certs/Partner Organization

☑ Look for MDN(s) in Same Folder as Files

MDN Folder: /home/myorg

MDN Filemask: *.mdn

MDN URL*: ftp://ftp.partnerorg.com

* The MDN URL value is typically ignored

☑ Use Default Retry Count — Retry Count: 3

☑ Use Default Retry Timeout — Retry Timeout: 30 seconds

AS3 Destination Options:

- **Folder** - The folder on the AS3 FTP server to write EDI data message files to. The Browse button may be used to easily select a folder on the remote host. You may use ***Macros*** (see "***Macro***" on page 137) in this field.
- **Use Original File Name(s)** - Indicates whether or not MOVEit Central should send the file with the name under which it was saved on the source. If this option is not checked, MOVEit Central will use the name defined in the **Filename** field. This name may contain macros.
- **Send all source files in a single ASx message** – When this option is checked, instead of an individual ASx message for each of the source files, this destination will send a single ASx message with multiple attachments.
- **Request MDN** - When this option is checked, MOVEit Central will request an MDN from the destination partner to verify that the data arrived, and will not consider the task complete until it has received one.
- **Request Signed MDN** - When this option is checked, MOVEit Central will request that the MDN sent by the destination partner be signed by the partner's SSL certificate, to verify the origin of the MDN message.
- **Use Partner Encryption Certificate for Signature Validation** - When this option is checked, MOVEit Central will use the Partner Certificate configured in the referenced AS1 host to validate the signature on the MDN received from the partner. If this option is not checked, a different SSL certificate may be configured for signature validation in the Validation Certificate field.
- **Look for MDN(s) in Same Folder as Files** - When this option is checked, MOVEit Central will look for MDNs from the destination partner in the same FTP folder that we uploaded the EDI data message file to. If this option is not checked, a different MDN folder may be entered in the **MDN Folder** field. The Browse button next to this field may be used to easily select a folder on the remote host. You may use Macros in the **MDN Folder** field.
- **MDN Filemask** - The filemask to use to search for MDNs from the destination partner. You may use Macros in this field, as well as * and ? wildcard characters.
- **MDN URL** - The FTP URL which MDNs sent by the destination partner should be sent to. This value, while required by the AS3 specification, is typically ignored. By default, it is set to a properly formatted URL based on the referenced AS3 hostname or IP address.

Advanced Topics

FTP Source Integrity

Verifying a downloaded file's integrity requires a means of assuring that the local copy of the file is identical to the remote copy of the file. When downloading a file from a MOVEit DMZ host, MOVEit Central automatically sends a "hash" of the downloaded file to DMZ, to make sure the file it received is identical to the file on DMZ. This "hash" is essentially a fingerprint of the file, and is constructed so that the likelihood of two different files having the same hash is very remote.

FTP servers do not support a standard method for providing such an assurance for clients who download files from them. However, many FTP server operators opt to use a method which provides a partial assurance of the downloaded file's integrity. This method involves making available a file on the FTP server which contains a list of hashes of the other available files. The client can then check the hashes listed in that file against the files it downloaded.

Any hash system can be used for this method, but the most frequently used is the MD5 hash. Central now supports using an MD5 file on a source FTP server to check downloaded files against. The option is available on FTP and SSH hosts, and is overridable on sources using FTP or SSH hosts. When properly configured, Central can check for an MD5 hash file (normally these files are named MD5SUM, but Central does support supplying a different name), and verify its downloaded files against the hashes contained in it. If a file does not match the hash listed for it, or if the file does not have a hash listed for it (only if MD5 checking is set to Required), Central will generate an error and discontinue processing of that file.

Note that because this method relies on downloading a list of file hashes, it cannot provide complete integrity verification, since there is no way for Central to make sure that the MD5 hash file was not altered in transit. It does, however, provide more verification than a normal FTP transfer, and under normal circumstances, will provide a defense against files that are somehow corrupted during transport.

Setting Up MD5 Hash Files on an FTP Server

The majority of FTP server operators that provide MD5 files use a program called "md5sum" to generate those files. This program takes a list of files and generates a list of MD5 hashes for those files. This output is then redirected to a file, normally called MD5SUM, which resides in the directory along with the files it contains hashes for. FTP operators wishing to provide MD5 hash files for a MOVEit Central client should use this program. It is widely available on the internet, as well as being included in most UNIX distributions today. Use your favorite search engine to find a copy for your specific system, if you don't have it installed already.

To generate an MD5 hash file with md5sum, simply execute it with the list of files you wish to create hashes for, and redirect its output to a file called MD5SUM. For example, to create a hash file of all the files in the /ftproot/products directory on a server, issue the following command:

```
cd /ftproot/products

md5sum * > MD5SUM
```

Issuing a command like this for all important FTP content directories on a frequent basis will help provide added assurance that the files downloaded by clients such as MOVEit Central are identical to the files on your FTP server.

Custom Directory Parsing

MOVEit Central provides a high degree of flexibility for downloading from unusual FTP and SSH servers.

When downloading from an FTP server, an automated FTP client must request a directory listing and "parse" the results in order to determine the names, date stamps, sizes, and other information about the files on the server. A problem faced by any automated FTP client is that there is no official standard format for this information. Each FTP server vendor chooses its own format for this information. As a result, there are scores of different and incompatible formats. FTP clients must make sense of these many different types of directory listings. SSH clients face a similar situation, although the problem is not as severe.

MOVEit Central provides a great deal of flexibility in dealing with this unfortunate situation by providing several different options:

- **Automatic recognition of common servers.** By default, MOVEit Central will automatically recognize and parse directory listings from the most common types of FTP and SSH servers, including Windows, UNIX, Novell, MVS, Unisys, and Van Dyke.
- **"Blind" downloads.** (see "**Hosts Tab**" on page 149) If the name of the file is known in advance, you can instruct MOVEit Central to download the file without requesting a directory listing, bypassing the problem altogether.
- **Column-based custom parsing (on page 401).** If the directory listing has a simple tabular format that can be described by rows and columns, you can specify these parameters in the host definition.
- **Directory parsing script (on page 402).** For the ultimate in flexibility, you can write a script in VBScript to parse a directory listing. Literally any format can be handled this way.

The options below are configured in the host's Advanced Options dialog, under Custom Parsing.

Column-based Custom Parsing

With column-based directory parsing, directory listings are assumed to contain one file per line, with optional header and trailer information that is ignored. The following parameters are configured for the host:

- **Filename start column.** This is the column number (with 1 being the first column) in which the filename starts. The filename ends at the first space, or end-of-line.
- **Date start column.** If non-zero, this specifies the column at which the file's date stamp starts. The date/time format must match one of the formats described in ***Date and Time Formats*** (on page 404) below. It is permissible to leave this field zero, but then the "Only New Files" option will not be available.
- **Skip Lines Top.** Specifies the number of lines of header information that should be skipped at the beginning of the listing. Typically this is 0.
- **Skip Lines Bottom.** Specifies the number of lines of trailer information that should be skipped at the end of the listing. Typically this is 0.

For the following fictitious 5-line FTP directory listing:

```
XYZZY FTP Server Directory Listing, prepared at 14:10:55

         267 2006-02-15 15:27:39 trnreport.txt
      537401 2005-11-29 21:12:47 xyz2005.rpt
*** END OF FILE LIST.
```

the settings would be:

Filename column	34
Date column	14
Skip Lines Top	2
Skip Lines Bottom	1

Directory Parsing Script

With this option, you write a script (or use a vendor-supplied script) to parse a directory listing. Directory parsing scripts are written in VBScript and are configured and edited the same as other MOVEit Central scripts. Two directory-parsing-specific functions are available:

- sDirListing = **MIDirGetListing()**

  Returns the entire verbatim listing from the FTP or SSH server. This typically contains lines separated by CR and LF (ASCII 13 and 10).

- **MIDirAddEntry** FilenameToMatch, Date, Size, bIsDir, FilenameForGet, FilenameOriginal

  Adds an entry to the FTP or SSH directory listing being parsed.

  FilenameToMatch is the filename against which MOVEit Central should match when doing filename wildcard matches.

  Date is a string in one of the ***date formats*** (on page 404) specified below. This can be "", but in that case, the "Only New Files" feature will not work.

  Size is the size in bytes. Set this to 0 if the size is unknown.

  bIsDir is a boolean variable that should be True if this entry is a directory rather than a file.

  FilenameForGet is the filename to send to the server when requesting a download of the file. It is usually the same as FilenameToMatch

  FilenameOriginal is the filename to return as the original filename, in such contexts as the [OrigName] macro. It is usually the same as FilenameToMatch.

  The last two parameters, FilenameForGet and FilenameOriginal, are for use with FTP servers running on operating systems with unusual filesystems. Normally all three filenames should be set the same.

Most other MOVEit Central MIxxx functions are not available in a directory parsing script.

To explain the differences between the three versions of the filename, consider a hypothetical FTP server that allows multiple numbered versions of a file, with the version following the filename in a directory listing. Suppose the directory listing looks like this:

```
MYFILE.DAT;22 45321 2006-05-06 08:11:56

MYFILE.DAT;21 44090 2006-05-05 17:20:40

README.TXT;3 8192 2005-12-30 21:38:27
```

In this directory listing, there are two versions of MYFILE.DAT, with version 22 being the more recent.

Ordinarily, the user will not know in advance which numeric version is desired; the user will only know that they want the most recent version, or perhaps the next-to-most-recent version, etc. Therefore, it would be unreasonable to configure a MOVEit Central source with a filemask that refers to a specific version number.

For the purposes of this FTP server, we can invent a filemask syntax in which the most recent version is referred to as MYFILE.DAT(0), the next most recent version as MYFILE.DAT(-1), etc. However, when transferring the file to the destination, we don't care about the version number at all, because most destination servers will not recognize file versions. We want to name the file simply MYFILE.DAT.

Thus, there are three versions of the name

- The name we use in the file mask in the source to select the file, e.g., MYFILE.DAT(0)
- The name that MOVEit Central must use when retrieving the file, e.g. MYFILE.DAT;22
- The name used in the destination as the Original Name, e.g., MYFILE.DAT

So, a script parsing this directory listing would do the equivalent of:

```
FilenameToMatch = "MYFILE.DAT(0)"

MyDate = "2006-05-06 08:11:56"

MySize = 45321

bIsDir = False

FilenameForGet = "MYFILE.DAT;22"

FilenameOriginal = "MYFILE.DAT"

MIDirAddEntry FilenameToMatch, MyDate, MySize, bIsDir, FilenameForGet,
FilenameOriginal
```

Date and Time Formats

Both of MOVEit Central's custom directory parsing options recognize several datestamp formats. If the date format used by an FTP server does not match one of the following, you will not be able to use column-based parsing. Instead, you will have to use a script to massage the date before sending it to MIDirAddEntry.

A file date/time stamp is assumed to consist of a date, followed by one or more spaces, followed by a time. If the time is not recognized, it will be treated as midnight (00:00:00).

The date formats are:

- **YYYY-MM-DD** - The preferred format.
- **YY-MM-DD** - This uses a Y2K-like "pivot year" of 1970. Values from 0 to 70 are assumed to be 2000 through 2070. Values 71-99 are assumed to be 1971-1999.
- **MM/DD/YY** - Uses the same pivot year.
- **MM/DD** - Assumes that the date is within the last 12 months. If the date is today or prior to the current day of the year, it's assumed to be in this year, else it's assumed to be in the previous year.

The time formats are:

- **hh:mm** - Time in 24-hour format.
- **hh:mm:ss** - Time in 24-hour format.
- **hh:mm*AMPM*** - Time in 12-hour format. ***AMPM*** must be **AM**, **am**, **PM**, or **pm**.
- **hh:mm:ss*AMPM*** - Time in 12-hour format, as above

Sample Script

The following script demonstrates custom directory parsing.

```
' This script parses a directory listing from a Windows FTP server.
' In real life, this script would not be necessary, because
' MOVEit Central is able to natively recognize and parse directory
' listings on Windows FTP servers.
'
' A Windows FTP server returns a directory list like: ' 05-02-06 04:22PM 734
ModsNotes.txt
' 10-13-05 09:13AM <DIR> Incoming
' 123456789a123456789b123456789c123456789d123456789
'
Option Explicit
Sub Main()
  Dim sDirListing, aryLines, MyLine, TestForDir, MyName, j
  Dim MyYear, MyMonthDay, MyTime, MyDate, MySize, bIsDir, NFiles, NDirs sDirListing
= MIDirGetListing()
   ' Break apart the listing into an array of lines.
   aryLines = Split(sDirListing, vbCrLf)
   NFiles = 0
   NDirs = 0
  For j = LBound(aryLines) To UBound(aryLines)
      MyLine = aryLines(j)
      ' Heuristic to ignore any unreasonably short lines.
    If Len(MyLine) > 39 Then
         ' MOVEit Central doesn't understand mm-dd-yy format,
         ' so change a date like 10-13-05 to 05-10-13.
         MyMonthDay = Mid(MyLine, 1, 5)
         MyYear = Mid(MyLine, 7, 2)
         MyTime = Mid(MyLine, 11, 7)
         MyDate = MyYear & "-" & MyMonthDay & " " & MyTime
         MyName = Mid(MyLine, 40)
         TestForDir = Mid(MyLine, 25, 5)
      If TestForDir = "<DIR>" Then
            bIsDir = True
            MySize = 0
            NDirs = NDirs + 1
      Else
            bIsDir = False
            MySize = Mid(MyLine, 19, 38-19+1)
            NFiles = NFiles + 1
      End If
         MIDirAddEntry MyName, MyDate, MySize, bIsDir, MyName, MyName
    End If
  Next
  If MIGetDebugLevel() >= 50 Then
      MILogMsg "Found " & NFiles & " files and " & NDirs & " dirs"
  End If
End Sub

Main
```

SysLog and SNMP

MOVEit Central does not directly log events to SysLog or SNMP management consoles, but MOVEit Central does log to the Windows Event Log. This guide briefly describes several easy-to-obtain utilities which will send MOVEit Central entries from the Windows Event Log to a Syslog or SNMP management console. It is generally best to log events into the Windows "MOVEit" Event Log instead of the Windows "Application" Event Log if you plan on using any of these utilities to avoid having to screen for particular event log entry sources.

Syslog Utilities

SysLog is based on UDP (usually port 514). SysLog is an "unreliable" protocol in the sense that neither the client nor the server will know (or care) if SysLog messages are dropped by the network.

Event Reporter

An eight-year-old commercial client called "***Event Reporter*** (see http://www.eventreporter.com/en - ***http://www.eventreporter.com/en***)" is available to perform filtering on event logs before sending them to a SysLog.

Snare

A freeware client called ***Snare*** (see http://www.intersectalliance.com/projects/SnareWindows - ***http://www.intersectalliance.com/projects/SnareWindows***) is available to perform filtering on event logs before sending.

WinAgents Event Log Translation Service

A commercial client called "***WinAgents Event Log Translation Service*** (see http://www.winagents.com/en/products/eventlog-syslog/ - ***http://www.winagents.com/en/products/eventlog-syslog/***)" is available to perform some filtering on event logs before sending them to a SysLog server and/or an SNMP management console.

winlogd

A freeware utility called ***winlogd*** (see http://www.edoceo.com/creo/winlogd/ - ***http://www.edoceo.com/creo/winlogd/***) can be used to scoot all events from all event logs to a designated SysLog server.

```
D:\temp>winlogd -i

Installation successful, say `net start winlogd`



D:\temp>winlogd --show

Server:   192.168.101.1

Port:     514

Facility: LOCAL3

Monitor:  6000

Flush:    6000



D:\temp>net start winlogd

The winlogd service is starting.

The winlogd service was started successfully.
```

This program does not have a lot of options (Server, Port and Facility), but it is a quick and effective way to get MOVEit DMZ events and other interesting messages into a designated SysLog server.

SNMP

The SNMP protocol uses the concepts of "community"; typically events are fired off into a community and an SNMP management console collects, logs and perhaps acts upon them. Ipswitch makes no suggestion regarding SNMP management consoles; our customers usually either have one or do not have one, and selection of this type of server goes well beyond this documentation. However, Ipswitch does suggest a couple of clients which would likely work as an SNMP "client" in most SNMP situations.

Like SysLog, SNMP is based on UDP (usually port 161). As such, SNMP is not the most reliable protocol out there.

Unlike SysLog clients, SNMP "clients" tend to be purchased in bulk. In fact, if you own an SNMP management console, you likely already also own an SNMP client you can use. (Ask the group in charge of your SNMP management console.) Nonetheless, there are a handful of vendors who will offer you a compatible, standalone SNMP client.

WinAgents Event Log Translation Service

A commercial client called "***WinAgents Event Log Translation Service*** (see http://www.winagents.com/en/products/eventlog-syslog/ - ***http://www.winagents.com/en/products/eventlog-syslog/***)" is available to perform some filtering on event logs before sending them to a SysLog server and/or an SNMP management console.

Antivirus

Using Real-Time Scanners

MOVEit Central can be used to scan downloaded files via its interface to third-party real-time antivirus utilities. These utilities work by immediately deleting infected files as they are written to or read from MOVEit Central's cache directory. MOVEit Central will notice that the file is no longer available and will obtain the infection information from the antivirus logs. It will then take the action that you have configured on the configuration program's ***Virus tab*** (on page 27).

MOVEit Central will consider any individual file transfer that failed because a virus was detected to be a "normal" failure in the sense that it will log a specific "virus found" message in the file failure record and will initiate any configured "failure" next actions (including email alerts) configured for the task. Furthermore, MOVEit Central will consider any task that finds a virus in one of its files to have partially failed, although it will normally continue to transfer all files that did not contain viruses in the same task run.

MOVEit Central currently interfaces with the following antivirus programs:

- Symantec AntiVirus
- McAfee VirusScan
- Trend Micro OfficeScan

MOVEit Central will notice and handle infections detected by other real-time antivirus programs, but it will not be able to report the name of the specific virus that was detected.

After connecting to MOVEit Central, use the "Command | Test Antivirus" command from MOVEit Central Admin to test if MOVEit Central and your local antivirus package are successfully communicating.

Notes on Trend Micro OfficeScan. If you are using Trend Micro's OfficeScan, you should be aware that the default installation options enable scanning for only a few file extensions. This will cause the scanner to miss most infections, since by default, MOVEit Central uses random temporary filenames in its cache, not the original filenames. To instruct OfficeScan to scan all filenames, point your browser at its web interface and choose the following links: Clients, Scan Options, Real-Time Scan Settings, Scan Target, All scannable files.

Using Processes to Scan Files On Demand

Less commonly, MOVEit Central can be used to individually scan files in its cache using a third-party antivirus program. To actively scan each file passing through MOVEit Central, you would probably use the included "Run DOS Command.vbs" script or a derivation to kick off the command-line utility provided by your antivirus client. This script runs a single command and errors out if a command-line antivirus client returns a code other than 0. Alternatively, you could compose a script to invoke a COM interface of an antivirus client. This approach is more work, but could also supply MOVEit Central with more information.

One caveat that applies to this approach is that you must configure your real-time antivirus client to ignore the MOVEit Central cache folder to avoid interference between the two scanning mechanisms.

Note: When setting files to scan in your Antivirus program, you should exclude mic*.xml config/state/hash files to improve the performance.

POP3 Sources

POP3 sources download email messages from a POP3 server. Each attachment in a message is considered a distinct file. The body of a POP3 email message is not considered a file, so an email message with no attachments is considered to have no files.

The fact that an email message may have multiple attachments makes POP3 sources unique from the point of view of Collect Only New Files and Delete Original processing. For instance, if an email message has two attachments:

- report1.txt
- fig1.gif

and a task specifies that only *.txt attachments be downloaded, then only report1.txt will be processed. MOVEit Central will note (in the POP3 host's corresponding State File) the fact that this report1.txt has been processed, and that fig1.gif has not been processed. Subsequent attempts to download *.txt files from this source will not collect report1.txt if Collect Only New Files is checked.

If Delete Original is checked, this message will not be deleted, because some other task may wish to download *.gif files. If some other task does download and successfully process fig1.gif, and Delete Original is marked for this task, then the task will see that all attachments for this message have now been processed, and the task will delete the message.

The ramifications of this processing are:

- Messages containing attachments with filenames that do not match any masks from any POP3 sources will never be deleted, even if Delete Original is checked in some or all sources.
- Messages containing no attachments will never be deleted, because they will never be processed.

It is therefore a good idea to periodically manually check the list of messages waiting on the server for this user, especially if the server is Internet accessible and therefore likely to receive unwanted bulk email.

GetMICConfig Utility

Included with MOVEit Central is a command-line utility, GetMICConfig.exe, to retrieve the current configuration from a running copy of MOVEit Central on the local machine. The ability to retrieve the current configuration useful for certain advanced tasks, such as generating custom reports.

Although MOVEit Central's configuration is already stored in a disk file named miccfg.xml, this file is encrypted and is therefore not usable by external applications. And although a similar config export capability is available via MOVEit Central Admin, MOVEit Central Admin requires human interaction. By contrast, GetMICConfig is suitable for running from a script or batch file.

GetMICConfig is installed in the same directory as MOVEit Central, typically \Program Files\MOVEit.

GetMICConfig's command line is:

```
GetMICConfig -o outfile [-k]
```

where:

outfile is the name of the desired output file. This file will contain the entire MOVEit Central configuration in plaintext XML format. (This does not include the small number of settings, such as the license key, that are maintained in the registry and administered by the ***MICentralCfg*** (see "***Central Config Utility***" on page 17) program.)

-k specifies that the old copy of *outfile*, if any, should be kept if GetMICConfig is unable to retrieve the settings. By default, GetMICConfig will delete any old *outfile* before connecting to MOVEit Central.

The program exit code is:

0 if all OK
1 if command-line error
2 if communication error with MOVEit Central
3 if bad response from MOVEit Central
4 if could not write output file

This can be checked from a batch file using IF ERRORLEVEL.

Port Numbers

This technical document describes the IP port numbers used by MOVEit Central. This information is provided to allow network administrators to configure firewalls appropriately.

Most protocols (marked with * below) allow non-standard ports to be used, so at some sites, some additional ports not mentioned here may need to be opened up on the firewall.

MOVEit Central (MICentral.exe)

Port	Direction	Description
21 *	Outgoing	Typical port number for traditional, or "explicit" secure, FTP servers.
22 *	Outgoing	Typical port number for SSH servers.
25 *	Outgoing	Typical port number used for outbound email using SMTP (Simple Mail Transfer Protocol).
80 *	Outgoing	Typical port number for insecure HTTP servers, including MOVEit DMZ.
110 *	Outgoing	Typical port number used to fetch incoming email using POP3 (Post Office Protocol).
139	Outgoing	Port used for Windows filesystem shares. The protocol is known as SMB (Server Message Block).
443 *	Outgoing	Typical port number for secure HTTPS servers, including MOVEit DMZ.
990 *	Outgoing	Typical port number implicit secure FTP servers.
1433	Outgoing	MOVEit Central generally connects to Microsoft SQL Server on this port, if SQL Server is the database engine.
3306	Outgoing	MOVEit Central connects to MySQL on this port, if MySQL is the database engine.
3471-3473	Incoming	MOVEit Central Admin connects to MOVEit Central on these ports.
3472	Outgoing	On a failover system, MOVEit Central connects to the other MOVEit Central on this port.

Port	Direction	Description
3478-3479	Outgoing	MOVEit Central connects to the AS/2 module, MIAS2.exe, on these ports.
Various	Incoming	Unpredictable port numbers > 1023 used for active mode FTP data transfers.
Various	Outgoing	Generally unpredictable port numbers > 1023 used for passive mode FTP data transfers.

MOVEit Central Admin (miadmin.exe)

Port	Direction	Description
3471-3473	Outgoing	MOVEit Central Admin connects to MOVEit Central on these ports.

MOVEit Central AS/2 helper (MIAS2.exe)

Port	Direction	Description
21 *	Outgoing	Typical port number for traditional, or "explicit" secure, FTP servers.
25 *	Outgoing	Typical port number used for outbound email using SMTP (Simple Mail Transfer Protocol).
80 *	Outgoing	Typical port number for insecure HTTP servers, including MOVEit DMZ.
110 *	Outgoing	Typical port number used to fetch incoming email using POP3 (Post Office Protocol).
443 *	Outgoing	Typical port number for secure HTTPS servers, including MOVEit DMZ.
990 *	Outgoing	Typical port number implicit secure FTP servers.
3478-3479	Incoming	MOVEit Central connects to the AS/2 module, MIAS2.exe, on these ports.
Various	Incoming	Unpredictable port numbers > 1023 used for active mode FTP data transfers.
Various	Outgoing	Generally unpredictable port numbers > 1023 used for passive mode FTP data transfers.

MySQL (mysqld-nt.exe)

MySQL is one of the database engines that is supported by MOVEit Central.

Port	Direction	Description
3306	Incoming	Database server listens on this port number. Only local (127.0.0.1) connections are needed.

* indicates a default port number that can be overridden.

System Internals

This technical document describes the registry settings used by MOVEit Central. This information is rarely needed, as most of the settings here are managed by the MOVEit Central Config program. However, there are a few rarely-used settings, documented in this style, which can be configured only by direct manipulation of the registry by a program like RegEdit. These values normally do not appear in the registry at all.

Hidden Configuration File Settings

The following are hidden settings that can be set from within the MOVEit Central XML configuration file (miccfg.xml):

XPath	Description
Settings/Globals/MaxMaxSimulTasks	The maximum allowed value for the MaxSimulTasks setting. If this doesn't exist in the config, then it defaults to 100.
Settings/Globals/ProcessFilesAddedInLoop	Whether an Advanced Task For loop should process files added in that loop. If this doesn't exist in the config, then it defaults to 0, which means that a file added by a script within a For loop will not be processed by further iterations of that loop. (However, it will be processed by other For loops.) A value of 1 causes script-added files to be processed by future iterations of the loop, likely causing an undesirable infinite loop. MOVEit Central 7.1 and previous versions defaulted this value to 1; 7.1.1 and subsequent versions default it to the less dangerous 0 value.

XPath	Description
Settings/Globals/KeepAliveIntervalSecs	The KeepAliveIntervalSecs setting is used to prevent dropped connections between the MOVEit Central Service and the Admin console when MOVEit Central is used in a network environment that monitors idle connections. When the KeepAliveIntervalSecs setting is set to the default value of 540 seconds (9 minutes), the Admin console sends a keep alive command (at a 9 minute interval) to the MOVEit Central service. A value of -1 for KeepAliveIntervalSecs will disable keep alive commands completely.
Settings/Globals/KeepAliveTimeoutSecs	When set to the default value of 1800 seconds (30 minutes), the KeepAliveTimeoutSecs setting ignores a socket timeout of up to 30 minutes. A value of -1 for KeepAliveTimeoutSecs will disable keep alive socket timeouts, but keep alive commands will continue to be sent.

Registry Settings

The following values appear under HKEY_LOCAL_MACHINE \ Software \ Standard Networks \ MOVEitCentral:

Name	Type	Description
CertIssuer	String	The name on the SSL certificate that MOVEit Central uses to encrypt communications with MOVEit Central Admin.
CertSerial	String	The serial number (typically "00") of the SSL certificate that MOVEit Central uses to encrypt communications with MOVEit Central Admin.
DeleteCacheInsecurely	DWORD	If 0, then at the end of a task, MOVEit Central will overwrite temporary files with random bytes before deleting them. If 1, MOVEit Central will simply delete the files.

Name	Type	Description
DMZBigBufSize	DWORD	The size, in bytes, of the large buffer used by the MOVEit DMZ client. The default is rather large at 104857600 (100 MB), to accommodate very large responses from MOVEit DMZ. You may wish to decrease this value, perhaps to 1000000, in order to have MOVEit Central use less memory, and start up and shut down faster.
EmailFrom	String	The "From:" email address used in error emails.
EmailServer	String	The host name or IP address of the SMTP server used for error emails.
ErrorEmail	String	The "To:" email address(es) used in error emails.
FlushLogAlways	DWORD	If 1, MOVEit Central will flush the debug log to disk after every write. This greatly slows performance, and should be used only if you want to be certain to have the entire log file available if MOVEit Central crashes.
HashKey	String	This is the encrypted value used as the basis of an encryption key for hash-chaining the records in the database, in order to be able to detect tampering. If you are performing a MOVEit Central Failover or a migration operation, do not copy the "HashKey" value from the registry into any of the fields on the "Tamper" tab in the MOVEit Central Config utility. Instead copy "HashKey" registry values from one registry to another to avoid reencrypting an encrypted value.
LicenseKey	String	The license key that enables this copy of MOVEit Central.
MaxHTTPSessionsPerServer	DWORD	The maximum number of HTTP connections that can be maintained simultaneously to a given webserver. The default is 100, and there is rarely a need to change this.
MinAdminVersion	String	The minimum version of MOVEit Central Admin required, in a format like 4.5.0.0. If present, this non-standard setting overrides the value coded into MOVEit Central.
MySQLDir	String	The directory in which MySQL is installed; typically C:\MySQL.

Name	Type	Description
MySQLRootPW	String	The password to the MySQL database user named root; strongly encrypted.
RequireSSL	DWORD	1 if connections from MOVEit Central Admin are required to be encrypted with SSL; else 0 if they are not encrypted.
SchedDisabled	DWORD	1 if the task scheduler should be disabled when MOVEit Central starts; else 0 if the scheduler should run normally.
SSHBufferSize	DWORD	The size, in bytes, of the buffer used by the SSH client. The default will work well for almost all cases. This value should be set only if needed for compatibility with unusual SSH servers, or if a very large value is needed to enhance WAN performance.
StatsDSN	String	The ODBC Data Set Name of the database used by MOVEit Central, if StatsUseConnStr is missing or 0. This is used when MySQL is the database engine. This is nearly always "DSN=micstats;".
StatsConnStr	String	The database connection string, used if StatsUseConnStr is 1. At runtime, a reference to the macro [DBPassword] is filled in with the actual password, decrypted from StatsConnStrPW.
StatsConnStrPW	String	The encrypted password to the database user, used if StatsUseConnStr is 1 and if the macro [DBPassword] appears in StatsConnStr.
StatsUseConnStr	DWORD	1 if StatsConnStr should be used for database connection settings. This is used for Microsoft SQL Server. If the setting is 0 or is missing, StatsDSN is used instead.
StoreLocation	DWORD	A numeric value used to find the certificate that MOVEit Central uses to encrypt communications with MOVEit Central Admin; nearly always 0x00020000.
StoreName	String	The name of the certificate store containing the certificate that MOVEit Central uses to encrypt communications with MOVEit Central Admin; nearly always "My".

Name	Type	Description
SuppressLowFragHeap	DWORD	If 1, this non-standard setting prevents MOVEit Central from using the "low fragmentation heap" for memory management. Use this only if you have a specific reason for doing so.
TempDir	String	The name of the parent temporary folder used for cache files; typically C:\TEMP\MIC.
Update	DWORD	An arbitrary value changed by the configuration program to alert MOVEit Central that the registry values have changed.
VirusHandlingIDed	DWORD	A numeric code indicating how MOVEit Central should react to files that appear to be infected with a specific, identifiable virus.
VirusHandlingNotIDed	DWORD	A numeric code indicating how MOVEit Central should react to files that appear to be infected with a virus, but we don't know which virus.

The following values appear under HKEY_LOCAL_MACHINE \ Software \ Standard Networks \ MOVEitCentral \ Install. They are used only by the install program:

Name	Type	Description
MICAdminUserName	String	The username of the MOVEit Central Admin user created during the install.
MICAdminUserWhetherCreated	DWORD	1 if the install program created the above user, else 0 if an existing user was selected.
ServiceUserName	String	The username of the user under which the MOVEit Central service is running.
ServiceUserWhetherCreated	DWORD	1 if the install program created the above user, else 0 if an existing user was selected.

The following values appear under HKEY_LOCAL_MACHINE \ Software \ Standard Networks \ MOVEitCentral \ Resil. They apply only to a failover installation:

Name	Type	Description

Name	Type	Description
AdminPassword	String	The password to the user on the remote MOVEit Central system (strongly encrypted).
AdminUser	String	The username of the MOVEit Central user on the remote system.
HostsToPing	String	A comma-separated list of hosts to ping before a secondary assumes the primary role.
Node	DWORD	The number of this node: 0 for non-failover; else 1 or 2.
OtherHost	String	The hostname or IP address of the other MOVEit Central.
StartupRole	DWORD	The failover role that MOVEit Central should assume at startup; 1 means primary and 2 means secondary. This is ignored if the node number is 0.
SuppressDBRep	DWORD	Whether replication of the database should be suppressed. The default is 0, which means that in failover mode, the database will be replicated. 1 means to not replicate the database in failover mode, and should be used only by advanced users. 1 should be specified if, for instance, both nodes are connected to the same clustered database, where the cluster is providing the high availability normally provided by MOVEit Central itself.

Local Mail Relay

You should consider using Windows Server's IIS SMTP server as a local mail relay on your MOVEit Central system any of the following conditions apply.

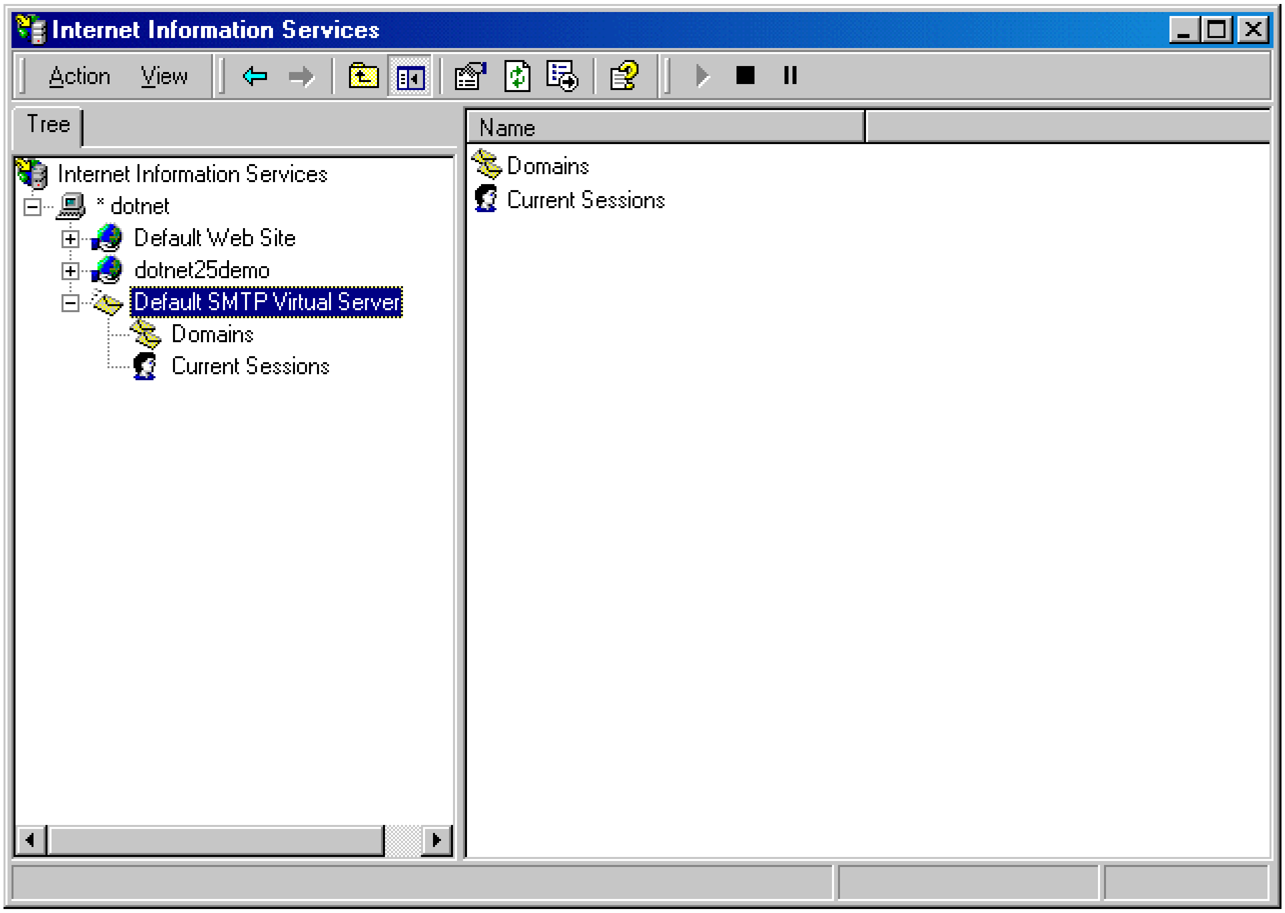
- You have many tasks that send email notifications
- You have a slow or busy mail server
- Your mail server requires an advanced method of authentication for relaying mail

MOVEit Central can send files by email, or send email alerts on completion of a task. These notifications happen as part of the task run, so MOVEit Central must wait for each message to be sent before the task is completed. When MOVEit Central is dealing with busy email servers or large numbers of recipients, tasks may run significantly longer than normal. To keep MOVEit Central from having to wait for each message to be sent, we can instead spool these messages to a local SMTP server which will queue up the messages and send them out to "real" email servers when they are better able to accept the traffic.

Instructions

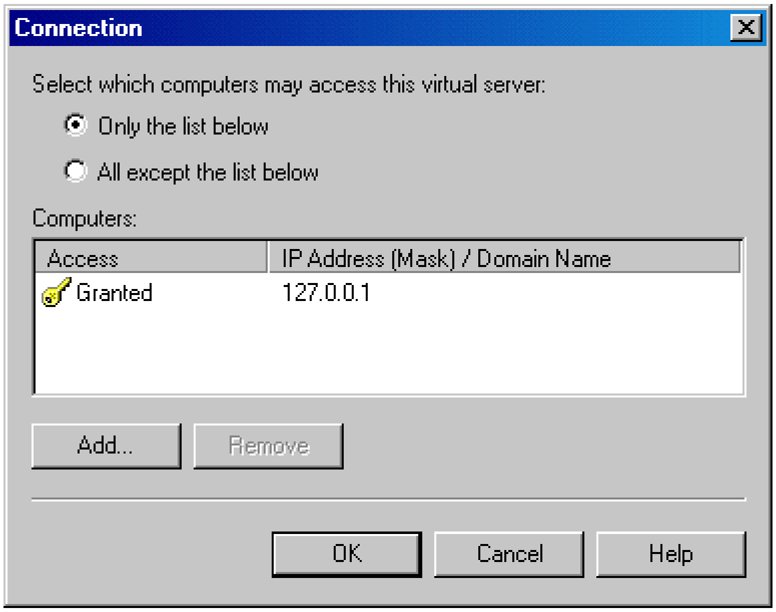
Step 1

Ensure that you have the SMTP component installed in your local IIS server. When installed correctly, you should see a Default SMTP Virtual Server node in your IIS administration window under the local machine. If you do not have the SMTP component installed, or do not have IIS installed, you will need to install them through the Add/Remove Windows Components option of the Add/Remove Programs window, which can be found in the Control Panel.



Step 2

Open up the properties window of the SMTP service by right-clicking on the SMTP service node and selecting Properties. In the properties window, select the Access tab. In the Access tab, open the Connection Control window by clicking on the Connection button in the Connection Control section. Restrict access to the SMTP server by selecting the Only The List Below option and adding the localhost IP address 127.0.0.1 to the access list. Click OK to exit the window.



Connection

Select which computers may access this virtual server:

● Only the list below

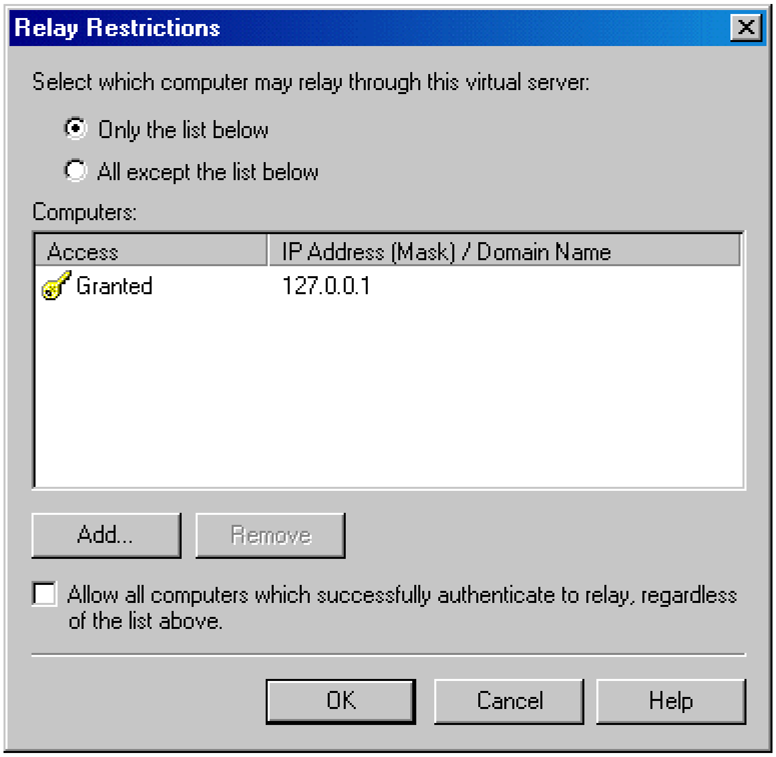
○ All except the list below

Computers:

Access	IP Address (Mask) / Domain Name
Granted	127.0.0.1

Step 3

In the Access tab, open the Relay Restrictions window by clicking the Relay button in the Relay Restrictions section. Restrict relay access to the SMTP server by selecting the Only The List Below option and adding the localhost IP address 127.0.0.1 to the access list. Make sure the Successful Authentication Relay option is turned off. Click OK to exit the window.



Relay Restrictions

Select which computer may relay through this virtual server:

● Only the list below

○ All except the list below

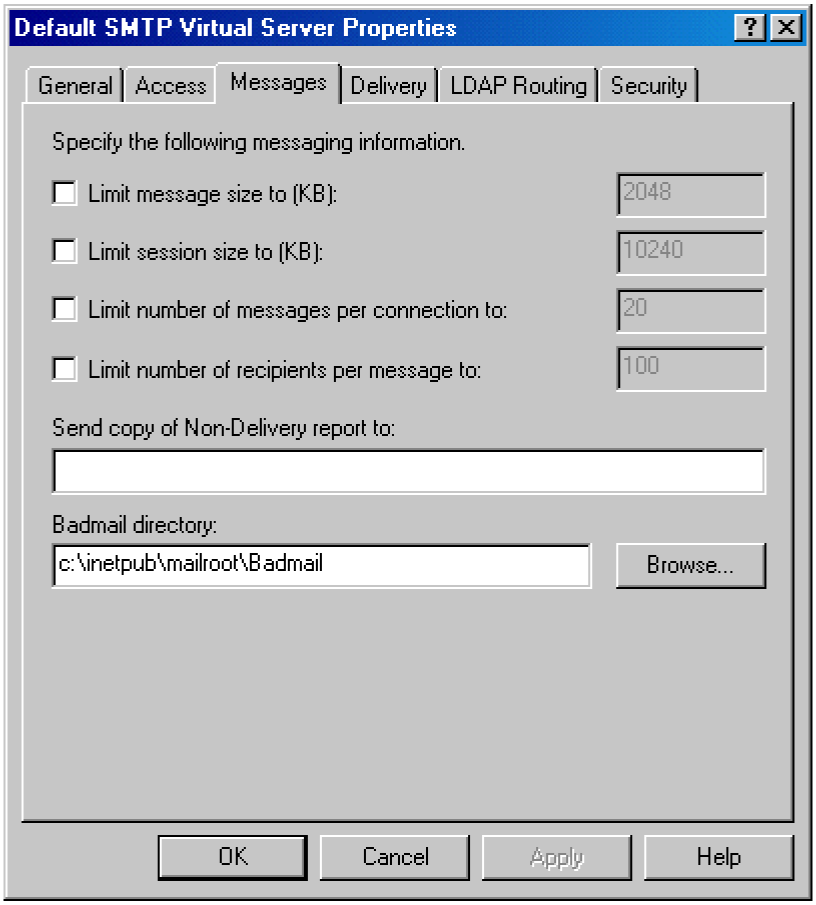
Computers:

Access	IP Address (Mask) / Domain Name
Granted	127.0.0.1

□ Allow all computers which successfully authenticate to relay, regardless of the list above.

Step 4

In the Properties window, switch to the Messages tab. In the Messages tab, turn off all the message limits.



Specify the following messaging information.

☐ Limit message size to (KB): 2048

☐ Limit session size to (KB): 10240

☐ Limit number of messages per connection to: 20

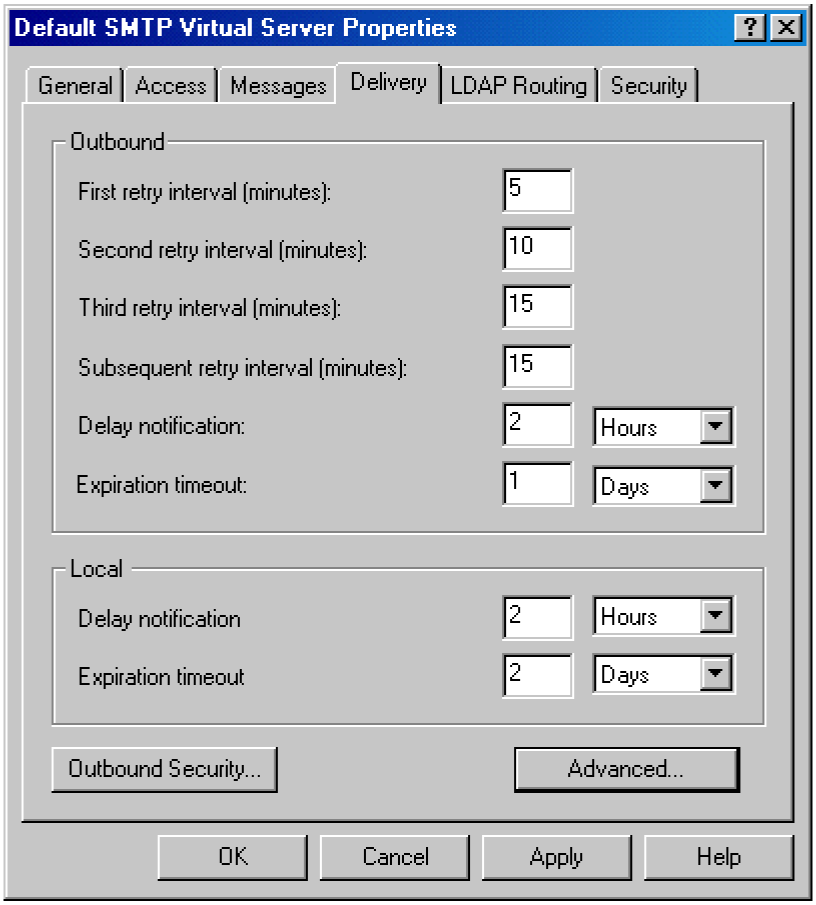
☐ Limit number of recipients per message to: 100

Send copy of Non-Delivery report to:

Badmail directory:
c:\inetpub\mailroot\Badmail

Step 5

In the Properties window, switch to the Delivery tab. In the Delivery tab, change the default delivery intervals and timeouts to smaller values. Recommended values are shown in the image below.



Default SMTP Virtual Server Properties

Outbound

First retry interval (minutes): 5

Second retry interval (minutes): 10

Third retry interval (minutes): 15

Subsequent retry interval (minutes): 15

Delay notification: 2 Hours

Expiration timeout: 1 Days

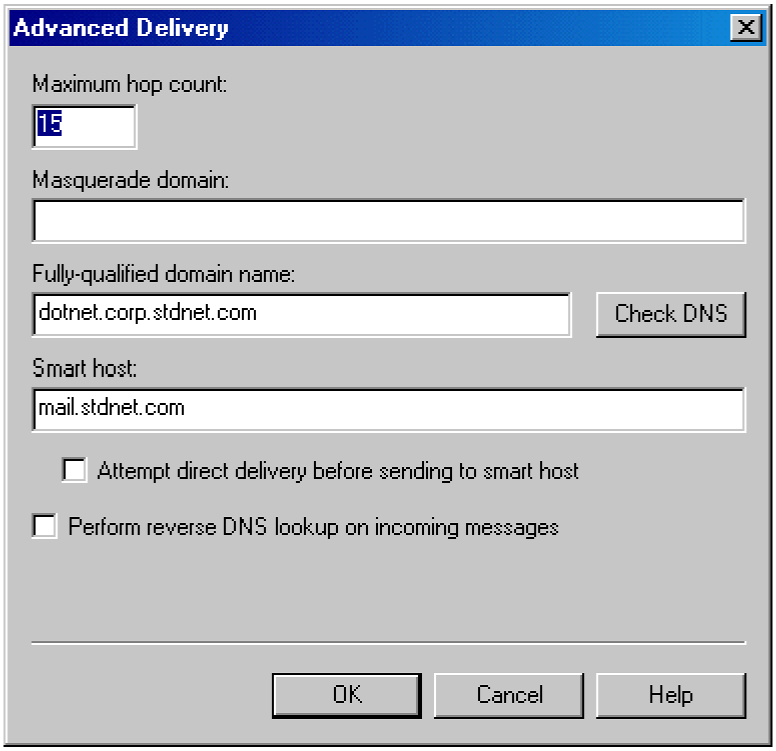
Local

Delay notification 2 Hours

Expiration timeout 2 Days

Step 6

In the Delivery tab, open the Advanced Delivery Options window by clicking the Advanced button. Set the Fully Qualified Domain Name setting to the name of your MOVEit Central server. Set the Smart Host setting to the name of your main SMTP server. Click OK to exit the window. Configuration of the SMTP server is now complete. Click OK in the Properties window and make sure the SMTP service is started.



Advanced Delivery

Maximum hop count: 15

Masquerade domain:

Fully-qualified domain name: dotnet.corp.stdnet.com

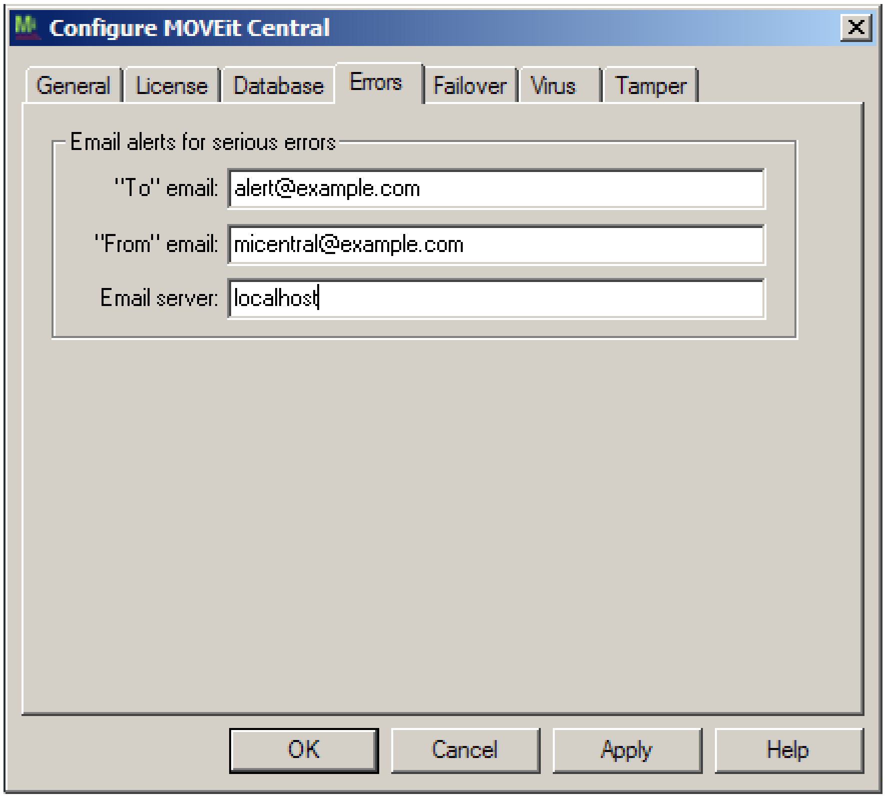
Smart host: mail.stdnet.com

☐ Attempt direct delivery before sending to smart host

☐ Perform reverse DNS lookup on incoming messages

Step 7

The final step is configuring your Central server to use the new local SMTP service. First, open the MOVEit Central Config program (Start -> Programs -> MOVEit Central) and switch to the Errors tab. Enter localhost as the "Email server" value. Click OK to exit the Config program. The change should happen immediately; no restart is required.



Email alerts for serious errors

"To" email: alert@example.com

"From" email: micentral@example.com

Email server: localhost

Next, sign on to the Central server using MOVEit Central Admin and switch to the Hosts tab. If you have an SMTP host configured for your outgoing email server, open it by double-clicking the host entry and change the Host value to localhost. Remove any authentication values as they will not be needed.

Tuning

You will probably want to tinker with the "outgoing connection limit" (default is 1000) if one of your goals is to keep MOVEit Central from overloading your "real" mail server. (Typical "throttled" values are from 1-5.) To alter this setting, open the SMTP properties, go to the "General" tab and open the "connection" dialog.

Finished

Your local SMTP relay server should now be set up, and your MOVEit Central server configured to use it. If you have any questions about or problems with this process, please contact the MOVEit ***technical support*** (***http://www.ipswitchft.com/company/contactsupport.aspx***) department for additional assistance.

Repeat on Each Node if Running MOVEit Central Failover

If you are running MOVEit Central Failover, you must repeat this procedure on each node in the cluster.

Troubleshooting

Problem: Cannot connect to local mail relay.

- **Solution 1:** Open the "Services" from "Start | Program Files | Administrative Tools". Make sure the "Simple Mail Transport Protocol" service is started and that it is set up to start "Automatically."
- **Solution 2:** Open the "Internet Services Manager" from "Start | Program Files | Administrative Tools". Make sure the "Default SMTP Virtual Server" is NOT "stopped".
- **Solution 3:** Open the "Internet Services Manager" from "Start | Programs | Administrative Tools". Right-click on "Default SMTP Virtual Server" and select Properties. In the General tab make sure the IP Address is set for "All Unassigned".
- **Solution 4:** Go to the command line and type "netstat -a -n". Look for any TCP entries with a local address ENDING with ":25". If there are none, the SMTP server failed to bind to its listening port; reboot the server.

If MOVEit Central reports that it is sending email OK, but the mail messages are not actually reaching their destination, open the local SMTP server queue folder and look for messages there which correspond with your MOVEit Central messages. (The queue folder is usually named something like "c:\inetpub\mailroot\queue".)

Problem: Mail is being queued on the local SMTP server and is not being delivered.

- **Solution 1:** Make sure your SMART HOST contains the value which used to be the Email Server field in your MOVEit Central configuration.
- **Solution 2:** Make sure the "Attempt Direct Delivery" box (near the Smart Host setting) is NOT CHECKED.
- **Solution 3:** Look for entries in your SYSTEM event log from SMTP or SMTPSVC which complain about "DNS" problem. If you see events like these, change the SMART HOST (described above) to an IP address surrounded by square brackets. (e.g. "[66.170.5.142]")

MessageWay CLI

MOVEit Central's built-in MessageWay Translator script uses a command-line program, xformviamway, to communicate with a MessageWay server. In ordinary use, MOVEit Central administrators can rely upon the built-in script to handle all interaction with the command-line program. Thus, ordinarily, MOVEit Central administrators do not need to know how xformviamway works, or even that it exists at all. However, advanced MOVEit Central administrators may wish to invoke the command-line program themselves, to handle unusual or complex scenarios. This section describes xformviamway for those advanced administrators.

See also: "***Common Applications - MessageWay Translation*** (on page 277)" and "***Configuring Tasks - Processes/Scripts - Built-In - MessageWay Translation*** (see "***MessageWay Translation***" on page 195)."

xformviamway.exe, which by default is installed in \Program Files\MOVEit, is a program that sends a single file to MessageWay and, after MessageWay has completed processing the file, receives the resulting output files, writes two status files, and terminates.

Program Arguments

The program is invoked as follows:

`xformviamway.exe -i` *infile* `-o` *outfile* `-c` *completionfile*

infile is the name of an input file giving such information as how to connect to the MessageWay server, where the input file is, and where the output files should be created. See below for a description of the format of this file.

outfile is the name of an output file to be created by xformviamway, giving the status of the completed translation, and listing the names of the data and report files returned from MessageWay. See below for a description of the format of this file.

completionfile is the name of a completion file to be created by xformviamway when it finishes. The contents of this file are unimportant; the creation of this file indicates that xformviamway has completed writing *outfile*.

Input File

The input file is a text file in ".INI file" format, with one input value per line. Here's a sample file:

```
[Params]
Host=172.16.23.204
SSL=False
Port=6280
SSLFingerprint=
User=micentral
Password=G7z3fN9wP
Recipient=translate:moveit
Sender=X850TEST
MIMEType=
ExceptionsInsteadOfData=True
FilenameToProcess=C:\TEMP\MIC\c88-0002\atc10001.tmp
OriginalFilename=X850test-MultOut.txt OutputDir=C:\TEMP\MIC\c88-0002
MaxSeconds=300
PollIntervalSeconds=5
TraceFilename=
ForceAtLeastSeconds=20
```

The input values are described below. All values are required except where marked optional.

Name	Description
Host	The hostname or IP address of the MessageWay server.
SSL	True if SSL should be used, else False. Note: if you use SSL, you must specify the MessageWay server's certificate's fingerprint in SSLFingerprint. If the server is on the same computer as MOVEit Central, you can safely specify False here and avoid having to know the certificate's fingerprint.

Name	Description
Port	The TCP port to which the program should connect. Typically 6280 if not SSL, or 6243 if SSL.
SSLFingerprint	(Optional) Hexadecimal fingerprint (MD5 or SHA1) of the server's certificate. Required if SSL is True. (There is no way to specify that any certificate should be accepted.) The string consists of groups of 2 hex characters separated by spaces.
User	The MessageWay username. This user must have sufficient permission to access the recipient location.
Password	The password of the MessageWay user.
Recipient	Destination (in MessageWay terminology) of the translated files. Typically this will be something like "translate:moveit", which means that there must be a translation location named "translate" and a mailbox named "moveit" configured in MessageWay. The specified user must have sufficient access to these locations.
Sender	An arbitrary sender's name. The MessageWay translation engine may base its translation partly on the sender's name.
MIMEType	(Optional) An arbitrary MIME type string.
ExceptionsInsteadOfData	Tells the script how to behave when any exception occurs (meaning poorly formatted data). True means no data files should be returned if an exception occurs; instead, the exception report files are returned. Defaults to False, which means only data files are returned. If False and exceptions do occur, you will have to look up the exception reports directly through MessageWay.
FilenameToProcess	The full path to the input data file to process. However, MessageWay is not informed of this filename; instead, MessageWay is told that the filename is OriginalFilename (below).
OriginalFilename	The filename to present to MessageWay. Depending upon MessageWay's configuration, the type of processing done may be partially determined by this filename. This filename should not include a path.
OutputDir	The full path of the directory into which xformviamway should write its data and report files. For instance, C:\data\xlate.

Name	Description
MaxSeconds	(Optional) The maximum number of seconds to wait for MessageWay to process the file. A value of 0 means no limit. May include macros. Defaults to 7200 (two hours).
PollIntervalSeconds	(Optional) The number of seconds to wait between queries to MessageWay to determine whether processing has completed. May include macros. Defaults to 5 seconds.
TraceFilename	(Optional) The full path to a file which will receive a detailed trace log of xformviamway's communications with the MessageWay server. For example, C:\tmp\MWTrace.txt. Use this parameter only to debug problems interacting with the MessageWay server.
ForceAtLeastSeconds	(Optional) A rarely-used parameter which specifies the minimum amount of time that xformviamway should take before responding. Specified as an integer number of seconds. If specified, xformviamway will wait until at least ForceAtLeastSeconds seconds have passed before returning, even if the processing was complete before that amount of time. This parameter was implemented to allow testing of progress bars.

Output File

xformviamway's *outfile* is an XML file describing the results of the translation. The actual data and report files resulting from the MessageWay processing are separate files which are pointed to by *outfile*. Here's a sample file:

```
<Output>

  <InputProcessingStatus>Accepted</InputProcessingStatus>

  <RFiles>

    <RFile>

      <MessageID>2010080413120504btdb</MessageID>


<CacheFilename>C:\TEMP\MIC\c88-0002/2010080413120504btdb.tmp</CacheFilename>

      <FileType>Output</FileType>

      <Filename>M2010080413120504btdb.dat</Filename>

    </RFile>

    <RFile>

      <MessageID>2010080413120504c55l</MessageID>


<CacheFilename>C:\TEMP\MIC\c88-0002/2010080413120504c55l.tmp</CacheFilename>

      <FileType>Output</FileType>

      <Filename>M2010080413120504c55l.dat</Filename>

    </RFile>

    <RFile>

      <MessageID>2010080413120504deg9</MessageID>


<CacheFilename>C:\TEMP\MIC\c88-0002/2010080413120504deg9.tmp</CacheFilename>

      <FileType>Output</FileType>

      <Filename>M2010080413120504deg9.dat</Filename>

    </RFile>
    <RFile>
      <MessageID>2010080413120504egd8</MessageID>

<CacheFilename>C:\TEMP\MIC\c88-0002/2010080413120504egd8.tmp</CacheFilename>
      <FileType>Report</FileType>
      <Filename>2010080413120504ac2j.txt</Filename>
    </RFile>
  </RFiles>
  <ErrorCode>0</ErrorCode>
  <ErrorDescription></ErrorDescription>
  <ShouldRetry>false</ShouldRetry>
  <OriginalMessageID>2010080413120504ac2j</OriginalMessageID>
</Output>
```

The XML tags are described below.

Name	**Description**
InputProcessingStatus	The processing status as returned by MessageWay. The possible values are: ▪ Accepted ▪ Rejected ▪ Accepted with errors ▪ Partially accepted ▪ *(empty)* An empty value usually indicates an error.

Name	Description
RFile	Each RFile node represents a single file returned from MessageWay. The subnodes are: ▪ MessageID - The Message ID of the file inside MessageWay. This is typically useful only if you are going to look up the message from the MessageWay Dashboard. ▪ CacheFilename - The filename of a file created by MessageWay. This file will be in the OutputDir specified in the input file. ▪ FileType - Either Data or Report. MessageWay Data files contain the translated output. A single input file might result in multiple data output files. MessageWay Report files contain descriptions of the processing of the input file, including detailed error messages if the input file contained incorrect data. ▪ Filename - The name of the file (message) as it is known inside MessageWay.
ErrorCode	An error code giving the overall success of the process. 0 means success. Non-zero values mean failure. Generally, translation runs that result in exceptions due, for instance, to invalid input data result in an error code of 0. Non-zero errors are normally returned only if xformviamway cannot connect to or login to the MessageWay error, or if the MessageWay server returns an ill-formatted response.
ErrorDescription	An error description elaborating on the error that causes a non-zero ErrorCode. If ErrorCode is 0, ErrorDescription will be empty.
ShouldRetry	true if the xformviamway run failed, but in a way that implies that a subsequent run may succeed. For instance, if xformviamway cannot not connect to the MessageWay server, it returns a ShouldRetry of true, because the MessageWay server may be down only temporarily. ShouldRetry is false if the xformviamway run succeeded, or if it failed in a way that implies that a retry is unlikely to succeed. ShouldRetry is intended to be used by retry logic of the process invoking xformviamway.
OriginalMessageID	The message ID assigned by MessageWay to the input file. This can be useful for analysingThe message ID assigned by MessageWay to the input file. This can be useful for analysing message flow via MessageWay Dashboard. OriginalMessageID will be empty if MessageWay did not accept the input file - for instance, if the user could not login.

Return Code

The program returns 0 if processing succeeded; this includes translation that resulted in exceptions. The program returns a non-zero error code upon failure.

Database

This section explores database issues.

Schema

This topic is provided for users who wish to know how MOVEit Central keeps track of histories of task runs and file transfers. MOVEit Central manages its database automatically, so very few sites will need the information contained in this topic. Both MySQL and Microsoft SQL Server are supported.

MOVEit Central uses an ODBC-compliant database to store statistics and status information on task runs and file transfers. To configure the database, see ***Central Config Utility*** (on page 21). See also ***Trimming the database*** (see "***Trimming***" on page 466).

The database contains these tables:

Stats contains one record for each attempt to send a file. The fields are:

Field Name	Type	Description
ID	bigint	A record ID which is incremented automatically for each record added to the table. Primary key.
LogStamp	char	Date/time of record
TaskID	int	The ID of the task.
Node	int	The failover node number of the copy of MOVEit Central that logged this record. This is 0 if failover is not being used.
NominalStart	char	The time at which the task started or was scheduled to start. There is a key that consists of TaskID and NominalStart.
Action	char	The action being logged. This can be one of: ▪ "get" - logged only if there is an error retrieving a file. Successful gets are not logged; instead, we wait until sending or processing the file before logging it. ▪ "send" - logged after trying to send a file. Most statistics records are of this type. ▪ "process" - logged after running a script. ▪ "delete" - logged if there is an error deleting a file. ▪ "internal" - logged if there is an internal error.
SourceHost	char	The source host of the file. This is the "friendly" name configured in MOVEit Central Admin, not the IP domain name. For "process" records, the name of the host if per-file, or blank if per-task.
SourceFilename	char	The filename of the source file. On send records, for process-created files, the script-assigned name. For unzipped files, reflects the original file. On process records, the name of the source file if per-file, or blank if per-task.
SourceFilenameOnly	char	The filename of the source file, without the pathname.
SourceFileID	char	The ID of the source file if it originated from MOVEit DMZ, else empty.

Field Name	Type	Description
SourceNBytes	double	The number of bytes in the source file. Always 0 for process-created files. For unzipped files, reflects the original file's size.
SourceDuration	double	The number of seconds the download took. Always 0 for process-created files. For unzipped files, reflects the original file's transfer.
DestHost	char	The destination host of the file. This is the "friendly" name, not the IP domain name. For process records, the name of the script.
DestFilename	char	The filename of the destination file. For process records, empty.
DestFilenameOnly	char	The filename of the destination file, without the pathname.
DestFileID	char	The ID of the destination file if it was sent to MOVEit DMZ, else empty.
NBytes	double	Number of bytes transferred. 0 if there is any error. For records of successful sends, always populated, even for process-created files. In case of upload error, this will be 0. Always 0 for process records
DestDuration	double	The number of seconds the upload took. For process records, the time taken by the script. (Note inconsistency with NBytes.) In case of upload error, this is 0, to be consistent with NBytes.
ErrCode	int	An error code, where 0 indicates success.
Message	char	An error message, or other text describing this action. Usually empty if success.
Hash	char	Cryptographic hash of this record and the previous record's hash. This is used to implement tamper detection.

The table **TaskRuns** contains one record for each run of a task. The fields are:

Field Name	Type	Description
ID	bigint	A record ID which is incremented automatically for each record added to the table. Primary key.

Field Name	Type	Description
LogStamp	datetime	Date/time of record
TaskID	int	The ID of the task.
NominalStart	char	The time at which the task started or was scheduled to start. TaskID and NominalStart together uniquely identify a record. There is a key that consists of these two fields.
TaskName	char	Name of task.
TimeStarted	char	The date and time the task started.
TimeEnded	char	The date and time the task ended.
StartedBy	char	Who started the task. If a remote logged-in user started the task (via Run Now), this is the username. If a user from localhost started the task, this is "Local". If the scheduler started the task, this is "Scheduler".
Success	char	"Failure", "Success", or "No action". The latter is logged when no matching files could be found.
FilesSent	int	The number of files successfully sent.
TotalBytesSent	double	The number of bytes successfully sent. This is a double because not all databases support huge integers, and the number may exceed the capacity of a 4-byte integer.
HasBeenRead	int	A flag used by MOVEit Central Admin to keep track of whether the operator has said "don't show me this task run again". The default value is 0; it's set to 1 to mean the task should not be shown anymore.
LastErrorType	int	The type of the last error. The following values are possible: 0 = no error; 5 = warning; 6 = error; 7 = internal error
LastErrorText	char	The text of the last error, if any.
Hash	char	Cryptographic hash of this record and the previous record's hash. This is used to implement tamper detection.

The table **TaskGroups** contains the task groups and their members. This table duplicates the information in the configuration file, and is provided only as a convenience for organizations doing custom report generation from the database. The task groups table is updated every time the user edits the task groups with MOVEit Central Admin. The fields are:

FieldName	Type	Description
GroupName	char	The name of a task group. There may be several records with the same GroupName, one for each task belonging to this group.
TaskID	int	The ID of a task belonging to this group. A task may belong to several groups, so there may be several records with the same TaskID.

The **audit** table (introduced in MOVEit Central 4.0) includes one record for each configuration change made by an administrator:

Field Name	Type	Description
ID	bigint	A record ID which is incremented automatically for each record added to the table. Primary key.
LogTime	char	The date/time stamp of when the change was made.
Node	int	The failover node number, or 0 if failover isn't being used.
Action	char	The action being performed, such as "cfgsec_update".
TargetType	char	The type of entity being changed, such as "task".
TargetID	int	The ID of the entity being changed, such as 239634085.
TargetName	char	The name of the entity being changed, such as "Detroit Monthly Summary".
CentralVersion	char	The version of MOVEit Central that was in use, such as "3.5.6.0".
AgentBrand	char	The name of the client program, such as "MOVEit Central Admin".
AgentVersion	char	The version of the client program, such as "3.5.6.1".
Username	char	The username of the user who performed the action, such as "lukey".
IPAddress	char	The IP address of the user who performed the action, such as "129.168.1.45".

Field Name	**Type**	**Description**
Error	int	An error code; 0 if no error.
ErrorText	char	An error message, if Error was not 0.
Message	char	Optional details of the change.
Hash	char	Cryptographic hash of this record and the previous record's hash. This is used to implement tamper detection.

MySQL

This topic is provided for users who wish to know MySQL-specific details of how MOVEit Central interfaces to its database. When MySQL has been selected as the database engine (and this is the default), MOVEit Central installs, upgrades, manages, and updates its database automatically, so very few sites will need the information contained in this topic.

In MySQL, the tables can be created with SQL statements like:

```
CREATE TABLE `stats` (

  `ID` bigint(20) NOT NULL auto_increment,

  `LogStamp` varchar(24) default NULL,

  `TaskID` int(11) NOT NULL default '0',

  `Node` smallint(6) NOT NULL default '0',

  `NominalStart` varchar(24) NOT NULL default '',

  `Action` varchar(12) default NULL,

  `SourceHost` varchar(100) default NULL,

  `SourceFilename` varchar(255) default NULL,

  `SourceFilenameOnly` varchar(255) default NULL,

  `SourceFileID` varchar(24) NOT NULL default '',

  `SourceStamp` varchar(24) default NULL,

  `SourceNBytes` double default '-1',

  `SourceDuration` double default '-1',

  `SourceMsgID` text,

  `SourceMDN` text,

  `DestHost` varchar(100) default NULL,

  `DestFilename` varchar(255) default NULL,

  `DestFilenameOnly` varchar(255) default NULL,

  `DestFileID` varchar(24) NOT NULL default '',

  `NBytes` double default NULL,
  `DestDuration` double default '-1',
  `DestMsgID` text,
  `DestMDN` text,
  `ErrCode` int(11) default NULL,
  `Message` varchar(250) default NULL,
  `Hash` varchar(40) default NULL,
  PRIMARY KEY (`ID`),
  KEY `StatsUniqueRun` (`TaskID`,`NominalStart`),
  KEY `Action` (`Action`),
  KEY `ErrCode` (`ErrCode`),
  KEY `LogStampTaskIDIndex` (`LogStamp`,`TaskID`)
);

CREATE TABLE `taskruns` (
  `ID` bigint(20) NOT NULL auto_increment,
  `LogStamp` varchar(24) default NULL,
  `TaskID` int(11) NOT NULL default '0',
  `Node` smallint(6) NOT NULL default '0',
  `NominalStart` varchar(24) NOT NULL default '',
  `TaskName` varchar(200) default NULL,
  `RecType` varchar(8) default NULL,
  `TimeStarted` varchar(24) default NULL,
  `TimeEnded` varchar(24) default NULL,
  `StartedBy` varchar(32) default NULL,
  `Success` varchar(12) default NULL,
  `FilesSent` int(11) default NULL,
  `TotalBytesSent` double default NULL,
  `HasBeenRead` int(11) default '0',
  `LastErrorType` int(11) default NULL,
  `LastErrorText` varchar(250) default NULL,
  `Hash` varchar(40) default NULL,
  PRIMARY KEY (`ID`),
  KEY `TaskRunsUniqueRun` (`TaskID`,`NominalStart`),
  KEY `Success` (`Success`),
  KEY `HasBeenRead` (`HasBeenRead`),
  KEY `LogStampTaskIDIndex` (`LogStamp`,`TaskID`)
);

CREATE TABLE `taskgroups` (
  `GroupName` varchar(50) default NULL,
  `TaskID` int(11) NOT NULL default '0'
);

CREATE TABLE `audit` (
  `ID` bigint(20) NOT NULL auto_increment,
  `LogTime` varchar(24) default NULL,
  `Node` smallint(6) default NULL,
  `Action` varchar(24) default NULL,
  `TargetType` varchar(24) default NULL,
  `TargetID` varchar(50) default NULL,
  `TargetName` varchar(200) default NULL,
  `CentralVersion` varchar(12) default NULL,
  `AgentBrand` varchar(32) default NULL,
  `AgentVersion` varchar(12) default NULL,
  `Username` varchar(80) default NULL,
  `IPAddress` varchar(16) default NULL,
  `Error` int(11) default NULL,
  `ErrorText` text,
  `Message` text,
  `Hash` varchar(40) default NULL,
  PRIMARY KEY (`ID`),
  KEY `LogTime` (`LogTime`)
);

CREATE TABLE `tmplastruns` (
  `TaskIDOfMax` int(11) default NULL,
  `IDOfMax` bigint(20) default NULL
);
```

You must also grant access to the MySQL database with a statement like:

```
GRANT ALL ON MICStats.* TO MICentral@localhost IDENTIFIED BY 'mypassword123';
```

This example creates a user named MICentral with a password of mypassword123.

Then create an ODBC DSN and specify the username and password you gave above. Be sure to check the "Change BIGINT columns to INT" option.

The DSN associated with this database is provided to MOVEit Central by configuring the "DSN" field in MOVEit Central's "Central Config" program.

MSSQL

This topic is provided for users who wish to know Microsoft SQL Server-specific details of how MOVEit Central interfaces to its database.

When SQL Server has been selected as the database engine, MOVEit Central manages its database automatically, so very few sites will need the information contained in this topic. However, unlike with MySQL, MOVEit Central's installs do not install or update the SQL Server software itself. Thus, a system administrator must see to it that periodic Microsoft updates are applied.

For the supported versions of Microsoft SQL Server, see MOVEit Central Service Requirements.

To configure MOVEit Central's connection to MS SQL Server, use the ***Central Config Utility*** (on page 21).

MOVEit Central creates the database using T-SQL statements like this:

```
USE [master]

GO

IF EXISTS (SELECT name FROM sys.databases WHERE name = N'micstats') DROP DATABASE
[micstats];

GO

CREATE DATABASE [micstats]

GO

USE [micstats]

GO

CREATE TABLE

  [dbo].[audit]

(

  ID [bigint] NOT NULL IDENTITY(1,2) NOT FOR REPLICATION,

  LogTime [varchar](24) NULL,

  Node [smallint] NULL,

  Action [varchar](24) NULL,

  TargetType [varchar](24) NULL,

  TargetID [varchar](50) NULL,
  TargetName [varchar](200) NULL,
  CentralVersion [varchar](12) NULL,
  AgentBrand [varchar](32) NULL,
  AgentVersion [varchar](12) NULL,
  Username [varchar](80) NULL,
  IPAddress [varchar](16) NULL,
  Error [int] NULL,
  ErrorText text,
  Message text,
  Hash [varchar](40) NULL
);
GO
ALTER TABLE
  [dbo].[audit]
ADD
  CONSTRAINT [DF_audit_LogTime] DEFAULT NULL FOR [LogTime],
  CONSTRAINT [DF_audit_Node] DEFAULT NULL FOR [Node],
  CONSTRAINT [DF_audit_Action] DEFAULT NULL FOR [Action],
  CONSTRAINT [DF_audit_TargetType] DEFAULT NULL FOR [TargetType],
  CONSTRAINT [DF_audit_TargetID] DEFAULT NULL FOR [TargetID],
  CONSTRAINT [DF_audit_TargetName] DEFAULT NULL FOR [TargetName],
  CONSTRAINT [DF_audit_CentralVersion] DEFAULT NULL FOR [CentralVersion],
  CONSTRAINT [DF_audit_AgentBrand] DEFAULT NULL FOR [AgentBrand],
  CONSTRAINT [DF_audit_AgentVersion] DEFAULT NULL FOR [AgentVersion],
  CONSTRAINT [DF_audit_Username] DEFAULT NULL FOR [Username],
  CONSTRAINT [DF_audit_IPAddress] DEFAULT NULL FOR [IPAddress],
  CONSTRAINT [DF_audit_Error] DEFAULT NULL FOR [Error],
  CONSTRAINT [DF_audit_Hash] DEFAULT NULL FOR [Hash],

  CONSTRAINT [PK_audit] PRIMARY KEY ([ID])

GO

CREATE NONCLUSTERED INDEX

        [IX_audit_LogTime]

ON

        [dbo].[audit]

(

        [LogTime] ASC

)

GO

CREATE TABLE

  [dbo].[stats]

(

  ID [bigint] NOT NULL IDENTITY (1,2) NOT FOR REPLICATION,

  LogStamp [varchar](24) NULL,

  TaskID [int] NOT NULL,

  Node [smallint] NOT NULL,

  NominalStart [varchar](24) NOT NULL,

  Action [varchar](12) NULL,

  SourceHost [varchar](100) NULL,

  SourceFilename [varchar](255) NULL,

  SourceFilenameOnly [varchar](255) NULL,

  SourceFileID [varchar](24) NOT NULL,

  SourceStamp [varchar](24) NULL,

  SourceNBytes float NULL,

  SourceDuration float NULL,
  SourceMsgID text,

  SourceMDN text,

  DestHost [varchar](100) NULL,

  DestFilename [varchar](255) NULL,

  DestFilenameOnly [varchar](255) NULL,

  DestFileID [varchar](24) NOT NULL,

  NBytes float NULL,

  DestDuration float NULL,

  DestMsgID text,

  DestMDN text,

  ErrCode [int] NULL,

  Message [varchar](250) NULL,

  Hash [varchar](40) NULL

);

GO

ALTER TABLE

  [dbo].[stats]

ADD

  CONSTRAINT [DF_stats_LogStamp] DEFAULT NULL FOR [LogStamp],

  CONSTRAINT [DF_stats_TaskID] DEFAULT 0 FOR [TaskID],

  CONSTRAINT [DF_stats_Node] DEFAULT 0 FOR [Node],

  CONSTRAINT [DF_stats_NominalStart] DEFAULT '' FOR [NominalStart],

  CONSTRAINT [DF_stats_Action] DEFAULT NULL FOR [Action],

  CONSTRAINT [DF_stats_SourceHost] DEFAULT NULL FOR [SourceHost],

  CONSTRAINT [DF_stats_SourceFilename] DEFAULT NULL FOR [SourceFilename],

  CONSTRAINT [DF_stats_SourceFilenameOnly] DEFAULT NULL FOR
[SourceFilenameOnly],
  CONSTRAINT [DF_stats_SourceFileID] DEFAULT '' FOR [SourceFileID],
  CONSTRAINT [DF_stats_SourceStamp] DEFAULT NULL FOR [SourceStamp],
  CONSTRAINT [DF_stats_SourceNBytes] DEFAULT '-1' FOR [SourceNBytes],
  CONSTRAINT [DF_stats_SourceDuration] DEFAULT '-1' FOR [SourceDuration],
  CONSTRAINT [DF_stats_DestHost] DEFAULT NULL FOR [DestHost],
  CONSTRAINT [DF_stats_DestFilename] DEFAULT NULL FOR [DestFilename],
  CONSTRAINT [DF_stats_DestFilenameOnly] DEFAULT NULL FOR [DestFilenameOnly],
  CONSTRAINT [DF_stats_DestFileID] DEFAULT '' FOR [DestFileID],
  CONSTRAINT [DF_stats_NBytes] DEFAULT NULL FOR [NBytes],
  CONSTRAINT [DF_stats_DestDuration] DEFAULT '-1' FOR [DestDuration],
  CONSTRAINT [DF_stats_ErrCode] DEFAULT NULL FOR [ErrCode],
  CONSTRAINT [DF_stats_Message] DEFAULT NULL FOR [Message],
  CONSTRAINT [DF_stats_Hash] DEFAULT NULL FOR [Hash],
  CONSTRAINT [PK_stats] PRIMARY KEY ([ID])
GO
CREATE NONCLUSTERED INDEX
        [IX_stats_StatsUniqueRun]
ON
        [dbo].[stats]
(
        TaskID ASC,NominalStart ASC
)
GO
CREATE NONCLUSTERED INDEX
        [IX_stats_Action]
ON
        [dbo].[stats]
```

```
(
        [Action] ASC
)
GO
CREATE NONCLUSTERED INDEX
        [IX_stats_ErrCode]
ON
        [dbo].[stats]
(
        [ErrCode] ASC
)
GO
CREATE NONCLUSTERED INDEX
        [IX_stats_LogStampTaskIDIndex]
ON
        [dbo].[stats]
(
        [LogStamp] ASC, [TaskID] ASC
)
GO
CREATE TABLE
  [dbo].[taskgroups]
(
  GroupName [varchar](50) NULL,
  TaskID [int] NOT NULL
);
GO
```

```
ALTER TABLE
  [dbo].[taskgroups]
ADD
  CONSTRAINT [DF_taskgroups_GroupName] DEFAULT NULL FOR [GroupName],
  CONSTRAINT [DF_taskgroups_TaskID] DEFAULT 0 FOR [TaskID]
GO
CREATE TABLE
  [dbo].[taskruns]
(
  ID [bigint] NOT NULL IDENTITY (1,2) NOT FOR REPLICATION,
  LogStamp [varchar](24) NULL,
  TaskID [int] NOT NULL,
  Node [smallint] NOT NULL,
  NominalStart [varchar](24) NOT NULL,
  TaskName [varchar](200) NULL,
  RecType [varchar](8) NULL,
  TimeStarted [varchar](24) NULL,
  TimeEnded [varchar](24) NULL,
  StartedBy [varchar](32) NULL,
  Success [varchar](12) NULL,
  FilesSent [int] NULL,
  TotalBytesSent float NULL,
  HasBeenRead [int] NULL,
  LastErrorType [int] NULL,
  LastErrorText [varchar](250) NULL,
  Hash [varchar](40) NULL,
);
```

```
GO
ALTER TABLE
  [dbo].[taskruns]
ADD
  CONSTRAINT [DF_taskruns_LogStamp] DEFAULT NULL FOR [LogStamp],
  CONSTRAINT [DF_taskruns_TaskID] DEFAULT 0 FOR [TaskID],
  CONSTRAINT [DF_taskruns_Node] DEFAULT 0 FOR [Node],
  CONSTRAINT [DF_taskruns_NominalStart] DEFAULT '' FOR [NominalStart],
  CONSTRAINT [DF_taskruns_TaskName] DEFAULT NULL FOR [TaskName],
  CONSTRAINT [DF_taskruns_RecType] DEFAULT NULL FOR [RecType],
  CONSTRAINT [DF_taskruns_TimeStarted] DEFAULT NULL FOR [TimeStarted],
  CONSTRAINT [DF_taskruns_TimeEnded] DEFAULT NULL FOR [TimeEnded],
  CONSTRAINT [DF_taskruns_StartedBy] DEFAULT NULL FOR [StartedBy],
  CONSTRAINT [DF_taskruns_Success] DEFAULT NULL FOR [Success],
  CONSTRAINT [DF_taskruns_FilesSent] DEFAULT NULL FOR [FilesSent],
  CONSTRAINT [DF_taskruns_TotalBytesSent] DEFAULT NULL FOR [TotalBytesSent],
  CONSTRAINT [DF_taskruns_HasBeenRead] DEFAULT 0 FOR [HasBeenRead],
  CONSTRAINT [DF_taskruns_LastErrorType] DEFAULT NULL FOR [LastErrorType],
  CONSTRAINT [DF_taskruns_LastErrorText] DEFAULT NULL FOR [LastErrorText],
  CONSTRAINT [DF_taskruns_Hash] DEFAULT NULL FOR [Hash],
  CONSTRAINT [PK_taskruns] PRIMARY KEY ([ID])
GO
CREATE NONCLUSTERED INDEX
        [IX_taskruns_TaskRunsUniqueRun]
ON
        [dbo].[taskruns]
(
        [TaskID] ASC, [NominalStart] ASC

)

GO

CREATE NONCLUSTERED INDEX

        [IX_taskruns_Success]

ON

        [dbo].[taskruns]

(

        [Success] ASC

)

GO

CREATE NONCLUSTERED INDEX

        [IX_taskruns_HasBeenRead]

ON

        [dbo].[taskruns]

(

        [HasBeenRead] ASC

)

GO

CREATE NONCLUSTERED INDEX

        [IX_taskruns_LogStampTaskIDIndex]

ON

        [dbo].[taskruns]

(

        [LogStamp] ASC, [TaskID] ASC

)

GO
```

```
CREATE TABLE tmplastruns
(
  TaskIDOfMax [int] NULL,
  IDOfMax [bigint] NULL
);
GO
ALTER TABLE
  [dbo].[tmplastruns]
ADD
  CONSTRAINT [DF_tmplastruns_TaskIDOfMax] DEFAULT NULL FOR [TaskIDOfMax],
  CONSTRAINT [DF_tmplastruns_IDOfMax] DEFAULT NULL FOR [IDOfMax]
GO
```

Converter

The *Convert to MS SQL Server* utility creates an empty MOVEit Central database on a Microsoft SQL Server and configures MOVEit Central to use that database.This utility is run only once to create the initial database. It provides an option to copy an existing MySQL database to the newly created SQL Server database. Once the process is complete, the ***Configure MOVEit Central*** (on page 21) program can be used to alter the settings.

Convert to MS SQL Server is not included in the MOVEit Central installation. Instead, you can download it from the MOVEit support site. Please read the article ***How do I get MOVEit Central to work with Microsoft SQL Server?*** (***http://ipswitchft.force.com/kb/articles/FAQ/How-do-I-get-MOVEit-Central-to-work-with-Microsoft-SQL-Server-1307565983335***) for information about prerequisites and where to find the download.

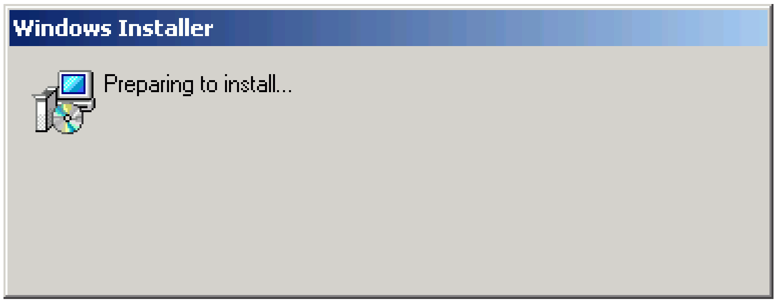
Note: This utility should NOT be run on a MOVEit Central older than version 6.0, as data loss could occur. If you want to convert a version of MOVEit Central older than 6.0, first upgrade to version 6.0 or later, and then run the conversion.

This following sections describe how to use the conversion utility.

Start the Convert to MS SQL Server Utility

Start by selecting **Programs > MOVEit Central > Convert to MS SQL Server**. The utility runs as a wizard, showing different pages as you progress through the process by choosing Next.

At startup, the utility checks to see whether the Microsoft SQL Native Client database driver is already installed. If it is not installed, the program installs it automatically. The database driver setup program does not require any input from you. It displays a window like:

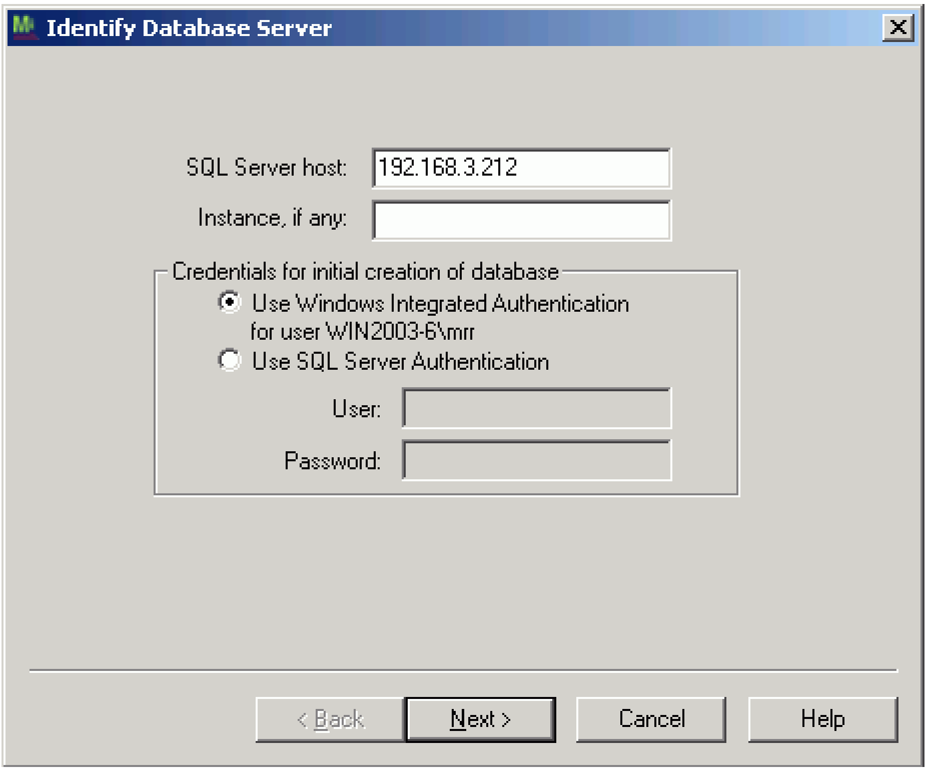


Windows Installer

Preparing to install...

Identify Database Server

The first page of the converter utility prompts for the credentials used to create the database. These credentials must already exist, and are typically not the credentials used by MOVEit Central to access the database once it's running.



Identify Database Server

SQL Server host: 192.168.3.212

Instance, if any:

Credentials for initial creation of database

● Use Windows Integrated Authentication for user WIN2003-6\mrr

○ Use SQL Server Authentication

User:

Password:

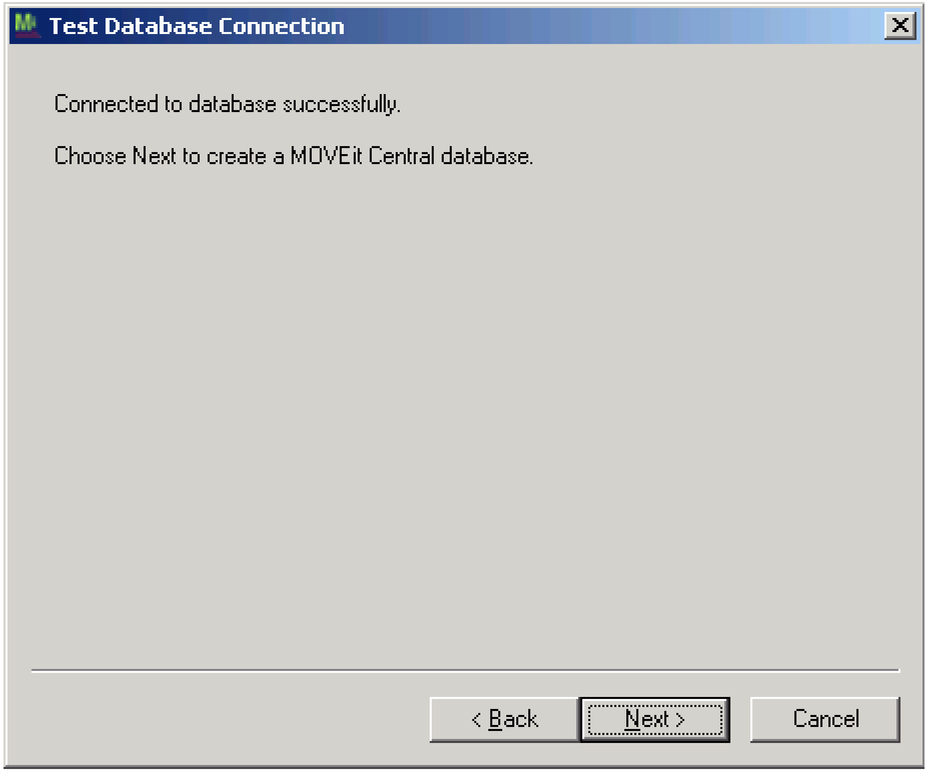
The settings on this page are:

- **SQL Server host** is the hostname or IP address of the database server.
- **Instance** is the name of the instance. Typically this is empty, meaning the default instance. In some configurations of Microsoft SQL Server Express, this must be SQL Express.
- **Use Windows Authentication** sets the credentials to the Windows user that is running the utility. This requires that the computer on which the SQL Server is running has an identical Windows user, and that SQL Server is configured to recognize that user.
- **Use SQL Server Authentication** sets the user to the specified SQL Server login and password; for example, the login "sa" might be used. Again, these must already exist.

When you choose **Next**, if the MOVEit Central service is running, the conversion utility will offer to stop it. If you do not choose to stop it, be aware that the new database will not go into use until you restart the service.

Test Database Connection

When you enter this page, the utility connects to SQL Server to test the credentials. It also checks to see whether a "micstats" database already exists on this server. If so, it will ask whether it is OK to delete the database.



Test Database Connection

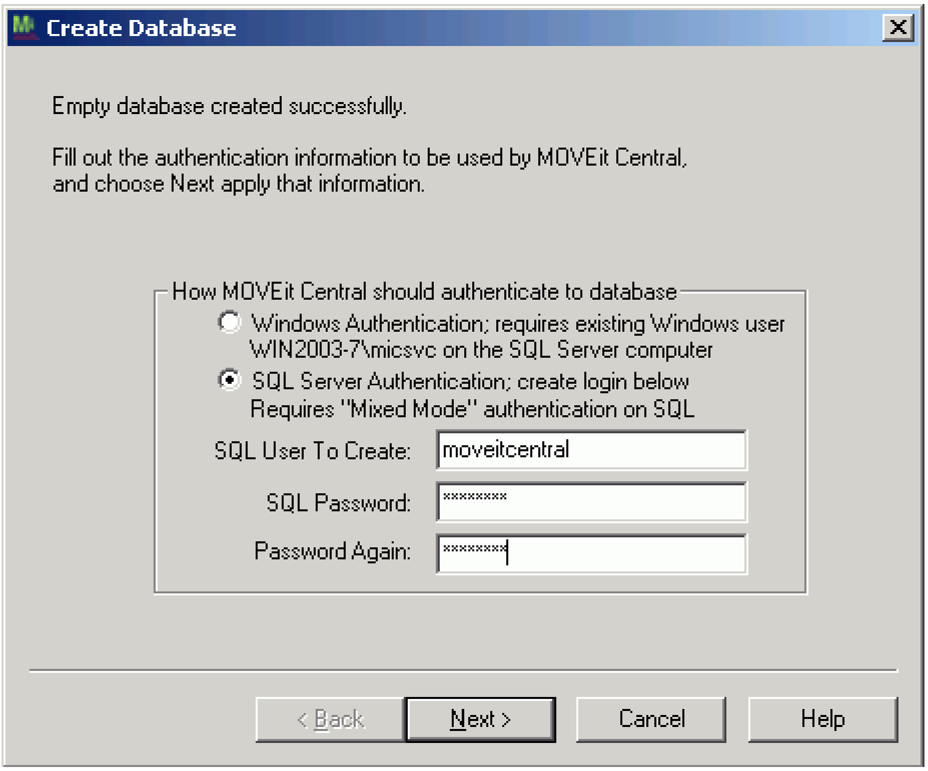
Connected to database successfully.

Choose Next to create a MOVEit Central database.

When you have connected to the database successfully and see the above message, choose **Next** to create the database. If you cannot connect, choose **Back** and change your connection settings.

Create Database

This page shows progress in creating the database. When the database has been created successfully, you will see a prompt for the credentials that MOVEit Central itself should use to connect to the database.



Create Database

Empty database created successfully.

Fill out the authentication information to be used by MOVEit Central, and choose Next apply that information.

How MOVEit Central should authenticate to database

○ Windows Authentication; requires existing Windows user WIN2003-7\micsvc on the SQL Server computer

● SQL Server Authentication; create login below Requires "Mixed Mode" authentication on SQL

SQL User To Create: moveitcentral

SQL Password: ********

Password Again: ********

The settings on this page are:

- **Windows Authentication** sets the credentials to the WIndows user that runs the MOVEit Central service. This requires that the computer on which the SQL Server is running have an identical user. The conversion program will, however, create the SQL Server login, as well as the corresponding user within the database.
- **SQL Server Authentication** sets the user to the specified SQL login and password when authenticating to the database. The conversion utility will create the specified SQL login and database user on the SQL Server. The password is stored encrypted in the registry.

Choose **Next** to create the SQL login and to make the necessary MOVEit Central settings.

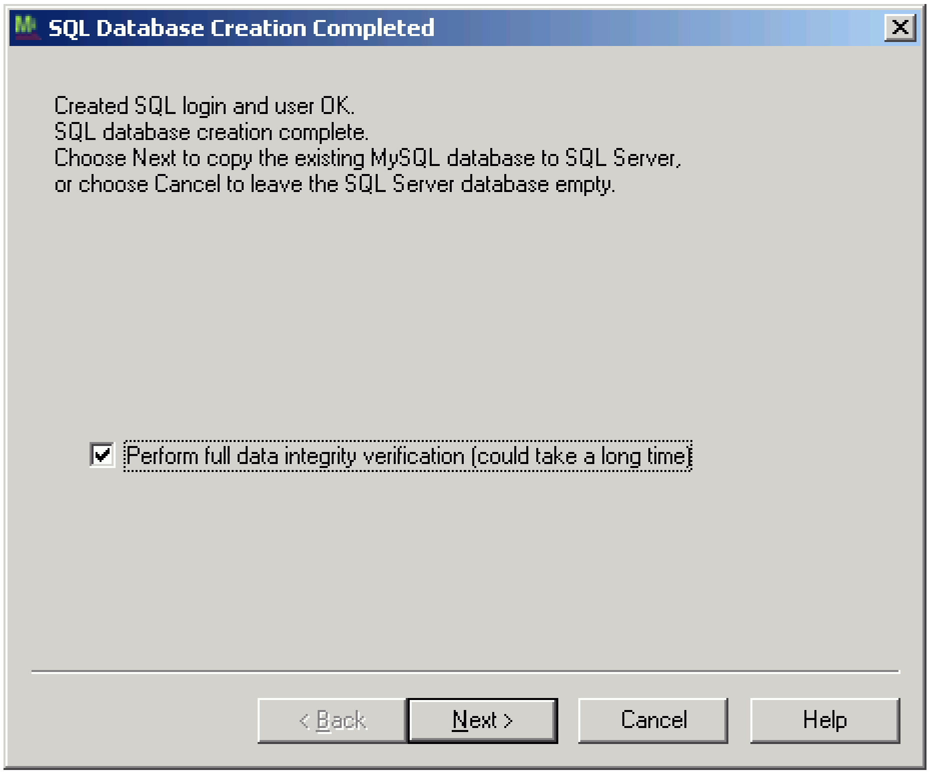
If you are using SQL Server authentication and see an error message reading "The user is not associated with a trusted SQL Server connection", then most likely the database is not configured to accept SQL Server logins. You can use SQL Server Management Studio to set SQL Server to allow SQL Server logins:

1. Open SQL Server Management Studio.
2. Right-click on the server name and choose Properties.
3. Choose Security, and then choose SQL Server and Windows Authentication mode.

You must stop and start the MSSQLSERVER service for the changes to take effect.

SQL Database Creation Completed

This page will be displayed when the SQL login has been created, and MOVEit Central has been set to use it.



Created SQL login and user OK.
SQL database creation complete.
Choose Next to copy the existing MySQL database to SQL Server,
or choose Cancel to leave the SQL Server database empty.

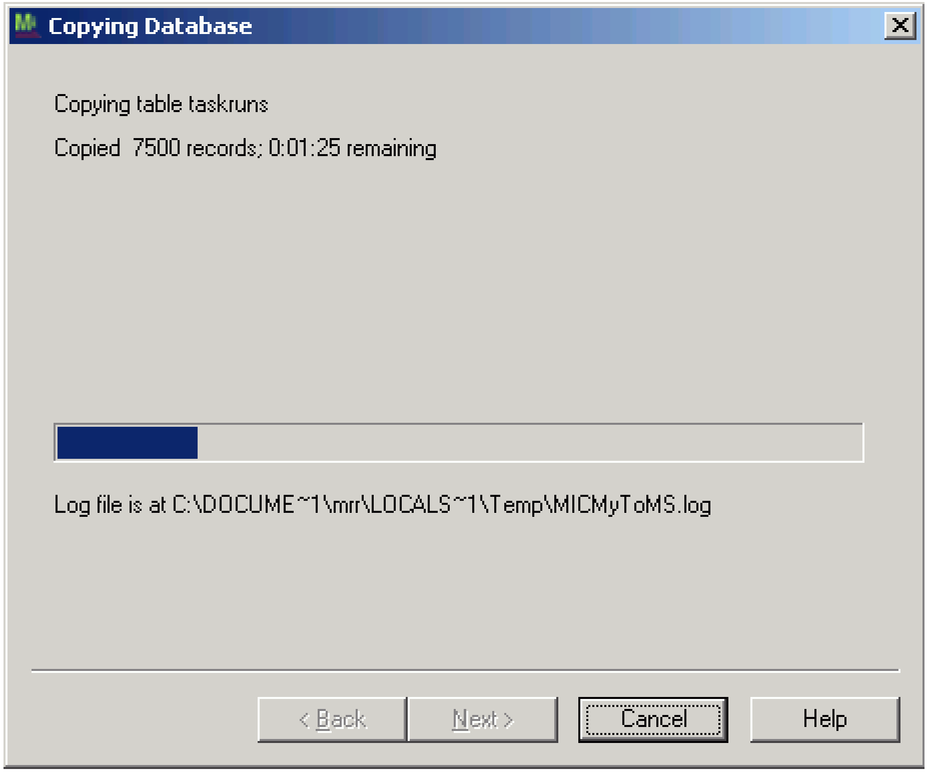
☑ Perform full data integrity verification (could take a long time)

Choose Next to start copying the existing MySQL database into the newly-created MS SQL Server database, or choose Cancel to leave the new database unpopulated.

Choosing Perform full data integrity verification will cause the program to scan the two databases and compare all records after the copy is done. This will add about 30% to the total conversion time. If you do not choose to perform the full verification, the program will only check that the correct number of records ended up in the destination database.

Copying Database

This page displays while the program copies records from the existing MySQL database into the newly-created MS SQL Server database.



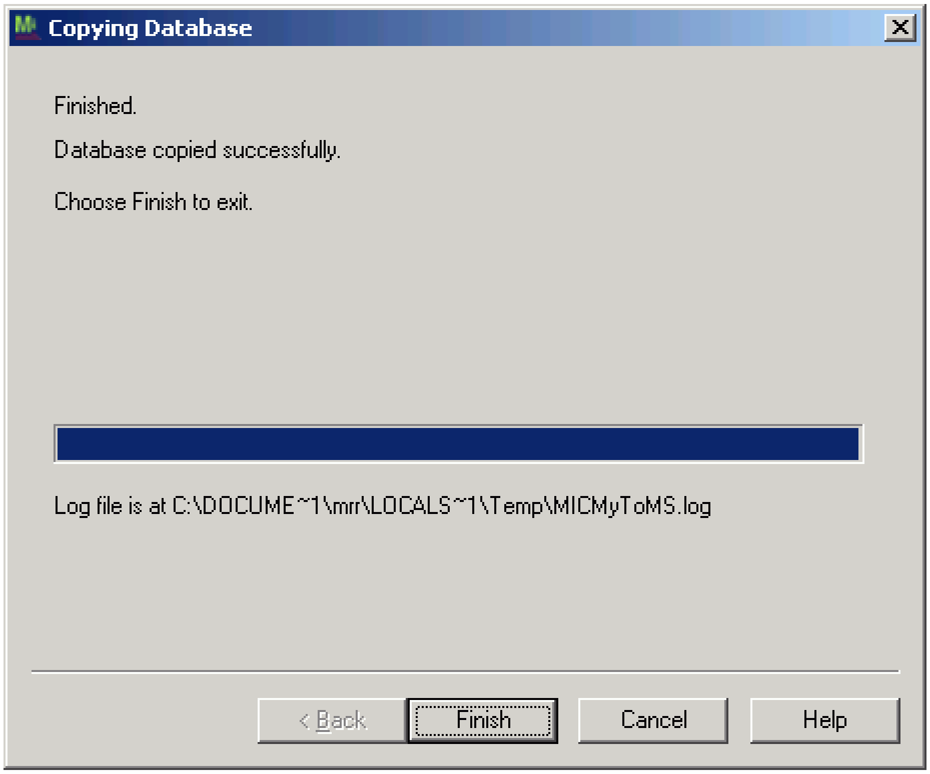
Copying table taskruns

Copied 7500 records; 0:01:25 remaining

Log file is at C:\DOCUME~1\mrr\LOCALS~1\Temp\MICMyToMS.log

If the database is very large, the copy process many take a long time--even hours for multi-gigabyte databases.

When the copying is complete, this message is shown:



Finished.

Database copied successfully.

Choose Finish to exit.

Log file is at C:\DOCUME~1\mrr\LOCALS~1\Temp\MICMyToMS.log

If you had earlier chosen to have the MOVEit Central service stopped, the conversion program will offer to start it again when you choose **Finish**.

Log File

The conversion program leaves a log file in the user's temporary directory, as given by the environment variable TMP. This directory is often named something like C:\Documents and Settings\username\Local Settings\Temp. The filename is MICMyToMS.log. If you need to contact technical support, please have this file on hand.

Tamper Detection

MOVEit Central has the ability to detect attempts by an intruder to alter the database tables containing audit information and activity history. An intruder might wish to alter these records in order to erase evidence of unauthorized use of the system, or to falsify file transfer histories.

MOVEit Central implements tamper detection by populating a field named Hash on each record of its three major database tables. This Hash field contains the cryptographic hash of the current record and the previous record's Hash value, and is therefore part of a "hash chain". MOVEit Central uses its built-in FIPS 140-2 validated SHA1-HMAC keyed hash algorithm. The key to each hash chain is derived from a tamper detection key which is entered during installation of the product, and which is stored (in a cryptographically altered form) in the registry.

Current tamper detection information is stored, in encrypted form, in a file named michash.xml, in the same directory as MOVEit Central's configuration and state files.

Detecting tampering

MOVEit Central's built-in task Tamper Detect checks for tampering. This task runs the built-in Tamper Detect script. By default, it runs nightly. It can also be run upon demand.

Recovering from problems

In the case of a system crash or certain other problems, the michash.xml file may become corrupted or out-of-date. MOVEit Central will continue to run, but the Tamper Detect task will begin to send alerts of possible tampering. Normally, tamper detection will reset itself after sending an email alert, but you can reset tamper detection by using MOVEit Central Admin's Reset Tamper Detection command. Subsequent to using this command, MOVEit Central will be able to detect future tampering, but it will ignore any tampering that has already occurred.

Trimming

Over time, the statistics database can accumulate many records, slowing performance and using megabytes of disk space. To prevent this, MOVEit Central run a built-in script called "Trim Statistics DB" periodically to delete old records from the database, optionally saving them to a file or another database before deletion.

For more information about the built-in "Trim Statistics DB" script, please see the ***Scripts - Built-In - Trim Statistics DB documentation*** (see "***Trim Statistics DB***" on page 207).

Troubleshooting

Normally, the statistics database operates silently, behind the scenes of MOVEit Central, and requires no active maintenance on the part of the administrator to operate. Rarely, however, one or more database tables can become corrupted, which may prevent MOVEit Central from successfully logging task run information. These corruptions are often caused by unexpected reboots, such as during a power failure. They can also occur when backup programs make copies of database table files while the database server is running. When a database table is corrupted, it can no longer be accessed by the database server until it has been repaired.

If you think you have had, or may be having a database corruption problem, the first thing to check is the log output. MOVEit Central accesses the database several times during a typical task run, and when serious database problems occur, they are always written to the running log, which is accessible from ***MOVEit Central Admin*** (see "***Debug Log Tab***" on page 240) and from the ***local system*** (see "***Direct Access***" on page 264). Here is an example of a table corruption error that would be found in the log:

```
Task "My Task": Could not log task end: [TCX][MyODBC]Can't open file: 'stats.MYD'.
(errno: 145)
```

MySQL Database

If database errors have occurred and you are using MySQL as the database engine, there are steps you can take to repair the database.

Automatic Repair

Recent versions of MOVEit Central have enabled a database option which automatically repairs tables that it finds corrupted, meaning most of these occurrences come and go with hardly any notice by end users. Though no action on the part of the administrators is required in these cases, administrators may wish to keep informed of any such happenings. Information is logged by the database server when such corruptions occur, and when they are automatically repaired. Look for this log information in the \mysql\data directory of your MOVEit Central server. It will be stored in a file named HOSTNAME.err, where HOSTNAME is the name of the server. A typical corruption detection and repair event will be logged like this:

```
041122 1:13:58 read_const: Got error 134 when reading table ./micstats/stats

041122 1:14:00 read_const: Got error 134 when reading table ./micstats/stats

041122 1:41:46 Warning: Checking table: './micstats/stats'

041122 1:41:46 Warning: Recovering table: './micstats/stats'
```

Manual Repair

In the very rare case that the automatic table repair functionality fails, you will need to repair the table manually. It is not necessary to stop the MOVEit Central service or the MySQL service during the manual repair process. In fact, the MySQL service MUST be running for this sequence of commands to succeed.

To manually repair a database table, open a command-prompt on your Central system and log in to the MySQL server using the "root" account created during the Central installation. To log onto the MySQL server using root, cd to your \mysql\bin directory and issue this command:

```
mysql --user=root --password=YOUR_ROOT_PASSWORD micstats
```

Once logged in, execute the CHECK TABLE command against the table you believe has been corrupted, like so:

```
CHECK TABLE stats;
```

This command will typically generate several lines of information. The last line will tell you the status of the table. If the CHECK response indicates the table needs to be repaired, issue the repair command like so:

```
REPAIR TABLE stats;
```

This may take several minutes, depending on the size of the table, and generate several lines of output. If the repair was successful, the last line of output will contain a status message of "OK".

If the manual repair process was unsuccessful after several tries, contact ***MOVEit support*** (***http://www.ipswitchft.com/company/contactsupport.aspx***) for assistance.

Microsoft SQL Server

SQL Server generally does not require manual repair of database tables. If you encounter database problems with SQL Server as your database, contact your database administrator, or ***MOVEit support*** (***http://www.ipswitchft.com/company/contactsupport.aspx***).

Legal Information

Software License

SOFTWARE LICENSE AND SUPPORT AGREEMENT APPLICABLE TO MESSAGEWAY AND MOVEIT SOFTWARE

This License and Support Agreement ("Agreement") is entered into as of today ("Effective Date"), by and between Ipswitch, Inc., with offices located at 83 Hartwell Avenue, Lexington, MA 02421 ("Licensor") and YOU ("Licensee").

WHEREAS, the parties hereto wish to provide the terms and conditions under which Licensor will supply Licensee Software (as defined below) for the term provided herein; and

WHEREAS, Licensee desires to obtain, and Licensor is willing to grant to Licensee a nonexclusive, royalty-free, perpetual, nontransferable license to use the Software subject to the terms and conditions set forth herein.

NOW, THEREFORE, in consideration of the foregoing, of the mutual covenants and undertakings contained herein and of other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties, intending to be legally bound, hereby agree as follows:

1. DEFINITION OF TERMS

1.1 "Software" means the Licensor’s standard, unmodified computer software programs in object code form for the MessageWay or MOVEit programs purchased by Licensee.

1.2 "Confidential Information" means any confidential information concerning the Software, Licensor’s and Licensee's business in general, all data pertaining to Licensor’s and Licensee's customers, and the terms and conditions of this Agreement.

1.3 "Total Fees" means the total sum for the Software, which includes license fees, first year support fee and any services.

1.4 "Taxes" means all sales, use, excise, value added, and other taxes and duties however designated levied by any taxing authority. Taxes shall not include any levies by any taxing authority based upon the net income of Licensor.

1.5 "Third Party" means any party other than Licensor or Licensee or their respective employees.

1.6. "Critical Problem" means a failure of the Software to perform in essential compliance with the material specifications set forth in its documentation, such failure being of the nature that Licensee is unable to utilize the Software for its operational purposes.

2. LICENSE

2.1 Licensor agrees to furnish the Software to Licensee and does hereby grant to Licensee a non-exclusive, royalty-free, non-transferable, perpetual license, without the right to sub-license, to use the Software, in its object code form only, on its premises, for the purpose of processing Licensee’s own electronic file exchange with its customers (the "License").

2.2 For use as authorized, Licensee may copy reasonable quantities of any standard end user documentation; and may copy machine language code, in whole or in part, in reasonable quantities, in printed or electronic form, for use by Licensee for archive, back-up, disaster recovery, or emergency restart purposes, or to replace copies made on defective media. Licensee shall reproduce and include Licensor’s proprietary rights and copyright notices on all such copies, in whole or in part, of the Software.

2.3 The License allows Software to be installed on one production server and also on one non-production server.

2.4 The License includes the unlimited right to distribute and use the Java Web browser plugins, Java and Windows command-line clients, the MOVEit Wizard ActiveX control, MOVEit Xfer, or other end-user components, as applicable.

2.5 Notwithstanding anything contained herein to the contrary, Licensee shall not allow any Software to be used on an external commercial (fee based) time-sharing basis or service bureau arrangement of any kind. As an exception to the preceding sentence, Licensee may use the Software to provide private cloud services to one (1) end user customer of Licensee specifically identified to Ipswitch, provided that Licensee completes and returns Schedule 1 to Ipswitch (available upon request from Ipswitch Sales Department) prior to providing such services.

2.6 Licensee assumes responsibility for selection of the Software to achieve Licensee's intended results and for the use and valid operation of the Software.

2.7 Licensee acknowledges that the Software (including any and all modifications, enhancements, or customizations thereof) consists of proprietary products of Licensor or its third party suppliers, and the proprietary rights that protect such property may include, but are not limited to, U.S. and international copyrights, trademarks, patents and trade secret laws of general applicability. All right, title and interest in and to the Software are and shall remain with Licensor or its third party suppliers, as applicable. This Agreement does not convey to Licensee any interest in or title to the Software, but only a limited right of use revocable in accordance with its terms.

2.8 Licensee shall not: decompile, disassemble, reverse engineer, extract, or otherwise produce any source code of the Software; disclose, divulge, communicate, or allow access to the Software to any person except Licensee's authorized agents, employees, or other parties expressly authorized hereunder, or as expressly permitted hereunder.

2.9 Licensee shall not isolate, extract, or otherwise utilize any components embedded in the Software for any purposes other than those supported by the core functions of the Software. Embedded Third Party components shall not be installed or configured, administered, customized, or directly accessed by way of component APIs independent from the APIs and functions of the Software. Embedded Third Party components shall not be independently upgraded or changed in any way except through officially released Ipswitch patches, updates or versions.

3. SUPPORT

3.1 Standard Support Coverage. If and for so long as Licensee purchases annual support, Licensor shall provide to Licensee unlimited telephone support and remote diagnostic assistance during Licensor's normal business hours. Licensor shall respond to support calls within one (1) hour of the initial call for such support by Licensee.

3.2. Extended Support Coverage. Extended Support Services ("Extended Support") provides Licensee with 24-hour, 7 day per week emergency assistance with guaranteed two (2) hour callback. Such service shall be restricted to Critical Problems. The Extended Support shall be available to Licensee either as specified and prepaid in Licensee's annual software support fee, or if not so specified, at the current fixed hourly rate for Extended Support provided by Licensor with a two (2) hour minimum charge per incident.

3.3 Licensor shall provide to Licensee at no charge Software updates and enhancements to licensed products when made available generally to Licensor's other customers, if and for so long as Licensee purchases annual support.

4. TERM

The term of this Agreement and the license grant shall begin on the Effective Date and continue until it is terminated under Section 10. Support may be renewed annually upon Licensee's payment of Licensor's then current fee for annual support for so long as Licensor offers support services.

5. PAYMENT

5.1 Licensee shall be responsible for and shall pay all applicable Taxes (including any interest and penalties thereon) if any, imposed by taxing authorities by reason of the sale and delivery of products herein provided. In no event will Licensee be obligated to pay taxes on Licensor's income.

5.2 Each payment to be made to Licensor under this Agreement shall be paid by Licensee.

6. WARRANTIES

6.1 Licensor warrants that the Software will perform in essential compliance with the material performance specifications set forth in its documentation for a period of one year following the Effective Date. In the event the Software does not so perform, Licensor shall resolve any such defect in a timely manner, or, at its option replace the defective portion thereof at no additional cost to Licensee, or refund the Software license fees paid, reduced by thirty-three per-cent (33%) per year from the Effective Date of this Agreement.

6.2 Licensor warrants that the services described in this Agreement shall be performed in a professional manner and with the standard of care and diligence in the industry, as well as industry standards of documentation, methodology, and control.

6.3 THERE ARE NO OTHER WARRANTIES EXPRESSED OR IMPLIED AND SELLER DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

7. INTELLECTUAL PROPERTY INDEMNITY

7.1 Licensor will defend Licensee and hold it harmless against any claim or action that alleges that the use of the Software infringes a patent, copyright, trade secret, or other proprietary right of a Third Party (a "Claim"), and Licensor will pay resulting costs, damages, and reasonable attorney fees awarded, provided that: (i) Licensee notifies Licensor in writing within thirty (30) days after learning that the Claim has been brought or might be asserted; (ii) allows Licensor sole control of the defense and all related settlement negotiations; and (iii) provides Licensor with the information, authority, and all assistance reasonably requested by the Licensor to provide the aforementioned defense. Licensee shall have the right to be represented in any such Claim by its own counsel, at its own expense.

7.2 In addition to Licensor's obligations under Section 7.1, if as a result of any such Claim, Licensee is enjoined from using the Software, Licensor will, at its sole option and expense (i) procure for Licensee the right to continue to use the Software; or (ii) replace or modify the Software so that it becomes non-infringing, which replacement or modification must be functionally equivalent, so as to settle such claim, or (iii) refund the Software fees paid, reduced by thirty-three per-cent (33%) per year or portion from the Effective Date of this Agreement and refund the annual software support fees paid for the current period. The indemnity hereunder shall not apply if and to the extent that the Claim results from (i) a correction or modification of the Software not provided by Licensor; (ii) a failure to promptly install and utilize an update; or (iii) the combination of the Software with any items not provided by Licensor.

8. LIMITATION OF LIABILITY

8.1 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR BE LIABLE TO LICENSEE FOR INDIRECT, INCIDENTAL, SPECIAL, ECONOMIC, EXEMPLARY OR CONSEQUENTIAL DAMAGES, WHETHER IN TORT OR IN CONTRACT, INCLUDING LOSS OF PROFITS ARISING OUT OF THE USE OF OR THE INABILITY TO USE IPSWITCH PRODUCTS OR SERVICES, INCLUDING, WITHOUT LIMITATION, DAMAGES OR COSTS RELATING TO THE LOSS OF PROFITS, BUSINESS, GOODWILL, DATA, OR COMPUTER PROGRAMS, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO LICENSEE. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT LIMIT LICENSOR'S OBLIGATIONS TO INDEMNIFY LICENSEE FOR ANY CLAIMS FOR DAMAGES AGAINST LICENSEE FOR INFRINGEMENT ON INTELLECTUAL PROPERTY.

8.2 Notwithstanding anything contained in this Agreement to the contrary, Licensor's cumulative liability to Licensee or any party resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the license fees paid to Licensor for the applicable Software.

9. NON-DISCLOSURE

9.1 Each party agrees to hold as confidential all Confidential Information received by such party ("Recipient") from the other party ("Disclosing Party"). All Confidential Information shall remain the property of Disclosing Party. Confidential Information will be returned to Disclosing Party at the termination of this Agreement.

9.2 Recipient will use the same care and discretion to avoid disclosure of Confidential Information as it uses with its own similar information that it does not wish disclosed, but in no event less than a reasonable standard of care for the industry and materials in question. Recipient may use Confidential Information only in the furtherance of the purposes of this Agreement. Recipient may disclose Confidential Information to (i) its employees and employees of its affiliates who have a need to know; and (ii) any other party with Disclosing Party's written consent. Recipient may disclose Confidential Information to the extent required by law. However, Recipient agrees to give Disclosing Party prompt notice and make a reasonable effort to obtain a protective order. The provisions of this paragraph survive any termination of this Agreement.

9.3 No obligation of confidentiality applies to any Confidential Information that Recipient (i) already possesses without obligation of confidentiality; (ii) develops independently; (iii) rightfully receives without obligation of confidentiality from a third party. No obligation of confidentiality applies to any Confidential Information that is, or becomes, publicly available without breach of this Agreement.

9.4 The terms of this Section 9 shall survive termination of this Agreement or any Schedules.

10. TERMINATION

10.1 Licensee may terminate this Agreement at any time by returning the Software, documentation, and all copies thereof to Licensor or by certifying their destruction. Licensee shall receive no refund of any fees or other amount on termination unless this Agreement is terminated under Section 6.1 or 7.2(iii) above.

10.2 Licensor may terminate this Agreement if (i) Licensee fails to pay any license or other fees or any part thereof, or (ii) Licensee breaches any material term or condition of this Agreement and does not remedy such breach within thirty (30) days after receiving written notice thereof. Licensor may terminate this Agreement immediately on written notice, if (a) Licensee copies, distributes or discloses the Software in violation of this Agreement or otherwise breaches its duty of confidentiality, or (b) bankruptcy or insolvency proceedings are instituted by or against Licensee, or a receiver is appointed, or if the Software in Licensee's possession is the object of attachment, sequestration or other comparable action, and any such proceeding or action is not vacated or terminated within sixty (60) days after commencement or filing. Upon any termination of this Agreement, Licensee shall (x) immediately cease all use of the Software, (y) return the Software, documentation, and all copies thereof to Licensor or certify their destruction, and (z) notify all third parties using the Software through Licensee to do the same.

10.3 Exercise of the right of termination afforded to either party in this Agreement shall not prejudice the legal rights or remedies either party may have against the other in respect of any breach of the terms of this Agreement.

10.4 Upon the termination of this Agreement for any reason, both parties shall return to the other as appropriate all Software and Confidential Information in the other’s possession or, with the other’s approval, destroy such information with certification by an officer.

11. NOTICES

Any notice required or permitted to be given hereunder shall be given by: (i) Registered or Certified Mail, Return Receipt Requested, postage prepaid; (ii) by confirmed facsimile; or (iii) by nationally recognized courier service to the other party at the addresses set forth above or to such other address as a party may designate in writing. All such notices shall be effective upon receipt.

12. GOVERNING LAW

This Agreement will be governed by the substantive laws of the Commonwealth of Massachusetts, without reference to provisions relating to conflict of laws.

13. EXPORT LAW

The Software may not be downloaded or otherwise exported or re-exported to any country subject to U.S. trade sanctions governing the Software, sanctioned countries including those restricted under License Exception ENC under Sections 740.17 (A) and (B)(3) of the Export Administration Regulations set forth by the United States Department of Commerce, Bureau of Industry and Security, or by citizens or residents of such countries except citizens who are lawful permanent residents of countries not subject to such sanctions, or by anyone on the U.S. Treasury Department's list of Specially Designated Nationals and Blocked Persons or the U.S. Commerce Department's Table of Denial Orders.

14. GENERAL

14.1 Licensor and Licensee expressly agree they are acting as independent contractors and under no circumstances shall any of the employees of one party be deemed the employees of the other for any purpose. This Agreement shall not be construed as authority for either party to act for the other party in any agency or other capacity, or to make commitments of any kind for the account of or on behalf of the other except as expressly authorized herein.

14.2 The section headings used herein are inserted only as a matter of convenience and for reference and shall not affect the construction or interpretation of this Agreement.

14.3 If any provision of this Agreement is held to be unenforceable or invalid, the other provisions shall continue in full force and effect.

14.4 The failure of either party to insist on strict performance of any of the provisions hereunder shall not be construed as the waiver of any subsequent default of a similar nature.

14.5 This instrument constitutes the complete and exclusive statement of the Agreement between the parties on the subject matter hereof unless superseded by a written agreement executed by specifically identified and duly authorized representatives of each party.

ZIP.exe and UNZIP.exe utility license:

Legal Information - Americans with Disabilities Act (ADA) Compliance

MOVEit Central is in full compliance with the Americans with Disabilities Act. Specifically, MOVEit Central complies with Section 1194.21 "Software Applications and Operating Systems". (This specification is online at this URL: "***http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/guide-to-the-section-508-standards*** (***http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/guide-to-the-section-508-standards***)")

- (a) Executing Function from Keyboard - Keyboard access to all functions is provided.
- (b) Accessibility Features - Applications do not interfere with existing accessibility features.
- (c) Input Focus - Focus is always clearly marked/displayed.
- (d) User Interface Element - Text is also provided for all images.
- (e) Bitmap Images - Bitmap images are consistent throughout application.
- (f) Textual Information - Text display occurs via OS functions.
- (g) User Selected Attributes - Applications accept user-selected color and contrast settings.
- (h) Animation - N/A. (Not used.)
- (i) Color Coding - Colors are never only method of displaying information.
- (j) Color and Contrast Settings - N/A. (OS color and contrast settings are used.)
- (k) Flashing or Blinking Text - Elements do not flash.
- (l) Electronic Forms - Consistent text/label presentation is used.

Legal Information - Export Restrictions

MOVEit Central makes use of MOVEit Crypto for its cryptographic services. Therefore, MOVEit Central is subject to the same export restrictions as MOVEit Crypto; these are described below.

MOVEit Crypto has undergone extensive review by an independent testing laboratory accredited under the Cryptographic Module Validation (CMV) Program run by NIST and the Communications Security Establishment (CSE) of the Canadian Government. As a result, MOVEit Crypto has received the following certifications.

- FIPS 140-2 "Security Requirements for Cryptographic Modules" validation (Certificate 310).
- FIPS 197 "Advanced Encryption Standard (AES) Algorithm" validation (Certificate 30).

MOVEit Crypto (and therefore, MOVEit Central) is subject to U.S. Department of Commerce export controls, which prohibit it from being downloaded or otherwise exported or re-exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria, or to a national or resident of any of these countries.

About Ipswitch

Contact...

The Ipswitch Support Center is an information and diagnostic center available for Ipswitch customers to:

- Obtain advice on proper product installation, configuration, and operation
- Report any product problems and receive timely resolutions
- Request software updates
- Inquire on software release contents and status

The support center provides support for all Ipswitch licensed products according to the terms of your Ipswitch Support Agreement. These support services are provided to Ipswitch's direct customers and resellers, while indirect customers are serviced by their own respective reseller. Support for customizations to Ipswitch software is the responsibility of the customer or their reseller's Integration Services group. For more information on support for customized software please contact your reseller's Integration Services manager.

To access the Support Center, you can use the following links:

- Visit our Web site for the latest ***contact information*** (***http://www.ipswitchft.com/company/contactsupport.aspx***).
- Visit the ***customer portal*** (***https://ipswitchft.secure.force.com/cp/***).

Index

A

Advanced Tasks • 307

Antivirus • 409

AS1

- AS Overview • 337
- Host • 376
- MOVEit Implementation • 368

AS2

- AS Overview • 337
- Host • 379
- MOVEit Implementation • 368

AS3

- AS Overview • 337
- Host • 387
- MOVEit Implementation • 368

B

Backup • 38

- Automatic Backup • 39

C

Client certificates • 217

Command menu • 95

D

Database • 438

- Conversion • 458
- MS SQL Server • 448
- MySQL • 444
- Trimming • 466

Debug log • 240

Destinations • 126

DFS • 55

Disaster Recovery (See Also 'Backup') • 38

E

Event-driven transfers • 160

F

Failover

- Installation • 47

Features • 3

File Notifications • 160

FTP Directory Parsing • 400

FTP Failover • 54

G

GetMICConfig • 412

H

Help menu • 100

Hosts • 148

Configuring • 149

Hosts - File Notifications • 160

I

Immediate transfers • 160

Importing keys • 216

Installation • 47, 81

L

Log • 240

M

Macros • 137

N

NAT (FTP configuration) • 149

NLB • 66

Notable features • 3

O

Options menu • 97

P

PGP • 325

POP3 • 411

Processes • 163

configuring • 132

samples • 171

syntax • 165

R

Restart failed transfer (• 149

Resume partial transfer • 3

S

S/MIME • 333

Schedules • 130

Script Functions • 165

Scripts • 163, 165, 173

Settings • 229

SNMP • 407

Sources • 120

SSH • 149

SSL Client Certificates • 217

Synchronization • 283

SysLog • 407

T

Tasks • 104

Tasks Menu • 98

- configuring • 101, 104, 109
- destination • 126
- menu • 98
- monitoring • 229
- process • 132
- schedule • 130
- source • 120
- tab • 109
- task failure entries • 109

Trigger Files • 265

Trimming the statistics DB • 466

Troubleshooting • 236