
MOVEit Administrator's Guide



Copyright

©1991-2014 Ipswitch, Inc. All rights reserved.

This document, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by such license, no part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the express prior written consent of Ipswitch, Inc.

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.

WS_FTP, the WS_FTP logos, Ipswitch, and the Ipswitch logo, MOVEit and the MOVEit logo, MessageWay and the MessageWay logo are trademarks of Ipswitch, Inc. Other products and their brands or company names, are or may be trademarks or registered trademarks, and are the property of their respective companies.

This document was published on Friday, August 08, 2014 at 10:40.

Contents

Introduction	1
Introduction and Overview	1
Overview	2
Access MOVEit	6
MOVEit Central	10
Technical Support.....	11
Additional Documentation.....	13
Typographical Conventions.....	14
File Transfer Folder Implementations.....	15
Ad Hoc Transfer Implementations	21
Admin 101	25
Feature Focus	31
High Availability, Failover and Disaster Recovery	31
Mobile Implementation	33
Ad Hoc Transfer Implementation.....	43
Ad Hoc Transfer Secure Note Option.....	47
Email Notifications	50
International Languages.....	57
Display Profiles.....	67
User Account Expiration.....	76
SAML Single Signon Service.....	87
WebPosts	92

Content Scanning	97
Multi-homing	116
Sync Client	120
System Configuration	127
Firewall Configuration	128
Configuration Utility	135
Backup/Restore Utility	150
SSL and SSH	170
Web Interface	265
Home Page	266
Users	271
Groups	303
Logs	316
Reports	325
Settings	349
Overview	349
Appearance	354
Security Policies	415
Ad Hoc Transfer	496
Miscellaneous	525
System	527

Organizations	547
Schemes	557
FTP Server	573

FTP - Overview	574
FTP - Configuration.....	577
FTP - Glossary	586
FTP - Supported Commands.....	590
FTP - Recommended Configuration	593
FTP - Troubleshooting	594
FTP - SSL Certificates	600
FTP - Specific Clients - z/OS	601
FTP - Specific Clients - cURL	622
FTP - Interoperability - IIS FTP	625
FTP - Interoperability - Integrity Check How-To	626
FTP - Certificates - Create Client Certificate.....	628
SSH Server	635

SSH - Overview	636
SSH - Configuration	639
SSH - Protocol Discussion.....	647
SSH - Server Keys - Overview	649
SSH - Specific Clients - OpenSSH Windows	652
SSH - Specific Clients - OpenSSH Unix	658
Generating SSH Keys	658

Web Farms	660
Web Farms - Overview	661
Webfarms - Architecture	663
Web Farms - Webfarm Tab	666
Web Farms - Technical Discussion	667
Web Farms - Installation - Prerequisites	668
Web Farms - Installation - Pre-Installation Steps	668
Web Farms - Installation - Installation Steps	670
Web Farms - Software Upgrade	672
 Advanced Topics	 675
AS2 and AS3	676
User Forms	679
Database - Schema	680
Database - Troubleshooting	693
Database - Remote Access	696
Package - Archives	700
Packages - Spell-Check Dictionaries	703
Service Integration - Anti-virus	704
Service Integration - CAC Integration	708
Service Integration - Local Mail Relay	712
Service Integration - RADIUS/ODBC Authentication	724
Service Integration - SiteMinder Integration	733
Service Integration - SysLog and SNMP	737
Service Integration - Time Synchronization	740

Service Integration - Web Integration	741
System Internals - Exception Handling	745
System Internals - MOVEit DMZ Error Codes.....	746
System Internals - NTFS Permissions	752
System Internals - Scheduled Tasks	754
System Internals - Technical Reference	764
Services	777
System Internals - Templates and Icons	778
System Internals - Timeouts.....	781
System Internals - URL Crafting.....	783
System Internals - Remote Filesystem	790
General Information	793

Client Support	793
Security.....	800
Regulations Overview	804
Privacy/Security/Auditing Requirements.....	805
Regulations FDA	807
Regulations ADA.....	809
Regulations Export	811

User's Guide	815
Introduction	1
Get Started	7
Work with Files and Folders.....	42
Work with Packages.....	83
Manage My Account	109
Sign Out.....	114
Index	117

Introduction

The **MOVEit™ portfolio** (<http://www.ipswitchft.com/moveit>) of products developed by **Ipswitch, Inc.** (<http://www.ipswitch.com/>) provides solutions for the secure handling of sensitive information, including financial files, medical records, legal documents, and personal data. While some of its solutions, such as MOVEit Central (workflow engines), are exclusively geared toward internal networks, others are internet-facing.

This guide covers the internet-facing tier, which securely collects, stores, manages, and distributes information between organizations and external entities. Two deployment options are available. MOVEit DMZ is a secure file transfer server deployed on-premises. The cloud-deployed service counterpart is called MOVEit Cloud.

Note: This guide does not distinguish between the deployment options. It refers to the overall tier simply as "MOVEit".

MOVEit encompasses two major functional products, which can be installed alone or together:

- MOVEit File Transfer – Transfer files among *systems* and *workgroups*, through shared MOVEit folders. File Transfer supports both automated transfers and manual transfers.
- MOVEit Ad Hoc Transfer – Manually exchange files and messages *person-to-person*, through personal MOVEit mailboxes.

For users, MOVEit works the way you do...

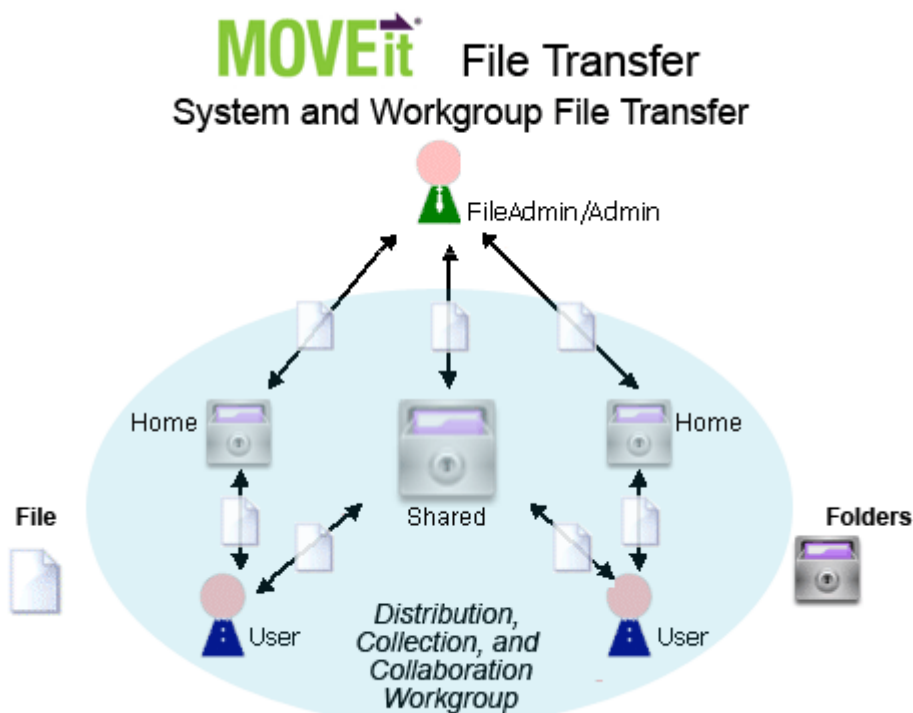
Whenever you need to perform transfers manually, you can easily access MOVEit in a web browser, on mobile devices, and even within your desktop email client:

- MOVEit Web Interface – A full-size web browser is all you need to quickly, easily, and securely exchange files with MOVEit DMZ over encrypted connections using the HTTP over SSL (HTTPS) protocol.
- MOVEit Wizard Web Browser Plugins – From within the browser interface, an optional, self-installing plug-in wizard is available. (There are two versions, ActiveX and Java, to support various browsers.) The wizard not only enables drag-and-drop simplicity; it provides faster and more reliable file transfers than HTTPS.
- MOVEit Mobile – A separate server module supports mobile for MOVEit. Mobile apps and the mobile web enable encrypted transfer using WiFi or your carrier plan. Native mobile apps for iOS and Android devices are available from your mobile app store. In addition, a mobile web offering (for Ad Hoc Transfer only) runs in the standard Safari and Chrome mobile browsers.
- Microsoft Outlook® Plug-in for Ad Hoc Transfer – Attach files to a message in Outlook with the MOVEit plug-in, and the files will be encrypted and sent by MOVEit. The message body itself can be sent encrypted or by email.

- MOVEit Sync - A Windows application that lets you create a Sync folder on your desktop and sync files with your MOVEit folder.
- FTP Clients - MOVEit supports most of the available FTP clients, including Ipswitch's own WS_FTP application.

File Transfer

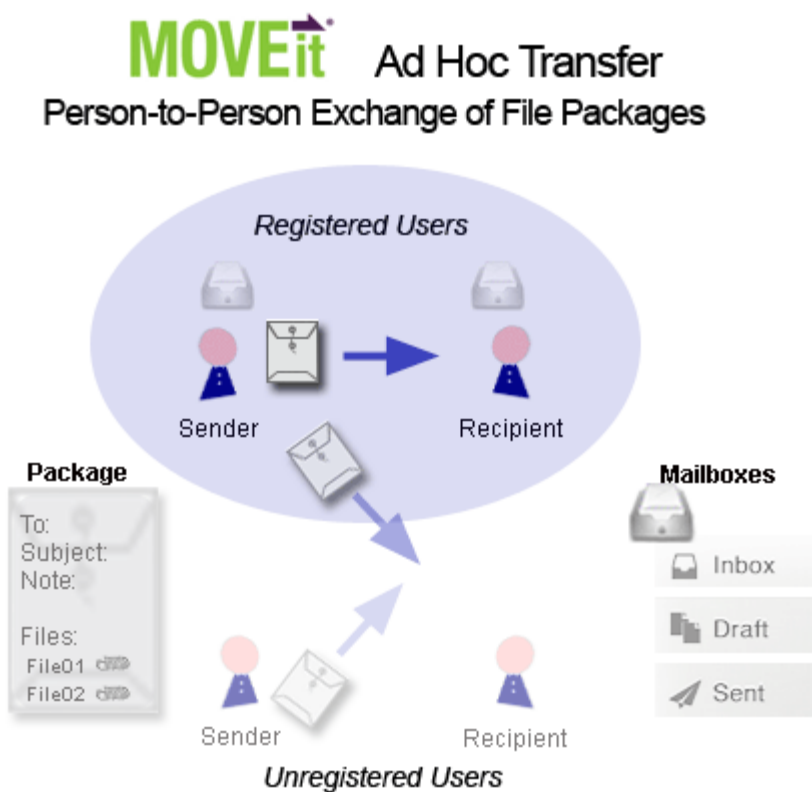
The File Transfer product provides a secure way to perform automated (scheduled) *system-to-system* file transfers. It also supports manual (user-performed) transfers in and among *workgroups*. Users are set up with accounts and home *folders* where they can upload and download files. Administrators can set up user groups and shared folders to support of various business work flows, especially those involving external entities. Work flows include organization-to-person, distribution groups, collection bins, and even direct person-to-person file exchange.



Ad Hoc Transfer

The Ad Hoc Transfer product provides a secure way to enable users to directly exchange file "packages" with each other. Each package typically consists of a "note" (a basic message) and one or more attached files. Users are set up with accounts and *mailboxes* where they can send and receive packages.

Note: The person-to-person transfer capability supports "*ad hoc*" use in several different respects: it is for unscheduled, manually performed transfers; it includes the mailbox and address book infrastructure needed for direct exchange; and it supports the inclusion of *unregistered users* (through the use of their email addresses).



Note: Unregistered users can be set up to become either *temporary users*, whose accounts expire, or *guest users* (also known as "package password" users), who are given access to a particular package only, not to mailboxes.

With Ad Hoc Transfer, users can avoid the limitations of a mail server. Large files, and multiple file attachments, can be sent quickly and securely. Senders can use a browser, a mobile app, or the Microsoft Outlook plug-in to attach files and send them to an email address.

Composing a MOVEit package with files is similar to composing an email with attachments, but there are some differences. File attachments sent as part of a package are uploaded to the MOVEit server. A 'new package notification' email will be sent to the recipients, to inform them that a package is waiting for them.

Note: An option enables the "note" in MOVEit (equivalent to the message body of an email) to also be sent securely, through MOVEit only. Alternatively, the note can be included in the emailed notification, for a personalized touch.

Recipients can click on the web link in the email notification, sign on to MOVEit, view the package, and download the files. If enabled, a recipient can also reply to a package and send additional attachments, which will also be uploaded to the MOVEit server.

The organization administrator can set options that determine who can send and receive packages. An option enables unregistered users to be recipients, and another option allows unregistered users to self-register and send packages. Other options include user- and package-level quotas, and package expiration and download limits.

Introduction and Overview

This is the MOVEit DMZ guide for administrators. This is the comprehensive set of information for organization administrators and system administrators as well as users.

Which guide users receive after sign on depends on user type:

- User Guide – for registered users (covers File Transfer and Ad Hoc Transfer). The other user guides have a subset of the information in this guide, and may also contain information specific to the user type.
- Temporary User Guide – for unregistered users (covers Ad Hoc Transfer only)
- Guest User Guide – for unregistered users (covers limited Ad Hoc Transfer features)
- Administrator Guide – for org admins and system admins (complete configuration, technical, and user information)

Note: Unregistered users sign on as either temporary users whose accounts expire, or guest users (also known as "package password" users) who are given access to a particular package only, not to mailboxes.



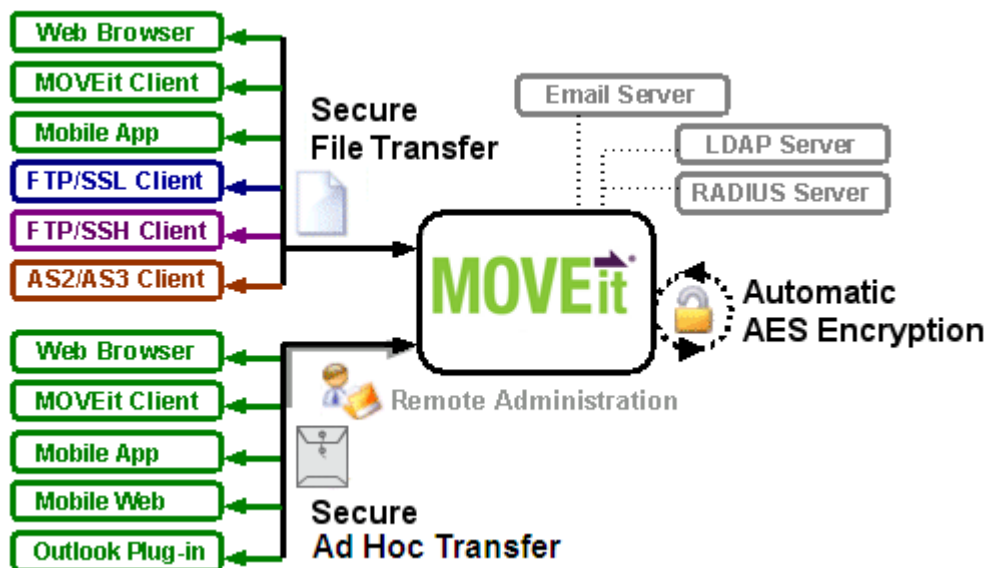
Ipswitch, Inc. (<http://www.ipswitchft.com>)

Overview

Web browsers and no cost/low cost secure FTP clients can quickly, easily, and securely exchange files with MOVEit over encrypted connections using the HTTP over SSL (https), FTP over SSL (ftps) and FTP over SSH (sftp) protocols. And all files received by MOVEit are securely stored using FIPS 140-2 validated AES encryption, the U.S. Federal and Canadian government encryption standard.

In addition, a web interface offers easy online administration and monitoring of MOVEit activities while a programmable interface (via MOVEit API Windows and MOVEit API Java) makes MOVEit accessible to custom applications.

MOVEit includes an optional MOVEit Wizard plug-in that works with Internet Explorer, Firefox and Mozilla to help web-based users to quickly upload and download large and/or multiple files and folder trees to and from MOVEit. There is also a Microsoft Outlook plug-in that users can use for Ad Hoc Transfer.



Encryption and Validation

Encryption capabilities throughout the MOVEit product line are provided by MOVEit Crypto, a compact and fast dynamically-linked library. The AES encryption in MOVEit Crypto has been FIPS 197 validated. The entire cryptographic module has been FIPS 140-2 validated after rigorous examination by cryptographic specialists in the United States' National Institute of Standards and Technology (NIST) and Canada's Communications Security Establishment (CSE).



MOVEit also has an approved Certificate of Networkiness (CoN) from the United States Army. This certification involves a review of how MOVEit meets Army requirements for network security, integration, interoperability, and ease of management and support.

Physical Specifications

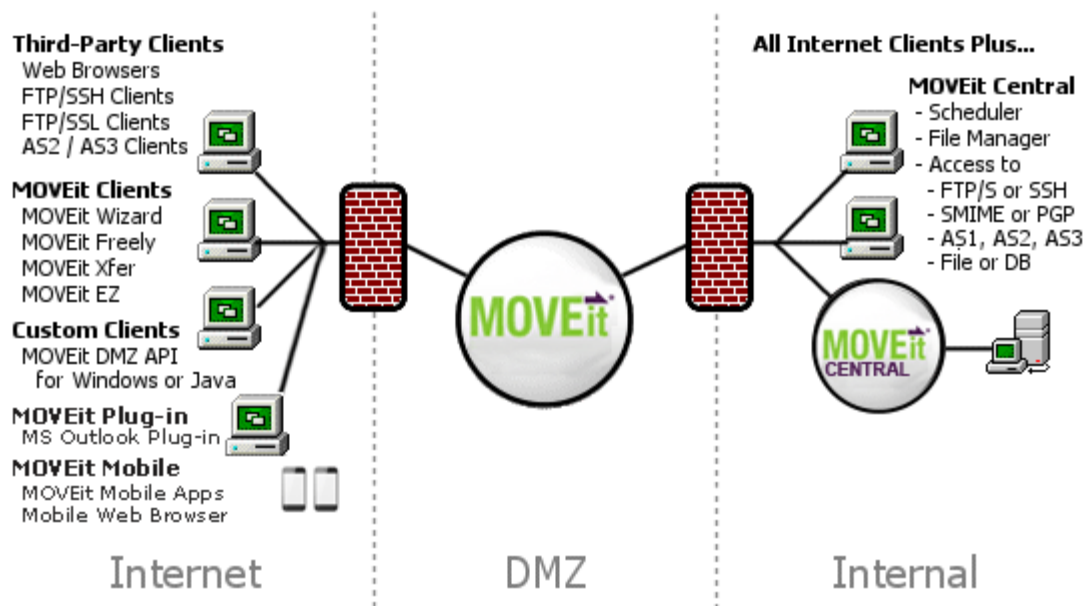
The MOVEit software itself resides on a Microsoft Windows Server platform hardened against threats from the Internet and trusted networks. Organizations that need to support very large volumes of file transfers and/or many users may require additional hardware, but for many organizations the minimum recommended specifications of a MOVEit should suffice:

- 2 GHz Pentium-compatible CPU
- 80 GB SATA or SAS Hard Drive
- 1 GB RAM
- 100/1000 Mb TCP/IP-capable ethernet interface

The latest production recommendations can be found in the **online Support Knowledge Base** (http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ).

Network Specifications

In a typical network topology MOVEit is best located on a secured "DMZ" segment accessible to both internal and external users. "DMZ" is short for DeMilitarized Zone - a network "no man's land" where both internal and internet hosts are allowed to connect. By default, connections originating from a DMZ network segment are not to be trusted and are usually not allowed unless there is a compelling case to allow a particular service through.



Web and secure FTP clients can upload and download files to MOVEit from internal and external networks. For security reasons, MOVEit is NOT permitted to establish connections with or push files to systems on either your internal network or on an external network. (If a "proxy push" or "proxy store-and-forward" solution is desired, MOVEit Central can be used with MOVEit to fill this role.)

MOVEit's Security Advantages Over Other "Secure FTP" Solutions

There are three areas where files are at risk when transferred between an external network (such as the Internet) and your internal network:

- When transferred over the Internet to a system in your DMZ.
- When temporarily stored on a system in your DMZ.
- When transferred from the system in your DMZ to a system on your internal network.

Most secure Web and FTP file transfer products reside on a system in a DMZ and use industry-standard SSL or SSH to provide secure transfers between the Internet and DMZ. (MOVEit does as well.)

Unfortunately, that is as far as most products go; they fail to secure files stored on the DMZ (at risk if the DMZ box gets hacked) and fail to secure files being transferred between DMZ and MY ORG (at risk if a hacker sets up a sniffer inside the DMZ).

MOVEit secures all three areas by using SSL/SSH-encrypted transfers for ALL transfers and by using FIPS 140-2 validated AES encryption to secure files on disk.

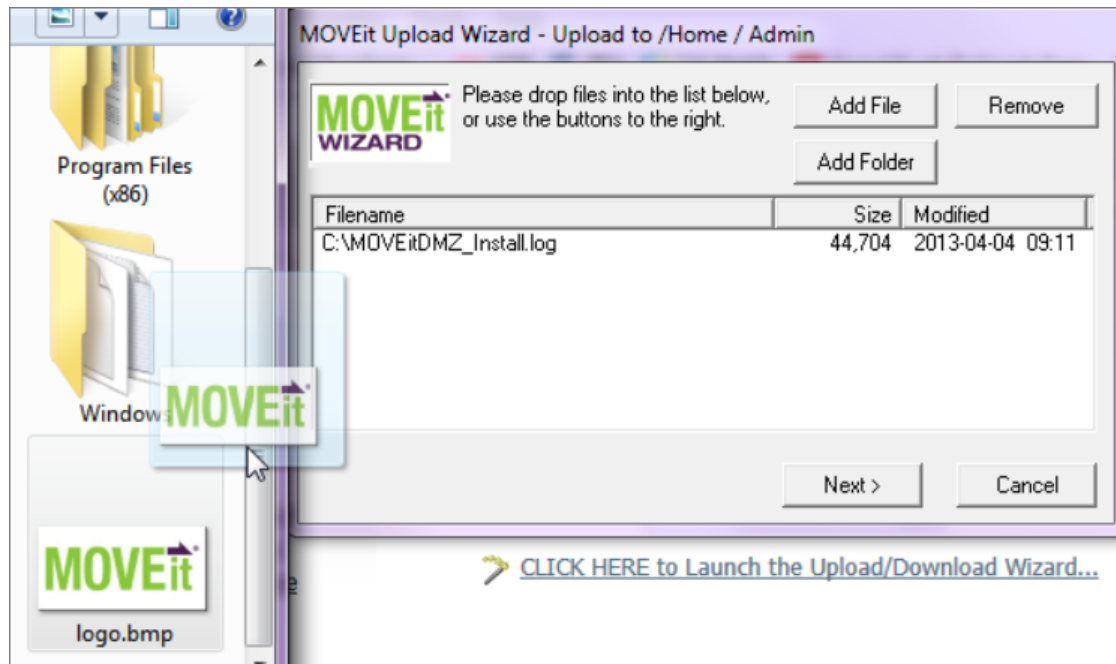
In addition, only MOVEit offers complete end-to-end file integrity over FTP. In other words, files transferred with secure FTP or web clients which support file integrity checks through the MOVEit system can be proven to be 100% identical to their source files through the use of SHA-1 cryptographic hashes. (When combined with authentication, complete file integrity provides non-repudiation.)

Access MOVEit

"Client" access to MOVEit is available through several interfaces, including HTTPS, FTP over SSL, and FTP over SSH.

The built-in web interface provides access to anyone with a desktop web browser (*see the complete list of supported browsers* (on page 793)). Authorized administrators may configure the MOVEit server from authorized locations while customers and partners use a simpler portal to move files in and out of the MOVEit system.

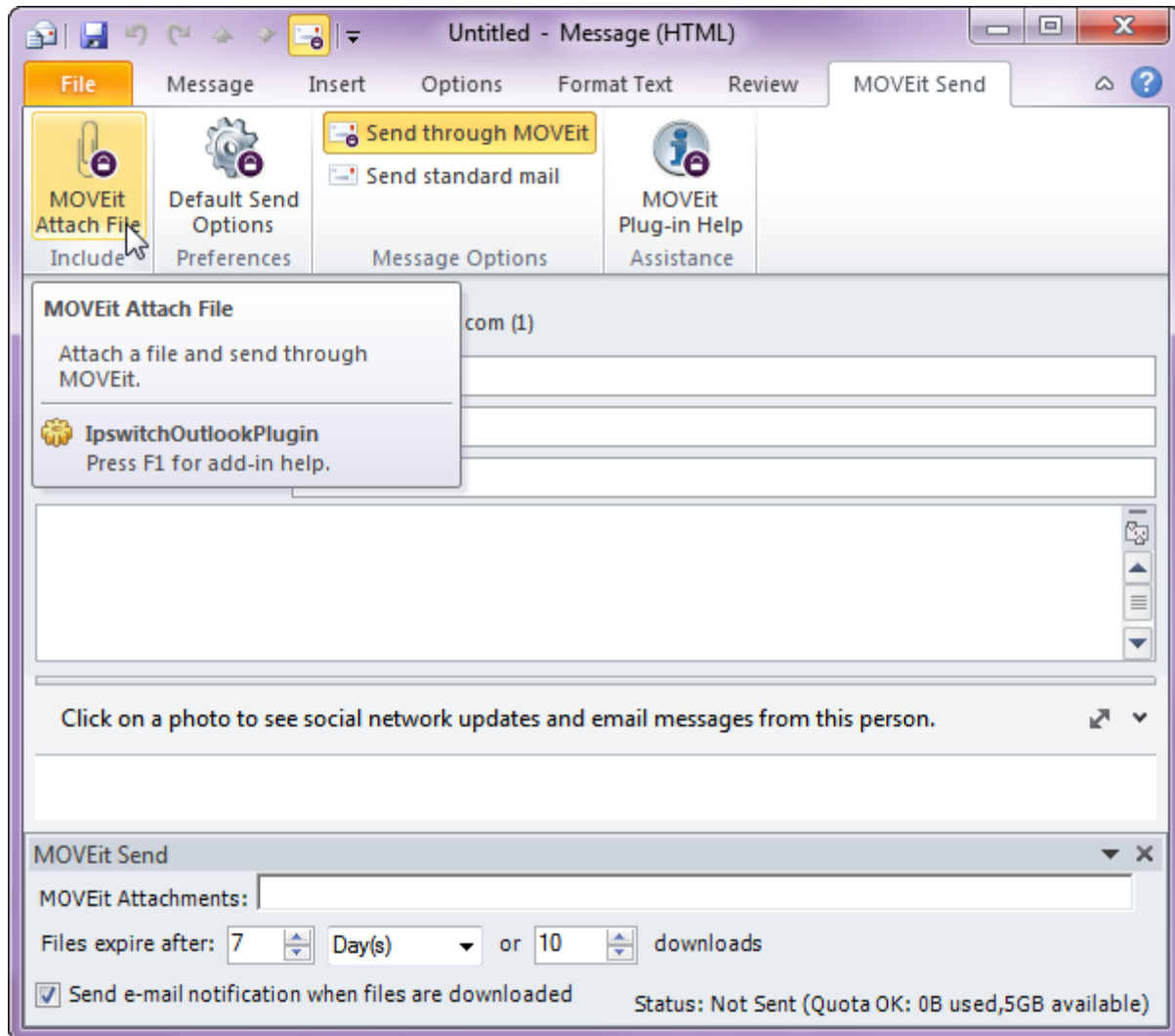
Also available through the web interface is the optional MOVEit Upload/Download Wizard. It provides for faster and more reliable file transfers using the web than are normally available through "stock HTTP". The MOVEit Wizard is also the only browser-based client that supports file integrity checking.



MOVEit offers the separately licensed mobile capability, which enables mobile apps (for iOS and Android) for registered users, plus a mobile web browser (providing Ad Hoc Transfer only, it is for temporary and guest users).



There is also a Microsoft Outlook plug-in (free with an Ad Hoc Transfer license), which registered users can use for sending packages with MOVEit Ad Hoc Transfer.



A secure FTP interface is also available on the MOVEit server for people or programs with secure FTP clients. The MOVEit family offers two free, scriptable command-line clients, **MOVEit Freely** (<http://www.ipswitchft.com/moveitfreely>) (FTP) and MOVEit Xfer (HTTPS) both of which support file integrity checking. Ipswitch also offers WS_FTP Professional, a Windows file transfer client with a robust feature set, which also supports file integrity checking. Many third-party companies manufacture secure FTP clients for desktops and servers which will also interface with MOVEit's secure FTP over SSL and FTP over SSH servers.

For IT departments who desire more control over the MOVEit environment than the FTP protocol can provide, the **MOVEit API** (<http://www.ipswitchft.com/getattachment/c51555fa-57a8-4e4c-ad08-5c7961d650e6/MOVEit-API-Interface-Data-Sheet>) products provide easy access to and control of MOVEit via a COM object (for Windows) or Java classes (for *nix, Windows, IBM, etc.). MOVEit API also supports file transfers with full integrity checking and ships with several command-line utilities for administrators who would rather script than program.

If desktop-to-server automation or the ability to access MOVEit as a local folder is desired, consider using **MOVEit EZ** (<http://www.ipswitchft.com/moveitez>). MOVEit EZ is a "tray icon application" which synchronizes content between a user's desktop and MOVEit and schedules transfers.

When coupled with MOVEit Central and the appropriate licensing, **MOVEit supports AS2 and AS3 file transfer** (on page 676). (MOVEit can be used as a standalone AS3 server, but without MOVEit Central it has no way of encrypting or decrypting specific messages.)

More information about these clients and the dozens of third-party clients which can also be used to securely exchange files with MOVEit can be found in **Client Support** (on page 793).

MOVEit Central

MOVEit Central (<http://www.ipswitchft.com/moveitcentral>) - a Windows Application and a separately installed product - is an enterprise file transfer manager capable of simultaneous file transfers to and from hundreds of Windows file systems.

It is the best tool to use if you are looking for any of the following:

- More than ten scheduled file transfers
- Immediate movement of files to/from backend servers from MOVEit
- Connectivity to other servers

MOVEit Central can support thousands of file transfer tasks and is used in production to securely move hundreds of thousands of files a day at major data centers. MOVEit Central instantly knows when a file has arrived on MOVEit or a Windows file system and can immediately begin transferring that file to its final destination. MOVEit Central supports the most popular secure protocols used across industries, including FTP, SSH, FTP over SSL, SMIME, PGP, email and AS1/AS2/AS3.

In short, when paired with MOVEit, MOVEit Central provides a complete secure transfer solution that can securely receive, record and send files to and from almost anyone supporting a secure transfer protocol.

Note: MOVEit Central should be installed on a separate machine. Running MOVEit Central and MOVEit DMZ on the same machine can cause MySql errors and is not supported.

Technical Support

The MOVEit support website is available 24/7 at ***<http://www.ipswitchft.com/support>*** (***<http://www.ipswitchft.com/support>***). This website provides links to all MOVEit documentation and help videos on the main Support page, as well as a form to contact support and customer support telephone numbers.

Additional Documentation

In addition to this manual, there are several pieces of documentation which may be obtained 24 hours a day, 7 days a week.

MOVEit Support Site

The official MOVEit Support site is located here:

<https://ipswitchft.secure.force.com/cp/>
(**http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ**)

You will likely be required to authenticate with your MOVEit support credentials before being allowed to retrieve additional documentation, but once you have authenticated, you will have access to everything.

- **Installation Guide:** An online MOVEit DMZ installation guide is available on the support site.
- **Release Notes:** Detailed release notes are a part of each and every release of MOVEit software. These notes detail features that have been added, bugs that have been fixed and changes made to critical user interfaces from one version to the next.
- **FAQ (Frequently Asked Questions) and Knowledge Base:** Our FAQ and Knowledge Base is updated monthly with new questions from the field and answers from our technicians. The Knowledge Base details several common operational procedures, troubleshooting assistance, and information about commonly encountered issues.
- **Support/Security Bulletins:** As needed, our support staff will issue a support/security bulletin to let all of our customers know about a vulnerability in our software or the underlying operating system software. Recommended patches and related information can be found in these bulletins, which are also archived on our support site.

Our support site is powered by MOVEit DMZ, so you can be assured that any files or messages you exchange with our technical staff will remain confidential and secure.

Ipswitch Marketing Site

The official Ipswitch Marketing site is located here:

<http://www.ipswitch.com> (**<http://www.ipswitch.com>**)

On our marketing site, you will find several white papers which may be useful to explain how MOVEit products can be applied to address common file transfer and secure messaging challenges.

Typographical Conventions

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

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

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

The following formatting is used to explain command syntax:

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

File Transfer Folder Implementations

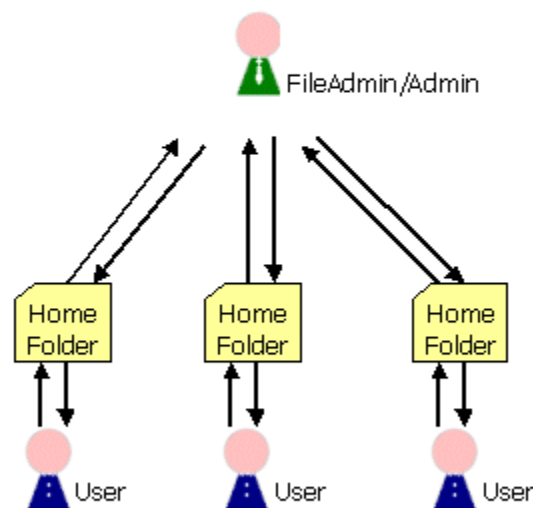
This section provides a quick overview of several common specialized workflows facilitated by MOVEit DMZ File Transfer. Each of these is achieved by how your organization deploys its MOVEit folder structures and permissions.

Secure Person-To-Organization File Exchange

(Using Home Folders)

This application of file transfer is the core around which MOVEit DMZ was built. It features Home Folders for Users within the Organization, with which the Organization can exchange files.

Secure Exchange Between Admin and Users Using Home Folders



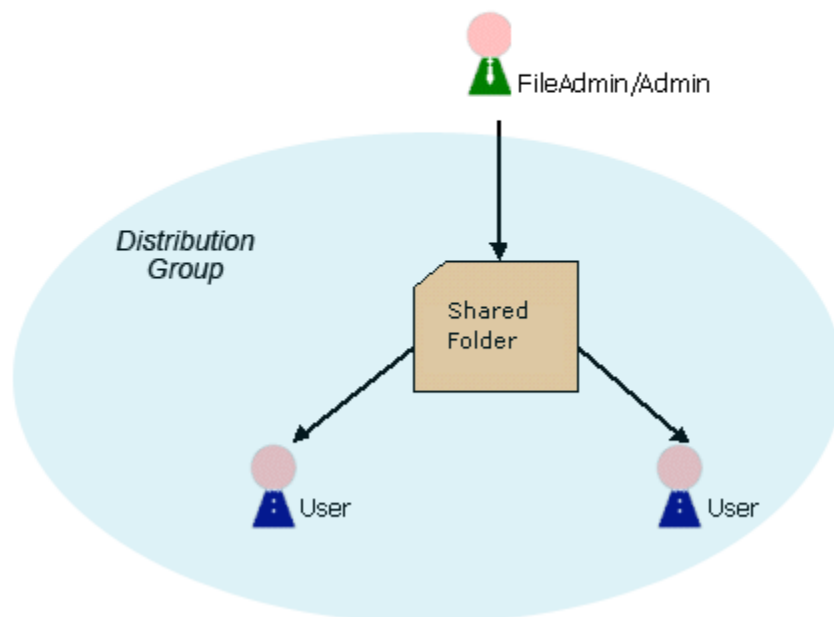
The Organization administrator can set this up by creating User accounts for each person with which the Organization would like to exchange files. A folder will automatically be created for each user. When your Organization (or your copy of MOVEit Central) copies a file into a user's folder, an email notification message will automatically be sent to the user. (If applicable, MOVEit Central - on the "backend," - watches for files and exchanges them with users automatically.)

Sensitive Material Distribution

(Using Group Read-Only Permissions on a Shared Folder)

Organizations often use MOVEit DMZ to distribute sensitive materials to authenticated users such as software, manuals or other materials.

Secure Distribution to Group Users Using Group Read-Only Permissions on a Shared Folder



This setup is best accomplished by creating a new shared folder in the Root folder ("Folders" tab, "Add" link) and a new distribution group (e.g., "BankingSoftware"). First assign READ, LIST and NOTIFY permissions to your new group on your new distribution folder (through the "Folders" tab, "Settings", "Folder Access" section). Then add individual Users to whom the materials should be distributed to the new group (through the "Users" tab, "Groups" section, "View" button, "Group Members" section).

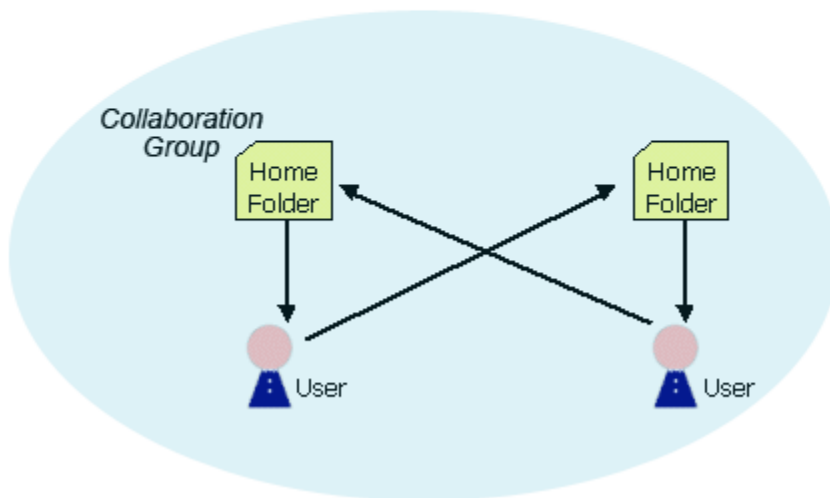
Note: Previous versions of MOVEitDMZ created a special folder type named "Distribution" for this purpose.

Secure Person-To-Person File Exchange

(Using Group Write Permissions to Home Folders)

Many organizations wish to let users, especially internal users, directly exchange files with each other.

Secure Exchange Among Group Users Using Group Write Permissions to Home Folders



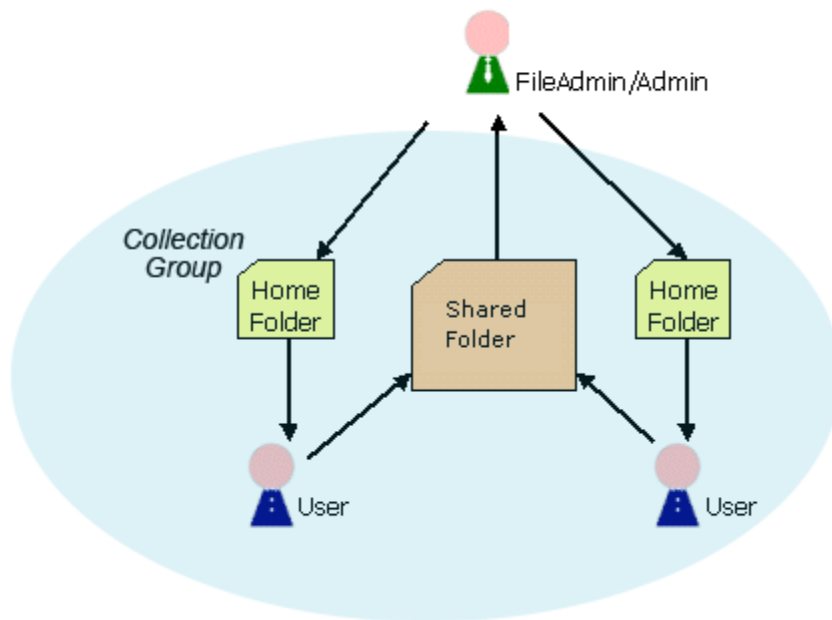
To set this up, create a new group (e.g., "InternalUsers"), add those users to which you would like to grant the privilege of uploading to other user's folders, and assign **WRITE** privileges to the group on each "destination" user's folder (though the "Folders" tab, "Settings", "Folder Access" section.)

Secure Collection Bin

(Using Group Write Permissions on a Shared Folder)

Many organizations would like their end users to upload similar materials into a common "collection bin" rather than to their own home folders.

Secure Collection from Group Users Using Group Write Permissions on a Shared Folder



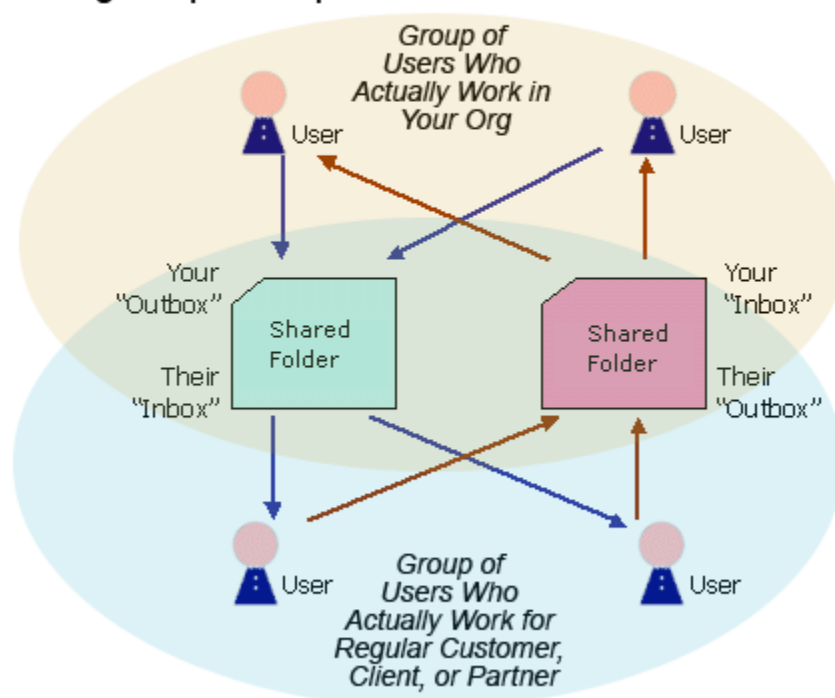
To set this up, create a new shared folder in the Root folder and a new "Collection Bin" Group. Give the new group Write (W) permission to the new folder. Finally, add those users who should be able to upload into the collection bin into the new group.

Secure (Large Business)-To-(Large Business) File Exchange

(Using Multiple Group Write Permissions to Shared Folders)

An organization frequently wants to be able to exchange information with customers, clients or partners whose members are given individual user accounts on your organization's MOVEit DMZ. The outside users do not "share" a single user account (just as your own organization's users); you want a setup that will enable work to continue without relying on particular individuals (*i.e.*, their Home folders).

Secure Exchange Among Users of Distinct Groups Using Multiple Group Write Permissions to Shared Folders



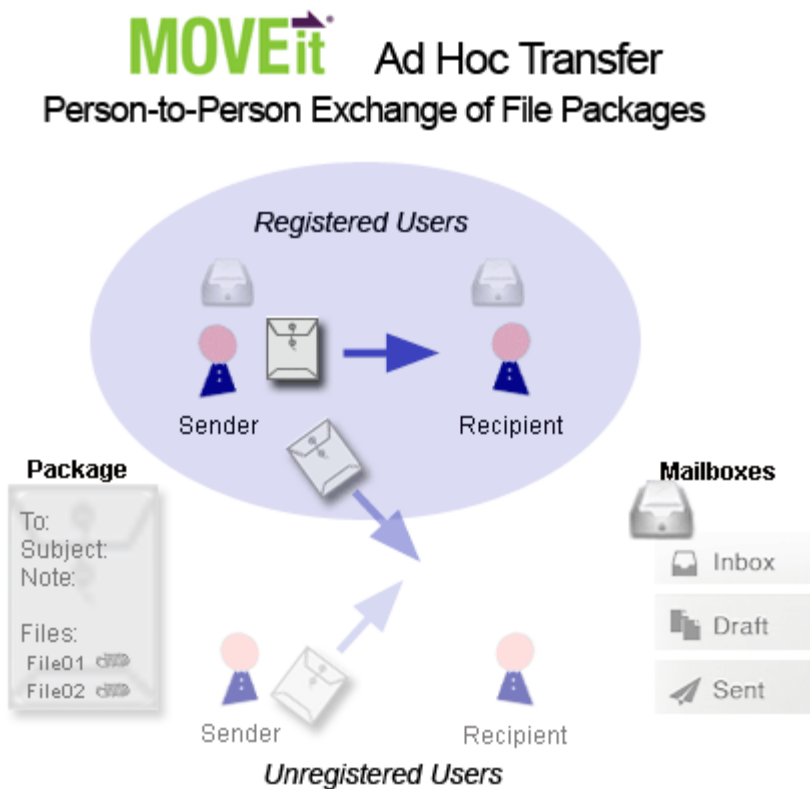
An easy way to handle this situation in a scalable fashion is to set up a root-level shared folder (*e.g.*, "Root/Company") and then two subfolders in this folder (*e.g.*, "Root/Company/ToCompany" and "Root/Company/FromCompany"). These two folders will serve as an "Inbox" and "Outbox" to the two sides of the exchange. Make two new groups, one for your organization and one for the other company. For your organization's group, give it read, list and notify (RLN) permissions on one folder and write only (W) on the other. For the other company's group, give the same permissions, but for the opposite folders. Add users to either your organization's own group or the outside company's group as appropriate.

Secure Webpost Collection

This application is covered in some depth in the "**WebPosts**" *Feature Focus* (on page 92).

Ad Hoc Transfer Implementations

Organizations can use MOVEit DMZ Ad Hoc Transfer for person to person file transfer. Registered users can send a "package," which contains a message and files, similar to an email message with attachments, to other registered members, and, if enabled, to unregistered users who are handled as temporary users or per-package guest users. If enabled, unregistered users can self-register in order to initiate the sending of packages.



Address Books

Control over which users can send packages to other users is controlled through the concept of "address books," which can be configured by the organization administrator. A user's address book can include registered and previously unregistered users who are now considered temporary users. Transfers to and from unregistered users is a feature of Ad Hoc Transfer only (*i.e.*, not to File Transfer with folders).

The Address Book is a list of users and groups to whom the user may send packages. If enabled, users can also send packages to registered users not in their Address Book, and also to unregistered users, in which case MOVEit creates a temporary user. Upon receiving a package from a user who is not in the recipient's address book, an entry will be added in the recipient's address book so that replies are possible.

Another option lets users send packages to an unregistered user with a "package password," in which case, a temporary user is not created. A "package password" provides access to the package sent only, and can be used for a one-time, or infrequent, correspondence with recipient(s).

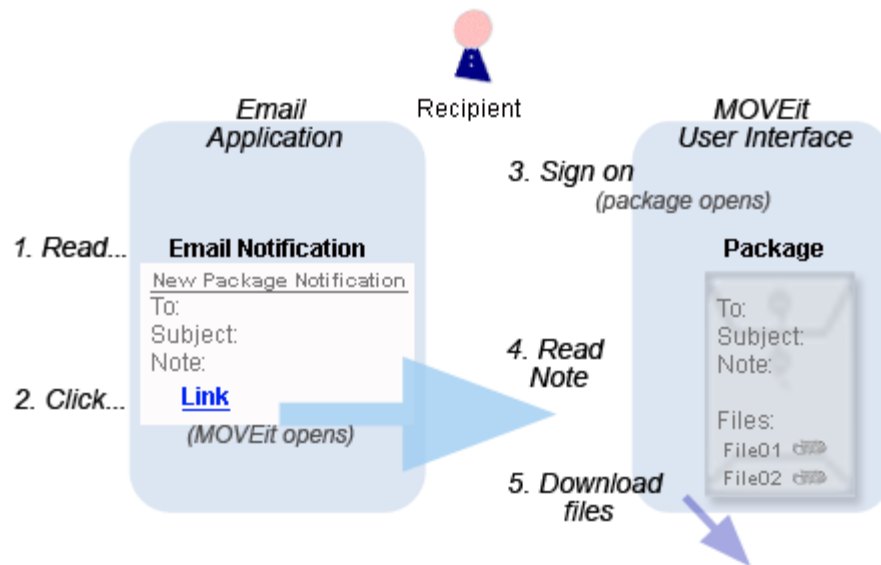
Groups may also have address books, and the entries in a group's address book are automatically available to the members of that group.

The Organization administrator can set options that determine who can send and receive packages. An option enables unregistered users to be recipients, and another option unregistered users to self-register and send packages. Options specify whether senders can send to additional recipients outside of their address book. If so, senders can enter a username, real name, or email address of any registered user, or the email address of any temporary or unregistered user. Other options include user- and package-level quotas, and package expiration and download limits.

Sending and Notification Options

An important aspect of Ad Hoc Transfer is the notification of recipients that they have received a new package. In most cases, it is a key part of the practical Ad Hoc Transfer workflow (and it is essential for the unregistered recipient workflow).

MOVEit[®] Ad Hoc Transfer and Email Notifications



Because the content of the email notifications can aid in usability but are not secure, the administrator can set policies for how much of file transfer content is included in email notifications, specifically the **Note** portion of the package and, to some extent, the **Subject** line. The administrator can set the default or absolute policy for how the **Note** portion of packages (the message body for packages composed in Outlook) should be handled. Should they be handled securely (sent by MOVEit only, and excluded from notification emails)? Or should they be included in the New Package Notification emails sent to recipients? After specifying the overall policy, administrators can also specify whether users get a per-package option to choose which approach to use.

Secure the Note is a package transfer-oriented approach to the message text composed by senders. An email notification is sent by the service, but it excludes the composed note. Securing the note is well suited for entering confidential and sensitive information directly into the package's note.

Turning off this option creates an email-oriented approach to the message text composed by senders. This is helpful for users who want to use the package's note to inform the recipient that they are sending the securely attached files through MOVEit and to introduce the files.

In Outlook, the note is the text the user enters in the email body when creating the package. If securing the note, that text is stripped out of the email that will be sent as a notification email to the recipients. The text will appear only in the package once it is accessed by the recipients. Senders who look in their Outlook Sent folder will see only the notification email that was sent by email to the recipients. To see the text and the package sent, they can sign on to their MOVEit account (either in the Web UI or the Mobile App) and access their Sent (packages) mailbox.

The **Subject** entered in Outlook will always be used in the New Package Notification. But for the MOVEit web UI and MOVEit Mobile, whether the Subject will be used in the New Package Notification depends initially on the **Secure the Note** setting in the package as well as the **Comment Field** administrator setting.

For the web UI and mobile, the **From:** field in email notifications (and the **Reply to:** field) can be set for more or less security. (For packages sent with the Outlook plug-in, emails always are identified as from the sender.) Decide whether the **From:** field should show either the system's notification service or the sender's email address.

- Choose **No** to always show the system's notification service in the **From:** field. Any replies to packages will be addressed to the notification service's email address.
- Choose **Yes** for one of four choices of varying degrees of sending on behalf of user. In all **Yes** cases, any replies to these packages will always be addressed to the sender's email address. The **Yes** option requires either **Include** or **Exclude**, each of which works with the optional **these domains** field to be conditional on each sender's email address.

Admin 101

This topic highlights some of the areas you need to consider when setting up MOVEit DMZ to integrate within your organization and network.

MOVEit DMZ can be almost entirely administered from a web browser. Some system configuration tasks are handled within the **Configuration Utility** (on page 135), which is a Windows application. **Backup and restore activities** (on page 150) are also handled outside of the MOVEit DMZ web interface.

Admin vs. SysAdmin

The difference between Admin and SysAdmin can be initially confusing, but it provides a logical and scalable separation of operations. SysAdmin is the more powerful permission class, but SysAdmin file and secure message privileges are minimal. (For example, SysAdmins can set up a user but cannot read that user's files.) For this reason, Ipswitch generally encourages people to use Admin accounts for daily administration (working with users, folders, etc.) and save SysAdmin account sign ons for special occasions (new org, IP lockout change, etc.)

More specifically, SysAdmins have exclusive access to the settings detailed in the documentation sections referenced below:

- Web Interface - Settings - System
- Web Interface - Schemes
- Web Interface - Organizations

...but are never allowed to upload/download files or send/receive secure messages in any organization other than the System organization.

Modern versions of MOVEit DMZ force you to set up both a SysAdmin and an Admin account when you install and encourage you to use the new Admin account unless you absolutely need to use a SysAdmin account. In fact, SysAdmin accounts are only permitted to sign on from the console (i.e., localhost, 127.0.0.1 or local IP addresses) by default. (To change this, you must sign on as a SysAdmin from the console and expand the IP range from which System Organization SysAdmins are allowed to sign in.)

For a complete explanation of Admins, SysAdmins and other user permissions classes, please see **Web Interface - Users - Permissions** (on page 277). For a complete explanation of what orgs are and when they should be used, please see **Web Interface - Organizations - Overview (Definition)** (on page 547).

Policies and Procedures

After you get comfortable with some key features, you will probably want to come up with answers to several policy and procedure issues. Fortunately, the flexibility of MOVEit DMZ allows you to answer these almost any way you want; options exist to establish and enforce many different policies in MOVEit DMZ. (Ipswitch can also help you come up with answers to these questions if you are unsure or need some advice.)

Authentication Policies

- Passwords - How long/strong do you want your passwords? How often should they be changed? How will you get them to your users (fax/phone, emailed when the user is created)? Are users allowed to reset their own passwords? If so, will you require users to sign on with their old credentials first?
- Interfaces - Will you allow FTP/SSL, FTP/SSH, HTTPS and/or AS2/AS3? Will you ever allow non-secure FTP? Do you want users connecting to "port 80" HTTP to be automatically redirected to your secure web interface or do you just want to drop the connection? Are you offering enough interface options to allow your clients to do ad-hoc and automated transfers?
- Shared Accounts - Will you ever allow shared accounts? If so, do you want individuals using the shared account to see files that others using the account have uploaded?
- Groups - How will you organize your users in groups? Where you have a choice, would you rather grant permissions, etc. by group or by user? Would you like certain users to enjoy delegated permissions over certain folders, users, etc.?
- External Authentication - Will all users authenticate to MOVEit DMZ's local database? Will they authenticate through a trusted LDAP or RADIUS server instead? Will there be a mix?
- Naming Conventions - Should usernames be "first initial, last name", employee numbers, company names or something else? Should full names contain the names of key people and/or their organizational role or just a company role? Will you be using different conventions for internal/external users?
- Lockouts and Expiration - How many tries should a user get before that user is locked out? How many tries should a particular IP address get before that IP is locked out? How long should we let a user dodge a requested password change before we disable the account? Should we automatically shut down accounts that have not been used in a while or have gone over their contract date?
- Allowed Hosts and IPs - By default MOVEit DMZ sets up an IP access policy that allows end users to connect from anywhere but only allows administrators to connect from an internal private network. Is this tight enough? Are there exceptions? Do you really want to specify a list/range of IP addresses and hostnames for each user instead?
- Client Certificates/Keys - Using these credentials is often more secure but usually requires more work. If you are using client certificates, what Certificate Authority(ies) will you use? Do you need "two factor" authentication or will the use of a particular cert/key be enough?
- Automated Users - Most sites set up a FileAdmin user for their MOVEit Central file transfer automation tool, but your end users or other internal processes may be completely automated too. Do you want these users to be exempt from periodic password changes? Do you want them further restricted by IP address, client cert/key or interface to mitigate the risk of an automated username or password getting compromised?

Folder Policies

- Structure - Do you want users to each have their own tree of folders in their home folder or do you want a shared folder structure? Should user home folders be in one top-level folder, or in multiple folders? Do you want to simply lock users to a single folder and "dumb down" the interface to keep them from making any mistakes? What should the main shared folder be named?
- Permissions - What permissions should users enjoy on various folders? On their home folder, by default? Do you want upload quotas? Do you want filename restrictions?
- Clean Up/Notification - How often should MOVEit DMZ automatically delete old files and folders? How rapidly (if at all) should it send notifications about whether or not files were uploaded OK, have been downloaded or have not been downloaded by some deadline?
- Naming Conventions - Should users' home folders bear the name of their usernames, their full names, user IDs (unique ID generated by MOVEit DMZ) or something else? Should MOVEit DMZ folder trees reflect internal trees or be named for specific customer needs? Will you be using specific folder names and file names to help people and automated tasks figure out what to do with various files?

Ad Hoc Transfer Policies

- Licensing, Option Enabled - First, make sure you have a valid Ad Hoc Transfer license (using the DMZ Config utility) and that you have enabled this feature through the **Registered Users** link on the **Settings** page's **Ad Hoc Transfer** section, next to **Access**. Also make sure the **Package Log Viewing** property on the organization's Profile (accessible with a SysAdmin account) is on if you want your Admins to see who is sending Ad Hoc packages within your organization.
- Address Book Contacts and Unregistered Recipients - Who should be able to talk to whom? Do you want to allow everyone to contact everyone else, including unregistered users, or do you want to control Ad Hoc Transfer relationships? Who should be able to create and send packages to unregistered recipients on the fly?
- Unregistered Recipients and Senders - When unregistered recipients sign in - and when unregistered senders self-register - should they be treated as per-package "guest users", or should they be registered as "temporary users" for a limited amount of time? Are there any domains that MOVEit DMZ should not be able to create temporary users for (such as your own or a free mail service)? How long should temporary users remain before they are automatically purged?
- Secure Note transfer vs. Email Note, per package sender option, and related options - Do you want to be assured of secure transfers, not only of files, but also of every note that senders compose when creating MOVEit Ad Hoc Transfer packages? Or would you rather provide your users with a consistently Outlook-style, email-oriented notification operation (with only the attached/uploaded files being sent exclusively by MOVEit)? Do you want to offer both flavors of operation by offering senders a per package choice? In addition, do want to add security for the packages' Senders and Subjects (of packages sent from the Web Interface and Mobile only; these settings do not affect packages sent from the Outlook Plug-in)?
- Permissions - Do you want attachment quotas? Do you want filename restrictions?
- Retention - How long should we keep packages online? Should we delete them or archive them?

Appearance

- Banner and Scheme - What banner logo will you use? What scheme will you use to match the colors and fonts to your main corporate site? What logo will you use for the mobile app and web?
- Display Profiles - Which parts of the web interface should your users see when they are signed on? Before they sign on? Do you have to worry about "power users"? Do you want to offer all users the ability to change language before sign on? Do you want to offer or withhold the ability for users to change their user interface's language when or after they sign on?
- International Languages - Which language do you want to be the default for the organization: English, French, German, or Spanish?
- Notifications - How much information (username, fileID, file names, etc.) should be sent in clear-text email notifications? Who should appear to be the sender? Are there any notification templates that you would like to alter? Do your users prefer good-looking HTML notifications or functional text notifications?
- Sign On Banners, Etc. - What should you display to users before they are allowed to sign on? What kind (if any) information will you put in the home page announcement? How should the first status message a user sees after signing on read?

Logging and Reporting

- Filtering Logs - Can you find what you want in the audit logs? Can you figure out why the following common problems occurred from the audit logs? (User could not sign on. File could not be uploaded, downloaded, etc. Folder or user could not be created, deleted, etc.) Are you comfortable selecting columns, sorting and hiding/showing sign on and notification entries?
- Reports - What reports will you use regularly? Do you want to schedule them? Do you expect to perform further processing on CSV or XML formatted reports? Do you want to alter the template used for HTML reports?
- Retention - How long should we keep audit records? Should we delete them or archive them?

Real World Administration

- People - Who is/are the main administrator(s) of each MOVEit DMZ organization? Are they the same people in charge of the firewall? Are there administrative tasks that can be delegated through GroupAdmins or using features such as **allow users to reset own password**?
- Automation - Are you using the automated features of MOVEit DMZ (such as old file/folder cleanup, notification, report creation) to your full advantage? If you own a companion MOVEit Central server, is it automating all the file transfers it can? Are your end user and internal transfers as automated as they can be?
- Disaster Recovery - How are you backing up your server? Do you have the MOVEit DMZ licenses you need for your backup servers? Is your backup/restore procedure automated? Have you tested it? Does your main site need active-active failover?

- End User Documentation - Do your end users know how to connect to you and where to go to upload/download files? (Or use secure messaging, as applicable.) (See **Advanced Topics - User Forms** (on page 679) for some suggestions here.) Do they know how to ask for help? Is there additional documentation you could post online to help? (MOVEit DMZ's **Tech Support** link/page and **Custom Help Link** feature help here.)
- Administrative Documentation - Is your configuration documented and explainable? (You can use the DMZBackup utility if you simply need a backup of the current configuration.) Do you know how to pull/schedule the reports that fulfill your audit requirements? Your billing requirements? Other business requirements?

Other Tasks

What else you do next depends a great deal on the application for which you are using MOVEit DMZ. (See **Common Setup** (on page 15) for a brief list of common applications.) However, most administrators will shortly find themselves making use of **Groups** (on page 303) to organize the way users may access files and folders. Many administrators will also be interested in setting up strong password requirements (on the **Settings page** (on page 349)) and/or folder settings to allow for automated cleanup of old files (on individual **Folder pages**. (on page 55))

Ongoing Maintenance

As an administrator you will most likely "hover over" the **Logs page** (on page 316) more than any other page. (You will likely want to familiarize yourself with the various log filters available.) Most of your changes will involve adding and removing individual users, or tracking down and dealing with files which have been placed in the wrong place, not processed by internal systems appropriately, etc.

Feature Focus

This section contains some specific information about MOVEit.

These topics include both:

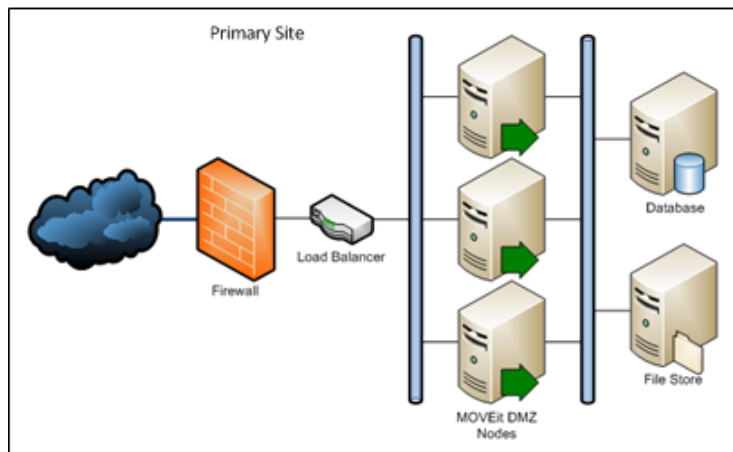
- Overall procedures to implement overall features
- Detailed descriptions of configuration options for specialized features

High Availability, Failover and Disaster Recovery

High Availability (HA) with Web Farms

The Web Farms feature of MOVEit is a good choice when you need a high availability environment, as you can add servers for to add capability. A Web Farm shares a common database and file store among nodes and provides increased availability by scaling the system to increase its capacity.

MOVEit Web Farm Architecture

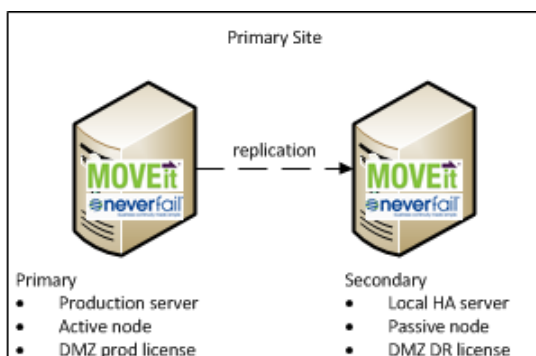


For more information see **Web Farms** (on page 660) in this guide. Note that the Web Farm solution is not currently qualified to work with the Neverfail solutions.

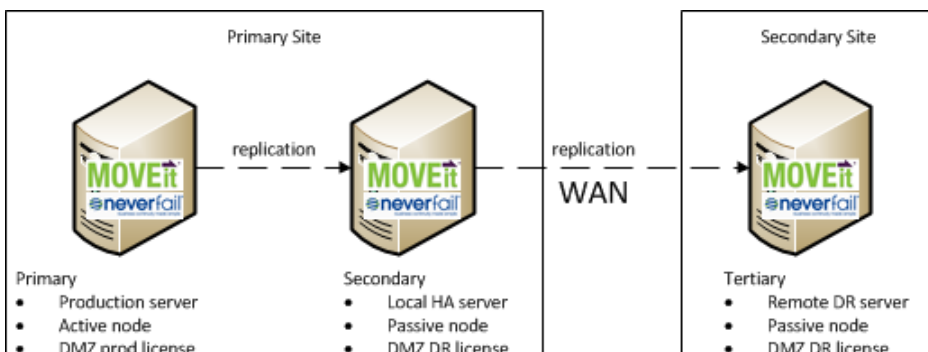
Failover and Disaster Recovery (DR) with Neverfail

For those in need of a failover and/or disaster recovery solution, we recommend our partner Neverfail. Neverfail consultants can work with you to configure three basic scenarios:

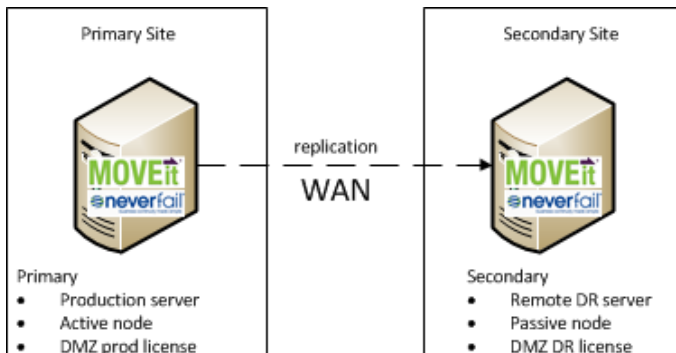
- Local failover using a primary and secondary server. This setup enables a redundant local system with complete replication of the local database and file store for failover to secondary node. It offers increased system availability, but not increased capacity.



- Remote Disaster Recovery (DR) by adding a tertiary server via WAN links. This setup adds a third redundant server on a WAN node that provides failover in the event the local network that houses the primary and secondary servers fails.



- Remote Disaster Recovery. This setup enables a redundant server on a WAN node that provides failover in the event the primary server fails.



We have tested the above scenarios using MOVEit DMZ 8.1 with Neverfail in the following test environment:

Machine 1 (Primary):

- MOVEit DMZ 8.1 with MySQL database (no Web Farms)
- Windows Server 2012
- Two network interface cards (one exclusively for Neverfail Heartbeat)

Machine 2 (secondary) on the local network and Machine 3 (Tertiary) on a remote network must have the same specifications as machine 1.

Refer to the Administrator's Guide for Neverfail Heartbeat for a description of the Neverfail setup and step-by-step instructions.

Neverfail consultants can help you configure MOVEit in these failover and disaster recovery scenarios.

Mobile Implementation

MOVEit Mobile, which requires a separate license, enables users to securely transfer large files and large numbers of files using their mobile devices (which connect to your organization's MOVEit server).

MOVEit offers both email-style and folder-based transfers. Depending on your organization and your permissions, users might have access to one of these or both methods. With both, users are able to send and receive packages and access their files securely from their iOS and Android devices.

The mobile app supports registered users with these capabilities:

- Navigating through the folder structure
- Uploading and downloading files, which includes opening them in other applications
- Sending and receiving secure packages

The mobile web supports unregistered (Guest/Temporary) users with the ability to receive and send secure packages.

This topic covers the mobile implementation for administrators, including server and app installation and configuration. It also describes both the mobile web and the mobile app, and when each is used. It provides both links to major topics and specific procedures and tips administrators can give to end users. Finally, it also includes some information about using mobile in conjunction with the full web interface and with the Outlook client interface.

MOVEit DMZ and MOVEit Mobile Server Architecture

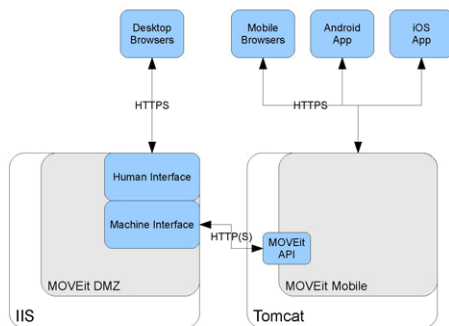
MOVEit DMZ and the MOVEit Mobile Server are installed on the same application server node; in the case of Web Farms, multiple nodes are used.

Microsoft IIS is the application server software that runs MOVEit DMZ. IIS also serves as MOVEit DMZ's HTTP server, taking connection requests from desktop browsers.

Apache Tomcat is the application server software that runs MOVEit Mobile. Tomcat also serves as MOVEit Mobile's HTTP server, taking connection requests from mobile browsers and apps.

MOVEit Mobile, in turn, interacts with MOVEit DMZ through the MOVEit API.

Refer to the following architecture diagram for the overall context of your installation and operation activities.



Server Installation and Deployment

This is an overview of how to install and deploy MOVEit DMZ and MOVEit Mobile on each MOVEit Application Server node, and configure the MOVEit system for mobile.

Note: You do not need a Mobile interface license to install mobile, but you need it in order to operate mobile.

➤ *To install MOVEit and MOVEit Mobile on each MOVEit DMZ node:*

- 1 Install MOVEit DMZ or upgrade to the latest version on each node. MOVEit DMZ 8 is the minimum version required for MOVEit Mobile. (See ***MOVEit DMZ Installation Guide*** <http://docs.ipswitch.com/MOVEit/DMZ8.0/Manuals/MOVEit%20DMZ%20Installation%20Guide.pdf>.)

Note: If you install MOVEit DMZ in a Virtual Directory, see the note under MOVEit System Configuration below.

- 2 Install MOVEit Mobile Server on each node. (See ***MOVEit Mobile Server Installation Guide*** <http://docs.ipswitch.com/MOVEit/DMZ8.0/Manuals/MOVEit%20Mobile%20Server%20Installation%20Guide.pdf>.)

Note: The install wizard includes possibly changing the Tomcat HTTP and HTTPS connector ports and an optionally specifying an IP address or hostname. (Any changes you make you will also need to make in System Configuration in the Mobile URL.)

Note: For each node in a Web Farm deployment (see ***Web Farms*** (on page 660)), use the Logon Information step within the installation wizard to specify the username and password of the Windows user account that will log on to run the Mobile Server. (See ***MOVEit Mobile Server Installation Guide*** <http://docs.ipswitch.com/MOVEit/DMZ8.0/Manuals/MOVEit%20Mobile%20Server%20Installation%20Guide.pdf>.)

- 3 Configure your firewall to enable the TCP ports for MOVEit Mobile client connections, as configured in during the installation. The default ports are 8080 for HTTP and 8443 for HTTPS. (See ***System Configuration - Firewall Configuration*** (on page 128).)
- 4 Run the MOVEit DMZ Config utility to validate installation. (See ***System Configuration - Configuration Utility*** (on page 135).)

1. Check the Licensing tab to verify the Mobile Interface license is installed.

Note: If the license is not installed, obtain the updated license file and install it using the Import function in the Licensing tab.

2. Check the Status tab to see if the Mobile service is running.

MOVEit System Configuration

Perform MOVEit System Configuration (as SysAdmin) for Mobile. Specifically, change (if necessary) the **Mobile URL** to match the mobile server installation, and change the default mobile settings as desired for all new organizations.

Note: If, during mobile server installation, the Tomcat HTTP and HTTPS connector ports were changed or if an IP address or hostname was specified, you must make corresponding changes in the **Mobile URL**.

Note: If MOVEit DMZ server installation was to a Virtual Directory, you must remove the name of the virtual directory from the *Base URL* as configured in **Mobile URL** (although the name of the virtual directory *will* be in the URL users use to connect to MOVEit DMZ and MOVEit Mobile). See **Orgs - [Org] - Profile - Mobile URL** (on page 550) for details.

➤ *To perform SysAdmin configuration:*

- 1 Open the URL for MOVEit DMZ and sign on as SysAdmin.
- 2 Go to Orgs and select an Organization. Check the Mobile URL in **Orgs - [Org] - Profile - Mobile URL** (on page 550). If needed, click **Change Information** and configure Mobile URL.
- 3 Repeat step 2 as needed for additional organizations.
- 4 Optionally, set new defaults for new Organizations. Select the "System" organization and perform steps 2 through 4 from the following procedure.

Note: For more information about SysAdmin and Admin Configuration, see **System Configuration - Admin 101** (on page 25).

MOVEit Organization Configuration

Perform organization configuration for Mobile.

➤ *To perform organization configuration:*

- 1 Open the URL for MOVEit DMZ and sign on as the org admin.
- 2 Configure the visibility requirements for the mobile **Security Notice** dialog in **Settings - Appearance - Info - Sign On Banner** (on page 354). Set it to show the Security Notice dialog either:
 - every time the user signs on
 - only when there is a new banner or notice
 - never

- 3 Optionally upload a .png logo image with your organization's branding for the mobile Sign on page. Go to **Web Interface - Settings - Appearance - Brand - Mobile** (on page 358).
- 4 Configure the default organization policies for accessing Mobile, caching of device credentials, and minimum PIN length. Go to **Settings-Security Policies-Interface-Mobile** (on page 482).

Note: You can also configure the first two of these policies (accessing Mobile and for caching of device credentials) for individual users. Go to **Web Interface - Users - Profile** (on page 286), and click Mobile Policy to make the edits.

Certified Devices and Supported Mobile OS Versions

Certified Devices

The following device models have been fully certified for use with the MOVEit Mobile App and Web interface:

- iOS phones: iPhone 5s/5c, iPhone 5, iPhone 4S, iPhone 4G with OS 6+, iPod Touch
- iOS tablets: iPad (3rd/4th generation), iPad 2, iPad mini
- Android phones: Samsung Galaxy S III/IV, Samsung Note II, Google Nexus 4, HTC One X+, HTC Droid DNA, Motorola Droid Razr Maxx HD, Motorola Moto X, LG Nexus 5
- Android tablets: Samsung Galaxy Tab 2/3 7", Samsung Galaxy Tab 2/3 10", Samsung Galaxy Note 8, Google Nexus 7", Google Nexus 10"

Supported Operating Systems

Supported mobile operating systems include:

- iOS: 7.x, 6.x
- Android: 4.4.x, 4.3.x, 4.2.x, 4.1.x, 4.0.x

Org Admin Instructions to Registered Users

Here is a starting set of information and instructions that you can revise and then provide to registered users regarding the installation and configuration of the app.

Before you start:

- Check with your organization administrator for the mobile operating systems and devices supported by Ipswitch and by your organization. Mobile might not work correctly with some older devices.

- Check with your organization administrator about whether **Quick sign on** is available to you and whether it is required or recommended for you or not.

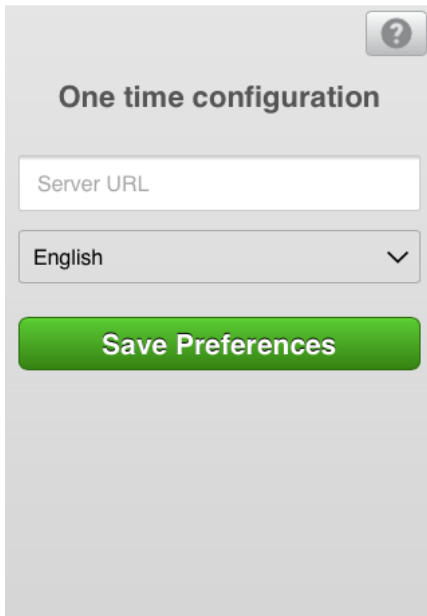
➤ *Instructions for mobile users:*

- 1 Go to the online app store for your device (iTunes or Android). Search for Managed File Transfer to locate the MOVEit app. Install the MOVEit app.

Note: Optionally choose to install a file manager app, as applicable, if your administrator suggests this for you.



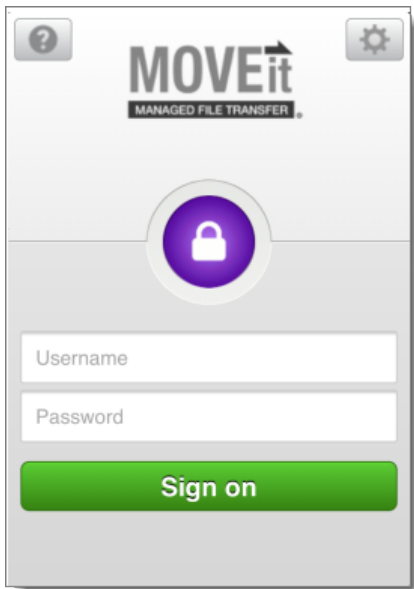
- 2 Start the app with  on the home screen of your device.
- 3 In the **One time configuration** screen, enter the **Server URL**. Use the same URL that you would enter into a browser to access MOVEit. (The system automatically redirects mobile requests as needed.)

The image shows a screenshot of the "One time configuration" screen within the MOVEit mobile application. The screen has a light gray background. At the top right, there is a small square button with a question mark icon. Below this, the title "One time configuration" is displayed in a bold, dark gray font. Underneath the title, there is a white text input field with the placeholder text "Server URL". Below the input field is a dropdown menu showing "English" with a downward-pointing chevron icon to its right. At the bottom of the configuration section, there is a prominent green button with the text "Save Preferences" in white.

- 4 Also in that screen, select your preferred **Language**.

Note: Signing on with this language will change the language in your MOVEit user profile (for use with the MOVEit desktop web interface and other user interfaces). Admin users must use English to be able to sign on. The **Sign on** screen itself does not provide a change language option.

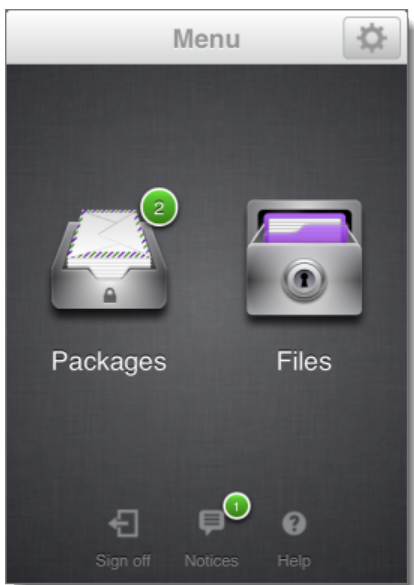
- 5 Tap Save Preferences. The Sign on screen opens.



- 6 Enter your MOVEit username and password.

Note: Admin users are not allowed to sign on with any other language than English. If the current language is non-English, sign on as a non-Admin user and change the language to English. Alternatively on Android, clear data for the app in an app manager, and then select English in the One time configuration screen.

- 7 Tap Sign on. The Menu screen opens.



- 8 After you sign on, you can tap Help  for online help on common user activities.

Note: The English version of the app help is located at:

<http://docs.ipswitch.com/MOVEit/DMZ8.0/mobile/app/en/index.htm>

<http://docs.ipswitch.com/MOVEit/DMZ8.0/mobile/app/en/index.htm>

- 9** Tap  for **Settings**. If your administrator has made **Quick sign on** is available, and depending on organization policy or recommendations, select **Quick sign on**, to create a PIN.
-

Note: Five failed PIN entries will require users to reset their username and password before continuing.

Note: While the PIN is set, there is no way to sign on as a different user or to a different org. If a PIN is established, the user who set the PIN must sign on to remove the PIN before another org can be selected or another user sign on. In other words, while a PIN is in place, the MOVEit app on that device is dedicated exclusively to that one user account and org.

- 10** In **Settings**, optionally set **Network preferences**, to set whether or not to use a data plan for file transfers (as opposed to WiFi), and if so, whether to prompt you every time or not.

Here are some other points to be aware of:

- Opening an emailed URL link in a New Package Notification or New File Notification opens the app.
- While in MOVEit mobile, when opening a file, you might get an app chooser dialog that lists MOVEit itself. Choose another app to open the file, and optionally indicate if you want to always use the selected app to open that type of file.
- When you attach a picture to a package or upload a picture (or if you take a picture to attach or upload), the photo is automatically named sequentially (such as cdv_photo_001.jpg), not with the date and time that the picture was taken. You are not given an opportunity to change the name within the mobile app.
- On Android, if you take a picture to attach or upload, and the send or upload fails, you are prompted about whether you want to save the picture locally or discard the picture. (With iOS, the picture is discarded.)

Mobile Web Use

The mobile web serves users who do not have the installed app on their mobile device. It was primarily designed with unregistered users in mind. That is why it presents the **Packages** function but not the **Files** function. However, the mobile web can also be used by registered users to access packages from a mobile device that does not have the app installed.

Note: Attaching files from the device is not supported in the mobile web.

Be aware of the following use cases for unregistered users using the mobile web (without the mobile app being installed on device):

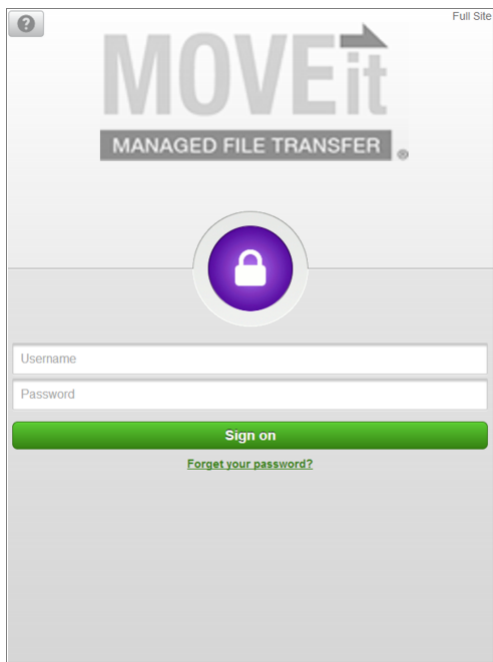
- Unregistered recipient, as a guest user, opening an emailed URL link in a New Package Notification. The Sign on page opens, and they enter the password they have been sent or told about. After sign on, the package is displayed. There is no access to the Menu screen.
- Unregistered recipient, temporary user, opening an emailed URL link in a New Package Notification. The Sign on page opens, and they enter the password they have been sent or told about. After sign on, the package is typically displayed. However, they can access the Menu screen.
- Temporary user going back to use MOVEit.
- A registered user, opening an emailed URL link in a New Package Notification or New File Notification.

Switching from Mobile Web to the Full Site

The mobile web offers a link to the Full Site. This is useful for:

- Tablets
- Administrators who want to use configuration functions
- Registered users who do not have the app installed on a device but wish to access the Files functionality

- Unregistered users who would like to attach files to packages and send them



Ad Hoc Transfer Implementation

The Ad Hoc Transfer Module, which requires a separate license, provides a secure way to do person-to-person file transfers. Registered MOVEit DMZ users can use a browser or an Outlook plug-in to send files and/or a message (which is called a 'package') to an email address. Composing a MOVEit package that includes files is like composing an email with attachments.

However, there are differences. File attachments sent as part of a package are uploaded to a MOVEit DMZ server. A 'new package notification' email will be sent to the recipients, to inform them that a package is waiting for them. Recipients can click on the web link in this notification, sign on to MOVEit DMZ, and view the package, where they can download the files.

If enabled, a recipient can also reply to a package and send additional attachments, which will also be uploaded to the file transfer server. The organization administrator can set options that determine who can send and receive packages, enforce user- and package-level quotas, and control package expiration and download limits.

Large files and multiple attachments can be sent quickly and securely, avoiding the limitations of a mail server.

Enable Ad Hoc Transfer

An Organization administrator can enable or disable the Ad Hoc Transfer feature for an organization, as well as set access rules, limits, and quotas. Many of these settings can also be set at the group and user levels.

The organization settings for Ad Hoc Transfer can be found in the administrator's Settings page, in the Ad Hoc Transfer section.

To enable and configure Ad Hoc Transfer:

- 1 To enable access to Ad Hoc Transfer for all users in the organization, from the Home page, click **Settings - Ad Hoc Transfer - Access** and select **Registered Senders**.
- 2 Under **Which users may send packages?**, select **All**.

The other settings on this page determine whether registered users (those with an account on MOVEit DMZ) can send packages to registered users not in their Address Book, or to unregistered users. You can use these settings to control access to the Ad Hoc Transfer feature. To allow the most open access, select **All except temporary users** for both settings.

For detailed information, see **Web Interface - Settings - Ad Hoc Transfer - Access** (on page 496).

- 3 Click **Save** to make the changes.

- 4** Optionally, allow access to unregistered recipients. If you allow registered users to send packages to unregistered users, you can set how the unregistered recipient is handled by MOVEit DMZ. For unregistered recipients settings, go to **Settings - Ad Hoc Transfer- Access - Unregistered Recipients**.

The unregistered recipient will need to access the MOVEit DMZ system to retrieve a package and any attached files. You can choose to have MOVEit DMZ treat these recipients as temporary users (the default setting), in which case MOVEit DMZ creates a temporary account for the recipient. You can also choose to treat the recipient as a guest user, who will have access to only the package sent to them.

For detailed information, see **Web Interface - Settings - Ad Hoc Transfer - Access** (on page 499).

- 5** Optionally, allow access to unregistered senders. Unregistered senders need to access the MOVEit DMZ system to send a package and any attached files. For unregistered senders settings, go to **Settings - Ad Hoc Transfer - Access - Unregistered Senders**.

If you allow unregistered users to send packages it is handled the same as the unregistered recipient is handled by MOVEit DMZ. Go to **Settings - Ad Hoc Transfer - Access - Unregistered Recipients** to change the Temporary Users vs. Package Password setting.

For detailed information, see **Web Interface - Settings - Ad Hoc Transfer - Access - Unregistered Senders** (on page 505).

- 6** To give senders the ability to either **Secure the Note** or **Email the Note**, and to configure related settings for the package **Subject** and **From/Reply-to** fields, go to **Settings - Ad Hoc Transfer - Content - Sending Files**.

For more information, see **Feature Focus - Ad Hoc Transfer Secure Note and Related Options** (on page 47).

- 7** To configure user limits and quotas for sending packages, go to **Settings - Ad Hoc Transfer - Content - Package Quotas**. You can set the following limits and quotas that determine how users can use Ad Hoc Transfer:

- **Which users can send files in a package:** By default, all users can send packages. You can set this to none, which prevents all users from adding files to a package. You can choose to use the Group setting so that whether users can send files can be determined by group.
- **Rules for files sent in a package:** By default, files with any filename are allowed. This can be set to allow only certain file types.
- **Maximum download limit for a file in a package:** By default, the limit is set to 999.
- **Which users can set their download limit:** By default, all users have the limit of 999 and cannot set their own limit.
- **Package quotas:** By default, no package quotas are applied at the organization level. Package quotas can be set on the total size of packages sent by a user within a given time period, and the total size of any one package. The package size includes the notes and any attached files.

- **Delivery notifications:** Delivery notifications are emails sent to the sender when packages are read and/or attachments are downloaded. By default, these notifications are sent immediately, when a package is first read by a recipient. Delivery notifications can be configured to be sent when a file is downloaded, and can also be consolidated and sent at regular intervals.

For detailed information about the quota and limit settings, see the topic ***Web Interface - Settings - Ad Hoc Transfer - Content*** (on page 513).

- 8** Optionally, change maintenance settings that determine the expiration of packages. By default, packages remain new for 7 days, after which they are archived to /Archive/Packages, and are not available to recipients.

For detailed information about maintenance settings, see ***Web Interface - Settings - Ad Hoc Transfer - Maintenance*** (on page 522).

Be aware that many of the Ad Hoc Transfer organization settings can also be set in user profiles and group profiles.

User Access to Ad Hoc Transfer

Registered users can send and receive packages using either of these interfaces:

- MOVEit DMZ web interface
- Microsoft Outlook
- MOVEit DMZ mobile interface (apps and web)

Sending and receiving packages using the MOVEit DMZ web interface

When Ad Hoc Transfer is enabled, users can send packages from their Home page, or by selecting **Packages** in the left navigation. In either case, under **Package Actions** the user selects **Send a new package** to display the **New Package** page, where they can enter recipient's email address, subject, note, and add files.

Sending and receiving packages in Microsoft Outlook

When the Ad Hoc Transfer Plug-in for Microsoft Outlook is installed on the user's computer, that user can send packages using Outlook by creating a new message, attaching files, and clicking the **Send Secure** button. The **Send Secure** button is added to Outlook by the plug-in. As with the web interface, the attached files will be uploaded to MOVEit DMZ. Recipients receive a notification with a link to access the MOVEit DMZ server, where they can download the files.

To send and receive packages in Microsoft Outlook, the following is required:

- Users must install the Ad Hoc Transfer Plug-in for Outlook on the PC on which Microsoft Outlook is installed. The installation program is available on the MOVEit DMZ support site.
See the Ad Hoc Transfer Plug-in for Microsoft Outlook Installation Guide, available on the MOVEit DMZ support site, for information on installing and configuring the Outlook plug-in.
- Settings for the Outlook plugin: The Outlook plug-in needs to know how to connect to the MOVEit DMZ server. These settings can be configured during installation of the plug-in and also post-installation within the **Send Secure** options in Outlook (**Tools > Options > Send Secure**).
- Ad Hoc Transfer Organization settings: These settings are configured on the MOVEit DMZ server by the organization administrator. These settings enable Ad Hoc Transfer and determine how user authentication will be handled, as well as setting limits and quotas for packages. Note that the Outlook plugin requires some specific Ad Hoc Transfer settings in order to work properly. These are described in the Ad Hoc Transfer Plug-in for Microsoft Outlook Installation Guide.

Ad Hoc Transfer Secure Note Option

An Organization administrator can configure either Secure Note transfer or Email Note transfer for an organization and whether to give senders the option to select either method per package. You can also configure related settings for the package **Subject** and **From/Reply-to** fields.

The key, core Secure Attach concept concerns the Package's Note (the message body when creating the package in the Outlook plug-in).

Note: These settings affect the full Web Interface, the Outlook Plug-in, and the Mobile Apps & Web.

See **General Information - Ad Hoc Transfer Implementations** (on page 21) for an introduction to the concepts of email notification and the Secure Note vs. Email Note options.

The related settings affect the handling of the **From** and **Subject** fields in Package Notification emails.

Note: These settings affect the full Web Interface and the Mobile Apps & Web only; they do not affect the Outlook Plug-in.

Basic Considerations

Do you want to be assured of secure transfers, not only of files, but also of every note that senders compose when creating MOVEit Ad Hoc Transfer packages?

The advantage with this method is that senders can write a confidential note (with or without attached files) and be assured that the note will be securely transferred by MOVEit only, and not by email.

If so, you might want to set up this logical combination of Secure Note settings:

- Secure Note (or Outlook message body) transferred securely by MOVEit only; not included in emailed New Package Notifications.
- No Per Package choice for senders; this enforces security by ensuring exclusive use of this Secure the Note method.

Would you rather provide your users with a consistently Outlook-style, email-oriented notification operation (with only the attached/uploaded files being sent exclusively by MOVEit)?

The big advantage with this method is that senders can write a personalized note about the files and about the fact that the files themselves were secured with MOVEit... *and recipients will be able to read this note in their email **before** they open MOVEit and the package.*

If so, you might want to set up this logical combination of Secure Note settings:

- Choose Email the Note (which equals Secure Note being OFF); the Note (or Outlook message body) is included in emailed New Package Notifications.
- No Per Package choice for senders; this enforces consistency by ensuring exclusive use of this Email the Note method. (Not offering a per package choice also reduces the chance of Senders thinking that they were using the Secure the Note method when they were not.)

Do you want to offer both flavors of operation by offering senders a per package choice?

- Choose either method as the default option:
 - Email the Note
 - Secure the Note
- Set the Per Package option to ON - This provides senders a setting in each new package page (or Outlook message window), enabling senders to turn Secure Note on or off.

Considerations for Related Options

Do want to add security for the packages' Senders and Subjects? These settings apply to the Web Interface and the Mobile interfaces only, however; they do NOT apply to the Outlook Plug-in.

The advantage with these settings is that senders - working in the MOVEit Web Interface or Mobile - can write a secure transfer note, and be assured that the email notification sent about the package will have generically filled Subject and From fields.

- Subject field is configured to use a generic subject (New Package Notification or however you customize it within Email Notification templates).

Note: Packages composed in Outlook always send an email that contains the sender's subject.

- From/Reply-to set to the Notification Service in general and not to the Sender.

Note: Packages composed in Outlook always send an email that contains the sender's email address in the From field.

Would you rather ensure consistent operation across all clients (Outlook as well as Web Interface)? If so, you would use these settings.

- Subject field is configured to always use the sender's Subject.
- From field set to the Sender.

Configuring Secure Note and Related Options

The organization settings for Ad Hoc Transfer are on the administrator's Settings page, on several different pages.

The links are both the Ad Hoc Transfer section and the Appearance section.

The overall procedure to configure Secure Note and related options:

- 1** From the Home page, click **Settings**.
- 2** Under Ad Hoc Transfer, next to **Content**, click **Sending Files** to configure the **Secure the Note** option itself. Under **Sending Packages**:
 - a) Select **Secure the Note** or **Email the Note**.
 - b) Select on or off for **Per Package Option**.

For detailed information about these settings, see ***Web Interface - Settings - Ad Hoc Transfer - Content*** (on page 513), **Sending Packages**.

- 3** Under **Appearance**, next to **Notification**, click **Items Displayed** to configure the **Comment Field**, which might determine whether the sender's **Subject** is used. (It is only applicable for packages transferred using the **Secure the Note** method. It never applies to Outlook.)

For detailed information about these settings, see ***Web Interface - Settings - Appearance - Notification - Items Displayed*** (on page 371), **Comment Field**.

- 4** Under Ad Hoc Transfer, next to **Content**, click **Package Notifications** to configure the **From/Reply-to** option (which applies to the Web Interface and Mobile only, and not Outlook).

For detailed information about these settings, see ***Web Interface - Settings - Ad Hoc Transfer - Content*** (on page 513), **Package Notifications**.

Email Notifications

To keep users informed, MOVEit DMZ can send out a number of different email notifications, alerting users about the arrival of new files or packages, informing them of impending password expirations, and so forth. Notification emails can also be sent out to administrators, informing them of user password expirations, account expirations, and account lockout events. By default, notifications go out as HTML email and use the same stylesheet as the organization that originated them, meaning organization color schemes, icons, and font information are all maintained in the emails that end users receive.

Example New File notification:

Example Email Notification Message



New File Notification

A new file from Joe User has arrived into the "/ Distribution / MyParent / MyFolder" folder.

Name: Example.bt

Tracking ID: 1234567

Original Size: 1,234 bytes

Uploaded By: Joe User (joe@user.com)

☒ For non-repudiation purposes, it has been confirmed that the file received by MOVEit DMZ is IDENTICAL to the file uploaded by Joe User.

Please use the following URL and your username/password to DOWNLOAD or view the current status of this file, including its full upload and download history.

(<https://KEaston-08R2DOC.FTQA.com/human.aspx?OrgID=9999&Arg12=fileview&Arg07=1234567&Arg06=123456&username=janeuser>)

Regards,
Org 1 Notification Service

General Settings

All outgoing email notifications are subject to a group of settings which control the different informational elements that are included in such emails. For some organizations, user awareness may be important, so the administrators may decide to include as much information as possible. For other organizations, security is a priority, which would lead administrators to restrict the plain-text sending of information. The settings that control these elements can be found by going to the **Settings** page and clicking the **Appearance | Notification | Items Displayed** link. See **Web Interface - Settings - Appearance - Notification - Items Displayed** (on page 371) for more information.

In addition to the general notification settings, each group of notifications usually has its own settings which determine how specific notifications will be sent. Some notifications have multiple send settings, while others simply determine whether a notification will be sent or not. Finally, each notification recipient can choose not to receive notifications (or be denied notifications by the administrator) by setting their Email address to a blank string in their **Web Interface - Common Navigation - My Account** (on page 109) page. Administrators may alternately wish to set the **Notifications** setting on the user's **Web Interface - Users - Profile** (on page 286) page to **Off**, which provides the same effect.

Custom Notifications

The content of email notifications is defined by a number of standard templates. Although the settings described above allow you to turn on and off specific components of the notifications, they do not let you control the actual text. The Custom Notifications feature allows you override the standard template with a customized version for all users within an organization, or for just a specific group. You can load a standard notification template, edit its content, see what it looks like, and test it before turning it on for use in production.

A web-based editing environment lets you preview your custom notification as an HTML message or a TEXT message. You can also send the sample notification to yourself as an email to see how it looks in your email browser. Once you are satisfied with your notification, a simple switch will enable it for use in your production organization, overriding the standard notification template. Or you can configure a specific user group to receive the custom notification, while other users, not in the group, continue to receive the standard template. The editing function for creating custom notifications can be found by going to the **Settings** page and clicking the **Appearance | Notification | Custom** link. See **Web Interface - Settings - Appearance - Custom Notifications** (on page 373) for more information.

File Notifications

File notifications inform file senders and recipients about file actions, such as new uploads and downloads. This group of notifications is controlled from the **Web Interface - Folders - Settings** (on page 55) page of the destination folder. The notifications (and their corresponding settings) are:

- **File Upload Confirmation - (Upload Confirmation to Sender setting)** - Sent to the uploader of a new file informing them that the file has arrived and that the appropriate users have been notified of its arrival. File Upload Confirmations can be sent either individually (immediately after a file has been uploaded), or as a delayed batch message listing all the files that were uploaded by the user within a configurable time frame.
- **New File Notification - (New File Upload to Recipient setting)** - Sent to users with Notify rights to the uploaded file's parent folder, informing them of the arrival of the new file. New File Notifications can be sent either individually (immediately after a file has arrived), or as a delayed batch message listing all the files that have arrived within a configurable time frame.
- **File Delivery Receipt - (Delivery Receipt to Sender setting)** - Sent to the uploader of a file when another user downloads that file or deletes it before downloading it. File Delivery Receipts are only sent out individually, as soon as the download or delete action has occurred.
- **File Non-Delivery Receipt - (Alert Sender if File is Not Downloaded setting)** - Sent to the uploader of a file when another user deletes it before downloading it. File Non-Delivery Receipts are only sent out individually, as soon as the delete action has occurred.

These notifications work with all folder types, including virtual folders.

Package Notifications

Package notifications inform package senders and recipients about package actions, such as new posts and views. These notifications are controlled at the organization level by the Ad Hoc Transfer **Access** (on page 496) and **Content** (on page 513) settings. If enabled, the delivery receipts can be controlled on a package-by-package basis by the sender. Notifications included in this group are:

- **New Package Notification** - Sent to recipients of packages informing them that a new package has been posted for them to view. New Package Notifications are always sent, unless the recipient's Notification setting is set to Off, or the user has no email address. Depending on the settings in **Unregistered users** (on page 496) for the current organization, this notification may also include account information for newly created Temporary Users.
- **New Temp User Package (with password)** - Sent to temp user recipients of packages informing them that a new package has been posted for them to view and includes account information for the new user, including a password.

- New Temp User Package (with password link) - Sent to temp user recipients of packages informing them that a new package has been posted for them to view and includes account information for the new user, including a link to where the user can set a password.
- New Guest Package - Sent to guest user recipients of packages informing them that a new package has been posted for them to view and includes a package password for the guest user.
- Package Password Notification - Sent to guest user recipients of packages to provide a password for the guest user to view the package. This is sent if package passwords are configured to be sent separately from the New Guest Package notification.
- Package Delivery Receipt - Sent to the sender of a package when a recipient views the package, deletes the package before viewing it, or is herself deleted before viewing the package. Package Delivery Receipts are also sent if the package is deleted before one or more recipients has viewed it. Package Delivery Receipts are only sent if the sender of the package enables the Delivery Receipt(s) setting on an individual package before sending it. See the Web Interface - Packages - Sending page for more information.
- Package Download Receipt - Sent to the sender of a package when a recipient downloads a file from the package. Package Download Receipts are sent only if the sender of the package enables the Delivery Receipt(s) setting on an individual package before sending it.
- Package Deleted By User - Sent to the sender of a package when a recipient deletes the package notification before viewing it. This notification is sent only if the sender of the package enables the Delivery Receipt(s) setting on an individual package before sending it.
- Package User Was Deleted - Sent to the sender of a package when a recipient is deleted before viewing the package.
- Package Expiration - Sent to the sender of a package when the package expires. A package expires when it meets either the package expiration number of days, or the maximum downloads specified in the individual package options (if available), or otherwise set by the administrator in the Ad Hoc Transfer - Package Quotas.
- Package Delayed Delivery Receipt - For bulk notification of package delivery events. Sent to the sender of a package to provide bulk notification of when a recipient views the package. Package Delivery Receipts are only sent if the sender of the package enables the Delivery Receipt(s) setting on an individual package before sending it.

Webpost Notifications

Webpost notifications inform posters and recipients about Webpost actions. This group of notifications is controlled from the **Web Interface - Folders - Settings** (on page 55) page of the destination folder. Notification messages included in this group are:

- New Webpost Notification - Sent to users with Notify rights to the Webpost folder, informing them of the arrival of the new post.

- Webpost Confirmation - Sent to the poster of a new Webpost informing them that the post has arrived and that the appropriate users have been notified of its arrival. The confirmation includes a "Thank You" message configured for the Webpost folder.

User / Password Notifications

User / Password notifications inform users about changes in the status of their user accounts. Notifications included in this group are:

- New User Welcome (with password) - Informs a new user that their account has been created on the system. Includes the account username, and the account password.
- New User Welcome (with password link) - Informs a new user that their account has been created on the system. Includes the account username, and a link to where the user can set a password.
- Guest Self Registration Welcome - Sent to self-registering guest users when the emailed password option is being used. The notification includes a URL link and a password. It explains that they can sign in and then send the package.
- Temp User Self Registration Welcome - Sent to self-registering temporary users who self-register using the reCAPTCHA option. It confirms creation of their new temporary user account.
- Temp Self Registration Welcome (with password) - Sent to self-registering temporary users when an emailed password is being used. The notification includes the account username, a password, and a URL link. It explains that a new account has been created and that they can use the link to sign in.
- Temp Self Registration Welcome (with password link) - Sent to self-registering temporary users when an emailed password request link is being used. The notification includes the account username and a URL link. It explains that a new account has been created and that they can use the link to begin using the account.
- New Password Notification (with password) - Sends the password of a new or existing user to that user. These messages are only available if the proper Permissions are set in an organization's **Password Policy** (on page 415).
- Password Change Request Confirmation - Sent to a user who requests a password change from the signon screen (this feature must be turned on for the organization.) The link on the email must be used to complete the password change process. These messages are only available if the proper Permissions are set in an organization's **Password Policy** (on page 415).
- Password Change Request Error - Sent to a user who requests a password change from the signon screen when he has been configured to not allow password change. These messages are only available if the proper Permissions are set in an organization's **Password Policy** (on page 415).
- New User Password Request Confirmation Sent to a new user who received a password link notification and sets a password successfully. These messages are only available if the proper Permissions are set in an organization's **Password Policy** (on page 415).

- New User Password Request Error Sent to a new user who received a password link notification and sets a password that does not meet the password rules. . These messages are only available if the proper Permissions are set in an organization's **Password Policy** (on page 415).
- Password Expiration Warning - Sent to a user informing them that their password expiration time is approaching. Users still have time to log on and change their password before their account is locked out. This group of warnings is controlled from the **Web Interface - Settings - Security Policies - Password** (on page 415) page.
- Password Expiration - Sent to a user informing them that their password expiration time has run out. Users are directed to their administrator for reinstatement.
- User Account Expiration Warning - Account expiration warnings inform users that their account is either about to expire, or has expired already. This group of notifications is controlled from the **Web Interface - Settings - Security Policies - User Authentication** (on page 419) page.
- User Account Expiration - Sent to a user informing them that their account has expired and is no longer accessible.

Administrator Notifications

Administrator alerts inform interested administrators of various important user events in an organization. These notifications are always sent, but only to administrators who have their Notification setting set to On + Admin. Notifications included in this group are:

- Admin User Expired Notice - Informs administrators that one or more user accounts have either expired, or are about to expire. User Expired Notices contain a list of users and their account status (either Expired or Warned and the reason for expiration).
- Admin User Locked Out Notice - Informs administrators that a user has been locked out of the system due to a signon violation.
- Admin User Password Notice - Informs administrators that one or more user passwords have either expired, or are about to expire. User Password Notices contain a list of users and their password status (either Suspended or Warned).
- Admin IP Locked Out Notice - Informs administrators that an IP address has been locked out of the system due to a signon violation.
- Admin User Counts Notice - Sent to Admins when the number of users is approaching the licensed or configured maximums.

Summary File Notifications

These templates are for bulk notification of file events. The first three are used for TEXT format notification and the last three for HTML format. While the TEXT versions list each folder and the newly uploaded files in each folder as a block of text information, the HTML notifications use an HTML table format for the list.

- File Upload List Notification TEXT - This notification is sent to users with Notify rights to the uploaded file's parent folder, informing them of the arrival of new files. It is a delayed batch message listing all the files that have arrived within a configurable time frame.
- File Upload List Confirmation TEXT - This is the corresponding batch notification listing all files uploaded by a user within a configurable time frame.
- File Not Downloaded List TEXT - This batch notification list files for which a configurable time frame has expired without anyone downloading the files.
- File Upload List Notification HTML - This notification lists all the files that have arrived for an interested user within the time frame.
- File Upload List Confirmation HTML - This HTML message is the corresponding batch notification confirming all files uploaded by a user within a configurable time frame.
- File Not Downloaded List HTML - This HTML batch notification is returned to a user who uploaded files for which a configurable time frame has expired without anyone downloading them.

International Languages

(a.k.a. Localization or Internationalization or Translation)

The Web, FTP and SSH Interfaces of MOVEit DMZ (for end users) can be displayed in non-English languages. French, Spanish, and German are the non-English languages supported.

Note: In the interface, the name of each language is referred to in its own language, as: English, Français, Deutsch, and Español.

Administrators can set the organization's default language to one of the non-English languages.

In addition, end users can normally pick for themselves which language they wish to use. Their choice is recorded on their user profile and is also written to a cookie in their browser.

However, administrators can also configure their organization and users to prevent end users from selecting languages.

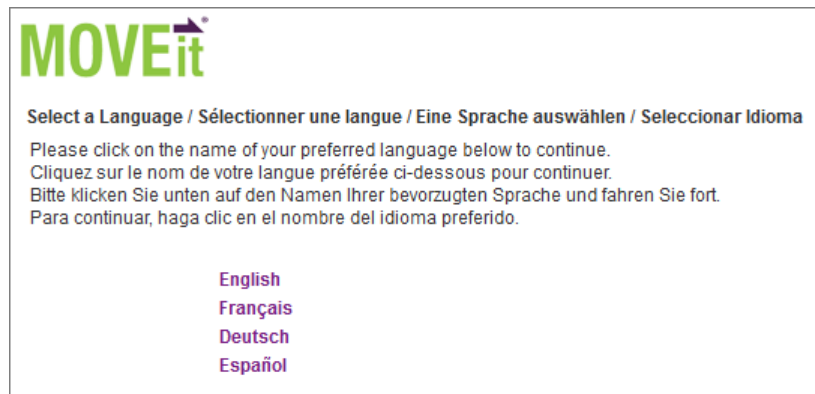
Places Users Might Select Their Own Language

Each end user can be given several opportunities to select a language, even before signing on. User selection of language can occur at any or all of these three points when using the MOVEit desktop web interface:

- On the Pre-Signon Language Select page
- On the Sign On page
- After sign on, first with the Change Language... page, and anytime after that from the My Account page.

Pre-Signon Language Select Page

In the style of many Canadian bilingual sites, MOVEit DMZ has an option which presents a dedicated screen that asks a user to pick a language before being presented with MOVEit DMZ's sign on page. The instructions are repeated in every language.

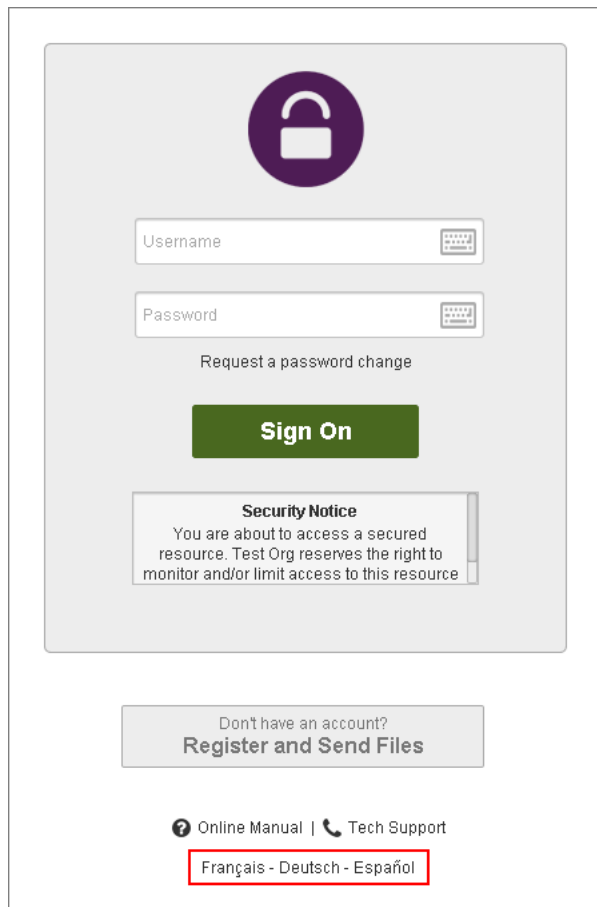


This page is enabled by default. When it is enabled, the end user's choice from this page will be remembered in a cookie in her browser, and this page will be suppressed as long as this cookie is available.

Note: Administrators can disable this page for their organization by going to **Web Interface - Settings - Appearance - International** (on page 414) - Interface. Turn off the Pre-Signon Language Select Page.

Sign On Page Language Selection Links

Also in the style of many Canadian bilingual sites, MOVEit DMZ can display links on the Sign on page to allow users to select a language before signing on. All available languages are displayed. (The actual link for the current language is inactive so users don't mistakenly think they need to click the current language before signing on.)



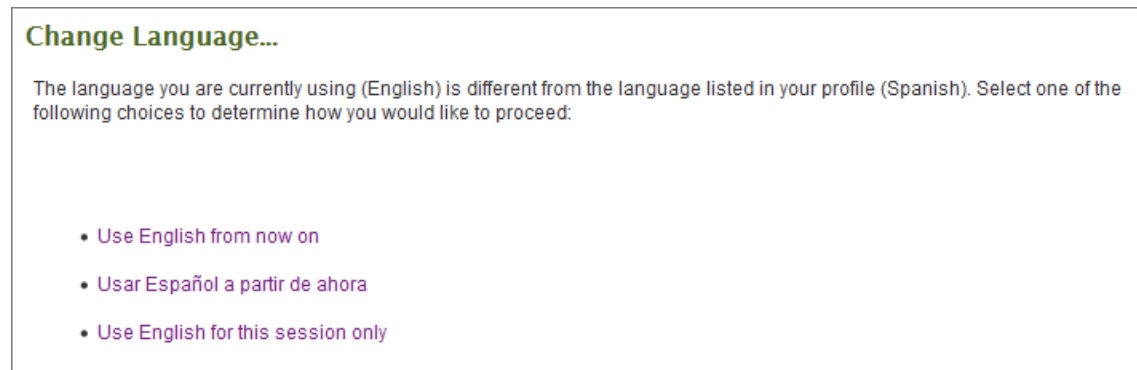
The screenshot displays the Sign On page of the MOVEit DMZ interface. At the top, there is a purple circular icon with a white padlock. Below this, there are two input fields: 'Username' and 'Password', each with a small icon to its right. Under the password field is a link that says 'Request a password change'. A large green button labeled 'Sign On' is positioned below these fields. A 'Security Notice' box follows, containing the text: 'You are about to access a secured resource. Test Org reserves the right to monitor and/or limit access to this resource'. Below the notice is a button that says 'Don't have an account? Register and Send Files'. At the bottom, there are links for 'Online Manual' and 'Tech Support', and a language selection bar with the text 'Français - Deutsch - Español' highlighted by a red rectangle.

The language links on the **Sign on** page are enabled by default.

Note: Administrators can hide the language links for their page for users in their organization by going to **Web Interface - Settings - Appearance - Display - *Display Profiles*** (on page 67), editing the **Guest/Anonymous User Profile**, and turning off **Account Options | Display language selection**.

Post-Signon Language Reconciliation "Change Language..." Page

If, in either the **Pre-Signon** page or the **Sign On** page, a user selects a language (*e.g.*, English) that is different from the one currently listed in her user profile (*e.g.*, Français), a Post-Signon Language Reconciliation **Change Language...** page may be presented to help MOVEit DMZ figure out which language to really use.



The page has three links:

- Use the current language - from the **Pre-Signon** page or the **Sign On** page - from now on (*e.g.*, English).
- Use the language from your user profile (*e.g.*, Français).
- Use the current language (*e.g.*, English) for this session only.

The **Change Language...** page is not shown if any of the following is the case:

- The language choice from the **Pre-Signon** page or **Sign On** page agrees with the user profile.
- The end user is following a link from an email notification.
- The current user's display profile (**User Profile** or **Temporary User Profile**) has the **Account Options | Display language selection** turned off.

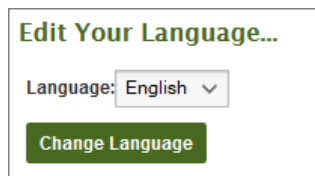
This page is similar to the page that prompts end users to download and install the MOVEit Wizard in that both pages are suppressed if an end user is following a link from a notification. In both cases, the purpose is to avoid making users click through numerous screens just to view a single file or package.

The Change Language... page is enabled by default.

Note: Administrators can hide the Change Language... page for end users in their organization by going to Web Interface - Settings - Appearance - Display - **Display Profiles** (on page 67), editing the User Profile, and turning off Account Options | Display language selection. Do the same for the Temporary User Profile.

My Account Language Selection Option

After signing on, end users can change their language selection on their My Account page.



This section of the My Account page is hidden if the current user's display profile has the Account Options | Display language selection turned off.

This section of the My Account page is enabled by default.

Administrator Configuration Options

Default Organization Language

Each organization administrator can select a default language from the complete list of available languages. The default language controls the language in which the Sign on page is displayed when there is no input from language cookies and the Pre-Signon language select page is not available. The org-level default language also controls which language end users are set up under by default.

➤ *To set the default language for the organization:*

1. Go to **Web Interface - Settings - Appearance - International** (on page 414) - Languages.
2. For Default language, select English, Français, Deutsch, or Español.
3. Click Save.

There is no single organization-wide restriction of available languages. If administrators want to enforce the use of the organization's default language, they must completely prohibit end users from changing language (doing this separately for the **Pre-Signon** page, the **Sign On** page, and for after sign on).

Permissions for End User Language Selection

User selection of language can occur at the **Pre-Signon** page, the **Sign On** page, and after sign on.

You configure these three points separately, and you can configure them in whatever combination suits your organization.

For the **Pre-Signon** page and the **Sign On** page, you configure each once for the organization. While all users see the **Pre-Signon** page and the **Sign On** page language links, any language selections made on those pages will only be effective for end users, not administrator users.

➤ *To disable (or enable) the Pre-Signon language select page:*

1. Go to **Web Interface - Settings - Appearance - International** (on page 414) - Interface.
2. Turn off (or on) the Pre-Signon Language Select Page.

➤ *To disable (or enable) the Sign On page selection links:*

1. Go to **Web Interface - Settings - Appearance - Display - Display Profiles** (on page 67) page.
2. In the **Edit User Class Display Profiles...** section, look for the **Guest/Anonymous User Profile class** and identify the selected display profile.
3. In the **Display Profiles** section, find that specific profile, and click its corresponding **Edit** link.
4. In **Edit Display Profile...**, go to the **Account Options** group, and turn off (or on) **Display language selection**.
5. Click **Save**.

Note: As **Guest/Anonymous User** covers both **Guest Users** and other users who have yet to sign on, all three classes of end users are essentially being configured for the **Sign on** page: **Users** (including group admins), **Temporary Users**, and **Guest Users**.

➤ *To disable (or enable) the Post-Sign on Change Language... page and the My Account page's Language selection:*

1. Go to **Web Interface - Settings - Appearance - Display - Display Profiles** (on page 67) page.
2. In the **Edit User Class Display Profiles...** section, look for the **class** that you want to disable - either **User Profile** or **Temporary User Profile** - and identify the selected display profile.
3. In the **Display Profiles** section, find the specific profile, and click its corresponding **Edit** link.
4. In **Edit Display Profile...**, go to the **Account Options** group, and turn off (or on) the **Display language selection**.

5. Click **Save**.
6. Optionally repeat steps 2-5 for the remaining end-user profile class (for example, **Temporary User Profile**).
7. You can select a different setting for the **Temporary User Profile** than you did for **User Profile**.

Note: Unlike the **Pre-Signon** and **Sign On** permissions, the "after sign on" permissions can be configured differently for the two applicable user classes within the organization. You can configure them one way for **Users** (for example, enable language selection) and the other way for **Temporary Users** (for example, disable language selection).

Coverage

Unlike end users, the administrator class of users - SysAdmins, Admins, and FileAdmins - will only see an English-only interface. (However, administrators arriving at the **Sign on** page may still be prompted for a choice of languages, especially if signing on from public terminals.)

Although international language support has been extended throughout the MOVEit DMZ product, not all administrative strings have been converted. The administrative interface, specifically administrative templates and the MOVEit DMZ Config and Check utilities, remains largely untranslated.

Some items which have been fully internationalized:

- Folders and Files
- Packages
- New File, New Message and other email Notifications
- Users (*i.e.*, GroupAdmin components)
- End User Documentation

Some items which have NOT been fully internationalized:

- Schemes
- Organization Settings
- Administrator Documentation

Sign On Banner and Other Custom Fields

Most MOVEit DMZ settings which support a text phrase can be properly internationalized. To delimit the phrases used for different languages, administrators use an intra-string [Language:XX] tag which indicates which message is for which language, where XX is fr, es, en or any other language code (ISO 639-1) which corresponds to a language MOVEit DMZ supports.

For example, consider the Custom Help Link Name. Today our link name is currently configured to be Ipswitch Home Page. If we wanted to display a Spanish version, we would enter a value like Ipswitch Home Page[Language:es]Ipswitch Casa Pagina into the Custom Help Link Name field and let the MOVEit DMZ code figure out which message (Ipswitch Home Page or Ipswitch Casa Pagina) to actually use based on the current user's language preference.

International-Ready MOVEit DMZ Settings

The following list briefly covers fields in MOVEit DMZ which are International-Ready because they support the [Language:XX] tags described above. Fields which begin with a name in parentheses are duplicates of another field mentioned elsewhere in this list.

Sign On Page:

- Sign On Banner
- Sign On Notice
- (Custom Help) Name and Link

Home Page:

- Welcome Banner
- Announcement
- (Custom Help) Name and Link

Technical Support Page:

- General Information
- Name of Primary Contact
- Phone Number
- Email Address
- Information Link
- Information Link Name
- Contact Link
- Contact Link Name

Custom Help:

- Custom Help Name
- Custom Help Link

Notification:

- Notification Message Signature
- (Technical Support) Name of Primary Contact
- (Technical Support) Phone Number
- (Technical Support) Email Address

WebPost:

- WebPost Response
- WebPost Redirect URL

FTP Server:

- (Sign On Page) Sign On Banner
- (Sign On Page) Sign On Notice

- (Home Page) Welcome Banner
- (Home Page) Announcement

Email Notifications

All of the email notifications that are sent to end users, and most of the ones that go to administrators have been internationalized. The Custom Notification feature allows administrators the ability to edit the content of email notifications to override standard templates. When international language support is enabled, this feature also allows you to create and edit email notifications for each supported language.

Display Profiles

Display Profiles allow administrators to fine tune the look and feel of the web interface for their organization on a MOVEit DMZ server. A display profile consists of a name and a set of options which can either be enabled or disabled. Administrators may then assign a display profile to a class of user, the classes being Ad Hoc Transfer Only, Guest/Anonymous User, Power User, Temporary User and User, or to individual groups, in which case the group members would be assigned the display profile. When a user with an assigned display profile signs on to the web interface of MOVEit DMZ, they will see the items specified by that display profile.

Note: The **Guest/Anonymous** profile controls what is shown on the **Sign on** page to unauthenticated users. Those display profile options that do not affect the **Sign on** page are ignored.

Display Profiles Setting Page

The **Display Profiles** setting page consists of two parts. The first part, titled **Edit User Class Display Profiles**, allows the administrator to assign various display profiles to each of the four available user classes. By default, the class name profile is selected for each user class. Existing display profiles can be selected for each user class in that class' dropdown menu. Clicking **Update Profiles** will make the display profile assignment changes.

Edit User Class Display Profiles...

User Class Display Profiles determine what a standard user in each given user class may see through the MOVEit DMZ web interface. Select a profile for each user class and then click the "Update Profiles" button. Profiles may be viewed and edited by clicking the "Edit Profiles" link.

Administrator Profile: Power User 

User Profile: User 

Temporary User Profile: Temp User 

Guest/Anonymous User Profile: Guest/Anonymous User 

Update Profiles

Display Profiles

Profile Name

Ad Hoc Transfer Only



Guest/Anonymous User



Power User



Temp User



User



Add Display Profile

The second part, titled **Display Profiles**, lists the display profiles available in the organization. Each profile may be edited or deleted, and new profiles may be added. The settings in the **Default Profile** can be seen on the **Add New Profile** page. The page starts out with the default profile options selected. The default profile options cannot be changed.

Note: If a display profile that is currently assigned to one or more user classes is deleted, those user classes will be reset to use the **Default Profile**.

Display Profile Options

Each display profile must have a name. This is the name that is listed in both sections of the **Display Profiles** setting page. A name for a new display profile should be selected to convey the allowances and restrictions of the given profile. Names such as **Messaging Only Profile**, or **Advanced Views By Default** are good choices. Names such as **Profile 1**, or **User Profile** are less desirable. The profile name can be changed after creation without affecting the users assigned to that profile.

Add Display Profile...

Name:

There are six sections of options available in a display profile.

Home Page Options

These options control what items the user sees on their **Home Page**. This is normally the first page a user sees when they sign on to the DMZ system.

- **Display the default folder:** When enabled, the user will see a list of all subfolders and files in their default folder in place of a list of all new files (the default folder is usually the user's home folder). When disabled, the user will see a list of new files available in all folders.
Disabled in Default Profile.
- **Display the package inbox:** When enabled, the user will see the **Inbox**, which displays a list of packages that the user has received, and the **Package Actions** section. New files, or the default (home) folder will not be displayed.
Disabled in Default Profile.
- **Display the Home page with the following options:** When enabled, displays the sections as set in the following options:
 - **Display Browse Folders/New Files and Upload File(s) Now sections:** When enabled, displays the **Browse Folder/New Files** section, which lists the users' folders and any new files that have been uploaded to those folders; and also displays the **Upload File(s) Now** section, from which a user can start a file upload.
Enabled in Default Profile.
 - **Within the "Browse Folders/New Files" section, display the contents of the default folder instead of new files:** When enabled, users can directly view files available to them, as well as start a file upload.
 - **Display Packages Sections:** When enabled, displays the **Packages** section, which lists any new packages the user has received, and displays the **Packages Action** section from which the user can send a new package and manage their address book.
Enabled in Default Profile.

- Within the Packages Sections, display the contents of the packages inbox instead of new packages: When enabled, users can directly view packages available to them, as well as begin composing new packages. When disabled, these sections will not appear.
Disabled in Default Profile.

Account Options

These options deal with the links users are allowed to see regarding the changing of their account options, which include email address and account password.

- Display "My Account" Link: When enabled, a user will see a My Account link on the right-hand side of their user bar, next to the Sign Out link. Clicking this link will open the My Account page, allowing the user to change various account parameters. If disabled, the My Account link will not appear.
Enabled in Default Profile.
- Display Notification Settings: When enabled, the Account Options page will contain a section allowing the user to edit the email address for their account. If disabled, this section will not appear. If the Display My Account Link option is disabled, this option has no effect.
Enabled in Default Profile.
- Display Language Selection: When enabled for the selected Guest/Anonymous User class profile, all users are provided with links on the Sign On page for changing their language. *This fully affects all end users, not just Guest users.* (For Administrator class users, the links have no effect beyond the Sign On page.) When disabled for the Guest/Anonymous User class profile, the Sign On page links will not be provided.

Enabled in the default Guest/Anonymous User Profile.

When enabled for all other user class profiles, those users will be provided the selection option in the My Account page, and they will be offered the Change Language... page if, after they sign on, they are using a language that is different from their profile. When disabled for other user profiles, neither the My Account page selection option nor the Change Language... page will be displayed for applicable users.

Enabled in Default Profile.

Global Navigation

These options control the links and sections a user sees in the left-hand navigation section of the web interface.

- **Display Global Navigation:** When disabled, the entire left-hand navigation section will not appear to the user. In this case, no other options in this section will have any effect.
Enabled in Default Profile.
- **Display "Packages" Link:** When enabled, a Packages link will appear if the Ad Hoc Transfer feature is licensed and enable for the organization. When disabled, the link will not appear even if Ad Hoc Transfer is enabled.
Enabled in Default Profile.
- **Display "Folders" Link:** When enabled, a Folders link will appear which leads to the root folder list page. The Find Files and Go To Folders sections will also appear, allowing the user to search for a file on the system, and to head directly to a selected folder. When disabled, the link and the Find Files and Go To Folders sections will not appear.
Enabled in Default Profile.
- **Display "Logs" Link:** When enabled, a Logs link will appear which leads to the audit log view page. When disabled, the link will not appear.
Enabled in Default Profile.
- **Display "Find" Section:** When enabled, a section containing Find File/Folder, Find User, and Go To Folder options will be displayed (one or more of these options may not appear depending on user and folder permissions).
Enabled in Default Profile.
- **Display "Need Help?" Section:** When enabled, the Need Help section will be displayed, including the Online Manual link, the Tech Support link, and, if configured, the custom help link. When disabled, this section will not appear, and the next option will have no effect.
Enabled in Default Profile.
- **Display "Online Manual" Link:** When enabled, an Online Manual link will be included in the Need Help section. This link opens a copy of the online manual in a separate window (javascript is required for this operation). When disabled, the link will not appear.
Enabled in Default Profile.

File List Options

These options control what is shown in the various file lists available to the user, as well as which file lists are shown by default.

- **Display "ID" Column:** When enabled, the basic folders and files list page will include a column indicating the ID of each folder and file. When disabled, the column will not appear. This option has no effect when viewing a file list page in a webpost folder, since webposts are only known by their IDs.
Disabled in Default Profile.
- **Display "Created" Column:** When enabled, the basic folders and files list page will include a column indicating the date and time each folder was created and each file was uploaded. When disabled, the column will not appear.
Enabled in Default Profile.
- **Display "Creator" Column:** When enabled, the basic folders and files list page will include a column indicating the name of the user who created each folder and who uploaded each file. When disabled, the column will not appear.
Enabled in Default Profile.
- **Display "Size/Contents" Column:** When enabled, the basic folders and files list page will include a column indicating the number of subfolders and files in each folder, and the size of each file. When disabled, the column will not appear.
Disabled in Default Profile.
- **Display "Action" Column:** When enabled, the folders and files list page will include a column providing links to execute various actions on each folder and file. The links available are dependent on the rights the user has to the given folder and include **Delete** and **Download**.
Enabled in Default Profile.
- **File name is download link:** When enabled, the hyperlinked filename (or ID, if the folder is a webpost folder) will download the given file when clicked. When disabled, the link will take the user to the fileview page for that file.
Disabled in Default Profile.
- **Display folder navigation links:** When enabled, the folder path listed at the top of each folders and files list page, as well as folder view and file view pages, will be hyperlinked, allowing the user to navigate to the parent folders of the current folder. **Parent Folder** links are also shown allowing the user to ascend one level in the directory tree. When disabled, these links will not appear.
Enabled in Default Profile.
- **Display comments under each file entry:** When enabled, any comments uploaded with a file will be shown on the folders and files list page, below the file entry.
Disabled in Default Profile.
- **Display checkboxes for each folder/file entry plus "Download" and "Delete" buttons (when permissions allow):** When enabled, a checkbox is displayed next to each folder and file entry (on the folders and files list page). The **Download** and **Delete** buttons are also displayed below the list. You can also select to display the **Copy** and **Move** buttons.
Disabled in Default Profile.

Package List Options

These options control what is shown in the various package lists available to the user, as well as which package lists are shown by default. When the Ad Hoc Transfer feature is disabled, these options have no effect.

- **Display Trash:** When enabled, displays the **Trash** button in the **Actions** column, and below the package list. When disabled, the **Trash** button will not appear.
Enabled in Default Profile.
- **Display Drafts and Templates:** When enabled, displays the **Save as Draft** and **Save as Template** buttons on the **New Package** page. When disabled, these buttons will not appear .
Enabled in Default Profile.
- **Display custom folders:** When enabled, displays custom mailboxes in the **Mailboxes** list and displays the **Add mailbox** link. When disabled, hides custom mailboxes and does not display the **Add mailbox** link.
- **Display "Actions" column:**When enabled, the packages list page will include a column providing links to execute various actions on each package. The links available are dependent on the rights the user has to the given mailbox and include **Delete** and **Download**.
Enabled in Default Profile.
- **File name is download link:** When enabled, the hyperlinked filename will download the given file when clicked. When disabled, the link will take the user to the fileview page for that file.
Disabled in Default Profile.
- **Display checkboxes for each package entry plus "Trash" or "Delete" button (when permissions allow):**When enabled, a checkbox is displayed next to each package entry (on the packages list page). The **Trash** or **Delete** buttons are also displayed below the list.
Enabled in Default Profile.
- **Display "Move", "Mark as New", and "Mark as Read" buttons (when permissions allow):**When enabled, displays these buttons at the bottom of the packages list. When disabled, does not display them. The buttons available are dependent on the rights the user has to the given mailbox.
Enabled in Default Profile.

Package Composition Options

These options control what is shown in the **New Package** page, where a user can compose and send a package. When the Ad Hoc Transfer feature is disabled, these options have no effect.

- **Display "Preview" button:** When enabled, displays the **Preview** button which allows a user to see how the package being composed will appear to a recipient. When disabled, does not display the button.
Enabled in Default Profile.
- **Display rich text editor:** When enabled, displays the rich text editor, if the browser supports it. When disabled, displays the text-only editor.
Enabled in Default Profile.

- **Display file attachments above note:** When enabled, displays the **Files** section (on the **New package** page) immediately after the subject, and above the **Note**. When disabled, the **Note** field is displayed above the **Files** section.
Disabled in Default Profile.
- **Require note:** When enabled, the **Note** on the **New Package** page is a required field, and the package cannot be sent without it. When disabled, the **Note** is not required.
Enabled in Default Profile.
- **Require file attachments:** When enabled, a new package must have at least one attached file. When disabled, an attached file is not required.
Disabled in Default Profile.

User Account Expiration

Expiration Policies allow administrators to precisely define if, how, and when a user account will be considered expired and deleted from the system. Expiration policies can be applied globally to all members of a user class, or they can be applied to individual users, providing a high degree of control and flexibility in the expiration of old or unwanted accounts.

Expiration Policies Setting Page

Edit User Class Expiration Policies...

The User Class Expiration Policies control the default expiration policies applied to each user class when users are added. Also, changing a user class expiration policy will provide the option to apply the new policy to all users of that class.

Admin Expiration Policy:	- None -	Change Policy
FileAdmin Expiration Policy:	- None -	Change Policy
User Expiration Policy:	- None -	Change Policy
TempUser Expiration Policy:	Default TempUser Expiration Policy	Change Policy

Expiration Policies

Policy Name

Default TempUser Expiration Policy



test



Expiration Settings

Expired users will be deleted based on the following setting. A value of "0" indicates that expired users should never be deleted.

NOTE: This value is limited by the current [Log Retention Period](#), which is 30.

Delete users day(s) after expiration

The **Expiration Policies** setting page consists of three parts. The first part, titled **Edit User Class Expiration Policies**, allows the administrator to assign various expiration policies to each of the four available user classes. By default, no policy is selected for each user class (indicated by the - **None** - entry in the drop-down menu). Existing expiration policies can be selected for each user class in that class' drop-down menu. Clicking the **Change Policy** button for a specific user class will make the expiration policy assignment change for that user class.

If an expiration policy is assigned (or unassigned) to a user class, a confirmation page will appear asking the administrator if they wish to apply the new policy to all existing members of that user class, or leave existing policies in place and simply make the change for all future members of that user class. The administrator may also cancel the operation entirely from the confirmation page.

The second part of the expiration policy settings page, titled **Expiration Policies**, lists the expiration policies available in the organization. Each policy may be edited, and those policies which are not currently selected as a default user class policy may be deleted. New profiles may also be added. Clicking the **Edit** link opens the **Edit Expiration Policy** page; clicking the **Add New Policy** link opens the **Add Expiration Policy** page.

Note: If an expiration policy that is currently assigned to one or more user accounts is deleted, those users will be reset to use the default policy for their user class (or no policy if - **None** - is selected).

The third section, titled **Expiration Settings**, is a setting for deletion of expired accounts. The setting lets you set whether and when, an expired account should be deleted. The default value is that, 7 days after a user account is marked as **Inactive**, the account will be deleted. You can change the time period, or you can enter 0 to never delete the inactive user accounts.

Note: If an expired user account is deleted, the user's home folder will be retained to avoid any data loss. You can manually delete the home folder or set folder expiration rules to remove home folders associated with an expired account.

Edit Expiration Policy or Add Expiration Policy

Each expiration policy must have a name, and can optionally have a description. The policy name is listed in both sections of the expiration policy settings page. A name for a new expiration policy should be chosen to convey the expiration settings of the given policy. Names such as **Expire After One Signon**, or **Expire Thirty Days After Creation** are good choices. Names such as **Policy 1**, or **User Policy** are less desirable. The policy name can be changed after creation without affecting the users assigned to that profile.

Edit Expiration Policy...

The name of the policy will be shown in places where the policy needs to be selected from a list of possible policies.

Name:

Description:

Policy Options:

☐ Expire after

☐ Expire day(s) after creation

☒ Expire day(s) after last activity

☐ Receiving packages counts as "activity"

☐ Expire after successful signon(s)

☐ Warn day(s) before expiration

☒ Notify user when their account expires

~ OR ~ [Return](#) to the policy list.

The options available to each expiration policy determine how users who are assigned this policy will be expired from the system, and how, if at all, they will be notified of impending expiration or the expiration itself. Several different expiration options may be selected in a single policy, and in those cases, accounts assigned the policy will be expired by the first applicable method.

Here is a list of the available expiration policy options, and descriptions of each:

- **Expire after (specific date):** Causes a user account to be expired after the selected date.
- **Expire X days after creation:** Causes a user account to be expired a configurable number of days after the creation date of the account.
- **Expire X days after last activity:** Causes a user account to be expired a configurable number of days after the last successful signon to the account occurred.
 - **Receiving packages counts as "activity":** Causes a user account to be expired a configurable number of days after the last package was sent to the account.

- **Expire after X successful signons:** Causes a user account to be expired after a configurable number of successful signons to the account.
- **Warn X days before expiration:** Sends an email notification to a user account a configurable number of days before the account is due to be expired.
- **Notify user when their account expires:** Sends an email notification to the user account upon expiration of that account, notifying them of the expiration.

Expiration Results

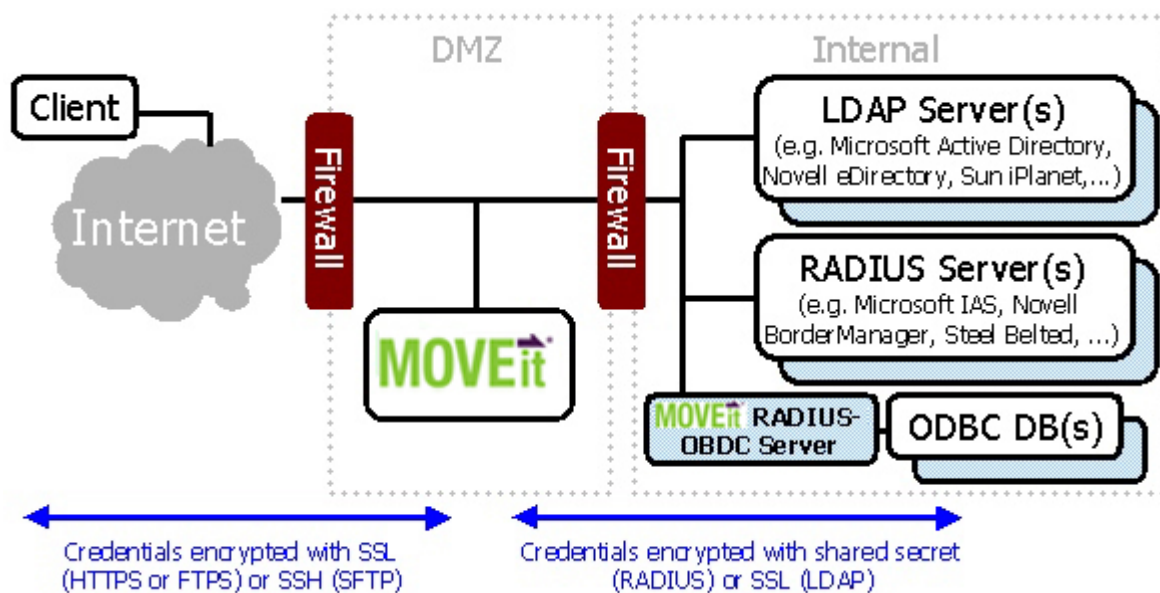
Actual expiration of a user account happens in two steps. First, upon determining that an account is expired, MOVEit DMZ's nightly scheduled task will change the account status to **Inactive (account expired)**, preventing the user from signing on. If the expiration policy allows it, a notification email will be sent to the expired user informing them of their status. Notifications will also be sent to interested administrators and GroupAdmins informing them of the account expiration.

For the next seven days (or for the number of days set in **Expiration Settings**) following expiration of the account, administrators will have an opportunity to undo the expiration by changing the user's status back to **Active**. This seven day window is provided to help prevent inadvertent and unwanted expirations. Administrators can also set the **Expiration Setting** to 0, and the inactive accounts will not be deleted.

The second expiration step happens seven days after expiration, when the user account is finally deleted. Once this has happened, it is no longer possible to recover the account, although the user's home folder is retained.

User Authentication

MOVEit DMZ provides the ability to authenticate users to external LDAP and/or RADIUS servers. Microsoft Active Directory (AD) operates as an LDAP server, so MOVEit DMZ can authenticate to it natively. MOVEit DMZ can also authenticate users against ODBC-compliant databases through the use of the optional RADIUS-ODBC authentication service. Both of these transports can be secured at the transport level (we encourage the use of LDAP over SSL) and related credentials are stored encrypted on MOVEit DMZ.



In addition to authenticating existing users against external sources, MOVEit DMZ has the ability to create new users, often as a clone of an existing template user. MOVEit DMZ also has the ability to split an organization's user base into External Users and Internal Users with one group using an external authentication source and the other using MOVEit DMZ's built-in user database. When accessing an LDAP server, MOVEit DMZ has the ability to replicate group membership information and information such as email address from that LDAP server as well.

Single Signon

In enterprise environments, an externally authenticated MOVEit DMZ site can participate in Single Signon (SSO) arrangements in two different ways:

- **CA SiteMinder** - MOVEit DMZ can accept preauthenticated credentials from CA SiteMinder. More information about this feature is available in the *Advanced Topics - Service Integration - SiteMinder Integration* (on page 733) documentation.
- **Common Access Card (CAC)** - MOVEit DMZ can authenticate users using hardware client certificates in CAC Smart Card environments. More information about this feature is available in the *Advanced Topics - Service Integration - CAC Integration* (on page 708) documentation.

Note: MOVEit now supports single signon using a SAML compliant federated identity provider as the authentication source. This feature can be used along with the existing user authentication sources. For more information, see *Feature Focus - Single Signon* (on page 87).

Authentication Sources

An Authentication Source is any RADIUS, LDAP, or WS-Trust server the MOVEit DMZ queries. Multiple Authentication Sources may be configured within any particular organization, and each may be of a different type (e.g., 2 RADIUS sources and 3 LDAP sources) and each may reference a different template user so users already belong to the appropriate groups when they are automatically added.

The following Authentication Source types are currently supported:

- **RADIUS (Authentication Only)** (on page 448): Incoming usernames and passwords will be tried against a remote RADIUS server. If authentication is successful, a new user may be created on the fly as a clone of an existing template user.
- **LDAP (Authentication Only)** (on page 451): Incoming usernames and passwords will be tried against a remote LDAP server. If authentication is successful, a new user may be created on the fly as a clone of an existing template user.

- **LDAP (Lookup and Authentication)** (on page 454): Incoming usernames and passwords will be tried against a remote LDAP server. If authentication is successful, a new user may be created on the fly as a clone of an existing template user. However, user attributes such as email address and group memberships will be carried over from the LDAP server. (This is currently the most popular option.)
- **WS-Trust (Authentication Only)** (on page 466): Incoming usernames and passwords will be tried against a remote WS-Trust server. If authentication is successful, a new user may be created on the fly as a clone of an existing user template.

Complete documentation and examples for Active Directory, Novell eDirectory, IBM Domino and iPlanet LDAP servers are provided. Other LDAP servers (such as IBM Tivoli Access Manager - SecureWay) are also supported through the use of flexible connection and attribute templates. (RADIUS server configuration is relatively generic compared to LDAP server configuration.)

More Information

Connecting to external authentication resources often requires some additional firewall rules. The various rules associated with LDAP and RADIUS services are covered in **MOVEit DMZ Firewall Configuration** (on page 128).

The settings which control how MOVEit DMZ accesses external authentication sources and how new user records are configured for external authentication users are covered in **Authentication Method section of the Settings - Security - User Policy** (on page 419).

The settings which control how individual users access external authentication sources are covered in **Authentication Method section of the Users - Profile** (on page 286).

Information about configuring individual authentication sources can be found in the **Web Interface - Settings - Security Policies - External Authentication** (on page 444) documentation.

Complete information about the optional RADIUS-ODBC authentication service can be found in **Advanced Topics - RADIUS-ODBC Authentication** (on page 724). More information about SiteMinder SSO integration is available in **Advanced Topics - SiteMinder Integration** (on page 733).

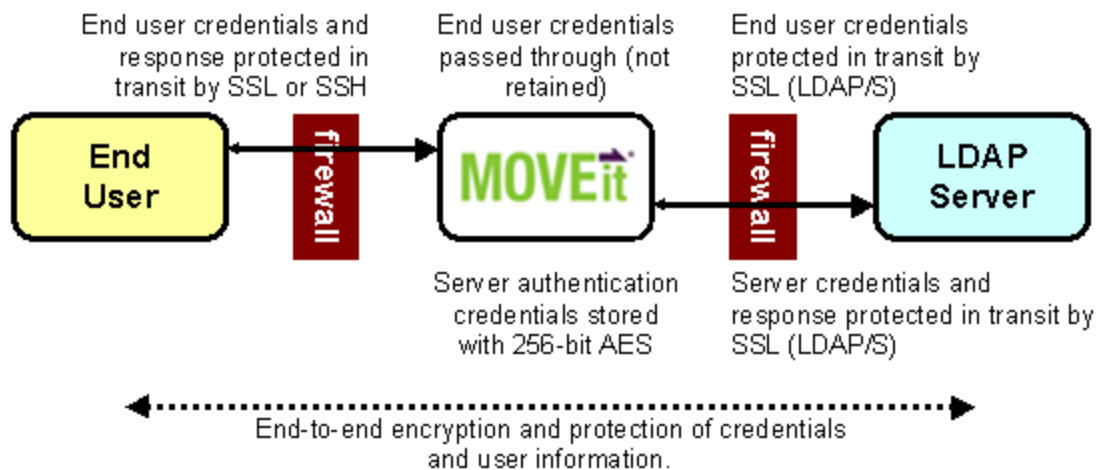
Securely Accessing Internal LDAP Servers (e.g., Active Directory)

There are two ways MOVEit DMZ can securely connect to internal LDAP sources from a DMZ segment. Both offer strong encryption of user credentials and information in transit, and neither requires anonymous access.

Direct, Authenticated SSL Connection to Internal LDAP Server

This scenario is quite common. First, an end user presents his or her credentials to MOVEit DMZ over an encrypted SSH (FTP/SSH) or SSL (FTP/SSL or HTTP/S) link. MOVEit DMZ turns around and passes those credentials to the LDAP server over an encrypted SSL (LDAP/SSL) link to figure out if that user may sign on to MOVEit DMZ at that time. MOVEit DMZ does not retain the credentials in its own store.

Depending how you have configured your system, MOVEit DMZ may sign on as an LDAP user with permission to browse the LDAP directory to replicate settings such as email and group membership. In this case, the credentials MOVEit DMZ uses to browse are encrypted on MOVEit DMZ using 256-bit AES.



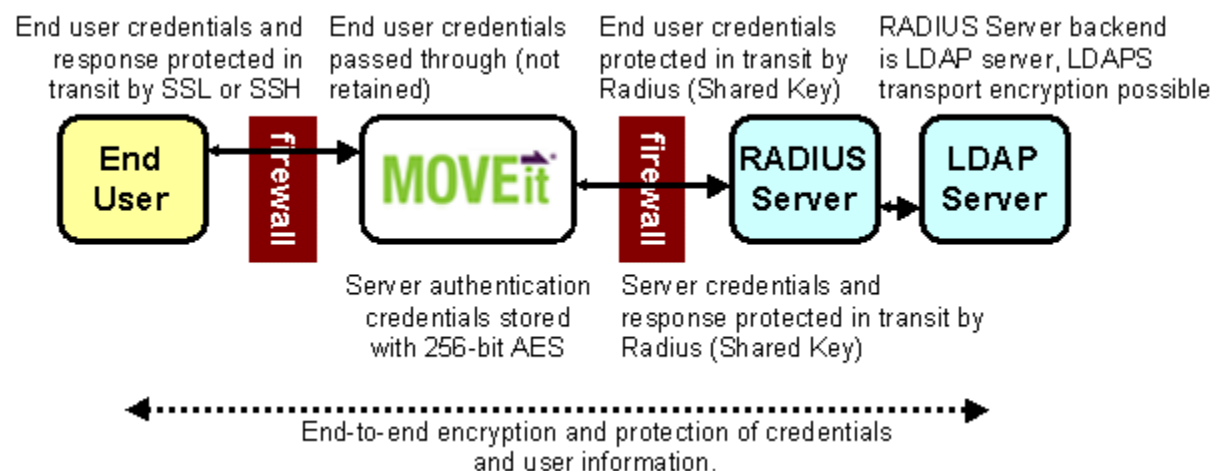
To access an internal LDAP server directly from a DMZ-based MOVEit DMZ server, there are several steps to take:

- Set up your LDAP server to require authentication and SSL connections when receiving connections from the internal firewall's IP address, MOVEit DMZ server or DMZ segment.
- Set up an internal firewall rule to allow MOVEit DMZ to connect to the LDAP server on TCP port 636 (the standard port for LDAP over SSL)
- Set up an external authentication source on MOVEit DMZ. Fill in the appropriate credentials to access the LDAP server and specify LDAPS (LDAP over SSL) as the authentication protocol.

Authenticated SSL Connection to Internal LDAP Server via RADIUS

This scenario is less common but still popular in situations where LDAP (even encrypted with SSL) is a banned protocol. First, an end user presents his or her credentials to MOVEit DMZ over an encrypted SSH (FTP/SSH) or SSL (FTP/SSL or HTTP/S) link. MOVEit DMZ turns around and passes those credentials to a RADIUS server with encrypted RADIUS packets to figure out if that user may sign on to MOVEit DMZ at that time. MOVEit DMZ does not retain the credentials in its own store. The RADIUS server (often Microsoft Internet Authentication Service, a.k.a. IAS) doesn't really have a user store of its own, but instead is usually tied into a Windows Domain, Active Directory or other LDAP server.

The RADIUS protocol is UDP-based and all packets are encrypted with a key. This key is stored on MOVEit DMZ using 256-bit AES. MOVEit DMZ does not need to know anything about the LDAP server(s) that really hold the user information because the RADIUS server acts as a complete front end. (Some sites have commented that they enjoy the fact that RADIUS queries, by design, return less information about their users than a similar LDAP query would.)



To access an internal LDAP server securely via RADIUS from a DMZ-based MOVEit DMZ server, there are several steps to take:

Set up your RADIUS server to get authentication information from your LDAP server. (Often when using free add-on tools such as Microsoft's IAS server with Active Directory, this is your only option.)

Set up an internal firewall rule to allow MOVEit DMZ to connect to the LDAP server on UDP port 1645 (the standard port for RADIUS)

Set up an external authentication source on MOVEit DMZ. Fill in the appropriate key to encrypt RADIUS traffic for your particular RADIUS server.

Active Directory SSL Notes

People have reported that enabling SSL services on Active Directory LDAP services is harder than it ought to be. Specifically, implementing Microsoft's recommendation involving the deployment of an Enterprise Certificate Authority can take some time.

- **#Q247078 - How To Enable Secure Socket Layer (SSL) Communication over LDAP for Windows 2000 Domain Controllers** (<http://support.microsoft.com/default.aspx?scid=kb;en-us;247078>)
(External Link)

There is, however, an easier way to enable SSL on Active Directory - and it does not involve Enterprise Certificate Authority.

- 1 Get a CA-signed server certificate with the AD server's fully qualified domain name (FQDN) listed in as the certificate's common name (CN). For a server named ad.internal.mycorp.com, a server certificate named ad.internal.mycorp.com signed by any CA will do.
- 2 On the AD server, use the **Certificates MMC** plug-in (for Local Computer) to add the CA-signed server certificate into the Local Computer's **Personal** certificate store. Make sure the imported certificate has a **private key** listed on its property dialog.
- 3 On the AD server, use the **Certificates MMC** plug-in (for Local Computer) to add the CA certificate into the Local Computer's **Trusted Root** certificate store. The imported certificate should not have **private key** listed on its property dialog.
- 4 On the MOVEit DMZ server (or other LDAP client), use the **Certificates MMC** plug-in (for Local Computer) to add the CA certificate into the Local Computer's **Trusted Root** certificate store. The imported certificate should not have **private key** listed on its property dialog.
- 5 Restart the domain controller. AD will automatically find the current SSL server certificate to use based on its name and will make its LDAPS interface available accordingly.
- 6 At this point MOVEit DMZ (or other LDAP client) should be able to securely connect to Active Directory using LDAPS over TCP port 636.

There is more information about this procedure on Microsoft's site, but the primary difference between Microsoft's procedure and the one laid out here is that Microsoft's recommends the use of Microsoft's certreq add-on utility in place of OpenSSL.

- **#Q321051 - How to enable LDAP over SSL with a third-party certification authority**
(<http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>) (External Link)

Finally, there are at least two alternatives to these procedures; both involve an SSL tunnel that adds SSL encryption to Active Directory's existing LDAP protocol.

- Configure your firewall to accept LDAP/SSL connections on TCP port 636 and forward them to Active Directory on port 389. In this case, an SSL certificate will be installed on your firewall. (Not all firewalls support this configuration.)
- Install a utility called STunnel (available from MOVEit support) on your Active Directory or any other internal machine that has access to Active Directory. Configure STunnel to accept LDAP/SSL connections on TCP port 636 and forward them to Active Directory on port 389. In this case, an SSL certificate will be installed on the machine which runs STunnel.

Contact our support staff for more information about any of these procedures.

SAML Single Signon Service

Security Assertion Markup Language (SAML) 2.0 provides a mechanism for exchanging authentication data among secure web domains. SAML 2.0 is an XML-based protocol, and an OASIS standard. For more information about SAML, refer to **SAML Overview** (<https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf>) from OASIS.

The SAML Single Signon service allows your users to connect to MOVEit Server using a third-party Identity Provider to authenticate. Thus, a user who is signed on using their network or corporate account can access MOVEit without needing to enter credentials again.

This topic covers:

- Third-party requirements for Single Signon
- Single Signon for the MOVEit Server web interface
- Single Signon for the Ipswitch Clients
- Single Signon for FTP and SSH clients
- Instructions for End Users
- How Session Termination and Timeouts are Handled
- Single Signon Automatic Authentication For Windows Users Using Internet Explorer

Third-party requirements for Single Signon

Through support of SAML 2.0 functionality, MOVEit can use a third-party "identity provider" to authenticate users. An identity provider is an application that provides identity assertions via SAML, in response to authentication requests from a service provider. MOVEit acts as the service provider, also known as the "SAML consumer."

MOVEit supports authentication from the following as the Identity Provider:

- Microsoft Active Directory Federation Services (ADFS)
- Shibboleth
- OneLogin

Authentication with these Identity Providers has been tested and is supported by Ipswitch. Other servers that support the SAML 2.0 protocol should also work with MOVEit.

Single Signon for the MOVEit Server web interface

When Single Signon is configured for the MOVEit web interface, a user session works like this:

- 1 User accesses MOVEit Server URL using a browser.
- 2 MOVEit Server redirects browser to Identity Provider with an authentication request.

- 3 Identity Provider authenticates user.
- 4 Identity Provider redirects browser to MOVEit Server with an authentication assertion.
- 5 MOVEit Server validates the assertion and signs the user on.
- 6 If the Single Logout service is configured, when the user logs out of their network (Identity Provider) account, they will also be signed off from MOVEit.

To set up Single Signon for users signing on to MOVEit DMZ web interface, you need to do the following:

- Make sure the requirements for the Identity Provider are identified and met. Refer to your Identity Provider's documentation for the required configuration settings.

Note: If you are using Active Directory as your user store (configured in User Authentication as External Only); then you can use that same user store with the Identity Provider. You will need to install and configure ADFS so that Active Directory can act as the Identity Provider.

- Configure Service Provider/Relying Party settings: See **Settings - User Authentication - Single Signon** (on page 422) for details on setting up MOVEit Server as a SAML Service Provider.
- Configure Federated Identity Provider settings: See **Settings - User Authentication - Single Signon** (on page 422) for details on adding one or more Identity Providers.

Single Signon for the Ipswitch Clients

When Single Signon is configured for the Outlook plug-in and MOVEit Sync clients, a user session works like this:

- 1 User sends a file using the Ad Hoc Transfer client (Outlook plug-in) or a Sync operation is initiated.
- 2 MOVEit Connector (on the client computer) requests SAML information from MOVEit Server.
- 3 MOVEit Server returns SAML information, including the Service Provider URL and an Identity Provider URL.
- 4 MOVEit Connector uses the SAML information to obtain a SAML token from the Identity Provider.
- 5 MOVEit Connector sends a signon request (which includes the SAML token) to MOVEit Server.
- 6 MOVEit Server signs the user on.

To set up Single Signon for users signing on to MOVEit DMZ from the Outlook plug-in and MOVEit Sync clients, you need to use ADFS as the Identity Provider. Both clients can use MOVEit DMZ's Single Signon services to sign on using a Windows domain account. Currently, only ADFS supports using Windows Authentication.

Assuming the Service Provider and Identity Provider settings are configured (see "Single Signon for MOVEit web interface"), Outlook plug-in and MOVEit Sync users can complete the configuration as described in the following procedure.

➤ *Single Signon using Windows Authentication from Ipswitch clients*

If MOVEit is configured for Single Signon through an Identity Provider using the same Domain Controller that your users use to perform Windows Authentication, it is possible to configure the Outlook plug-in and MOVEit Sync clients to automatically sign those users on without requiring credentials. To achieve this, follow these steps:

Note: This procedure must be run on the end user computer

- 1** Log into Windows as a user on the same Domain Controller that the MOVEit Identity Provider uses for authentication.

Note: If the client was installed using silent install with the Windows Authentication and Organization ID properties already set, then the user will not need to signon. The user will be signed on when they log into their Windows account.

- 2** In the system tray, right-click the MOVEit Connector, then select **Configuration**.
- 3** In either the MOVEit Send tab or the MOVEit Sync tab, select the **Use Windows Authentication** option. Instead of using the username and password from this dialog, the MOVEit Connector will initiate a SAML signon by requesting the SAML information from MOVEit. The user will not have to enter their user name and password here.
- 4** When **Use Windows Authentication** is selected, the Username and Password fields will be hidden, and the **Organization ID** will appear. The user should enter their MOVEit Organization name provided by you, the Org administrator. If the user uses the default MOVEit organization, they can leave this option blank.

Note: The Ipswitch clients can also be configured to use WS-Trust authentication, which can allow users to sign on using Windows Authentication when ADFS is not available, for example, if the user signs on from a home network. For information about setting up WS-Trust Authentication, see the "Single Signon for FTP and SSH Clients" section.

Single Signon for FTP and SSH clients

WS-Trust authentication allows MOVEit to directly authenticate users using the same identity provider that is used for single signon with SAML. We recommend configuring a WS-Trust authentication source in addition to SAML Single Signon services for customers who want to provide FTP and SSH access to MOVEit using the same credentials the user uses to authenticate to their Identity Provider.

Currently, only the ADFS Identity Provider supports WS-Trust.

If you have a requirement to use WS-Trust, you can do so by setting up the following components:

Note: If you have already configured the Service Provider settings and added ADFS as the Identity Provider, you do not need to complete this setup again.

- Configure Service Provider/Relying Party settings: See **Settings - User Authentication - Single Signon** (on page 422) for details on setting up MOVEit Server as a SAML Service Provider.
- Configure Federated Identity Provider: See **Settings - User Authentication - Single Signon** (on page 422) for details on adding one or more Identity Providers.
- Configure External authentication - WS-Trust: See **Settings - Service Integration - WS-Trust** for details on setting up the external authentication method.

Instructions for End Users

After you have configured the Single Signon components, you need to provide the following information to your end users.

- For signing on from a web browser, provide the Direct Signon URL (shown on the Single Signon page).
- For signing on from the Outlook plug-in or Sync clients, direct your users to select the Windows Authentication option in the configuration options (on the client computer, right-click the MOVEit Connector (in the system tray), then select Configuration. In either the MOVEit Send tab or the MOVEit Sync tab, select the Windows Authentication option. Instead of using the username and password from this dialog, the MOVEit Connector will initiate a SAML signon by requesting the SAML information from MOVEit.
- Single Logout service: If this service is enabled, when the user logs out of their identity provider account, they will also be logged out of any MOVEit sessions.

How Session Termination and Timeouts are Handled

- MOVEit Server session termination: As a SAML authenticated user, if your MOVEit Server session is manually terminated by an administrator, a flag is set for that user. If that user navigates to any page in MOVEit Server that requires an active session, the user will be redirected to the MOVEit Server Signon page. The user will also see a notification that the session has been terminated.
- If the MOVEit Server session terminates due to a timeout, or the Identity Provider terminates due to session timeout, user logout, or admin terminated session, the browser may handle the subsequent re-authentication sequence. Some browsers may re-authenticate users within the same browser session without requiring the user to re-enter credentials. To prevent this "silent" re-authentication by the browser, the user should close the browser after logging out of MOVEit Server.

Note: If you use the ADFS Identity Provider and want to avoid silent re-authentication by the browser, you can configure HTML form-based sign on. For more information, see the procedure below.

➤ *HTML Form-based Signon for ADFS*

Depending on how the Identity Provider is configured, many browsers will silently re-authenticate the user when they initiate the next session, which may be the desired behavior. However, if you want users to have to re-enter their password after doing a full SAML sign off, you can configure HTML Form-based signon. This procedure describes how to configure form-based signon for ADFS.

- 1 Open the ADFS web application's web.config file (by default, C:\inetpub\adfs\ls\web.config) in a text editor.
- 2 Locate the <microsoft.identityServer.web><localAuthenticationTypes> element.
- 3 Move the child element of the localAuthenticationTypes element with the name "Forms" to the top of the list of child elements.
- 4 Save the web.config file and restart the ADFS service.

➤ *Single Signon Using Windows Authentication from Internet Explorer*

If MOVEit is configured for Single Signon through an Identity Provider using the same Domain Controller that your users use to perform Windows Authentication, it is possible to configure Internet Explorer to automatically sign those users on without requiring credentials. To achieve this, follow these steps:

Note: This procedure must be run on the end user computer.

- 1 Log into Windows as a user on the same Domain Controller that the MOVEit Identity Provider uses for authentication.
- 2 Open up Internet Explorer.
- 3 Go to Internet Options > Security, select Local intranet, then click Sites. The Local intranet dialog opens. Click Advanced.
- 4 Add the base identity provider URL as a trusted site. This URL is the location you are redirected to during SAML Authentication. For example, an ADFS URL might look something like this:
https://adfs.mycompany.internal

- 5 Close Internet Options.
- 6 Navigate to the MOVEit Signon page and attempt a SAML Authentication.
You should automatically sign on to MOVEit using your Windows account without being prompted for credentials.

WebPosts

Website Integration

MOVEit DMZ offers a unique capability among secure file transfer and processing solutions in its WebPost processor. MOVEit DMZ WebPosts offer ease-of-use in several areas:

- 1 Secure Transport & Storage - By pointing existing or new forms to a MOVEit DMZ server, organizations gain not only the transfer security of SSL but the storage security of MOVEit DMZ.
- 2 Automatic Thank-You Messages - If the form user fills out a designated email field, a customizable thank you note is immediately sent to this address. (The content of the thank-you note may even include other variables such as a the name of the person filling out the form.)
- 3 Automatic Notification - An email notification will be sent to each and every party interested in reviewing the results of web form submissions.
- 4 Multiple Views - The individual or collected results of web form submissions may be previewed online, retrieved as a CSV file for import into Excel or similar programs, or as an XML document for a variety of uses.

WebPost Submissions

Forms which take advantage of MOVEit DMZ's WebPost capability may be hosted on the MOVEit DMZ server itself, another secure server or an insecure server. There are advantages and disadvantages of each approach, but ALL approaches will transport data over a secure channel to the MOVEit DMZ server.

WebPosts Submissions from Forms Served by Insecure Servers

Hosting forms on an insecure server has two disadvantages:

- 1 No "key" icon indicating a secure transmission will appear in the lower corner of their browser, and
- 2 Users must normally correctly answer a **transmit to secure server** dialog before being allowed to really submit the results of their form.

The advantage of this method is that it is the easiest to integrate into existing websites - especially since they may be using vulnerable software such as Microsoft's FrontPage which should not be installed on sensitive servers such as MOVEit DMZ.

WebPost Submissions from Forms Served by a Remote Secure Server

Hosting forms on a separate secure server will restore the "key" in the lower corner of your user's browser, but it will pop up a different forms submission is being retransmitted to another server message your users must answer correctly before really submitting the results of their form. Besides the "key" the advantage of this method is again the ease of integration into existing systems.

WebPost Submissions from Forms Served by the MOVEit DMZ Server

Hosting forms on the MOVEit DMZ server is the only option which will prevent your users from having to answer any "secure" or "redirect" message, and it also presents the secure key in the corner of their browser. The disadvantage of this method is that it is the hardest to integrate with existing websites.

Pointing Form Data to a MOVEit DMZ

MOVEit DMZ reads several fields from user-defined forms to figure out what to do with them. At a minimum, every form which points to MOVEit DMZ must have the following characteristics:

- ACTION = "webpost.aspx": An "action" attribute in the "form" tag which points to a copy of "webpost.aspx" on the secure port of the MOVEit DMZ server. For example:
<form method='POST' action='https://moveit.myhost.com/webpost.aspx'>
- moveit_orgid field: A hidden field indicating the ID of the organization this form belongs to. For example:
<input type='hidden' name='moveit_orgid' value='9876'>
- moveit_foldername field: A hidden field indicating into which folder results from this form should be stored. For example:
<input type='hidden' name='moveit_foldername' value='Marketing Survey'>

Optional fields:

- moveit_email field: A normal "text" field into which the person filling out the survey will put his or her email address. When the form is submitted MOVEit DMZ will attempt to send an email "thank you" message to this address AS WELL AS logging the address in a normal "name/value pair" named "email."
- moveit_additionalfoldernames: Can contain a semicolon-delimited list of additional foldernames that the form information will be posted to. An additional copy of the form information will be posted to each folder specified, and recipient notifications will be sent, based on the settings for that folder. Sender confirmation messages will not be sent, nor will the folder's response settings be used.

Some caveats:

- The names of the tags **MUST** be spelled exactly as described above, but the names are **NOT** case-sensitive.
- Form field names **MUST NOT** begin with a number. If a webpost is received with a field name that begins with a number, an error message will be displayed and the post rejected.
- If the "moveit_orgid" tag is not provided, the default orgid will be used. The server attempts to send the form to the webpost folder in the default Org.
- If the "moveit_foldername" tag is provided with the name of a folder which does not exist, a new folder will be created to contain the results of the current post.
- You may use JavaScript to screen the values of your fields before submitting the form.

In addition to the contents of the fields just submitted, MOVEit DMZ also logs the following information about each web post:

- The IP address from which the form was submitted (*i.e.*, "192.10.3.24")
- The name (*i.e.*, "Opera", "Netscape") and version (*i.e.*, "5.5") of the browser used to submit the form
- The time and date of the submission
- The email address to which the "thank you" message was sent (if the "moveit_email" field is used)

Web Post Form HTML Code

When a webpost folder is viewed, a "cheat sheet" containing code you can cut and paste into your own web forms to get them to post data to this webpost folder is displayed at the bottom of the page.

Web Post Form HTML Code

```
<form action="https://192.168.197.189/webpost.aspx" method="Post">
  <input type="hidden" name="moveit_orgid" value="6685"/>
  <input type="hidden" name="moveit_foldername" value="Forms"/>
  Email Address: <input type="text" name="moveit_email"/>

  ...

</form>
```

MOVEit DMZ Form Post Response

By default, MOVEit DMZ reacts to the submission of a new web post by:

- 1 Creating a folder for the incoming web post if none exists.
- 2 Displaying to the user a generic thank you message that displays your "Banner Logo" (defined on the **SETTINGS** tab in the **Logo and Colors** section) and the tracking number of the form results just submitted.
- 3 Emailing the user the same generic "thank you" message if they filled out the **MOVEit_email** field. The format of the email (HTML or text) is determined by the current value of the organization-level **Notification Format** setting.
- 4 Redirecting the user to the "External URL" (defined on the **Settings** page in **Appearance - Brand** (on page 358)) after 10 seconds.

However, File Admins and Admins may customize the following behaviors:

- The content of the message displayed/emailed when this form is submitted. This message can contain macros which will be resolved into their respective values. Available macros and their definitions are:
 - [TIME] - The date and time of the webpost submission.
 - [TRACKINGID] - The ID of the webpost file that was created from the submission data.
 - [ORGNAME] - The name of the organization the webpost was posted to.

In addition to these macros, any key/value pairs submitted by the post are also available in macro form. For example, if the form post contained a field with the name "name", the value submitted in that field will be available using the macro [name]. Note that this includes the email field that is added to the form data if a moveit_email field is received. As expected, this field can be accessed using a [email] macro.

- The subject of the above message. Like the message body, this field supports the use of macros. All the macros available to the message body are also available to the subject.
- The banner displayed when this form is submitted.
- The URL to which users will be directed when this form is submitted.
- The amount of time after which users will be directed to the URL when this form is submitted (Immediate is an option).

Change Web Post Response...

When a web form is submitted to this folder, by default users will see this organization's logo and a brief message. The "web response" settings allow these defaults to be overridden with a form-specific banner, thank you message, and URL to which the user will be redirected.

URL:

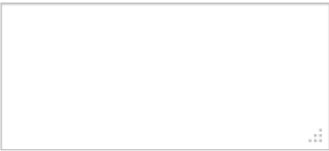
Redirect:

☐ Go to (URL) immediately.

☒ Go to (URL) after seconds.

Subject:

Package:



After customizing your web response settings, press the "Update Web Response Settings" button above BEFORE selecting and uploading your custom response banner. (You may also "reset" your banner to the organizational logo by pressing the "Clear Banner" button.)

Current Banner:  (scaled)

Step 1: Select a *.gif file: No file selected.

Step 2:

~ OR ~

All of these behaviors are controlled in the Change Web Post Response... section on any webpost folder settings page.

Note: The Response Banner settings are separate from the other settings; you must press the Update Web Response Settings button to save the URL, Redirect or Message settings BEFORE working with the custom banner.)

Content Scanning

Content Scanning is an option that allows MOVEit DMZ to control what data is sent to and from a MOVEit system based on the content of the data. This process protects a user's system from being infected by viruses or from losing or accepting critical data, typically when MOVEit DMZ is separated from the main system by a firewall. MOVEit DMZ will forward the data using Internet Content Adaptation Protocol (ICAP) to a user's Anti-Virus (AV) server and/or Data Loss Prevention (DLP) server before it completes the transmission. Depending on the results returned by the server(s), MOVEit will allow or block the transmission.

Users must install and configure the AV and/or DLP servers separately. Different scanning servers may have different capabilities. A server may be configured to do AV, DLP or both. You can configure MOVEit to communicate with multiple different AV and DLP servers. You enable scanning at the system level, but you can have only one AV and one DLP server enabled at a time. You can then disable a specific AV or DLP process at the organization level.

Important: When you configure scanning for both AV and DLP, MOVEit DMZ sends the data to both processes simultaneously. When the scanner reports a virus or a DLP policy violation that is configured in MOVEit to block the transmission, the transmission fails.

Anti-Virus

The Content Scanning feature allows scanning of incoming files using a remote anti-virus server. MOVEit DMZ will submit incoming files to the anti-virus server using the ICAP protocol. Files that are clean are then passed into the MOVEit DMZ filesystem.

Overview

MOVEit DMZ currently supports the following anti-virus programs:

- Sophos Anti-Virus Dynamic Interface (SAVDI) scanner, we recommend and have tested against SAVDI v2.0 or later.

For information on installing and configuring the Sophos AV scanner, refer to your Sophos documentation.

- Symantec Protection Engine, we recommend and have tested against v7.0.2.4.

For information on installing and configuring the Symantec ICAP AV scanner, refer to your Symantec documentation.

- McAfee Web Gateway
- McAfee VirusScan Enterprise for Storage

Note: These versions of the anti-virus scan engines support the ICAP protocol (RFC3507 for more information), which is required to interface with MOVEit DMZ. Other "desktop" versions from these same vendors will not work with MOVEit DMZ.

Before you can configure content scanning for incoming files, you must have one of these anti-virus scanners configured on a machine that is accessible to the MOVEit DMZ system.

Note: If you are using the AS2 Module to transfer files, be aware that content scanning does not apply to AS2 transfers. Use MOVEit Central to scan AS2 transfers for viruses.

Configuring Anti-Virus Scanning for MOVEit DMZ Hosts

After you have configured the anti-virus server, you need to set up content scanning for your MOVEit DMZ organizations. To access the Content Scanning settings, you must be logged on as **sysadmin**. These settings apply to all MOVEit DMZ organizations on the system. Under **System Settings, Content Scanning**, select **Anti-Virus**. For a description of each of the settings, see **Web Interface - Settings - System - Content Scanning** (on page 542).

You can enable or disable Content Scanning for each organization in **Settings - Security Policies - Content Scanning**. You need to be signed on as an Organization administrator.

Enabling the content scanning option causes MOVEit DMZ to scan uploaded files as follows:

- The size of the file, if known, must be less than the configured maximum. Files larger than this maximum size are entered into the MOVEit DMZ filesystem without being scanned.
- Files are scanned during the upload and are not entered into the MOVEit DMZ filesystem until the content scanner returns an indication that the file is not infected.
- If the file does have a virus, it will be rejected, and the user will receive an error message.
- If the ICAP server connection fails or the connection limit is exceeded, or if for some reason the file cannot be checked, the upload will be rejected and the user will receive an error message.
- There is no support for re-scanning files, quarantining, or scanning on downloads.

The following screen shows an example of the configuration for a Sophos ICAP AV scanner.



Settings (System)

Configure Content Scanning Settings...

Configure an optional content scanner to have MOVEit DMZ send uploaded files to an ICAP server for inspection. Rejected files will be immediately discarded. This feature is most commonly used for virus scanning. [Click here](#) for more information about Content Scanning in MOVEit DMZ.

Scan uploads:	Yes: ☒ No: ☐
Name:	Sophos AV
Server URL:	icap://192.168.195.83:1344/avscan (e.g. icap://scansrv:1344/avscan)
Server Type:	Sophos Anti-Virus Dynamic Interface ▼
Server allows "204" responses: (Allows faster scanning)	Yes: ☒ No: ☐
Maximum file size to scan:	15 (MB)
Server connection timeout:	5 (seconds)
Server send timeout:	30 (seconds)
Server receive timeout:	30 (seconds)
Server connection tries:	3

(Be sure to save your changes first, then Test Content Scanning)

Data Loss Prevention

The Content Scanning feature sends incoming data from file transfers and Ad Hoc transfers, including subject, note/body and attachments, to an external Data Loss Prevention (DLP) server before MOVEit DMZ determines whether to complete the transmission. MOVEit DMZ uses the ICAP protocol to submit incoming data to the DLP server. The DLP server applies configured data protection policies as it scans the data. When the DLP server returns its response, MOVEit configurations determine whether to block, quarantine or allow the transmission. MOVEit logs all DLP policy violations returned by the DLP server.

Overview

MOVEit DMZ currently supports the following data loss prevention (DLP) programs:

- McAfee Web Gateway 7.1
- Symantec Data Loss Prevention (DLP) 12 or 12.0.1

Note: We only claim support for Symantec DLP version 12 or 12.0.1 when integrated as described specifically in this section. Later versions may not provide scanning results in a consistent manner, potentially leading to false negatives.

- RSA Data Loss Prevention (DLP) 9.6

Before you can configure content scanning for incoming files, you must have one of these DLP scanners configured on a machine that is accessible to the MOVEit DMZ system.

For information on installing and configuring the various scanners, refer to their official documentation. Two of these scanners, McAfee and Symantec, require additional specific changes to their configurations to properly communicate with MOVEit. These requirements are described in the topic "Configuring DLP Scanning for MOVEit DMZ Hosts".

Note: These versions of the DLP scan engines support the ICAP protocol (RFC3507 for more information), which is required to interface with MOVEit DMZ. Other "desktop" versions from these same vendors will not work with MOVEit DMZ.

Note: If you are using the AS2 Module to transfer files, be aware that content scanning does not apply to AS2 transfers.

Configuring DLP Scanning for MOVEit DMZ Hosts

There are three major tasks to implement Data Loss Prevention (DLP) scanning in MOVEit DMZ.

- 1 Install and configure the external and typically remote DLP server
- 2 Configure DLP servers for a MOVEit system (you can enable only one DLP server at a time)

3 Configure DLP rulesets for user classes or users for each MOVEit organization

Enabling the content scanning option causes MOVEit DMZ to scan uploaded files as follows:

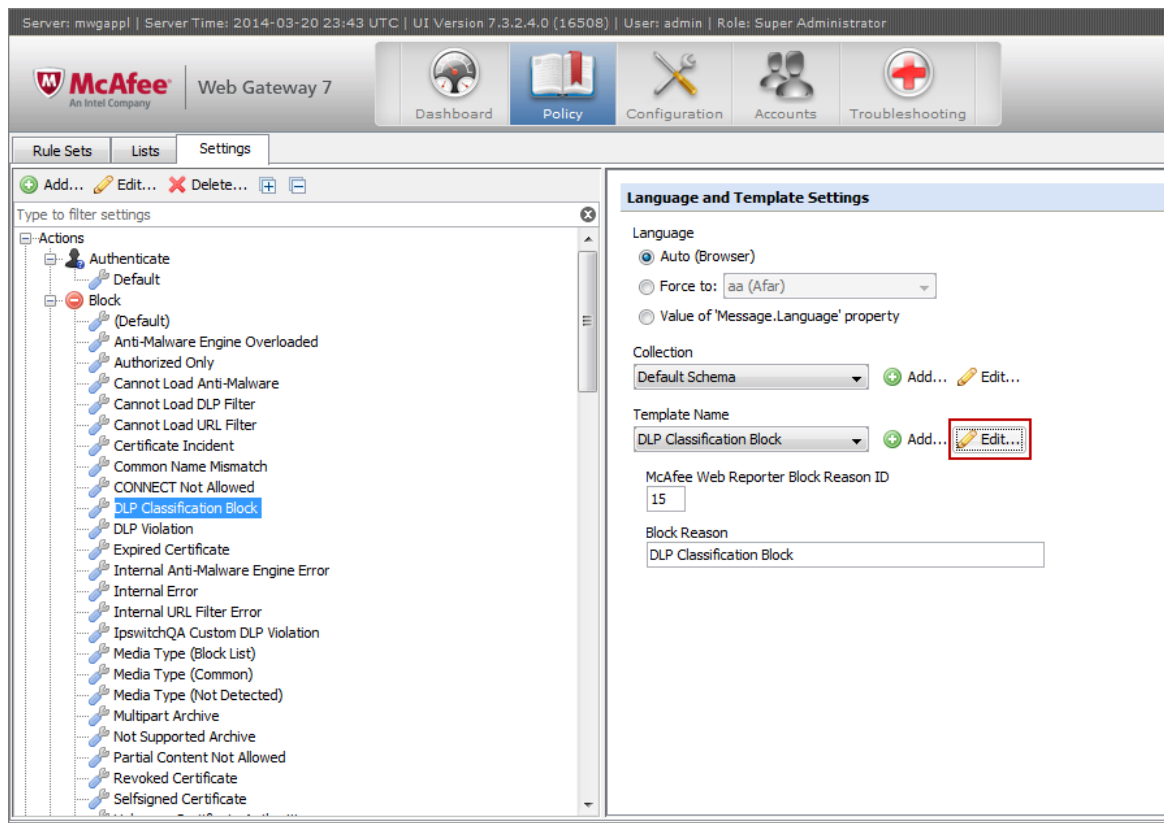
- The size of the file, if known, must be less than the configured maximum. Files larger than this maximum size are entered into the MOVEit DMZ filesystem without being scanned.
- Files are scanned during the upload and are not entered into the MOVEit DMZ filesystem until the content scanner returns an indication that the file is not blocked for the user that is uploading the file.
- If the file violates a DLP policy, it will be processed according to the MOVEit policy and rulesets, and the user attempting to upload will receive an error message. Note that if a virus is found during a concurrent anti-virus scan, the file is automatically blocked from upload.
- If the ICAP server connection fails or the connection limit is exceeded, or if for some reason the file cannot be scanned, the upload will be rejected and the user will receive an error message.
- There is no support for re-scanning files, or scanning on downloads. The ability to download files is based on the results of the scan when the file was uploaded and rights for the user attempting the download. Quarantined files may be cleared for download under special circumstances.

Two of these DLP scanners, McAfee and Symantec, require additional configurations. Perform the following tasks as appropriate for your installation.

➤ *Adding Required DLP Configuration to McAfee Web Gateway 7*

- 1** Log on to your McAfee Web Gateway as a valid administrator.
- 2** From the **Settings** tab, expand **Actions**, then expand **Block**.

You should see the following window.



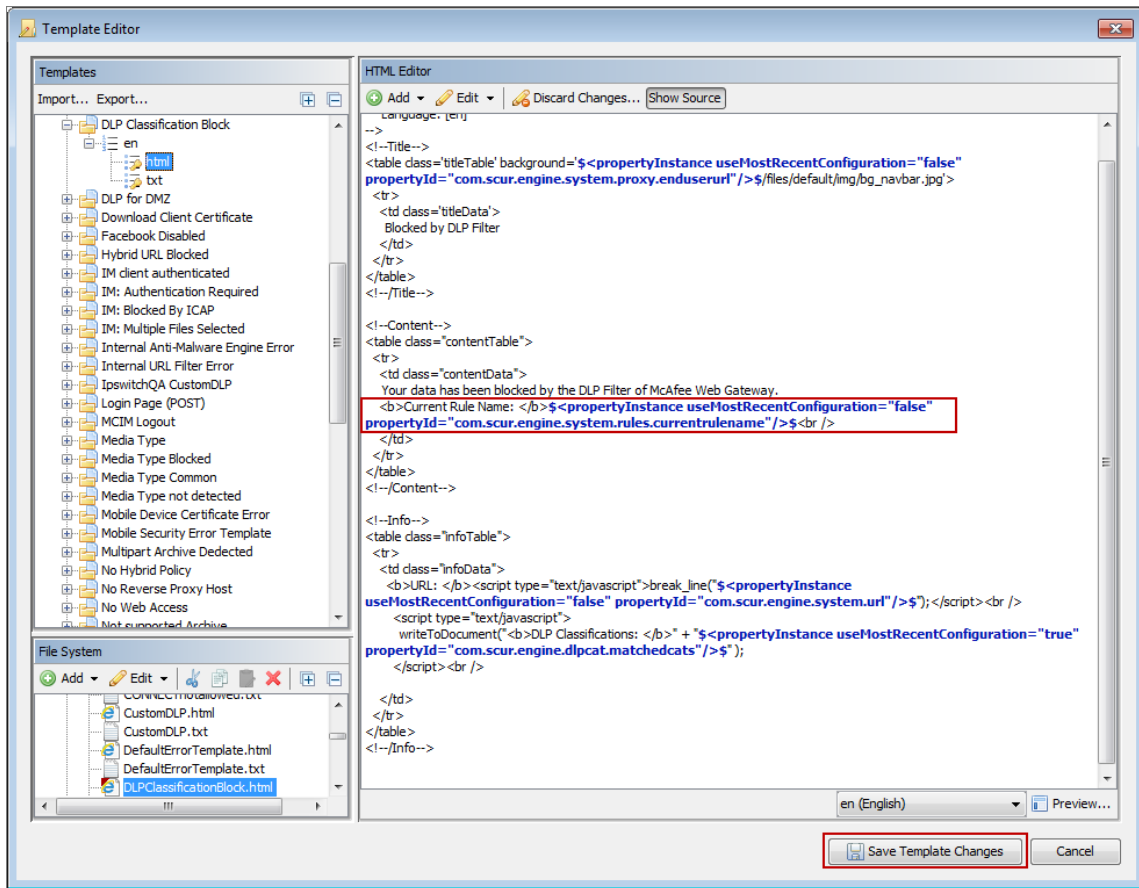
- 3 Under the Template Name for the DLP Classification Block, click Edit.
- 4 From the Template Editor window, expand DLP Classification Block, then expand en, and then click html.

The HTML Editor appears in the right pane.

- 5 From the right pane, scroll to the following text, "Your data has been blocked by the DLP Filter of McAfee Web Gateway."
- 6 Under this text, paste the following line:

```
<b>Current Rule Name: </b>${propertyInstance useMostRecentConfiguration="false"
propertyId="com.scur.engine.system.rules.currentrulename"}<br />
```
- 7 At the bottom of the window, click the Save Template Changes button.

Your window should appear as follows:

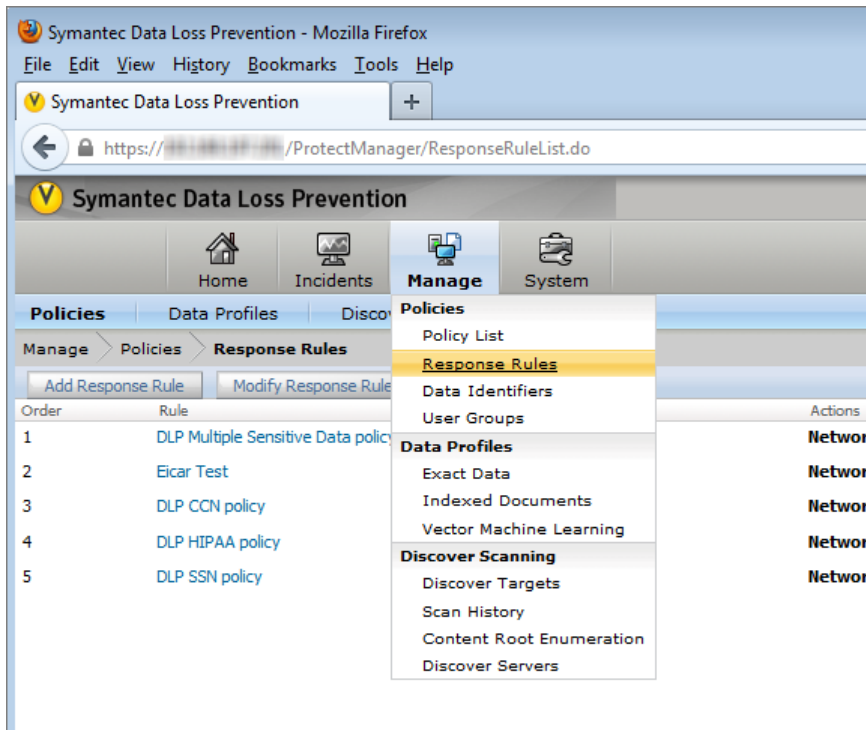


➤ Adding Required DLP Configuration to Symantec Data Loss Prevention Suite

Note: You should already have configured the policies in Symantec that you want to use.

- 1 Log on to your Symantec Data Loss Prevention application as an administrator.
- 2 From the Manage menu, under Policies click Response Rules.

The list of rules you configured for your system appears.



3 For each rule that you want to use:

- a) Click the rule.

The Configure Response Rule window appears.

- b) Within the Rejection Message box, type the following case-sensitive text that is within quotation marks (do not include the quotation marks, and note the space after the last word):

"Content blocked due to "

- c) After the last space, type the text that contains the value on which you want MOVEit to match, which would typically be some or all of the name of the rule, but it could be any text that contains the matching value. For example, if your matching value in MOVEit is *CCN*, then you might type, "DLP CCN Policy" or "CCN policy violation", as in the following example.

The screenshot shows the Symantec Data Loss Prevention interface. The top navigation bar includes Home, Incidents, Manage (selected), and System. Below this, the breadcrumb trail is Manage > Policies > Response Rules > Configure Response Rule. The 'Save' button is highlighted with a red box. The 'General' section shows 'Rule Name' as 'DLP CCN policy' and 'Used in active policy' as 'Credit Card Numbers'. The 'Conditions' section has an 'Add Condition' button. The 'Actions' section has a dropdown menu set to '<choose action type>' and an 'Add Action' button. Below the actions, the 'Network Prevent: Block HTTP/HTTPS' section is active, indicated by a red 'X' icon. The 'Rejection Message' field is highlighted with a red box and contains the text 'Content blocked due to DLP CCN policy'.

- d) Click the **Save** button.

After you have configured the DLP server, you need to set up content scanning for your MOVEit DMZ organizations.

➤ *Configuring Content Scanning for DLP for your MOVEit System*

- 1 Log on to MOVEit DMZ as a system administrator, typically SysAdmin.
- 2 In the left pane, click **Settings**.
- 3 In the right pane for Settings, under **System**, **Content Scanning**, click **Anti-Virus/DLP**.
- 4 To add a scanner, click the **Add Content Scanner** button.
The **Configure Content Scanning Settings** page appears.
- 5 For each DLP application you want DMZ to access, complete the fields and click **Change Content Scanning**.

For a description of each of the settings, see **Web Interface - Settings - System - Content Scanning** (on page 542). These settings apply to all MOVEit DMZ organizations on the system.

Important: You can set Scan Uploads to **Yes** for only one DLP scanner at a time. That is, only one DLP scanner can be enabled on your system at any give time.

- 6 Click the **Test Content Scanning** button to make sure the connection to the scanner works.

➤ *Configuring DLP Scanning for a MOVEit Organization*

Repeat this task for each organization in your system that will use DLP content scanning. You will perform four basic procedures:

- 1 Enable Content Scanning for the organization.
- 2 Create rulesets, which determine how MOVEit handles files that violate one or more DLP server policies. They can be applied at the user-class level or user level.
- 3 Create rules for a ruleset to define the action MOVEit DMZ will take for a specific DLP policy or set of matching policies.
- 4 Assign DLP rulesets to user classes, which will act as defaults for newly created users.

To enable content scanning for an organization, proceed as follows:

- 1 Log on to MOVEit DMZ as an Organization administrator.
- 2 In the left pane, click **Settings**.
- 3 In the right pane, under **Security Policies, Content Scanning**, select **Data Loss Prevention (DLP)**.
- 4 Under **Edit Data Loss Prevention (DLP) Settings**, click **Yes** to enable Content Scanning for the organization. This affects the DLP server that is currently enabled for the system.
- 5 Click **Change DLP Settings**.

Edit Data Loss Prevention (DLP) Settings...

If a DLP scanner is configured for the system, these settings will control how it is used for this Organization.

Enable for this Organization:

☒ Enabled ☐ Disabled

Action on server error:

☒ Block Content ☐ Allow Content and Log

Change DLP Settings

To continue and create rulesets and their rules, proceed as follows:

- 1 In the right pane, under **Configure DLP Rulesets**, click the **Add DLP Ruleset** button.

The Add DLP Ruleset pane appears.

Settings (Security)

Add DLP Ruleset...

DLP Rulesets determine how DMZ handles files that violate one or more DLP server policies. They can be applied at the user-class level, or at the group or user level.

Name:

Description:

Default Action:

- ☐ **Block** - Transfer will not be allowed.
- ☐ **Quarantine** - Upload will be allowed, but Download will not be allowed. Files will be tagged, and an audit log entry will be recorded indicating that the file violates one or more DLP policies. Files may be untagged later, at which point normal permissions will take effect.
- ☒ **Allow** - Transfer will be allowed, and files will be tagged. An audit log entry will be recorded indicating that the file violates one or more DLP policies.

- 2 Complete the fields, and click Add Ruleset.

For a description of each of the settings, see **Web Interface - Settings - Security Policies - Content Scanning - Data Loss Prevention (DLP)** (on page 489)

- 3 In the right pane, under Edit DLP Rules, click Add DLP Rule.

The Add DLP Rule pane appears.

Settings (Security)

Add DLP Rule...

DLP Rules define the action MOVEit DMZ will take for a specific DLP policy or set of matching policies.

Policy Mask:

Action:

- ☐ Block - Transfer will not be allowed.
- ☒ Quarantine - Upload will be allowed, but Download will not be allowed. Files will be tagged, and an audit log entry will be recorded indicating that the file violates one or more DLP policies. Files may be untagged later, at which point normal permissions will take effect.
- ☐ Allow - Transfer will be allowed, and files will be tagged. An audit log entry will be recorded indicating that the file violates one or more DLP policies.

Comment:

[Return to DLP Ruleset](#)

- 4 For each rule in the ruleset, complete the fields, and click Add Rule.

For a description of each of the settings, see **Web Interface - Settings - Security Policies - Content Scanning - Data Loss Prevention (DLP)** (on page 489)

Success or error messages appear in the ribbon at the top of the pane.

- 5 When you have added all the rules for this ruleset, click Return to DLP Ruleset.
- 6 To create additional rulesets and their rules, repeat steps 1 through 5.

To continue and assign DLP rulesets to user classes, proceed as follows:

- 1 Under the Edit User Class DLP Rulesets section, for a user class, display the drop-down list of rulesets you configured.
- 2 Select the ruleset that you want to use for that user class.
- 3 Click the Change Ruleset button for that user class.

A confirmation pane appears.

- 4 Click Yes to confirm the change.

Note that this will apply to all users in the class, including those for whom a ruleset was applied at the user level.

- 5 Repeat steps 1 through 4 for each user class.

Edit User Class DLP Rulesets...

Assign DLP Rulesets to user classes, which will act as defaults for newly created users. You will also be prompted to apply changes to existing users.

Administrators:	Personal Data_Allow	Change Ruleset
File Admins:	Personal Data_Quarantine	Change Ruleset
Users:	Personal Data_Block	Change Ruleset
Temp/Guest Users:	Personal Data_Block	Change Ruleset

To continue and assign rulesets to specific users, which overrides the ruleset assigned to the user class for that user, proceed as follows:

- 1 In the left pane, click Users.
- 2 In the right pane, select the appropriate user.
- 3 In the right pane, for the User Profile, under User Settings, DLP Ruleset, click Change Ruleset.

User Settings

- Folder Quota: None - [Change Folder Quota](#)
- Ad Hoc Quota: None - [Change Ad Hoc Quota](#)
- Package Expiration: None - [Change Expiration](#)
- Send To Unregistered: Allowed (by Org) - [Change Unregistered Recipients](#)
- Send Attachments: Allowed (by Org) - [Change Attachment Settings](#)
- Attachment Download Limits: None - [Change Download Limits](#)
- Home Folder: /Home/ppm - [Change Home Folder](#)
- Default Folder: /Home/ppm - [Change Default Folder](#)
- Shared Account: No - [Change Shared Account Status](#)
- Upload/Download Wizard: Prompt - [Change Wizard Status](#)
- Sign On/Sign Off Logging: All - [Change Logging Status](#)
- DLP Ruleset: Personal Data_Quarantine - [Change Ruleset](#)**

A User Profile, Change DLP Ruleset pane appears.

- 4 From the Change DLP Ruleset pane, click the drop-down list, and select the appropriate ruleset for this user.
- 5 Click Change DLP Ruleset.

You should now be able to test your configurations.

➤ *Testing Data Transmissions with DLP Content Scanning*

The following steps are for administrators who configured DLP for an organization to do some initial testing.

- 1** Create test files with data that violate your DLP policies and with data that will not violate any policies.
- 2** Log on to MOVEit DMZ as a specific type of user.
- 3** Upload data by various means, including sensitive and non-sensitive data, also in subject strings and notes/body where possible:
 - a) Upload your test files to your filesystem.
 - b) Upload your test files as attachments to packages.
 - c) Use the Outlook Plug-in to send files as attachments.
- 4** Review the results, and note the following:
 - a) Attempts to upload data that show DLP violations, should be blocked, quarantined or allowed per the action specified in the ruleset for the uploading user.
 - Files, packages or e-mails that were blocked should not appear in DMZ.
 - Files, packages or e-mails that were quarantined will be uploaded, but Download will not be allowed. Files will be tagged, and an audit log entry will be recorded indicating that the file violates one or more DLP policies. Files may be untagged later, at which point normal permissions will take effect.
 - Files, packages or e-mails that were allowed will be uploaded and tagged. An audit log entry will be recorded indicating that the file violates one or more DLP policies.
 - b) In Folders, for lists of files that were uploaded with DLP policy violations, the DLP policy violation icon  appears to the right of the file name, and depending on the rights of the user, the name of the policy or policies that were violated appears.
 - c) In Packages, depending on the rights of the user, the name of the policy or policies that were violated appears following the package information.
 - d) In File Information, depending on the rights of the user, more information about the DLP violation and DLP server appears.
 - e) Administrators can override policy violations on quarantined files, for example in cases where the violation inappropriately blocked the recipient from downloading the file. For a specific file under the File Action section, administrators can click **Clear DLP Policy Violations**.

Scanner Availability

If Content Scanning is enabled, MOVEit DMZ checks every few minutes to make sure the enabled AV and/or DLP scanner is available. This is part of the SysCheck routine (see **Advanced Topics - System Internals - Scheduled Tasks** (on page 754)), which can generate a built-in notification. It first checks the AV scanner and then the DLP scanner. If the either scanner is unavailable, SysCheck sends an email message to the Send Errors To email address and warns that the MOVEit DMZ server will not be able to transfer files until this situation is addressed. When the scanner becomes available again, SysCheck sends an email that states that scanning is now working.

Note: The system administrator should always test the connection when configuring a content scanner. They can also run MOVEit DMZ Check on demand.

Logging

If a file was scanned, file detail pages will display the anti-virus (AV) or the data loss prevention (DLP) server information.

In the following example, the first line of Content Scanning information is for the AV server and the second line is for the DLP server.

File Information

Uploaded by Administrator (administrator) at 3/27/2014 9:13:59 AM from 127.0.0.1 via  MOVEit Wizard Win 8.0.0.0

File Size: 1,146 bytes # of Downloads: 0

Integrity Verified: Yes ☒ A SHA-1 hash has automatically been used to confirm this file is identical to the original file from which it was uploaded.

Virus Checking: Yes ☒ This file has been scanned and found to contain no viruses.

DLP Checking: Yes ☒ This file has been scanned and found to contain no DLP policy violations.

Content Scanning: This file was scanned with Symantec: Symantec Protection Engine/7.0.2.4 6945A30122CF3ED66BD055350720F6EE during upload.

Content Scanning: This file was scanned with McAfee: McAfee Web Gateway 00002834-1.139.64-00007389 during upload.

File Log

Time/Date	User	Action
3/27/2014 9:13:59 AM	Administrator	Uploaded file "adfs.cer" from 127.0.0.1; integrity verified; upload took 1.312 seconds (873 bytes/second)

If a file fails the scan, the user who uploaded the file will see an error message on the browser page, for example:

Home

Browse Files and Folders

To search for a particular file, enter the file name or file ID in the Find File box on the left side of the page and press the "Find File" button.

 [Go To Your Home Folder](#) -  [Browse Other Folders](#)

New Packages

 **** (Suppressed due to DLP violation) **** (from Admin at 4/2/2014 3:42:49 PM)

[Mark All Packages Not New](#)

Upload Files...

Select a folder: 

[Launch the Upload Wizard...](#)

Upload Wizard Transfer Report

Some files were not uploaded.
Virus detected: EICAR test file

Local File	Status
 C:\0Data\Release Projects\MOVEitDMZ 8.1\DMZ Tests\EICAR-AV-Test.txt	Not uploaded: Virus detected: EICAR test file

Log file entries will report the user-configured name of the AV or DLP server used during the file upload. File records will also report the self-identification, version, and AV virus definition tag or DLP policy violation from the server, for example:

Logs

Log Entry

Date/Time	4/8/2014 12:11:29 PM
User	Username: ppm Real Name: Pat IP Address: 127.0.0.1 Agent:  MOVEit Wizard Win 7.1.0.0
Folder	Path: /Home/ppm ID: 985785118
Description	FAILED: Uploaded file EICAR-AV-Test.txt to folder /Home/ppm This file was scanned by AV_DLP_McAfee and was blocked.
Technical	Error Code: 6100 Message: Virus detected: EICAR test file

[Return to Logs](#)

Error code numbers (6100 - 6103) are used to report AV errors. This will help when filtering logs. If an upload fails due to content scanning, the corresponding log table records will contain the AV server name and, if possible, the name of the virus.

Error code numbers 0 and 6150 are used to report DLP policy violations, as follows:

- Error number 0 for violations that have been allowed or quarantined
- Error number 6150 for violations that have been blocked

Notifications

Notification macros for content scanning, if enabled, can report the scan results for both anti-virus (AV) and data loss prevention (DLP) scans.

AV and/or DLP information may be included in the following notifications:

- New File Upload Notification
- File Upload Confirmation
- New Package
- New Package Secure Attach
- New Temp User Package (with password)
- New Temp User Package (with password) Secure Attach
- New Temp User Package (with password link)
- New Temp User Package (with password link) Secure Attach
- New Guest Package
- New Guest Package Secure Attach
- File Non-Delivery Receipt
- File Upload List Notification
- File Upload List Confirmation
- File Not Downloaded List
- File Delivery Receipt
- Package Delivery Receipt
- Package Download Receipt
- Package Deleted By User
- Package User Was Deleted

The standard templates for these notifications do not include the content scanning results. You can add the macros that report the scan results by creating custom notification templates. Custom notifications are set in an organization via [Settings | Appearance | Notification | Custom](#).

Reports

These reports show various types of content scanning activity. Two reports give specific information about scan results: *Violations Blocked* and *DLP Violations (Allowed and Blocked)*. The remaining reports are maintenance reports that show aggregate counts.

If you are logged in as an organization administrator, the report shows scan results for your organization. If you are logged in as a system administrator, the report can show multiple organizations.

Note: Typically, reports may contain up to 30 days of online audit records and 30 days of online performance statistics, depending on how you run the scheduled cleanup tasks that archive the older data.

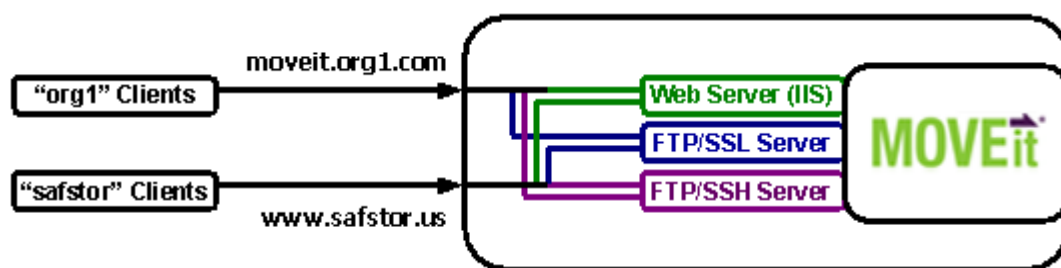
Multi-homing

What it Means with MOVEit

The term "multi-homing" generally suggests a single computer is handling requests addressed to multiple IP addresses. In MOVEit DMZ the definition is extended to mean a single MOVEit DMZ server is serving requests addressed to multiple hostnames with different SSL certificates and branding.

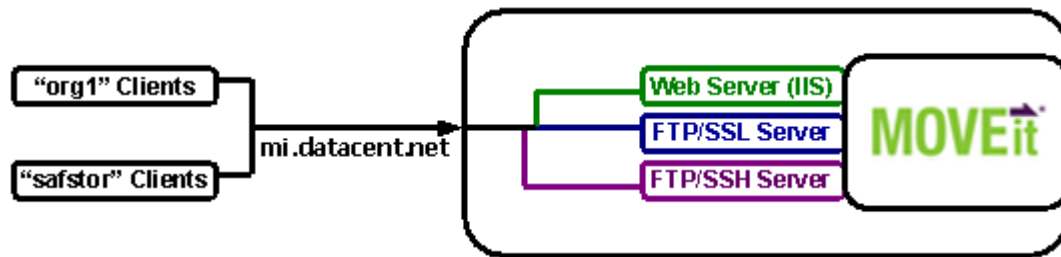
For example, if a single site was asked to support both "moveit.org1.com" and "www.safstor.us" for two different companies on the same MOVEit DMZ server, we would say that the MOVEit DMZ is multi-homing.

Multi-homing



However, if both "org1" and "safestor" used a common hostname of "mi.datacent.net" instead, we would be talking about setting up separate MOVEit DMZ Organizations but the MOVEit DMZ itself would NOT be multi-homing.

Not Multi-homing



Multi-homing Configuration Elements

Elements by Service

To support multi-homing, several MOVEit DMZ configuration items must be adjusted. These items can be broken down by the service they are related to.

- Core MOVEit DMZ Application
 - Create a separate organization for each hostname
 - Each organization's Base URL must be set to a unique hostname
 - Each organization should have its own branding
- HTTPS Server (IIS Service)
 - Add multiple SSL certificates, one for each hostname
 - Configure multiple IP addresses, one for each hostname
- FTPS Server (MOVEit DMZ Service)
 - Set up the default SSL host certificate to match one of the organizations
 - Other organizations will use other ("alternate") SSL host certificates as configured by FTP IP address. Set this list of IP addresses up to match those configured under IIS
- SFTP Server (MOVEit DMZ Service)
 - Only one SSH server key is currently available through the SFTP service. (SSH server keys, unlike SSL server certs, do not have a "hostname" or other organization-identifying element.)

Elements by Configuration Utility

These items can also be broken down by the configuration utility that must be used to configure them.

- Internet Information Services (IIS) Manager
 - Request and install commercial SSL host certificates.
 - Configure a separate IIS binding (Windows 2008) for each organization.
- MOVEit DMZ Configuration Utility
 - Select the default SSL host certificate to match one of the organizations. ("FTP Certs" tab)
 - Select alternate SSL host certificates for each additional organization.
- MOVEit DMZ Web Interface (Signed on as a SysAdmin)
 - Add a new production organization for each hostname. ("Orgs" page)
 - Set each organization's Base URL to its hostname. ("Organization Profile" page)
- MOVEit DMZ Web Interface (Signed on as an Admin)
 - Let each organization control its own scheme/colors, logos and other branding elements through their existing Admin accounts

Recommended Procedures

There are several ways to accomplish many of the tasks listed in the previous subsection, but the following procedures are recommended.

Requesting, obtaining and installing multiple SSL certs for different organizations

Windows Server 2008

For Windows Server 2008, you need not create additional IIS websites. Instead, you may create multiple SSL certificates at the webserver level, and then assign them to "bindings", as described below.

Creating and installing additional SSL certificates

- 1** Run Internet Information Services (IIS) Manager.
- 2** Choose the name of the server in the left pane.
- 3** In the Features View, double-click on **Server Certificates**.

- 4 Create a certificate request by choosing **Create Certificate Request...** in the right pane. After submitting the certificate request and receiving the response from the Certifying Authority, come back and choose **Complete Certificate Request**. Alternatively, you can create a self-signed certificate, but this is not recommended because it will cause browser warning messages for your users.

Creating additional IIS bindings

This procedure, available only on Windows Server 2008, allows you to assign multiple IP addresses and SSL certificates to a single website, thus bypassing the complexity of creating multiple websites.

- 1 Run Internet Information Services (IIS) Manager.
- 2 Right-click the name of the website (usually moveitdmz) and choose **Edit Bindings...**
- 3 Choose the **https** line and choose **Edit...**
- 4 Change the IP address from **All Unassigned** to one of the configured IP addresses.
- 5 Choose the appropriate SSL certificate.
- 6 Choose **OK**.

For the second and subsequent organizations, repeat the above procedure in the **Site Bindings** dialog, but choose **Add...** to add bindings and SSL certificates for the remaining organizations.

How do I configure MOVEit DMZ to identify each IIS site as its own organization?

MOVEit supports the display of an organization's branding based solely on the hostname provided in the base URL.

- 1 Sign on as a SysAdmin.
- 2 Go to the **Orgs** page and click the **NAME** of a specific organization to get into its **Organization Profile**.
- 3 While viewing the **Organization Profile**, click the first **edit** link.
- 4 Change the **Base URL** to match the hostname of the site. Include the **https://** prefix. For example, if the hostname is support.moveitdmz.com, the Base URL should be https://support.moveitdmz.com.
- 5 Save changes and repeat steps 3-5 for any remaining organizations.

How do I configure MOVEit DMZ to hand out different SSL certs on its FTP server for each organization?

The MOVEit DMZ FTP will offer the **Default Certificate** configured on the **FTP Certs** tab in the DMZConfig utility to all incoming FTP/SSL connections unless alternate certificates are configured in the **Alternate Certificates** window. Each **Server IP** value should match an IP address previously configured on an IIS site bearing an SSL certificate of the same name. (e.g., If an IIS site for mi.dmz.net is already listening for connections on IP address 10.1.1.2, add an alternate entry that will cause the FTP server to offer up the mi.dmz.net certificate to connections coming in to IP address 10.1.1.2.)

How do I handle future upgrades?

MOVEit DMZ upgrades will handle or avoid all elements of the multi-homing process except for specific IIS setting changes made to sites other than the IIS site into which MOVEit DMZ was original installed. Release notes will detail any IIS site setting changes made between MOVEit DMZ versions; consult our support department for specific instructions to make changes by hand.

Sync Client

MOVEit Sync is a Windows application that can synchronize files in a local folder with a folder on the MOVEit Server. Users can set any local folder to be their Local Sync Folder. The Local Sync Folder supports normal Windows file operations, such as add, modify, delete, rename, copy, and move. Users can set the Remote Sync Folder to be any MOVEit folder to which they have access. (See the notes below on **Setting Up Sync Folders and Permissions**). When the Sync process runs it will update the two folders so they both contain the same set of files and folders.

You can set up MOVEit Sync to provide the following capabilities to your end users:

- Synchronize a folder on a local computer with their MOVEit Home folder, or another personal folder on the MOVEit Server. In this way, the MOVEit folder can also be used as a backup folder for local files.
- Synchronize a folder on a local computer with a shared (group) folder on the MOVEit Server. This setup allows users to share files with a workgroup.

Requirements

The Sync client has the following requirements:

- **MOVEit Server:** The Sync client can work with MOVEit DMZ v7.5 or later.

Note: If MOVEit DMZ 7.5 will be used, it must be licensed to use the MOVEit API in order to support the Sync client. MOVEit DMZ 8.0 and later does not have this requirement.

- **Client computer:** The Sync client can be installed on the same Windows systems supported by the Ad Hoc Transfer Plug-in for Outlook client. See the ***Ipswitch Client Installation Guide (PDF)*** (http://docs.ipswitch.com/MOVEitDMZ_OutlookSync23/Ipswitch%20Client%20Installation%20Guide.pdf) for detailed requirements.
- The Sync client user must be a registered user on the MOVEit server.

Like other MOVEit clients, Sync provides support for English, German, French, and Spanish language versions.

Client Installation and Deployment

You can roll out the Sync client to registered users in two ways:

- Run the Ipswitch Client Installer program on the user's computer.
- Use silent install and group policy to install the client on multiple computers

Note: A separate license is not required for the Sync client.

To download the Ipswitch Client Installer, go to [customer portal location]

View or print the ***Ipswitch Client Installation Guide (PDF)*** (http://docs.ipswitch.com/MOVEitDMZ_OutlookSync23/Ipswitch%20Client%20Installation%20Guide.pdf).

The Ipswitch Client Installer can install Sync and the Outlook Plug-in.

The user will need to complete the configuration by entering their MOVEit server information, local Sync folder, and remote Sync folder (their MOVEit folder).

Setting Up the MOVEit Connection

After a silent install or a standard install where the server has not yet been configured, the settings needed to connect to a MOVEit server are configured in the MOVEit Connector (system tray) > Configuration > MOVEit Sync dialog. These settings are described for the end user in the Sync help.

- **MOVEit Server.** The host name or the IP address for your MOVEit server.
Sync uses the MOVEit Connector to connect to a MOVEit Server and upload and download files. The Outlook Plug-in also uses the MOVEit Connector (MOVEit Connector (system tray) > Configuration > Ad Hoc Transfer). If both clients are installed, they will share the configuration information for connecting to the MOVEit server. The two clients must connect to the same MOVEit server.

- **Username.** The user name to access the MOVEit server.
- **Password.** The password to access the MOVEit server.

This information is already populated if the user configures the server during the standard install, or after an upgrade where the data stores are retained.

Setting Up the Sync Folders and Permissions

The folder settings are configured in the **MOVEit Connector** (system tray) > **Configuration** > **MOVEit Sync** > **Sync options** dialog. These settings are described for the end user in the Sync help.

- **Local Sync folder.** This can be any folder on the user's local system (for example, C:\Documents\Sync). Any files or subfolders placed in the Sync folder will be synchronized with the remote sync folder.
- **Remote Sync folder.** This is the folder on the MOVEit server (for example, the user's home folder (usually /home/username) or a shared group folder). Any files or subfolders placed in the remote folder will be synchronized with the Local sync folder. When setting the remote Sync folder, the user can browse to select from their MOVEit folders.

Note: There are two restrictions on the Sync capabilities: The total size of files in the Sync folder must be less than 1 Gb; the total number of files in the Sync folder must be less than 100.

The Remote Sync folder should have the **Allow File Overwrite** setting set to **No**, which is the default setting on MOVEit folders. Sync will overwrite files in the Sync folder (even though the setting is **No**).

The different Sync user scenarios mentioned at the beginning of the topic are deployed by setting permissions and access to the MOVEit folder and its subfolders.

When a user wants to sync a local folder with their MOVEit folder, so they can have a backup of certain files, you should provide all permissions to the MOVEit folder: List, Read, Write, Delete, Subs.

When you are setting up a **shared remote Sync folder** on MOVEit, we recommend that each user have their own individual non-shared Sync folder and you set up a virtual subfolder within the user folder that points to the shared folder. In this case, if a Sync user deletes the virtual folder it does not delete the underlying real folder. Also, adding a sub-folder locally does not convey additional permissions to other users.

Note: When you create a sub-folder in MOVEit, the default behavior is that the subfolder inherits the permissions of the parent folder. When a Sync client user renames or moves a folder, Sync does an "add" to the new location, and a "delete" from the old location. This means that any custom permissions on the folder may be lost as the new folder takes on the permissions of the parent folder.

If you want to make the permissions and access settings different for each user, the setup requires more consideration. You should remove "Subs" permission from the shared folder for all users. Users will be unable to delete the shared virtual sub-folder and will also be unable to create new sub-folders.

You may also want some users to have access to only the top-level folder, or to certain subfolders; or you may want to restrict delete or upload permissions. Here are some examples:

- To disallow a user or group access to a subfolder: from the permissions settings of the subfolder (virtual folder), remove all permissions for the user or group.
- To disallow a user or group's ability to delete a subfolder: from the permissions settings of the parent folder of the subfolder, remove the Subs permission for the user or group. The user or group cannot delete or add a subfolder in the parent folder.
- To disallow a user or group's ability to delete files from a subfolder: from the permissions settings of the subfolder, remove the Delete permission for the user or group.
- To disallow a user or group's ability to upload files to a subfolder: from the permissions setting of the subfolder, remove Write permission for the user or group.

See **Notes on the Sync Process and Known Issues** below for important notes on folder settings and user access.

Error messages

The Sync client will display error messages for the following types of problems:

- Connection errors: If the MOVEit server name is incorrect or the MOVEit server is not available, the user will see a connection error. If the user credentials are invalid or the improperly specified, the user will see a connection error.
- Permission errors on the MOVEit folder:
 - To complete file operations such as list, add, and delete, the user must have the appropriate permissions set for their remote Sync folder (MOVEit folder).
 - If Sync cannot complete a file operation because of a permission issue, it displays the **User does not have permission** error, then Sync will be disabled to avoid any data loss. To enable Sync again, the user should back out the file operation that caused the error. For example, if the user adds a file to a subfolder of the local Sync folder, but they do not have write permission for the older, Sync will display a write permission error. The user must remove the file from the local folder, otherwise the error will occur again. After correcting the error, the user can enable Sync (right-click the MOVEit Connector and click **Enable Sync**.)
 - If the user gets a **User does not have Delete permission** error, this means the file the user deleted in the local Sync folder cannot be deleted in the remote Sync folder. The Sync client will restore the file to the local folder. In this case, the user does not need to enable Sync again.

The MOVEit administrator can change permissions on the MOVEit folders; Sync users cannot.

Notes on the Sync Process and Known Issues

- If **Ignore deletes** is enabled (in the MOVEit Connector (system tray) > Configuration > MOVEit Sync > Sync options dialog), then only add, rename, and copy operations will be reflected after a Sync.
- If **Ignore deletes** is enabled, a local move actually leaves a copy in the original location on the MOVEit folder. Thus, if you move a file from subfolder A to subfolder B in the Sync folder, you will see the file listed in subfolder B on the local system, but on the MOVEit folder, a copy remains in subfolder A. This is also true when moving folders. A copy of the folder remains in the original location in the MOVEit folder. Files within the moved folder also remain.
- If **Ignore deletes** is enabled, a remote move will not leave a copy in the original location on the local folder. Thus, if you move a file from subfolder A to subfolder B in the MOVEit folder, you will see the file listed in subfolder B on the MOVEit folder, and you will see the same change on the local Sync folder. When moving folders, a copy of the folder remains in the original location on the local Sync folder, although any files within the moved folder are deleted from the original location.
- If **Ignore deletes** is enabled, if a user creates a new folder in the local Sync folder, when the new folder is created in the remote Sync folder, a duplicate folder named "New Folder" may also be created. The user can delete this empty new folder.
- When multiple users add (or modify) a file with the same filename at the same time (within a relatively short time interval, less than 30 seconds), a conflict will occur. The Sync client resolves the conflict by renaming the file that gets synchronized last. The renamed file has the original file name appended with the user's MOVEit username.
- When multiple users move the same folder at the same time, the Sync client resolves the conflict by moving the folder to the location specified by the last move request. An empty folder may remain in the previously named locations. This folder should be deleted.
- An Administrator or FileAdmin user cannot sync with a remote Sync folder that is a virtual folder or that contains virtual folders, even if they are in standard folders to which the user has list, read, write, and subs permissions. MOVEit assigns Admin permissions to this type of user; there is not a way to grant the user additional permissions to the virtual folder.
- If a user moves or renames a folder within the local Sync folder, the folder on the remote Sync folder may lose the original permissions. This is because Sync does a "delete" from the original location (or name) and an "add" to the new location (or name). MOVEit folders inherit the permissions of the parent folder, so any custom settings for the folder may be lost.
- When multiple users use Sync on the same machine, users other than the user that Sync was installed under may see a "Cannot connect to the server" message after entering their configuration information. To correct this, the user needs to close the MOVEit Connector (right-click the system tray icon, then select **Exit**). Then, restart the MOVEit Connector from the Start menu, and right-click the icon again and select **Reconnect**.
- Data loss is possible in the following rare situations and can be avoided as noted:

- If the user changes any configuration information (local Sync folder, remote Sync folder, username, MOVEit server location), Sync will clear the "states" information. When the next Sync occurs, there will be file conflicts because without the states information, Sync cannot tell if the file with the same name on the local and remote is the same. To fix this issue, the user should **Disable Sync**, then delete all local Sync content, then **Enable Sync** and let it synchronize to the remote folder.
- By default, on the remote Sync (MOVEit) folder, the **Allow File Overwrite** setting is set to **No**. If it is set to **Yes**, the scenario described above, where multiple users add (or modify) a file and a conflict occurs, could result in the loss of changes made to one of the files. Make sure the **Allow File Overwrite** setting remains set to **No**.
- The Sync client does not have file locking capabilities. File locking prevents multiple users from editing the same file at the same time and should be handled by the file editing application. If the application does not handle file locking, then data loss is possible as Sync cannot know that multiple users have a file open.

System Configuration

This section describes how to view or change system configuration for MOVEit DMZ.

Firewall Configuration

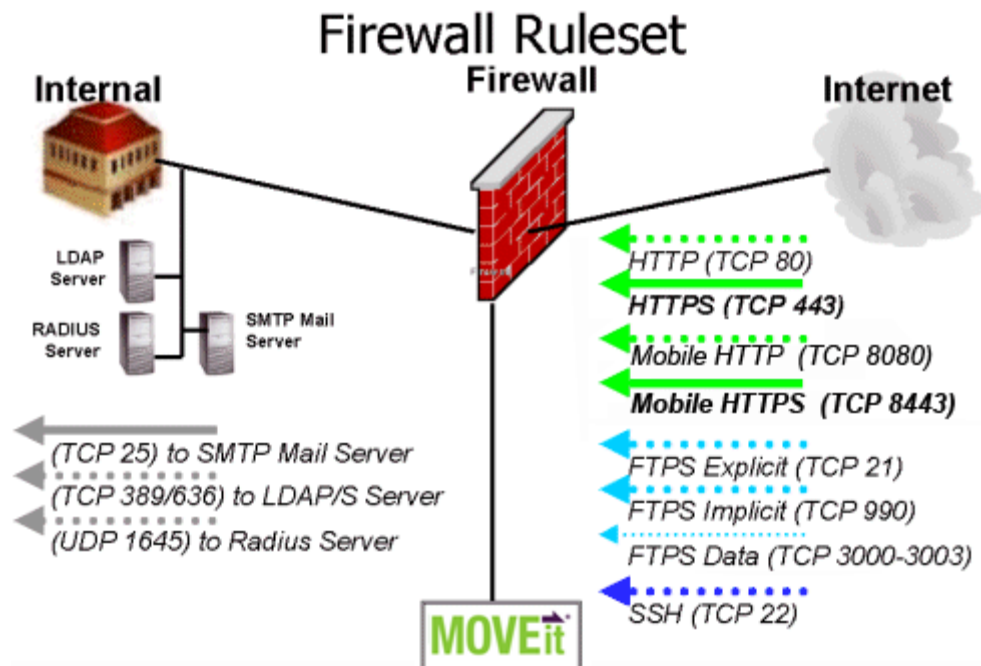
MOVEit DMZ was designed first and foremost to be secure on production DMZ segments exposed to the Internet. Like any well-behaved DMZ resident, MOVEit DMZ should "speak only when spoken to," and then only over ports MOVEit DMZ controls. You can enforce this behavior on your firewall using two very restrictive deny rules and a handful of permitted access rules.

Overview

The world normally uses HTTPS, FTP over SSL (FTP/SSL, ftps) and/or FTP over SSH (FTP/SSH, sftp) to communicate with MOVEit DMZ. MOVEit DMZ also normally needs to access the SMTP services of another mail server to deliver notification messages.

Nonsecure HTTP services are optional and generally not recommended. If nonsecure services ARE enabled, MOVEit will simply redirect users to the secure services. (IIS by itself doesn't redirect.) As suggested by the diagram below, access to different services from different locations (i.e., "Internal" vs. "Internet") can also be controlled by the firewall.

- GREEN ARROWS indicate web (HTTP/S) services.
- TEAL ARROWS indicate FTP over SSL services.
- BLUE ARROWS indicate FTP over SSH services.
- GREY ARROWS indicate other services (SMTP, RADIUS, LDAP).



Deny All

To prevent outside forces from opening unauthorized connections to MOVEit DMZ, use the following rule:

- **REQUIRED:** Deny (ALL CONNECTIONS) to MOVEitDMZ

To prevent MOVEit DMZ from opening unauthorized connections to outside computers, use the following rule:

- **REQUIRED:** Deny MOVEitDMZ to (ALL CONNECTIONS)

Now, depending on which services you elect to run on MOVEit DMZ, you will need to open a few ports. The criteria and specifics are covered below.

Remote Web Browsers (HTTP/S)

MOVEit DMZ normally listens for NONSECURE web connections on TCP port 80 and SECURE web connections on TCP port 443. Remote users **NEED** to be able to connect to the secure port (443) from remote addresses. Optionally, you may leave port 80 open as well if you would like MOVEit DMZ to "be friendly" and auto-redirect users connecting on the nonsecure port to the secure port instead.

- **REQUIRED:** Allow TCP (Remote) (Any Port) to MOVEitDMZ Port-443
- **Optional (and not recommended):** Allow TCP (Remote) (Any Port) to MOVEitDMZ Port-80

Remote Mobile Apps and Web Browsers (HTTP/S)

MOVEit Mobile normally listens for NONSECURE (HTTP) mobile client connections on TCP port 8080 and SECURE (HTTPS) web connections on TCP port 8443. If these ports are taken, you can configure different port numbers during mobile server installation and MOVEit system configuration. Mobile clients need to be able to connect to the configured secure port. The nonsecure port enables the auto-redirect of mobile clients to the secure port.

- **REQUIRED:** Allow TCP (Remote) (Any Port) to the MOVEit Mobile Port for HTTPS, as configured during Mobile Server Installation; the default is: 8443
- **Optional:** Allow TCP (Remote) (Any Port) to the MOVEit Mobile Port for HTTP, as configured during Mobile Server Installation; the default is: 8080

Remote Secure FTP over SSL Clients (FTP/S)

If MOVEit DMZ FTP needs to support clients over the Internet, Ipswitch strongly recommends you **REQUIRE PASSIVE MODE FTP TRANSFERS** and **LOCK PASSIVE DATA PORTS TO A SMALL RANGE** on MOVEit DMZ FTP.

Warning: Simply specifying FTP on your firewall will rarely be enough to allow secure FTP through (unless both client and server use the CCC option). Firewalls that understand FTP look for the phrase "PORT" in data channels and open temporary holes in the firewall for communications over the designated ports between the two machines on either side of the data channel. However, secure data channels are encrypted, meaning the firewall will be unable to open any temporary ports.

Explicit FTPS control connections take place on TCP port 21.

Implicit FTPS control connections take place on TCP port 990.

If you use FTPS on your MOVEit DMZ, it is **HIGHLY RECOMMENDED** that you configure it to use both explicit and implicit modes (for greatest client compatibility), passive mode (to allow the server to select port numbers) and to use a restricted range of ports (to avoid opening up a hole which a trojan horse could use).

CCC Command - Alternative to Range of High Open Ports

MOVEit DMZ supports the CCC FTP command. The CCC command allows FTP-aware firewalls to understand the PORT commands otherwise hidden by FTP over SSL. Specifically, the CCC command allows the PORT commands to be understood by firewalls by dropping the control channel (and only the control channel) out of encrypted mode and into cleartext mode.

Although it provides greater flexibility, there are two security risks involved when using the CCC command. The first is that someone could sniff the now cleartext port command to connect to the secure FTP server and either steal data by connecting as if they were the real client or cause a denial of service attack by preventing the real client from connecting. The second is that someone can sniff folder names, file names and custom commands such as "change password" while the control channel is unencrypted. (The security risk of the alternate solution - a limited number of open ports - is that another service could be installed on that server and could start listening on those ports.)

Active FTP - Not Recommended

(Active FTP is NOT recommended for Internet connections because remote firewalls will likely not permit active FTP data connections in, especially if they are encrypted!)

- **REQUIRED:** Allow TCP (Remote) (Any Port) to MOVEitDMZ Port-21
- **REQUIRED:** Allow TCP (Remote) (Any Port) to MOVEitDMZ Port-990
- **REQUIRED:** Allow TCP MOVEitDMZ Port-20 to (Remote) (Any Port)
- **REQUIRED:** Allow TCP MOVEitDMZ Port-989 to (Remote) (Any Port)

Passive FTP (Unrestricted) - Not Recommended

(Setting Passive FTP up in unrestricted mode is not recommended because proper operation of this mode requires a wide range of high ports (thousands) to be open on the firewall.)

- **REQUIRED:** Allow TCP (Remote) (Any Port) to MOVEitDMZ Port-21
- **REQUIRED:** Allow TCP (Remote) (Any Port) to MOVEitDMZ Port-990
- **REQUIRED:** Allow TCP (Remote) (Any Port) to MOVEitDMZ (High Ports)

MOVEit DMZ normally listens for SECURE FTP control connections on TCP port 21 (and 990 when using implicit mode). As a passive FTP server, MOVEit DMZ will then listen for a SECURE FTP data connection on the TCP high port (>1023) it negotiated with the client. These ports need to be left open for proper communication.

Passive FTP (Restricted) - Recommended

- REQUIRED: Allow TCP (Remote) (Any Port) to MOVEitDMZ Port-21
- REQUIRED: Allow TCP (Remote) (Any Port) to MOVEitDMZ Port-990
- REQUIRED: Allow TCP (Remote) (Any Port) to MOVEitDMZ Ports-3000_3003 (administrator's discretion)

MOVEit DMZ normally listens for SECURE FTP control connections on TCP port 21 (and 990 when using implicit mode). In restricted passive mode MOVEit DMZ listens for SECURE FTP data connections on a configurable finite range of contiguous TCP high ports (e.g., 3000,3001,3002,3003) that it specifies to a particular client. (Nothing extra needs to be configured on clients other than to specify passive mode transfers.) These ports need to be left open for proper communication.

Additional Ports for Client Certificates

If you require that all your FTP/SSL traffic authenticate with client certificates there is no need to set up additional FTP/SSL ports for this purpose. However, if you wish to require some FTP/SSL connections/users to authenticate with client certificates while others do not face this requirement (common during migrations), you will need to set up additional ports for FTP/SSL client certificate authentication.

Client certificate authenticated sessions use the same data ports as regular FTP/SSL sessions, so no additional data ports are needed. However, a second Explicit control port and a second Implicit control port are typically assigned to a MOVEit DMZ FTP server in this situation. For example, Ipswitch uses ports 21 and 990 to handle its non-client-cert-authenticated connections and ports 10021 and 10990 to handle its client-cert-authenticated connections.

Remote Secure FTP over SSH Clients (SSH)

MOVEit DMZ uses a one-port SSH tunnel to support FTP over SSH clients. The use of a single SSH tunnel has an advantage over the multiple encrypted data streams used by FTP over SSL: fewer ports need to be opened on a firewall. (FTP over SSH is a single port secure transfer protocol.) The one port normally used by SSH is TCP port 22.

- REQUIRED: Allow TCP (Remote) (Any Port) to MOVEitDMZ Port-22

Email Notification (SMTP)

The MOVEit DMZ server requires the use of an SMTP-compliant mail server to send email notifications. If your MOVEit DMZ server must pass through a firewall to reach a mail server, you should allow MOVEit DMZ access to it only over TCP port 25. If you would like the ability to queue messages if your mail server is unreliable, need special authentication parameters to relay mail, or generally plan on sending many notifications at once, please consider setting up the **local mail relay** (on page 712).

Note: The MOVEit DMZ server need not access an internal email server if you can point it to your upstream (ISP) mail relay instead.

- **REQUIRED:** Allow TCP MOVEitDMZ (High Ports) to (YOUR MAIL SERVER) Port-25

Remote Authentication (RADIUS)

If you intend to use RADIUS remote authentication, MOVEit DMZ must be able to communication via UDP to the remote RADIUS server. The UDP port normally used to support RADIUS is 1645, but this port is configurable (like most other ports in MOVEit DMZ).

- **OPTIONAL:** Allow UDP MOVEitDMZ (High Ports) to (YOUR RADIUS SERVER) Port-1645

Remote Authentication (LDAP)

If you intend to use LDAP remote authentication, MOVEit DMZ must be able to communication via TCP to the remote LDAP server. The TCP port normally used to support LDAP is 389 and the port normally used to support LDAP over SSL is 636, but these ports are configurable. (The use of LDAP over SSL is strongly recommended; most modern LDAP servers support this. For example, see Active Directory - SSL in **Feature Focus - External Authentication** (on page 80) for instructions to enable SSL access on Active Directory LDAP servers.)

- **OPTIONAL:** Allow TCP MOVEitDMZ (High Ports) to (YOUR LDAP SERVER) Port-389
- **OPTIONAL:** Allow TCP MOVEitDMZ (High Ports) to (YOUR LDAP SERVER) Port-63

Remote Microsoft SQL Server database

If MOVEit DMZ will connect to a remote Microsoft SQL Server database, such as in a web farm, the MOVEit DMZ node must be able to communicate over the SQL Server ports. Port 1433 is the default SQL Server port, if you have configured a different port for your SQL Server instance, use that port instead of 1433. You need to open port 1434 only if you plan on running SQL Server Studio or another SQL Server utility on the MOVEit DMZ application nodes themselves.

- **REQUIRED:** Allow TCP MOVEitDMZ to (Your MS SQL Server) (Port 1433) for SQLServer default instance
- **Optional:** Allow TCP MOVEitDMZ to (Your MS SQL Server) (Port 1434) for SQL Admin Connection

MOVEit DMZ Web Farms

If MOVEit DMZ Web Farms is in use, each node and the NAS must allow Microsoft networking protocols between them. This is normally accomplished by opening TCP port 445 between the various machines. However, this port should NOT be left open to or from the Internet.

Time Service

Some sites, such as those regulated by the FDA, may need to ensure that the clock on MOVEit DMZ is kept in sync with a known, external source. The hostnames of good external time sources such as time.nist.gov can be found on various lists of **public time servers** (<http://support.ntp.org/bin/view/Servers/NTPPoolServers>).

Time services (RFC 958) normally use UDP port 123. When setting up firewall rules to support external time service, you must allow UDP packets to travel from any high port on the MOVEit DMZ to remote UDP port 123, hopefully on one or a small collection of remote servers. Return traffic using the same UDP port must also be able to return to your MOVEit DMZ server.

Please note that your firewall itself MAY also be able to act as a time server, in which case the firewall queries external time servers itself instead of permitting every machine behind the firewall to get its own time.

Also note that servers that are members of a domain are automatically time synchronized with the domain controller, so no external time server is necessary.

SysLog Service

If you elect to send **MOVEit DMZ Audit Events to a SysLog server** (on page 737), you will likely need to allow UDP SysLog packets to travel from your MOVEit DMZ to the SysLog server on UDP port 514.

SNMP Service

If you elect to send **MOVEit DMZ Audit Events to a SNMP management console** (on page 737), you will likely need to allow UDP SNMP packets to travel from your MOVEit DMZ to the SNMP management console on UDP port 161.

ODBC stunnel (Largely Obsolete)

This procedure has largely been replaced by MOVEit DMZ API's ability to run ad-hoc custom reports against most MOVEit DMZ configuration elements and audit entries remotely over a secure connection.

If you elect to set up an ODBC stunnel connection (as described in **Advanced Topics - Database - Remote Access** (on page 696)), you will likely need to allow connections from MOVEit Central to MOVEit DMZ on TCP port 33062. This port is configurable and may be changed in both the stunnel_mysqlserver.conf and stunnel_mysqlclient.conf configuration files involved.

MOVEit Freely & MOVEit Buddy

MOVEit Freely and MOVEit Buddy are secure FTP clients. See the *Remote Secure FTP Over SSL Clients* section above for required port information

MOVEit Central

MOVEit Central normally communicates with MOVEit DMZ via HTTPS. See the *Remote Web Browser (HTTP/S)* section above for required port information.

MOVEit Wizard, MOVEit Xfer, MOVEit DMZ API or MOVEit EZ

The MOVEit Wizard, MOVEit Xfer, MOVEit DMZ API and MOVEit EZ clients all communicate with MOVEit DMZ via HTTPS. See the *Remote Web Browser (HTTP/S)* section above for required port information.

AS2 Clients

AS2 clients normally use HTTPS. In rare cases they may use HTTP instead. See the *Remote Web Browser (HTTP/S)* section above for required port information.

AS3 Clients

AS3 clients are secure FTP clients. See the *Remote Secure FTP Over SSL Clients* section above for required port information

Configuration Utility

The MOVEit DMZ Configuration program is a Windows application used to configure global settings from the local console. This utility is the only place certain licensing, debugging, FTP, and SSH options are set. Run the configuration program by choosing the Start menu shortcut **Configure MOVEit DMZ** from the local console (or terminal session) on your MOVEit DMZ server.

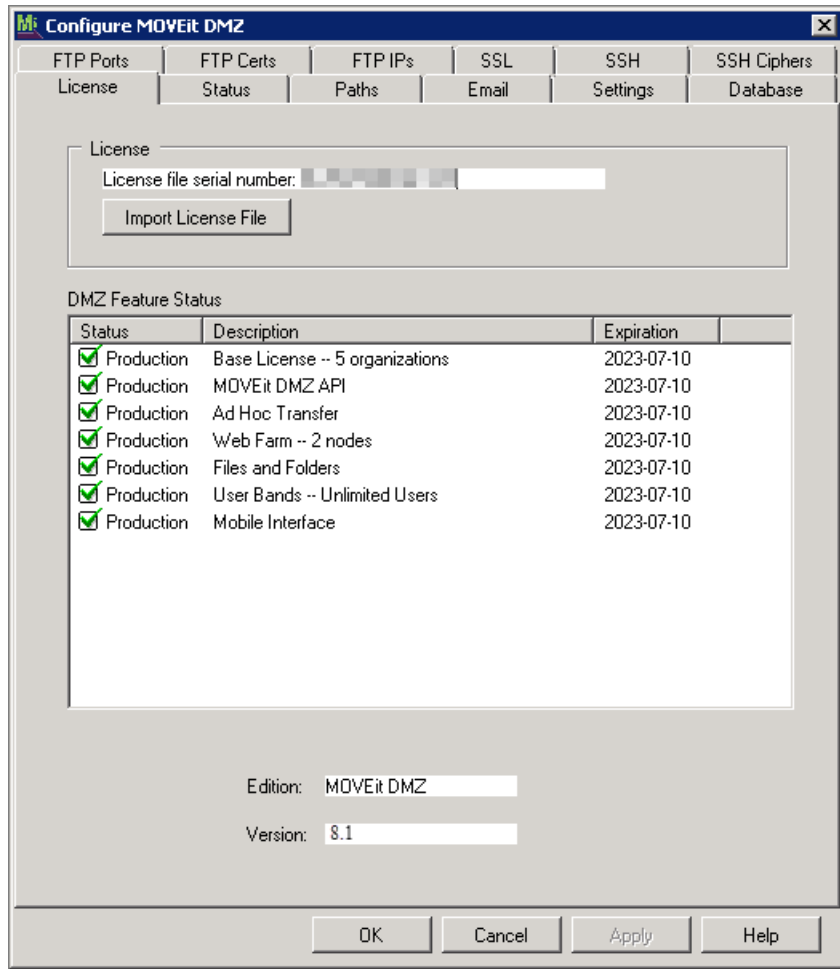
License Tab

You will have either a license file or license key.

Note: Beginning with MOVEit DMZ v.7.0, product licenses are distributed in the form of a license file rather than a license key. Existing customers who already have a license can use their current license key with releases up to and including v8.0. With v8.1, you must replace the key with a license file.

If you have a MOVEit DMZ license file, the license file serial number will be displayed in the **License** field. If you have a MOVEit DMZ license key, it will be displayed in the **License Key** field. Use the **License** field and the **Import** button to import a new license file. Any change to the license field will take place immediately.

The DMZ Feature Status lists the product features included in your current license and shows the status and expiration date for each.



The DMZ Feature Status is display only. Licensed features are set within the license file.

Status can be Production, Evaluation, or Off. Evaluation options behave exactly like production options, but evaluation options will shut off after their time has expired.

- **Base License - # organizations:** This item lists the number of organizations this MOVEit DMZ license is currently authorized to support. When you purchase MOVEit DMZ, a Base License for at least one organization is always included.
- **MOVEit DMZ API:** When enabled, this license option allows an unlimited number of copies of MOVEit DMZ API to connect to MOVEit DMZ. Your MOVEit DMZ API license may limit the number of clients which can actually be deployed, however.
- **Ad Hoc Transfer:** With this license option, people can use MOVEit DMZ to send secure, email-like packages with files included. Packages can be composed online using the web interface or read/composed using Microsoft Outlook.
- **Web Farm - # nodes:** This license option enables server deployment in a web farm environment and controls the number of nodes that may be so deployed. Each MOVEit DMZ server deployed in such an arrangement is counted as a node.
- **Files and Folders:** With this licensed option, people can use MOVEit DMZ to access files and folders using the web interface.
- **User Bands - # Users:** This item specifies the licensed (system) maximum number of users, per user band licensing:
 - 1 to 50 Users
 - 51 to 200 Users
 - 251 to 500 Users
 - Unlimited Users

Hint: MOVEit AS2 and AS3 support licensing is controlled in MOVEit Central; MOVEit DMZ requires no additional license.

- **Mobile interface:** With this licensed option, people can use MOVEit mobile apps (iOS and Android) and the mobile web (iOS and Android) to access MOVEit DMZ.

Status

The Status tab has two sections:

- **Diagnostic Log Settings:** Debug Level and Max Size for each component
- **Primary Services:** Status and Stop/Start button for each of service

The screenshot shows the 'Configure MOVEit DMZ' dialog box with the 'Status' tab selected. The dialog has a title bar with a close button. Below the title bar are several tabs: 'FTP Ports', 'FTP Certs', 'FTP IPs', 'SSL', 'SSH', 'SSH Ciphers', 'License', 'Status' (selected), 'Paths', 'Email', 'Settings', and 'Database'. The 'Status' tab is divided into two main sections: 'Diagnostic Log Settings' and 'Primary Services'. The 'Diagnostic Log Settings' section has a table with columns 'Component', 'Debug Level', and 'Max Size (MB)'. The 'Primary Services' section has a table with columns 'Service', 'Status', and 'Action'. To the right of the 'Primary Services' table are buttons for 'Start All' and 'Stop All', a 'Refresh' button, and a 'Last Refresh' timestamp. At the bottom of the dialog are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Component	Debug Level	Max Size (MB)
Web:	User Errors	8
FTP:	Connect Messages	8
SSH:	Connect Messages	8

Service	Status	Action
Web:	Running	Stop
FTP:	Running	Stop
SSH:	Running	Stop
Mobile:	Running	Stop
Database:	Running	Stop
SysStat:	Running	Stop
Helper:	Running	Stop
Scheduler:	Enabled	Stop

Start All
Stop All
Refresh: 2 (seconds)
Last Refresh: 16:07:17
(DMZ Config must be running with elevated privileges to show status)

Diagnostic Log Settings

Diagnostic logging levels and log file sizes for the major MOVEit DMZ components are set here. For each component, the Debug Level and Max Size settings can be adjusted.

- **Debug Level:** specifies the amount of debugging information to be logged. **All Debug** means log everything and **None** means log nothing. **Success** is the default and provides a good tradeoff between performance and troubleshooting capability. **Some Debug** is usually best for diagnosing errors on your own. Ipswitch support will typically ask you to run at least one test of a failed event at **All Debug**.
- **Max Size:** specifies the maximum size in megabytes of the log file before it is renamed and a new file is created in its place.

The three diagnostic MOVEit DMZ component options are:

- **Web:** sets the debug level for the Web Interface and scheduling components of MOVEit DMZ.
- **FTP:** sets the debug level for the FTP component of MOVEit DMZ.
- **SSH:** sets the debug level for the SSH component of MOVEit DMZ.

Hints: Set Core Application debug level to **User Errors** and the FTP and SSH debug levels to **Connect Messages** while in production. The debug levels listed here may also be set and the resulting logs may also be downloaded by any SysAdmin.

Primary Services

Here the status of each of the primary MOVEit DMZ services is available, and can be controlled. Each service displays its current status, along with a button to start or stop the service.

Note: **Mobile** enables you to stop and start the mobile server service.

Additionally, buttons are available to start and/or stop all MOVEit DMZ services. Finally, a refresh option is available to change how frequently the config program checks the status of the services, and the time of the most recent refresh is displayed.

High Availability and Load Balancing Services

If the MOVEit DMZ server is participating in a web farm, the High Availability Service section will be displayed. If Windows Network Load Balancing is used as the load balancer for the web farm, the Windows Network Load Balancing Service section will be displayed.

Here the status of each service is available, and can be controlled. As with the primary services, the current status is displayed, along with a button to start or stop the service.

Note: These services will also be started and stopped when the Start All and Stop All buttons in the Primary Services section are pressed.

Configure MOVEit DMZ

FTP Ports	FTP Certs	FTP IPs	SSL	SSH	SSH Ciphers
License	Status	Paths	Email	Settings	Database

Diagnostic Log Settings

	Debug Level	Max Size (MB)
Web:	User Errors	8
FTP:	Connect Messages	8
SSH:	Connect Messages	8

Primary Services

Web:	Running	Stop	Start All
FTP:	Running	Stop	
SSH:	Running	Stop	
Mobile:	Running	Stop	
Database:	Running	Stop	
SysStat:	Running	Stop	Refresh: 2 (seconds)
Helper:	Running	Stop	Last Refresh: 16:07:17
Scheduler:	Enabled	Stop	(DMZ Config must be running with elevated privileges to show status)

High Availability Service

Status:	Running	Stop

Windows Network Load Balancing Service

Status:	Running	Stop

OK Cancel Apply Help

Paths

The Paths tab has two sections:

- **Folders:** The locations of the primary components of the MOVEit system.
- **URLs:** The addresses used to access MOVEit services.

The screenshot shows the 'Configure MOVEit DMZ' dialog box with the 'Paths' tab selected. The dialog has a title bar with a close button. Below the title bar is a tabbed interface with the following tabs: FTP Ports, FTP Certs, FTP IPs, SSL, SSH, SSH Ciphers, License, Status, Paths (selected), Email, Settings, and Database. The 'Paths' tab is divided into two sections: 'Folders' and 'URLs'. The 'Folders' section contains six text input fields with browse buttons (...): 'Web App' (C:\MOVEitDMZ\wwwroot), 'Non Web' (C:\MOVEitDMZ), 'Files' (C:\MOVEitDMZ\Files), 'Logs' (C:\MOVEitDMZ\Logs), 'ISAPI' (C:\MOVEitDMZ\MOVEitISAPI), and 'Database' (C:\MySQL). Each field has a hint text below it. The 'Files' field has an 'Advanced' button. The 'URLs' section contains three text input fields: 'Machine' (http://localhost:8080/moveitdmz/machine.aspx), 'Machine 2' (http://localhost:8080/moveitdmz/machine2.aspx), and 'Base' (https://192.168.197.189/moveitdmz). There is a checkbox labeled 'Ignore Certificate Problems on Machine URL's' between the 'Machine 2' and 'Base' fields. At the bottom of the dialog are four buttons: OK, Cancel, Apply, and Help.

FTP Ports	FTP Certs	FTP IPs	SSL	SSH	SSH Ciphers
License	Status	Paths	Email	Settings	Database

Folders

Web App: C:\MOVEitDMZ\wwwroot
(e.g. d:\moveitdmz\wwwroot)

Non Web: C:\MOVEitDMZ
(e.g. d:\moveitdmz)

Files: C:\MOVEitDMZ\Files
(e.g. d:\moveitdmz\files; for UNC click Advanced) **Advanced**

Logs: C:\MOVEitDMZ\Logs
(e.g. d:\moveitdmz\logs)

ISAPI: C:\MOVEitDMZ\MOVEitISAPI
(e.g. d:\moveitdmz\moveitisapi)

Database: C:\MySQL
(e.g. d:\mysql -> only if using MySQL locally)

URLs

Machine: http://localhost:8080/moveitdmz/machine.aspx
(e.g. http://localhost/machine.aspx)

Machine 2: http://localhost:8080/moveitdmz/machine2.aspx
☐ Ignore Certificate Problems on Machine URL's

Base: https://192.168.197.189/moveitdmz
(e.g. https://moveit.example.com/)

OK Cancel Apply Help

Warning: Most of the **Folder** values listed below are also saved in locations currently outside the control of the MOVEit DMZ Config utility. If you wish to move the MySQL database to another location or move the encrypted filesystem to another location, please check Ipswitch's current recommendation in our **Support Site** (http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ) Knowledge Base first!

Folders

- **Web App:** this directory contains all of the web application files needed for MOVEit DMZ to run.
- **Non Web:** this directory contains MOVEit DMZ specific files that are needed for the internal functions of the program.
- **Files:** this directory contains the root filesystem for MOVEit DMZ. If the root filesystem is stored on a remote location, click the Advanced button to configure the UNC path of the remote location, as well as the username and password needed to access it. For more information about using a remote location for the root filesystem, see the **Remote Filesystem** (on page 790) doc page.
- **ISAPI:** this directory contains the MOVEit ISAPI files that are required for making secure transfers.
- **Database:** this directory specifies the location of MySQL, if MySQL is the database engine being used by MOVEit DMZ.

URLs

- **Machine:** this URL is used to access authentication and other services from MOVEit DMZ. This URL should refer to the local machines (localhost). The Machine URL's are generated during installation of MOVEit and rarely need to be changed, except in cases where IIS access rules have been changed.
- **Machine2:** is derived from the Machine URL.
- **Ignore certificate problems on machine URLs:** if checked, this option allows the use of Machine URLs starting with https even if the certificate on this webserver was not issued by a trusted Certificate Authority. This will allow you to set the IIS setting of **Require Secure connection**. In this case you will need to use https for the Machine URL.
- **Base:** is the URL that is used to connect users to the interface of MOVEit DMZ. If there is no DNS name available or it has not resolved yet, you need to use an IP address. Also, if you have installed an SSL certificate you should specify the https protocol here also. Whether to allow the secure connection with MOVEit DMZ with a test certificate which may not be able to be confirmed from a trusted source. Since the Machine URLs are usually set to the localhost, they do not normally need to use https encryption. But if they do, and if the certificate is not trusted, MOVEit DMZ FTP would not be able to communicate with the machine URLs unless this is set.

Email

The Email tab has two sections:

- **SMTP Configuration:** Settings for the SMTP mail server.
- **Key Email Addresses:** Email addresses used to send and receive messages from the MOVEit server.

Configure MOVEit DMZ

FTP Ports	FTP Certs	FTP IPs	SSL	SSH	SSH Ciphers
License	Status	Paths	Email	Settings	Database

SMTP Configuration

Server:
(e.g. mail.example.com)

Timeout: (Seconds)

Key Email Addresses

Default From:
(e.g. notify@example.com)

Send Errors To:
(e.g. admin@example.com)

OK Cancel Apply Help

SMTP Configuration

- **Server:** this is the the IP address or DNS name of the mail server to be used to send e-mail.
- **Timeout:** this is the number of seconds MOVEit DMZ will timeout after if it cannot connect to the mail server.

Key Email Addresses

- **Default From:** this specifies the return address that will be used to send out informational messages from MOVEit DMZ.
- **Send Errors To:** this specifies the e-mail address to whom error messages from MOVEit DMZ will be sent. The scheduler uses will send error reports to this address. Multiple email addresses may be specified by separating them with commas. For example, support1@mymoveit.com,support2@mymoveit.com is a valid address, although most sites use a mailing list or an alias controlled on the mail server to accomplish the same thing.

Hint: If you need more sophisticated email options such as authentication or queueing, please ***set up the local IIS SMTP server*** (on page 712). In fact, use of a local SMTP server is recommended at high volume sites to avoid waiting for responses from remote mail servers!

Settings

The Settings tab has two sections:

- **Statistics Gathering:** Settings for status and performance statistics.
- **Other Settings:** Server settings for IP mask, timeout, and disk space.

The screenshot shows the 'Configure MOVEit DMZ' dialog box with the 'Settings' tab selected. The dialog has a title bar with a close button. Below the title bar is a tabbed interface with the following tabs: FTP Ports, FTP Certs, FTP IPs, SSL, SSH, SSH Ciphers, License, Status, Paths, Email, Settings (selected), and Database. The 'Settings' tab contains two sections: 'Statistics Gathering' and 'Other Settings'. The 'Statistics Gathering' section has three input fields: 'Retention' (30 Days), 'Interval' (323 Seconds), and 'Long Process Skip Count' (72 Number of intervals). The 'Other Settings' section has three input fields: 'IP Masks to Ignore DNS' (empty), 'Max Session Timeout' (120 Minutes), and 'Disk Space Low Warning' (1024 MB). At the bottom of the dialog are four buttons: OK, Cancel, Apply, and Help.

FTP Ports	FTP Certs	FTP IPs	SSL	SSH	SSH Ciphers
License	Status	Paths	Email	Settings	Database

Statistics Gathering

Retention: (Days)

Interval: (Seconds)

Long Process Skip Count: (Number of intervals)

Other Settings

IP Masks to Ignore DNS: ...

Max Session Timeout: (Minutes)

Disk Space Low Warning: (MB)

OK Cancel Apply Help

Statistics Gathering

MOVEit DMZ periodically polls the local server for various status and performance statistics, and records them into a database for later processing. These settings determine how that statistics gathering mechanism operates. For more information, see the documentation on **SysStat Service** (on page 754).

- **Retention:** how long records will exist in the statistics database. Default: 30 days.
- **Interval:** how often the statistics gathering process will poll the local server. Default: 323 seconds.
- **Long Process Skip Count:** one of the statistics that MOVEit DMZ gathers is the amount of used disk space in various DMZ folders on the server. This involves recursively counting the bytecounts of all files and folders underneath the selected folders, a process which can take a significant amount of time and resources. Therefore, these particular statistics are not gathered every time the statistics gathering process runs. This value determines how many runs the process will skip before gathering the more intensive statistics. Default: 72.

Other Settings

- **IP Masks to Ignore DNS:** MOVEit DMZ uses the Windows DNS client to look up the hostnames of IP addresses. Sometimes internal IP addresses cannot be resolved by the available DNS servers, but timeouts involved obtaining this information can make operations which require reverse lookups (such as signons) very slow from the end user's perspective. Adding specific IP addresses and/or ranges of IP addresses into this list will cause MOVEit DMZ to skip DNS reverse lookups of those addresses and may speed signons and similar actions.
- **Max Session Timeout:** user sessions are automatically extended during file transfers to permit slow or very large transfers to succeed. This value indicates, in minutes, the maximum length of long file transfer sessions. Default: 120 minutes.
- **Disk Space Low Warning:** MOVEit DMZ periodically checks the remaining disk space on all local drives. If the remaining space on any of the drives falls below this level, an email will be sent to the Send Errors To email address containing a message about the low disk space. Default: 1024 MB.

Database

The database tab will reflect the settings of the current database engine being used by MOVEit DMZ.

MySQL

Configure MOVEit DMZ

FTP Ports	FTP Certs	FTP IPs	SSL	SSH	SSH Ciphers
License	Status	Paths	Email	Settings	Database

Configuration

Type: MySQL

Server:

Database Name:

MovEit User

Username:

Password:

Confirm:

MySQL Root User

Password:

Confirm:

- **Configuration**
 - **Server:** this is the IP address or host name and instance of the MySQL database server being used by MOVEit DMZ. Typically MOVEit DMZ will use a local MySQL database, so the server will usually be `localhost`.
 - **Database Name:** this is the name of the database used by MOVEit DMZ. This was configured during setup and should not be changed.
- **MovEit User**
 - **Username:** this is the name of the database user used by MOVEit DMZ to access the DMZ database. This was configured during setup and should normally not be changed.
 - **Password (and Confirm):** this is the password of the above database user. This password was configured during the MOVEit DMZ setup and should normally not be changed.
- **MySQL Root User**
 - **Username:** this is the name of the database root user. This was configured during setup and should normally not be changed.
 - **Password (and Confirm):** this is the root password that is used to access the MySQL database for MOVEit DMZ. This password was configured during setup and should normally not be changed.-->

Microsoft SQL Server

Configure MOVEit DMZ

FTP Ports | FTP Certs | FTP IPs | SSL | SSH | SSH Ciphers
License | Status | Paths | Email | Settings | Database

Configuration

Type: Microsoft SQL Server

Server\Instance: db.example.com

Database Name: moveitdmz

MOVEit User

Username: moveitdmz

Password: XXXXXXXX

Confirm: XXXXXXXX

Test Connection Advanced Settings

OK Cancel Apply Help

- **Server\Instance:** this is the IP address or host name of the SQL Server database server being used by MOVEit DMZ. When using a local SQL Server instance, this will typically be **localhost**. Otherwise, it will typically be the address of a separate database server or database cluster.
- **Database Name:** this is the name of the database used by MOVEit DMZ. This was configured during setup and should not be changed.
- **Username:** this is the name of the database user used by MOVEit DMZ to access the DMZ database. This was configured during setup and should normally not be changed.
- **Password (and Confirm):** this is the password of the above database user. This password was configured during the MOVEit DMZ setup and should normally not be changed.

FTP Tabs

See the **FTP Server Configuration** (on page 577) section of this document for information about these tabs.

SSL Tab

See the **SSL Configuration** (on page 175) section of this document for information about this tab.

SSH Tabs

See the **SSH Server Configuration** (on page 639) section for information about this tab.

Backup/Restore Utility

Backing up the MOVEit DMZ system can be done in one of two ways. First, you may elect to use existing backup procedures at your organization to handle backing up the system. If this is the case, you will want to consult the *Technical Reference* (on page 764) for a complete list of the files, folders, and registry settings that MOVEit DMZ uses, and that need to be backed up.

An alternative to a traditional backup-to-tape method is to use the MOVEit DMZ backup and restore utilities provided by Ipswitch. These command-line utilities perform complete backups and restorations of all the files, folders, certificates and registry settings necessary to replicate your current MOVEit DMZ configuration onto this or another platform.

Capabilities

The backup and restore utilities are capable of backing up and restoring:

- the MOVEit DMZ configuration database (MySQL only), configuration registry keys, folder structure, custom color schemes, logos, and templates.
- Optionally, encrypted files can also be backed up (they are not by default), as can both server and client SSL certificates (they are by default) to create a complete backup of the MOVEit DMZ state.
- MOVEit Mobile environment including the Mobile Server (Tomcat) directory and all settings (configuration file).

The backup and restore utilities automatically determine where the critical MOVEit DMZ files are located on the server, as well as how to connect to the MySQL database to perform lock operations. Both utilities also provide options to allow administrators to override these automatic detections.

Backups and restorations can be done across differing types of DMZ installations (but NOT differing versions), such as web farm and standalone installations, and installations with differing path structures. This capability requires the backup and restore utilities to NOT backup MOVEit DMZ installation path information, database access information, or email server settings. These are typically configured on a per-installation basis, and should not be replicated across differing servers.

Limitations

The backup utility's ability to back up the MOVEit DMZ database tables only applies to MySQL databases. When using Microsoft SQL Server as the database for MOVEit DMZ, the utility must be run with the `--without-database` option, and the MOVEit DMZ database should be backed up using other tools. If the utility detects that SQL Server is being used, and the `--without-database` option has not been specified, it will display an error message and exit.

The backup utility obtains a read lock on all MOVEit DMZ database tables before backing up the MySQL database information. This is to ensure that the data does not change during the backup process. As a result, any requests that come in to MOVEit DMZ while the tables are locked will wait until the tables are available again before continuing (the read locks are released once the database tables have been backed up). For this reason, it is best if the backup process is run during off hours.

The backup and restore utilities do NOT back up NTFS permissions, NT users/groups, or IIS settings. If you are using these utilities to maintain a "hot standby", you will need to set these items up on the second box ahead of time. (Frequently people create a hot standby by restoring a full tape backup onto a new machine, then use periodic runs of the backup utility to keep data on the hot standby fresh.)

The backup utility is also not able to override the **do not export private key** setting you may have set when you imported your SSL server certificates. If the utility encounters an SSL server certificate export error related to private keys it will immediately print the error encountered and then exit. You can use the **--ignore-cert-export-errors** option to prevent the utility from exiting like this, however the problem certificates will still not be backed up.

MOVEit Mobile

MOVEit DMZ and the MOVEit Mobile Server are installed on the same application server node; in the case of Web Farms, multiple nodes are used. Apache Tomcat is the application server software that runs MOVEit Mobile. The MOVEit Mobile Server (the MOVEit Mobile Tomcat directory) can be backed up and restored. All MOVEit Mobile data is stored in archive under the Mobile folder.

Mobile backup is disabled by default. To enable backup, you use the **--backup-mobile** option, which requires a password that is used to encrypt the Tomcat configuration files. Mobile restore is also disabled by default. To enable restore, you use the **--restore-mobile** option, and will need to provide the password used to encrypt the backup.

The utilities determine the directory path for MOVEit Mobile by using the Windows Registry entry. To specify the path, use the **--mobiledir** option.

The restore utility will stop and start the Mobile Windows Service (MIMobile) during the restore, which means the service will be unavailable during the restore.

When including MOVEit Mobile in your backup and restore, note the following:

- To manage MOVEit Mobile files, the **dmzbackup** and **dmzrestore** commands must be run from a Windows Administrator account.
- MOVEit Mobile must be installed prior to running the **dmzrestore** command with the **--restore-mobile** option.
- MOVEit Mobile is offered with 32-bit and 64-bit distributions. Before running **dmzrestore**, be sure you install the appropriate version and distribution of the MOVEit Mobile on the destination machine. It must be the same version that was on the machine that was backed up.

- The backup utility archives the entire MOVEit Mobile Tomcat directory and the restore utility overwrites the destination machine's Tomcat directory with this archive. When running the restore utility, keep in mind that any manual configurations made to existing files in the Tomcat directory on the destination machine will be overwritten. This also applies to any install options you choose regarding the hostname/IP address and ports. If you require different hostname/IP address and ports configurations on the destination machine, you will need to manually edit these values in the Tomcat\conf\server.xml file after the restoration is complete.
- The backup utility does not archive the following:
 - Mobile Windows Service User Account configuration that are set up during the MOVEit Mobile installation.
 - Windows Registry settings for MOVEit Mobile Tomcat

Installation

The backup and restore utilities are installed by the MOVEit DMZ setup program, and are placed in the MOVEitDMZ\Scheduler folder. The two application filenames are DMZBackup.exe and DMZRestore.exe. The programs need to be in this location in order to use some requisite libraries provided by MOVEit DMZ. These utilities may not work correctly if run from any path other than MOVEit DMZ's Scheduler folder. If the utilities are run from outside the Scheduler folder, an error message will be displayed and the utility will exit.

In addition to the backup and restore utilities themselves, two additional programs are installed for use by the utilities. The first is an archiving application which supports the creation of files larger than 2GB. This application is called 7-Zip and is run using the 7z.exe program file. The second is an SSL certificate extracting application which dumps the various Microsoft SSL certificate stores into a format which is usable by the backup and restore utilities. This application is called ExportCerts.exe.

Using the Backup Utility

To perform a simple backup, open a command prompt and cd to the Scheduler subdirectory of your MOVEit DMZ non-web directory. Next, execute the following command.

```
C:\MOVEitDMZ\Scheduler>dmzbackup
```

This will create a file called MOVEitDMZ_Backup_xxxxxxx.7z in your Scheduler directory, where xxxxxxxx is the current date in YYYYMMDD format. This file will contain all the necessary files and information to reconstruct your DMZ configuration. It will not backup the actual encrypted files in your DMZ configuration, however, it will backup the existing folder structure. To backup the encrypted files as well, add the **--with-files** command-line option to the above command.

Since doing a complete backup with files requires a large amount of free disk space on the server (roughly twice as much free disk space as the size of your \MOVEitDMZ\Files directory), many customers opt to run a config-only backup, and then backup the encrypted files in a different way (NTBackup, read-only FTP server, etc.). Customers who use this method should add the **--with-file-tables** option, to force the backup utility to back up the file-related database tables, which are normally skipped when a config-only backup is performed.

If you would like to see what the utility is doing while it runs, add the **--debug** command-line option to the above command. For a complete list of the options available in the DMZ backup utility, see the Backup Utility Commands section below, or execute the following command in your Scheduler subdirectory:

```
C:\MOVEitDMZ\Scheduler>dmzbackup --help
```

Backup Utility Commands

The DMZ Backup Utility is a .NET console application which runs in the Scheduler directory on a MOVEit DMZ system. The utility is command-line driven, so it can easily be integrated into a batch file. A list of available options can be generated by entering the command **dmzbackup --help**. The default values listed for the database location, DSN, and DMZ directories are gathered from the registry on the DMZ system. The values may be overridden by using the command-line options.

```
C:\MOVEitDMZ\Scheduler>dmzbackup --help
```

```
MOVEit DMZ Backup Utility
```

```
Version 8.0.0.0
```

```
Copyright c Ipswitch, Inc. 2013 by Ipswitch, Inc.
```

```
Usage: dmzbackup [options]
```

```
Options:
```

```
--backup-database-files
```

```
Backup the database by copying the table files instead of
using the mysqldump utility. This option should not be used
unless specifically required by the circumstances.
```

```
--backup-database-settings
```

```
By default the database connection settings are NOT backed up.
It is assumed that the system being restored to already has
its desired database connection configured. However, the
--backup-database-settings option can be used to include the
database connection settings in the backup file.
```

```
--backup-mobile=<password>
```

```
By default MOVEit Mobile files and settings are NOT backed up.
Use this option to include the Mobile Tomcat directory in the
backup file. Please provide a password to encrypt insecure
```

files.

--dbdatalocation=<directory>

Location of database data files (default C:\MySQL\data\)

--dbdsn=<dsn>

Database connection DSN name (default MOVEitDMZ)

--debug

Turn debug mode on

--dmznonwebdir=<directory>

DMZ non-web directory path (default C:\MOVEitDMZ)

--dmzprogramfilesdir=<directory>

DMZ Program Files path (default 'C:\Program Files
(x86)\MOVEit')

--dmzwebdir=<directory>

DMZ web directory path (default C:\MOVEitDMZ\wwwroot)

--exit-on-cert-export-errors

Exit immediately if an error is detected while backing up SSL
client and server certificates. This option has no effect if
--without-certs is enabled.

-h, --help

Display this help screen and exit

--ignore-cert-export-errors

Do not exit immediately if an error is detected while backing up SSL client and server certificates. This option has no effect if --without-certs is enabled. (default)

--mobiledir=<directory>

MOVEit Mobile directory path. If this option is not provided, DMZBackup will determine the Mobile directory path through the Windows Registry. This option has no effect if --backup-mobile is not enabled.

--output=<output_filename>

Relative or absolute output filepath

(default MOVEitDMZ_Backup_YYYYMMDD.[zip|7z])

The date macros [YYYY], [MM], and [DD] may be used and will be replaced by the current year, month, and day, respectively. The time macros [HH], [TT], and [SS] may also be used and will be replaced by the current hour, minute, and second respectively.

--tempdir=<directory>

Base temporary directory to use

(default C:\Users\Administrator\AppData\Local\Temp\1\)

--use-zip

Use Zip.exe to create the backup file instead of 7z.exe. This will generally result in a slightly larger backup file, and will fail if the size of the backup file exceeds roughly 2GB, but is faster than 7z. Use if your file collection is small (<2GB).

`--use-7z`

Use 7z.exe to create the backup file instead of zip.exe. This will generally result in a slightly smaller backup file, and supports backup files larger than 2GB, but is slower than zip. Use if your file collection is large (>2GB). (default)

`--with-certs`

Back up SSL client and server certificates from the Microsoft Certificate Store. Certificate backup files will be encrypted. (default)

`--without-certs`

Do not back up SSL server and client certificates

`--with-files`

Back up encrypted files along with DMZ filesystem structure

`--without-files`

Do not back up encrypted files along with DMZ filesystem structure (default)

--with-file-tables

Back up the file tables from the database. This is implied when using `--with-files`, but is not on by default when `--without-files` is in effect. Since `--without-files` is on by default, file tables are not backed up by default.

--without-database

Do not back up database (use if managing database backup by a different method)

--without-ftpnatmap

Do not back up FTP NAT mappings (use if backup DMZ has different IP address)

--without-ipbindings

Do not back up IP bindings for FTP and SSH services (use if backup DMZ has different IP address)

--7z-no-compression

Force 7z.exe to use no compression when creating the backup file. Will generally result in a larger backup file, but is much faster. Use if your file collection has many large, incompressible files (compressed video files, disk images, etc). This option has no effect if `--use-zip` is enabled.

NOTE: Paths with spaces can be entered by surrounding the entire argument with quotes. For example:

```
"--tempdir=D:\Temp Dir\Sub Folder"
```

Backup Utility Specifics

The backup utility creates a backup file by copying all desired files, folder structures, and settings into a temporary directory, and then archiving the contents of that directory using either Zip or 7-Zip. The temporary directory is then removed at the end of the procedure. The following details the specific actions taken by the backup utility:

- 1** The temporary directory is randomly generated and then created. All backup files will be copied to this location, and then archived.
- 2** Most registry keys in the HKLM\SOFTWARE\Standard Networks\siLock key are read up and copied to a Windows Registry Editor compatible file, which is placed in the temporary directory. Registry keys containing paths, database information, and administrator email information are skipped to allow restoring to machines with different configurations than the original.
- 3** If the MySQL database is being backed up, a read lock is obtained on all MOVEit DMZ database tables, and the appropriate table data is exported to the temporary directory using the `mysqldump` utility. If the `--with-files` or `--with-file-tables` options are specified, all table data will be exported. Otherwise, the `files`, `newfiles`, `folderfile`, and `log` tables are skipped. Once all table data has been exported, the read locks are released.
- 4** The complete encrypted filesystem folder structure is copied to the temporary directory. If the `--with-files` option is specified, the encrypted files themselves will also be copied, in their appropriate locations. If the `--with-files` or `--with-file-tables` options are specified, per-organization tamper checking hash information files will also be copied.
- 5** The contents of the `images` subdirectory of the DMZ web directory is copied to the temporary directory to preserve any custom images provided by the server operator or organization administrators.
- 6** Any custom CSS stylesheets, used to create MOVEit DMZ color schemes, are copied to the temporary directory.
- 7** Any custom templates are copied to the temporary directory.
- 8** The `ExportCerts.exe` utility program is run which exports all SSL certificates in the Microsoft Certificate Store and stores them as files in the temporary directory.
- 9** The contents of the temporary directory are archived and optionally compressed into a single file. The temporary directory is then removed.

Using the Restore Utility

To perform a simple restoration, you must first have completely installed MOVEit DMZ on your target system. For best results, the version of DMZ should be the same as the version that you backed up. (If this is not the case, such as if you are migrating your DMZ server to a new platform, and are upgrading to a new version at the same time, you will need to re-run the MOVEit DMZ installation program after the restoration and choose the Repair option. Be sure to read our ***MOVEit DMZ Migration Guide*** (http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ) if this is what you are doing.) You must also have transferred the backup file to the target system. Once you are ready to begin the restoration, open a command prompt and cd to the Scheduler subdirectory of your MOVEit DMZ non-web directory. Next, execute the following command, making sure to substitute your correct backup file path for the entry in the brackets below:

```
C:\MOVEitDMZ\Scheduler>dmzrestore <path to your backup file>
```

The restore utility will stop your webserver and database before actually restoring files. It will then decompress the backup file to a temporary location and then copy the backed up files to their appropriate locations. Finally, it will restart the database and web servers. If you would like to see what the utility is doing while it runs, add the `--debug` command-line option to the above command. For a complete list of the options available in the DMZ restore utility, see the MOVEit DMZ Restore Utility section below, or execute the following command in your Scheduler subdirectory:

```
C:\MOVEitDMZ\Scheduler>dmzrestore --help
```

Note: A DMZ restoration will overwrite all existing configuration information with the information found in the backup file. DO NOT run a restoration on a system that has information you want to keep.

Restore Utility Commands

Like the backup utility, the DMZ Restore Utility is a .NET console application which runs in the Scheduler directory on a MOVEit DMZ system. The utility is command-line driven, so it can easily be integrated into a batch file. A list of available options can be generated by entering the command `dmzrestore --help`. The default values listed for the database location, DSN, and DMZ directories are gathered from the registry on the DMZ system. The values may be overridden by using the command-line options.

```
C:\MOVEitDMZ\Scheduler>dmzrestore --help
```

```
MOVEit DMZ Restore Utility
```

```
Version 8.0.0.0
```

```
Copyright c Ipswitch, Inc. 2013 by Ipswitch, Inc.
```

```
Usage: dmzrestore [options] <dmzbackupfile>
```

Options:

--dbdatalocation=<directory>

Location of database data files (default C:\MySQL\data\)

--dbdsn=<dsn>

Database connection DSN name (default MOVEitDMZ)

--debug

Turn debug mode on

--dmznonwebdir=<directory>

DMZ non-web directory path (default C:\MOVEitDMZ)

--dmzwebdir=<directory>

DMZ web directory path (default C:\MOVEitDMZ\wwwroot)

-h, --help

Display this help screen and exit

--mobiledir=<directory>

MOVEit Mobile directory path. If this option is not provided DMZRestore will determine the Mobile directory path through the Windows Registry. This option has not effect if --restore-mobile is not enabled.

--restore-database-settings

By default the database connection settings that were saved to

the backup file (if any) are NOT restored. It is assumed that the target system already has its desired database connection configured. However, the `--restore-database-settings` option can be used to restore the database connection settings from the backup file.

`--restore-mobile=<password>`

By default MOVEit Mobile files and settings are NOT restored. If the dmz backup file includes Mobile files and settings, use this option to perform a Mobile restore. The restore will include Mobile's Tomcat directory. Please provide the password you used when backing up the Mobile files. The Mobile Windows Service will be stopped and started during the restoration. MOVEit Mobile of the same version and architecture as the backup must be installed prior to the restoration.

`--tempdir=<directory>`

Base temporary directory to use (default
C:\Users\Administrator\AppData\Local\Temp\1\)

`--use-zip`

Use Zip.exe to extract the backup file instead of 7z.exe. Use if you used the `--use-zip` option when creating the backup file. If neither this, or the `--use-7z` option is selected, the decompressor will be selected automatically, based on the backup file extension (.zip will cause zip.exe to be used, all other extensions will cause 7z.exe to be used).

--use-7z

Use 7z.exe to extract the backup file instead of zip.exe. Use if you used the --use-7z option when creating the backup file, or allowed the default action to occur. If neither this, or the --use-zip option is selected, the decompressor will be selected automatically, based on the backup file extension (.zip will cause zip.exe to be used, all other extensions will cause 7z.exe to be used). (default)

--with-files

Restore encrypted files along with DMZ filesystem structure if they exist in the backup file (default)

--without-files

Do not restore encrypted files along with DMZ filesystem structure even if they exist in the backup file

NOTE: Paths with spaces can be entered by surrounding the entire argument with quotes.

For Example:

```
"--tempdir=D:\Temp Dir\Sub Folder"
```

Restore Utility Specifics

The restore utility, like the backup utility, first creates a temporary directory. It then extracts all files from the backup file into the temporary directory, and then copies the backed up files to their appropriate locations, overwriting any existing files. In order to correctly perform the restore, it first stops the webserver and database server. The services are restarted once the restore is complete, and the temporary directory is removed. The following details the specific actions taken by the restore utility:

- 1** The temporary directory is randomly generated and then created. The backup file is extracted to this location.
- 2** The IIS webserver is stopped to allow proper restoration of appropriate files.
- 3** The keys contained in the registry backup file are restored into the window registry.
- 4** The database export is read back into the database, restoring the table structure and data entries.
- 5** The encrypted filesystem folder structure, and any files backup up, are copied into the appropriate encrypted filesystem directory.
- 6** The contents of the backed up images directory are copied into the appropriate images directory.
- 7** Any backed up custom stylesheets are copied to the appropriate templates directory.
- 8** Any backed up custom templates are copied to the appropriate templates directory, automatically creating any necessary custom subdirectories.
- 9** Any backed up SSL certificates are copied to the Certs\C00X subdirectory of the DMZ non-web directory, where X is 0 (meaning the server is standalone). From here, the MOVEit DMZ Helper service will process the certificate files and load them into the Microsoft Certificate Store.
- 10** The IIS webserver is restarted, and the temporary directory is removed.

Creating an Automated Backup Process

Ipswitch recommends backing up the configuration structure of a MOVEit DMZ server every night, preferably during off-peak hours. The following steps will show how to create such a backup process using the DMZ Backup Utility, the MOVEit Xfer command-line secure transfer client and the Windows Scheduled Tasks system. This backup process requires the MOVEit DMZ web service to be up. The process will consist of a batch file which stops the web server, backs up the DMZ system, restarts the web server, and finally uploads the backup file to a location on the DMZ server itself. From there, the backup file should be pulled down and stored in a safe location (the MOVEit Central super-client is recommended for this step).

Preparing for the Backup Process

Several things should be done before actually creating the backup process. First, a copy of all the needed software should be obtained and installed. On the MOVEit DMZ server, this should include the DMZ Backup Utility and a copy of MOVEit Xfer (MOVEit Xfer is a free command-line secure transfer client available from Ipswitch). Next, a user needs to be created to handle uploads, temporary storage, and downloads of backup files. This user should only be allowed to access DMZ from whatever internal machine will be handling the downloading of backup files from the system (access from the local machine is automatically allowed). Follow these steps to create a backup user:

- 1** Log on to DMZ as an administrator.
- 2** Switch to the **Users** page and click **Add New User**.
- 3** Enter a username such as `backup_user` and fill in the rest of the user account information. You may leave the email address blank if you do not want this user to receive emailed notifications. Set the permission level to **User**.
- 4** Open the user profile after creating the user and click **Select Ruleset** in the **Remote Access** line under the **Security Information Section**. Select **Use Custom Rules** and click the **Change** button.
- 5** Click the **View Custom Rules** link that appears next to the **Use Custom Rules** radio option. Add a rule to allow access from the host that will be handling the downloading of backup files from the system.
- 6** (You may also want to restrict this user to the **HTTP Clients** interface only and/or exempt this user from password expiration.)

Backup Process Batch File

The batch file commands that will execute the backup process are shown below. These commands should be copied to a batch file located in the MOVEitDMZ\Scheduler directory. Appropriate values must be substituted in for the pseudo-values surrounded by less-than (<) and greater-than (>) symbols. You may also remove or add any additional -- options you want to be part of the process.

```
rem *** AUTOMATED MOVEit DMZ Backup Procedure ***

SET Task=DMZBackup

del %Task%.err


rem Execute the backup process. This will create
rem a file with the name MOVEitDMZ_Backup_YYYYMMDD.7z,
rem where YYYYMMDD is the current year, month, and day.
rem A log of the results and another containing just the errors will also be saved
dmzbackup > %Task%.Log 2>%Task%.Err --tempdir=<temp directory> --without-files
rem If there were any errors in the logs, notify the administrators
for /F %A in ("%Task%.Err") do If %%~zA equ 0 del %Task%.Err
IF EXIST %Task%.Err GOTO errors

GOTO ok

:errors
echo ERRORS

ReportErrors.exe %Task% %Task%.err %Task%.Log

GOTO done

:ok echo OK


rem If all OK...

rem Upload the file to the DMZ server

xfer > %Task%xfer.Log 2>%Task%xfer.Err -quitererror -z -user:<backup account
username>
```

```
-password:<backup account password> -s:dmz_bkup_commands.txt localhost
```

```
rem If there were transfer errors, notify the administrators
```

```
IF NOT %ERRORLEVEL%==0 GOTO xferbad
```

```
:xferok
```

```
rem Delete backup file
```

```
del /Q MOVEitDMZ_Backup_*
```

```
GOTO done
```

```
:xferbad
```

```
ReportErrors.exe %Task%_During_Xfer %Task%xfer.Log %Task%xfer.Err
```

```
GOTO done
```

```
:done
```

MOVEit Xfer Commands File

The command file which MOVEit Xfer will execute to upload the backup file is a very simple file and should have the name `dmz_bkup_commands.txt`. It is shown below.

```
prompt
```

```
mput MOVEitDMZ_Backup_*
```

Scheduling the Backup Process

The Windows Scheduled Tasks service is used to schedule the running of the backup process. The process should be scheduled during off hours. Follow these steps to schedule the backup process:

- 1 Click **Start | Programs | Accessories | System Tools | Scheduled Tasks**. This will bring up the Scheduled Tasks window.
- 2 Double-click **Add Scheduled Task**. This will start the Schedule Task wizard. Click **Next** to start the wizard.
- 3 Click **Browse** to locate the backup process batch file. Click **Next**.
- 4 Select how often to run the backup process, and at what times. Ipswitch recommends running the backup process nightly.

- 5 Select an appropriate Windows user account to run the backup process as. The account should have permissions to create directories and files in the temp directory, and to read files from the various MOVEit DMZ directories. It should also have permissions to run the MOVEit Xfer program, as well as the ZIP program found in the MOVEitDMZ\Utilities directory.
- 6 Click **Finish** to complete the setting up of the schedule task.

Finished

The automated backup process should now be set up and ready to run. You may test the process by right-clicking the scheduled task entry for the backup process in the Scheduled Tasks window and selecting **Run**.

Handling the Backup File

At this point, a client on the internal network can be used to pull the backup file off of the MOVEit DMZ system and store it to a safe location, such as a fileserver location that gets regularly backed up to tape. MOVEit Central makes automating this task simple and effective. A MOVEit Central system on the internal network can be used to pull down the backup file at some time after the file is created, and then forward that file off to a safe location. Follow the steps below to configure MOVEit Central to perform this task.

- 1 Make sure Central is has the target MOVEit DMZ server configured as a DMZ host. Also make sure that whatever destination system you choose for the file is also configured as a host.
- 2 Create a new Task for the backup file gathering task.
- 3 Create a Source element and set the source as the target MOVEit DMZ server. If the DMZ server is already being used in other Central tasks, you should probably set the source to use a non-default user account, and then enter in the backup account username and password. Browse the DMZ server and select the backup user's home folder. Turn on the option to delete the source file after successful transfer.
- 4 Create a Destination element and set it to the location you wish to forward the file to. The name the file will end up with at the destination can be configured at this point using the Filename setting. If the destination is where the backup file will be stored, it is a good idea to include the date of the backup in the filename, with the four-digit year first for easier sorting. In that case, Macros can be used the generate the correct filename: `moveitdmz_backup_[yyyy][mm][dd].7z`. If the destination is a hot-standby machine which will be restoring from the backup file, the filename should be a fixed name, to allow an automated restore process to function correctly. In this case, a name such as `moveitdmz_backup.7z` is recommended. Also, in this case, the Overwrite Existing Files option should be turned on.
- 5 Create a schedule element and set it to run approximately one hour after the backup process is scheduled to run on the DMZ server.
- 6 If you wish to test the Task, you can do so by right-clicking on it and selecting **Run Now**. You should place a test file in the correct location to make sure the file transfers are working correctly.

Creating an Automated Restore Process

An automated restore process can be useful for keeping an up-to-date hot-standby copy of MOVEit DMZ for use during loss of the primary DMZ system. The process relies on one or more clients such as MOVEit Central to transfer the backup file from the primary DMZ to the backup DMZ. Once the backup file has been transferred to the backup DMZ, the restore process will download the file and restore it to the local system.

Preparing for the Restore Process

A copy of all the needed software should be obtained and installed. This should include the DMZ Restore Utility and a copy of MOVEit Xfer. No user configuration should be necessary, assuming the hot-standby machine has previously been manually synced to the primary machine. This process will use the same user account that the backup process used.

In order to allow the restore process to download and process the backup file correctly, it should always be put on the server with a constant name. Using MOVEit Central, this can be accomplished by configuring the Filename section of the Destination element to a fixed name, such as `moveitdmz_backup.7z`.

Restore Process Batch File

The batch file commands that will execute the restore process are shown below. These commands should be copied to a batch file located in the MOVEitDMZ\Scheduler directory. Appropriate values must be substituted in for the pseudo-values surrounded by less-than (<) and greater-than (>) symbols.

```
rem First, download the backup file from the
rem DMZ server

xfer -z -user:<backup account username> -password:<backup account password>
-s:dmz_rstr_commands.txt localhost

rem Next, execute the restore process..

dmzrestore --tempdir=<temp directory> <DMZ backup filename>

rem Delete backup file

del /Q <DMZ backup filename>
```

MOVEit Xfer Commands File

The command file which MOVEit Xfer will execute to download the backup file and then remove it from the DMZ server is a very simple file and should have the name `dmz_rstr_commands.txt`. It is shown below.

prompt

```
mget moveitdmz_backup_*.7z
mdel moveitdmz_backup_*.7z
```

Scheduling the Restore Process

As with the backup process, the Windows Scheduled Tasks service is used to schedule the running of the restore process. The process can be scheduled for any time after the file is scheduled to arrive on the DMZ server, since this DMZ server should be a hot-standby, and not currently in production use. Follow the directions in the Creating an Automated Backup Process section to create a scheduled process.

Finished

The automated restore process should now be set up and ready to run. You may test the process (assuming you have a file to download) by right-clicking the scheduled task entry for the backup process in the Scheduled Tasks window and selecting **Run**.

Disaster Recovery

With backup and restore processes properly configured to keep a hot-standby machine synced with a primary machine, as shown above, an organization can easily provide redundant DMZ services. If the primary machine goes down for any reason, the hot-standby should be able to jump in without any further configuration, since it should always be running and synced to the primary. The only configuration required to change over would be in the routing and DNS systems, to point customers at the standby instead of the primary.

Batch Files to Start and Stop MOVEit Services

Two batch files in the Scheduler folder allow administrators to easily start and stop all MOVEit DMZ services in a safe order with a single command.

- StartMOVEitDMZ.bat - Starts all MOVEit DMZ services, including MySQL
- StopMOVEitDMZ.bat - Stops all MOVEit DMZ services. MySQL will be stopped only if the administrator answers Y to the **stop MySQL?** prompt.

SSL and SSH

MOVEit DMZ uses the SSL and SSH standards to securely transport data between itself and various clients.

This section describes SSL and SSH.

Overview

MOVEit DMZ uses the SSL and SSH standards to securely transport data between itself and various clients. MOVEit DMZ acts as server during all these transfers, so MOVEit DMZ is required to have an SSL server certificate (a.k.a., "cert" or "X.509 certificate") and an SSH server key.

Client certificates and client keys are **OPTIONAL** pieces of information which can be used in place of, or in addition to, a password to authenticate a particular user. Client certificates may be used with the two SSL interfaces (HTTPS and FTPS) and client keys may be used with the SSH interface. In certain cases, client certificates will be stored on hardware tokens of some kind.

The sections in this topic describe the components and refer to other sections of the documentation that provide detailed setup information.

Also, the following procedures are also useful when getting started:

- ***Creating and processing*** (on page 184) a Certificate Signing Request (CSR) - Instructions for creating a CSR and processing the CSR in IIS. A CSR can be generated and processed on any server. The resulting certificate can then be exported to the MOVEit DMZ server as an SSL server cert.
- ***Importing, Exporting, and Removing*** (on page 191) an SSL certificate. - Instructions for importing and exporting SSL certificates using the Certificates Snap-in.
- ***Assigning an SSL Certificate to the MOVEit DMZ Web site and to the MOVEit DMZ FTP server*** (on page 215) - Instructions for assigning an SSL certificate to a IIS site and a FTP server.

SSL Server Certificates

SSL server certificates are usually obtained from Comodo, Thawte, Verisign or any other of the many commercial Certificate Authorities ("CAs") in the market. Self-generated certs may also be used, but the advantage of using a cert from a commercial CA is that many popular browsers, including IE and Firefox, will automatically trust your site (display the lock in the corner). Otherwise, your clients will need to explicitly opt to trust your certificate.

MOVEit DMZ server certs are configured in two places:

- HTTP/SSL (web) - A certificate must be assigned to your MOVEit DMZ web site via the Microsoft Internet Services Manager application. ([Site] Properties menu, Directory Security tab, Secure Communications section)
- FTP/SSL - The same certificate must also be assigned to your MOVEit DMZ FTP site via the MOVEit DMZ Config application. (FTP Certs **tab** (on page 577))

SSL Client Certificates

Users may be required to present an SSL client certificate during the signon process when using either the HTTPS or FTP/SSL interfaces. Complete information may be found in ***Client Certs - Overview*** (on page 222) and ***FTP - Configuration (Require Client Certificates)*** (on page 577).

SSH Server Keys

SSH keys do not have any relationship to a signer, so the MOVEit DMZ SSH server simply generates its own key the first time it runs.

You may view the fingerprint of your SSH key at any time via the MOVEit DMZ Config application. (**SSH tab** (on page 639))

See also SSH Keys - Server Keys - Overview.

SSH Client Keys

Any SSH user may be required to present an SSH client key during the signon process. Complete information may be found in **SSH Keys - Client Keys - Overview** (on page 253).

Relative Security of Passwords, Keys and Certificates

Passwords are easy to remember and easy for users to figure out how to use. To misuse these credentials, an attacker must guess, steal or record a password, but simply knowing a particular user's password is often enough to act as that user. (To protect passwords, MOVEit DMZ already features several industry-standard password defenses such as password strength requirements, password aging, per-user IP restrictions, per-user session restrictions, automatic lockouts and the use of SSL and SSH encrypted channels to securely transmit passwords.)

Client certificates ("certs") and keys are typically tied to specific computers or hardware tokens. To misuse these credentials, an attacker must typically gain control of a desktop/laptop machine (for an installed key/cert) or possess a hardware token. All client certs and client keys rely on "public key / private key" cryptography. Under this model, gaining possession of a particular user's private key is often enough to act as that user, so operating system and hardware solutions have evolved to protect private keys from unauthorized use. (MOVEit DMZ does not work directly with the private key halves of client cert/keys, and thus steers clear of private key protection issues.)

Because both passwords and client cert/keys have their own weaknesses, it has become increasingly common to require users to authenticate with both a password and a client cert/key. To defeat this scheme, an attacker must possess a user's password and access to that user's private key (i.e. access to their desktop/laptop or possession of their hardware token). While still possible, this "two factor" level of compromise is still harder for an attacker to achieve than either password or cert/key compromise alone, and affords a higher degree of security.

Difference Between Keys and Certificates

The main difference between SSH keys and (X.509) SSL certs is the concept of "trust": SSH keys are standalone credentials, while SSL certs must be verified.

SSH servers (MOVEit DMZ included) associate specific SSH client keys to specific users. If a SSH client presents an SSH key and it matches the one stored on the user record, the SSH client key will be authenticated - period.

SSL servers (MOVEit DMZ included) also associate specific SSL client certs to specific users, but SSL servers perform an additional background check on incoming SSL client certs. SSL client certs are signed (a.k.a. issued) by Certificate Authorities (CA). SSL servers maintain a list of CAs that they trust (all others are assumed to be untrusted.) If an SSL server receives an otherwise valid SSL client cert, but the client cert's CA isn't trusted, the SSL server will reject the connection.

With the extra CA check in mind, it could be said that SSL authentication is more secure than SSH authentication. For the same reason, however, configuring SSL authentication is more complicated than configuring SSH authentication.

Required Credentials

MOVEit DMZ users may authenticate with passwords, client keys (SSH only) or client certificates (HTTPS and FTP/SSL). Options on each user profile can be used to enforce exactly which combinations are allowed. (Default settings are available at the organization level.) The possible settings are:

- Password Only (Any key/certificate is ignored)
- Key/Cert Only (Any password is ignored)
- Password OR Key/Cert (If either credential matches, the other is ignored)
- Password AND Key/Cert (See also "Two-Factor Authentication")

Two-Factor Authentication

Systems which require "two-factor authentication" actually require three items:

- Statement of Identity (Usually, this is a username.)
- Unique Credential #1 (Usually, this is a password)
- Unique Credential #2 (Usually, this is a client certificate or client key.)

MOVEit DMZ supports "two-factor authentication" on its HTTPS and FTP/SSL interfaces with client certificates and on its FTP over SSH interface with client keys. To force this requirement on a particular user, the following user-level options **MUST** be enabled on each interface.

- Require client key/certificate
- Require password if a key/certificate is presented

It is worth noting that many FTP/SSL clients will work fine with two-factor settings ("Password And Cert") in both interactive and batch modes. However, the most popular SSH client (OpenSSH) will only work in interactive mode when two-factor settings are applied (OpenSSH requires a one-factor **Key Only** or **Password OR Key** setting while in batch mode.)



SSL

This section describes SSL Server Certificates and Client Certificates.

SSL Configuration

MOVEit DMZ 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.

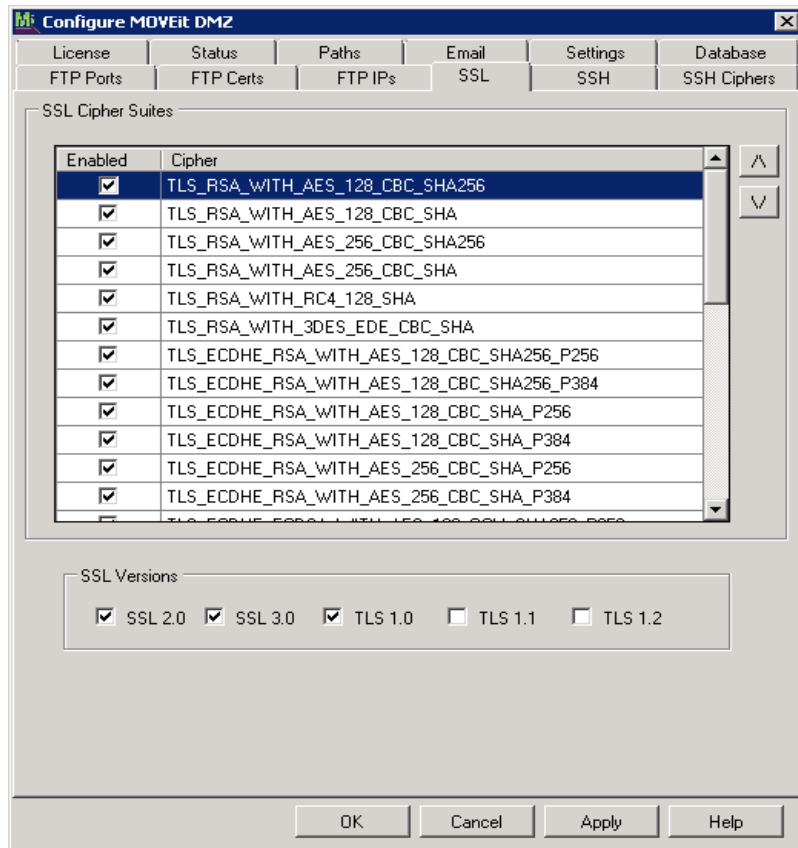
Warning: Changing the cipher suites or TLS/SSL versions can affect any applications that use TLS/SSL. Be sure you are aware of the requirements of other applications before making a change. For example, if you select SSL 2.0 only, MOVEit will not be able to connect to the Microsoft SQL database. The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

Note: The latest TLS 1.1 and 1.2 protocols will not work for many common browsers and operating systems, and may interfere with Remote Desktop. Including TLS 1.0 is a good choice for compatibility.

SSL Tab

In the Configure MOVEit DMZ program, you can use the SSL tab to select the cipher suites and SSL versions that can be used when establishing an SSL session. To run the configuration program, use the Start menu shortcut MOVEit DMZ Config.

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.



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 cipher suites enabled in the base Windows OS are enabled.

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.

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 SSL 3 is running on a remote server

This test was performed against our moveit.stdnet.com support server. It shows that a connection using SSL version 3, using a negotiated symmetric encryption algorithm called "RC4" and a "hash" algorithm called "MD5".

```
D:\OS0missions>openssl s_client -connect moveit.stdnet.com:443 -ssl3
```

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

```
CONNECTED(000002AC)
```

```
depth=0 /C=US/ST=Wisconsin/L=Madison/O=Standard Networks/OU=MOVEit
Site/CN=movei
```

t.stdnet.com

verify error:num=20:unable to get local issuer certificate

verify return:1

depth=0 /C=US/ST=Wisconsin/L=Madison/O=Standard Networks/OU=MOVEit
Site/CN=movei

t.stdnet.com

verify error:num=27:certificate not trusted

verify return:1

depth=0 /C=US/ST=Wisconsin/L=Madison/O=Standard Networks/OU=MOVEit
Site/CN=movei

t.stdnet.com

verify error:num=21:unable to verify the first certificate

verify return:1

Certificate chain

0 s:/C=US/ST=Wisconsin/L=Madison/O=Standard Networks/OU=MOVEit Site/CN=moveit.s
tdnet.com

i:/C=ZA/ST=Western Cape/L=Cape Town/O=Thawte Consulting cc/OU=Certification S
ervices Division/CN=Thawte Server CA/emailAddress=server-certs@thawte.com

Server certificate

-----BEGIN CERTIFICATE-----

MIIC5DCCAk2gAwIBAgIDCeniMA0GCSqGSIb3DQEBAUAMIHEMQswCQYDVQQGEwJa
QTEVMBMGGA1UECBMMV2VzdGVybiBDYXBIMRIwEAYDVQQHEwldYXBIFRvd24xHTAb
BgNVBAoTFFRoYXZ0ZSBDb25zdWx0aW5nIGNjMSgwJgYDVQQLEx9DZXJ0aWZpY2F0
aW9uIFNlcmlzaW9uMRkwFwYDVQQDEExBUaGF3dGU2VydmlvYIENB
MSYwJAYJKoZIhvcNAQkBFhdzZXJ2ZXItY2VydHNAAGhhd3RlLmNvbTAeFw0wMzAx

```
MTQxOTI0MDlaFw0wNTAyMDcyMjA0MThaMIGBMQswCQYDVQQGEwJVUzESMBAGA1UE
CBMJV2lzY29uc2luMRAwDgYDVQQHEwdNYWRpc29uMR0wGAYDVQQKExFTdGFuZGFy
ZCB0ZXR3b3JrczEUMBIGA1UECxMLTU9WRWl0IFNpdGUxGjAYBgNVBAMTEW1vdmVp
dC5zdGRuZXQuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCncZmY8wgL
6avPENjI3b7CDrIBVVYLBXs8eA+dZGXBQ6NfS2pP3bAG2Mi4atFp49EY4WKwz/CV
tyrPeTdyZ0xkuIZkiC5wH+iAFJg3J6DwpzkkVPMI4lXxi0nd6cke4ZZupwUPR/4R
w/CW2WWCllQLxv2Fg0zEkqFPazzpMEwcQIDAQABoyUwIzATBgNVHSUEDDAKBggr
BgEFBQcDATAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBAQUAA4GBAK7Jt0Ft5fw3
fEBc14waYvuzKVTSh+zBuskRSVt3C4uUtxLqMBbswUmx3n29TpHInmNoL+iXZJz2
IZEaGkMwLMXJxB0MwD19mlrK9EhZDA0I9ZUNWnZ+1gWep4SpF0DFP7U0SzuU0s1z
34xKpkqtN3nzR5iRkSEZU7nxPyl29CM0
```

-----END CERTIFICATE-----

subject=/C=US/ST=Wisconsin/L=Madison/O=Standard Networks/OU=MOVEit
Site/CN=movei

t.stdnet.com

issuer=/C=ZA/ST=Western Cape/L=Cape Town/O=Thawte Consulting cc/OU=Certification
Services Division/CN=Thawte Server CA/emailAddress=server-certs@thawte.com

No client certificate CA names sent

SSL handshake has read 904 bytes and written 304 bytes

New, TLSv1/SSLv3, Cipher is RC4-MD5

Server public key is 1024 bit

SSL-Session:

Protocol : SSLv3

Cipher : RC4-MD5

```
Session-ID:
F50400000B9D20B4B6D0605AE6BE88573A3A4D7503D861281CF0691B0FDAFC62

Session-ID-ctx:

Master-Key:
B556889277515F16889D048A003B1C827BF0F7DF01E2EAEEE7BD45F518912B24
F1FE19762809BA770E215C8FFA99C330

Key-Arg : None

Start Time: 1075827324

Timeout : 7200 (sec)

Verify return code: 21 (unable to verify the first certificate)

---

(ctrl+c)

DONE
```

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.)

```
D:\OS0missions>openssl s_client -connect localhost:443 -ssl3
```

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

```
CONNECTED(000002AC)
```

```
1484:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:../ssl/s3
```

```
_pkt.c:529:
```

Logging SSL Connection Events and Errors to the Event Log

By default, Microsoft SSL only logs serious SSL connection errors to the event log. However, you can change the level of SSL connection information logged here by making a Windows registry change. First, make sure the following REG_DWORD registry entry exists. (Add it if it does not.)

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
SecurityProviders\SCHANNEL\EventLogging
```

One of the following values should be used in this field.

- 0 - No logging.
- 1 - Errors only. (Default)
- 3 - Errors and warnings.
- 7 - Errors, warnings and informational messages (e.g., every connection).

You will need to restart your computer for this value to take effect. More information can be found on Microsoft's Support site under the "***How to enable schannel event logging***" topic (#260729) (<http://support.microsoft.com/?id=260729>)

Server Certs

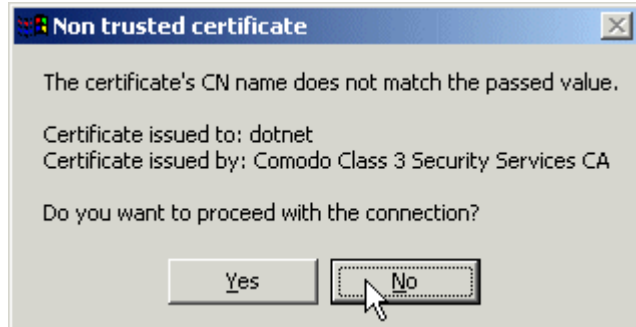
This subsection describes SSL Server Certificates.

SSL - Server Certs - Overview

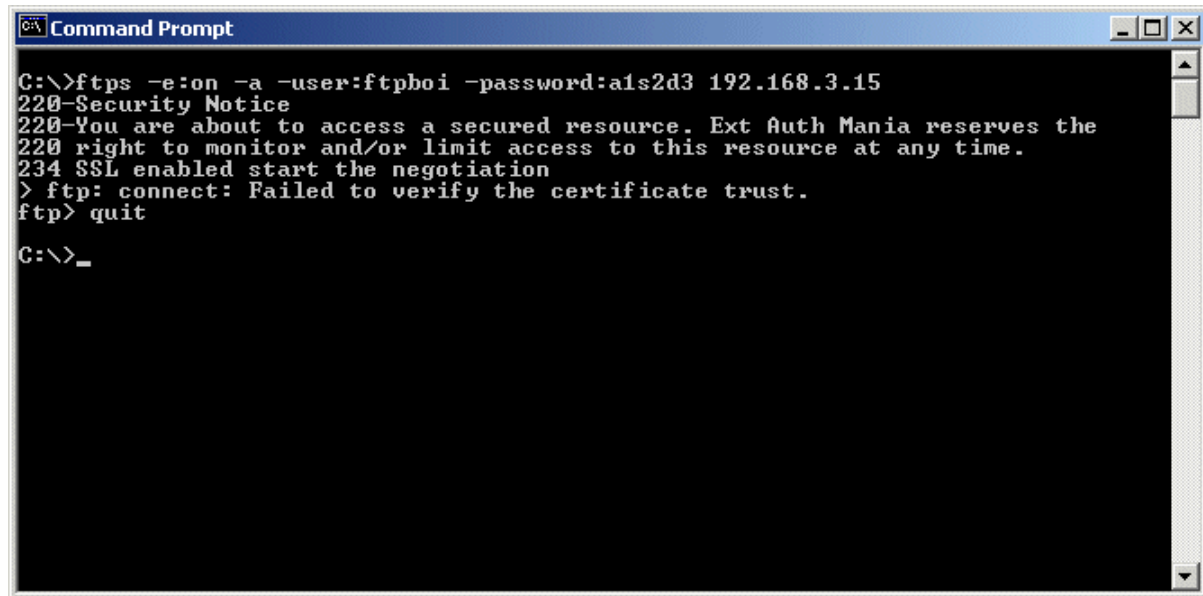
Establishing an SSL-secured connection between a client and a server begins with a server certificate, which is used to both verify the identity of the server and securely negotiate a shared encryption key to use during the rest of the encrypted session. Consequently, all SSL servers require a server certificate. Since MOVEit DMZ uses SSL to secure its web-based interface (HTTPS) and its FTP interface (FTP/SSL), both of these interfaces require server certificates. Typically, the same certificate is used by both interfaces.

HTTPS and FTP/SSL clients know to trust specific machines because the certificates presented by remote servers are valid within a specific time period, match the hostname of the server to which the user connected, and are signed by a chain of trusted Certificate Authorities (CAs), such as Thawte or Verisign. (Without these protections, anyone could spoof an SSL-secured server with a self-generated server certificate!) So, for production environments, the use of a certificate signed by a well-known CA is highly recommended in order to give end users the most secure experience. For evaluation, development, and/or testing environments, however, self-signed test certificates are often used to eliminate the cost of purchasing a fully trusted certificate. In these cases, clients often present alert messages informing the user that something is not right with the certificate.

The following MOVEit Freely session shows this mechanism in action. During the SSL negotiation, MOVEit Freely notices that the remote certificate (for "dotnet") does not match the hostname that the client was told to connect to (192.168.3.15). The end user is prompted with a warning message.



Assuming the end user decided not to complete the SSL connection to this server, MOVEit Freely displays a short description about why the SSL connection was refused.



```
Command Prompt
C:\>ftp -e:on -a -user:ftpboi -password:a1s2d3 192.168.3.15
220-Security Notice
220-You are about to access a secured resource. Ext Auth Mania reserves the
220 right to monitor and/or limit access to this resource at any time.
234 SSL enabled start the negotiation
> ftp: connect: Failed to verify the certificate trust.
ftp> quit
C:\>_
```

Configuring Server Certificates

On Windows platforms, server certificate requests and installations are typically performed through the IIS Internet Services Manager and its Web Server Certificate Server. For instructions on requesting a signed server certificate, see the ***Certificate Signing Requests*** (on page 184) documentation page.

Once a certificate is available, it must be installed in both IIS and the MOVEit DMZ FTP server in order to be used by MOVEit DMZ. For instructions on installing a server certificate in IIS and the MOVEit DMZ FTP server, see the ***Assign Components*** (on page 215) documentation page.

Finally, once a certificate is installed and operational, be sure that it is backed up at some point, so a replacement is not needed should a catastrophic system error happen. The ***MOVEit DMZ Backup and Restore utilities*** (on page 150) are capable of backing up both client and server certificate information from a MOVEit DMZ server. For additional instructions on manually backing up certificates, see the ***Backing Up Server Certificates*** (on page 220) documentation page.

SSL - Server Certs - CSRs

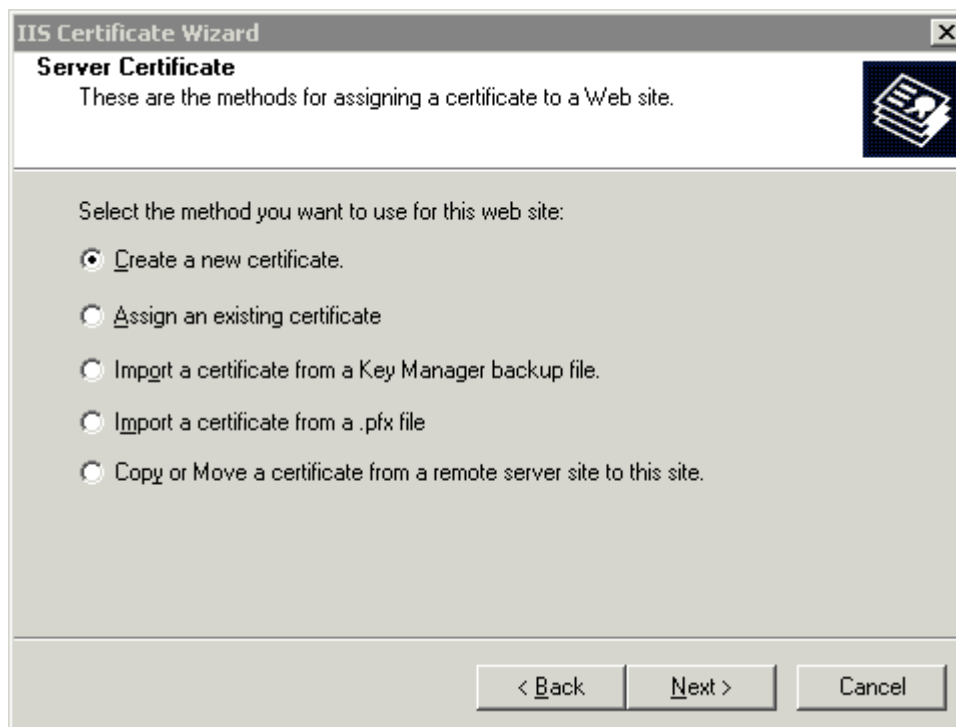
Creating a CSR (Certificate Signing Request)

Start with a server that does not have an SSL certificate or ***remove the current SSL certificate*** (on page 191).

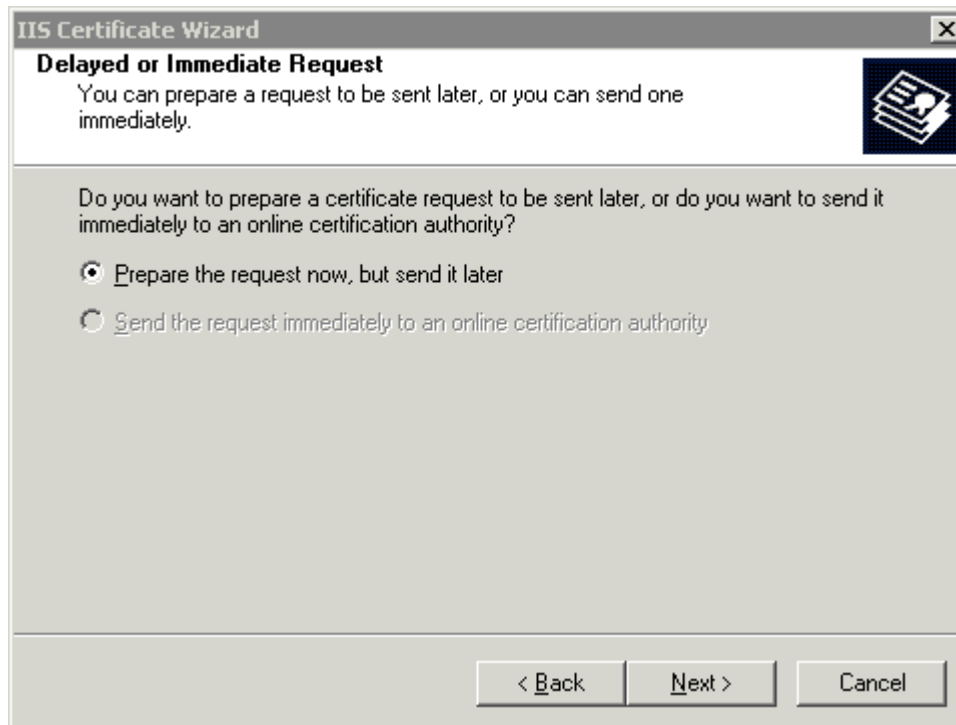
HINT: To request a production certificate while still using the 90-day test certificate that the MOVEit DMZ installation program installed in your moveitdmz IIS site, request the certificate from the default IIS site instead.

Click Start -> Programs -> Administrative Tools -> Internet Information Services Manager (IIS Manager). Select the web site you wish to work with and right-click then select Properties. Select the Directory Security tab then click **Server Certificate....** This will start the Web Server Certificate Wizard.

Select **Create a new certificate** and click Next.



Select Prepare the request now, but send later and click Next.



The screenshot shows the 'IIS Certificate Wizard' window at the 'Delayed or Immediate Request' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Delayed or Immediate Request'. Below it, a text box says 'You can prepare a request to be sent later, or you can send one immediately.' To the right is an icon of a document with a person. The main area contains the question 'Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?'. There are two radio buttons: the first is selected and labeled 'Prepare the request now, but send it later'; the second is labeled 'Send the request immediately to an online certification authority'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

IIS Certificate Wizard

Delayed or Immediate Request

You can prepare a request to be sent later, or you can send one immediately.

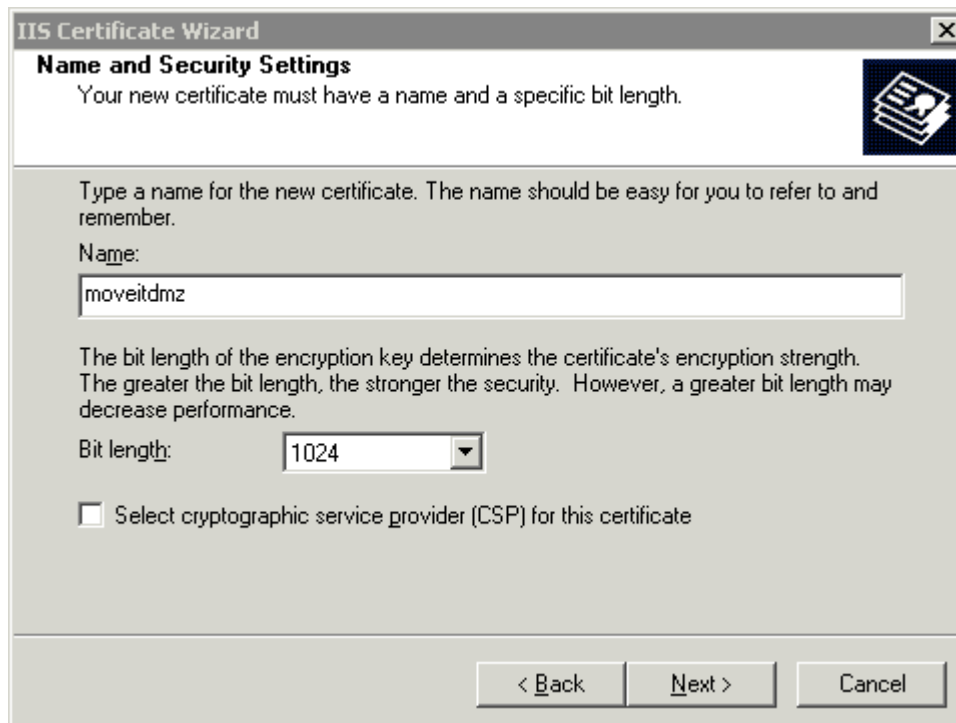
Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

☒ Prepare the request now, but send it later

☐ Send the request immediately to an online certification authority

< Back Next > Cancel

Select the name and security strength (1024 bit at least) and click Next.



The screenshot shows the 'IIS Certificate Wizard' window at the 'Name and Security Settings' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Name and Security Settings'. Below it, a text box says 'Your new certificate must have a name and a specific bit length.' To the right is an icon of a document with a person. The main area contains the instruction 'Type a name for the new certificate. The name should be easy for you to refer to and remember.' followed by a label 'Name:' and a text box containing 'moveitdmz'. Below that is the instruction 'The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.' followed by a label 'Bit length:' and a dropdown menu showing '1024'. At the bottom is a checkbox labeled 'Select cryptographic service provider (CSP) for this certificate' which is unchecked. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

IIS Certificate Wizard

Name and Security Settings

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Name:

moveitdmz

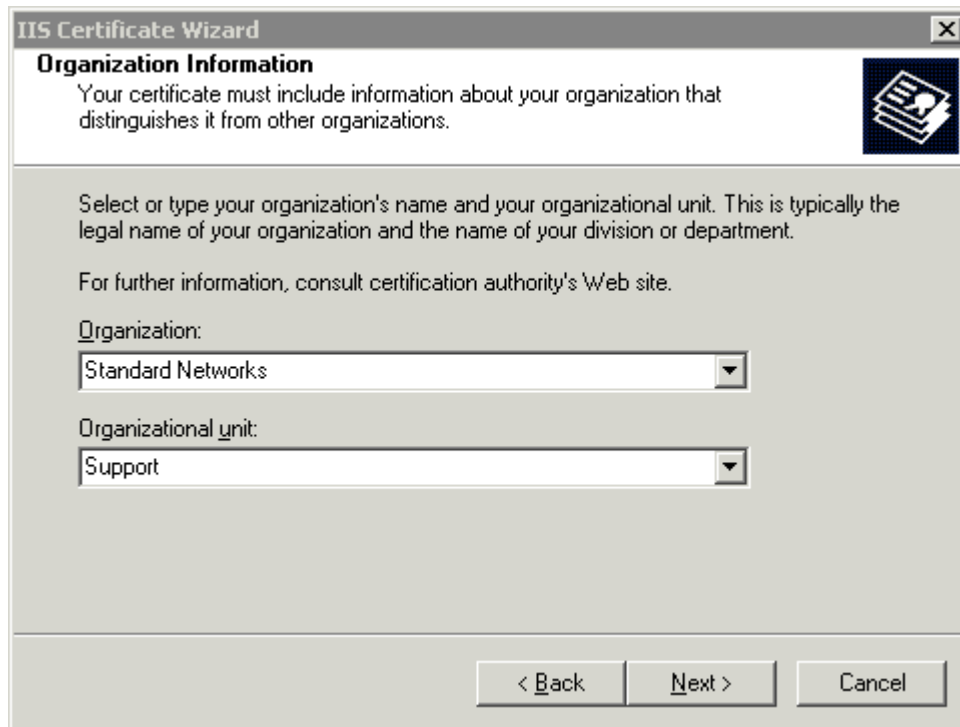
The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length: 1024

☐ Select cryptographic service provider (CSP) for this certificate

< Back Next > Cancel

Type your Organization Information and click Next.



The screenshot shows a Windows-style dialog box titled "IIS Certificate Wizard". The main heading is "Organization Information". Below the heading, a message states: "Your certificate must include information about your organization that distinguishes it from other organizations." To the right of this text is an icon of a document with a person silhouette. Further down, instructions read: "Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department." and "For further information, consult certification authority's Web site." There are two dropdown menus: "Organization:" with "Standard Networks" selected, and "Organizational unit:" with "Support" selected. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

IIS Certificate Wizard

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization:
Standard Networks

Organizational unit:
Support

< Back Next > Cancel

Type the **Common Name** that will be used for this certificate and click **Next**. This is the Fully Qualified Domain Name (FQDN) for your MOVEit DMZ site, for example moveitdmz.com. Make sure to have the name approved with the DNS administrator before sending the CSR to the Certificate Authority.



The screenshot shows the 'IIS Certificate Wizard' window. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Your Site's Common Name'. Below the heading, it says 'Your Web site's common name is its fully qualified domain name.' To the right of this text is an icon of a document with a keyhole. The main text area contains the following instructions: 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.' and 'If the common name changes, you will need to obtain a new certificate.' Below this is a label 'Common name:' followed by a text input field containing 'moveit.xyz.tld'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

IIS Certificate Wizard

Your Site's Common Name

Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

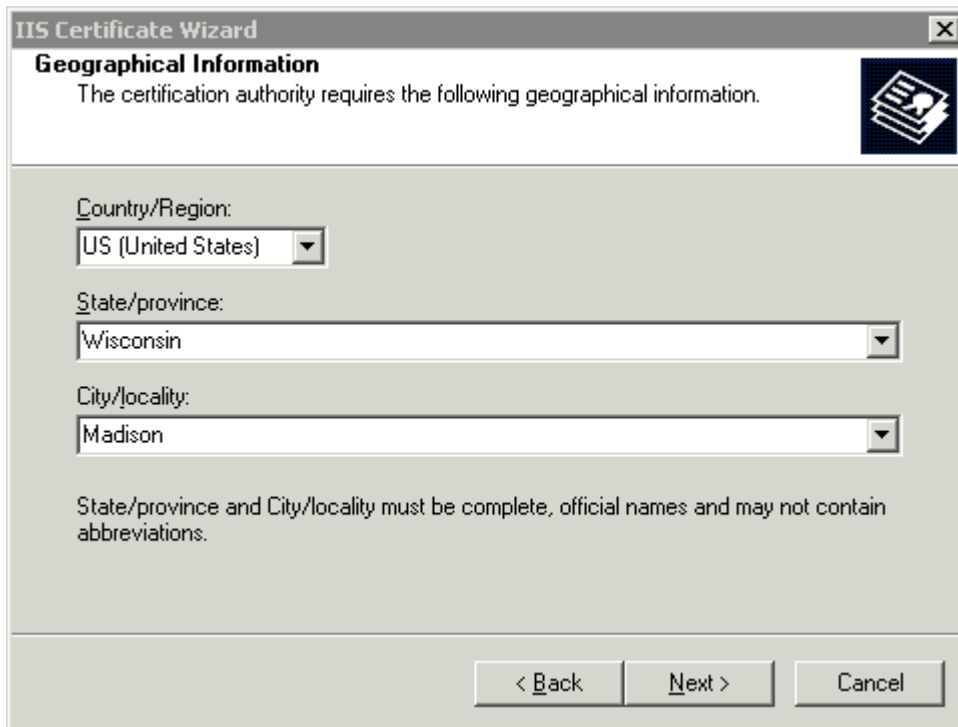
If the common name changes, you will need to obtain a new certificate.

Common name:

moveit.xyz.tld

< Back Next > Cancel

Type the Geographical Information that will be used for this certificate and click Next



The screenshot shows the 'IIS Certificate Wizard' window, specifically the 'Geographical Information' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Geographical Information'. Below the heading, a message states: 'The certification authority requires the following geographical information.' To the right of this message is an icon of a document with a person silhouette. The form contains three dropdown menus: 'Country/Region:' with 'US (United States)' selected, 'State/province:' with 'Wisconsin' selected, and 'City/locality:' with 'Madison' selected. Below these fields, a note reads: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

IIS Certificate Wizard

Geographical Information

The certification authority requires the following geographical information.

Country/Region:
US (United States)

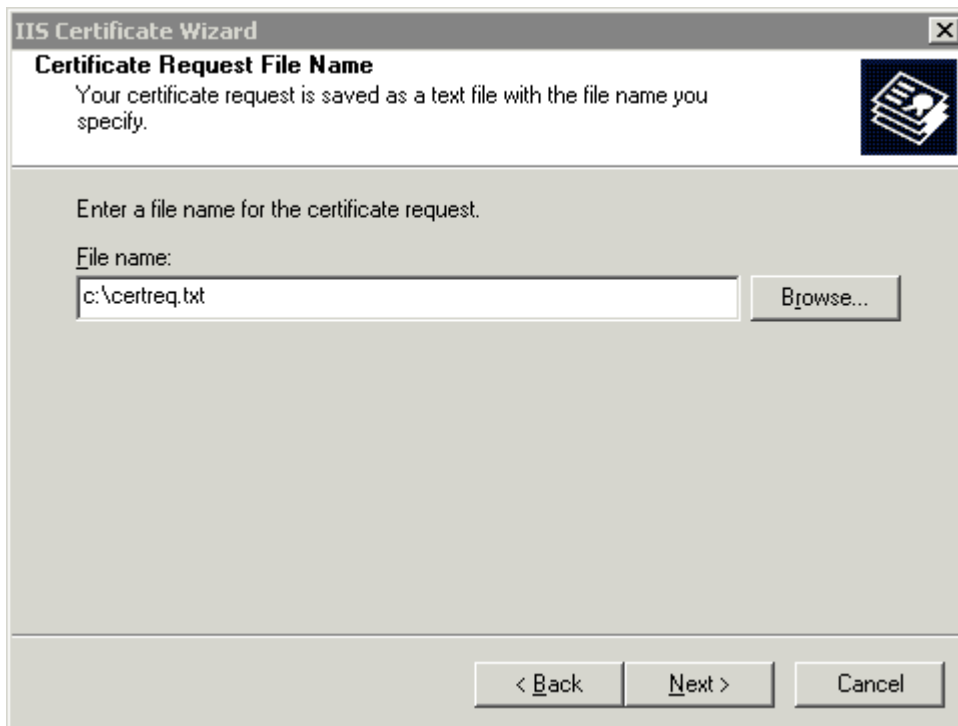
State/province:
Wisconsin

City/locality:
Madison

State/province and City/locality must be complete, official names and may not contain abbreviations.

< Back Next > Cancel

Select the filename to be used for the certificate request and click Next.



The screenshot shows the 'IIS Certificate Wizard' window, specifically the 'Certificate Request File Name' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Certificate Request File Name'. Below the heading, a message states: 'Your certificate request is saved as a text file with the file name you specify.' To the right of this message is an icon of a document with a person silhouette. The form contains a text input field labeled 'File name:' with the text 'c:\certreq.txt' entered. To the right of the text field is a 'Browse...' button. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

IIS Certificate Wizard

Certificate Request File Name

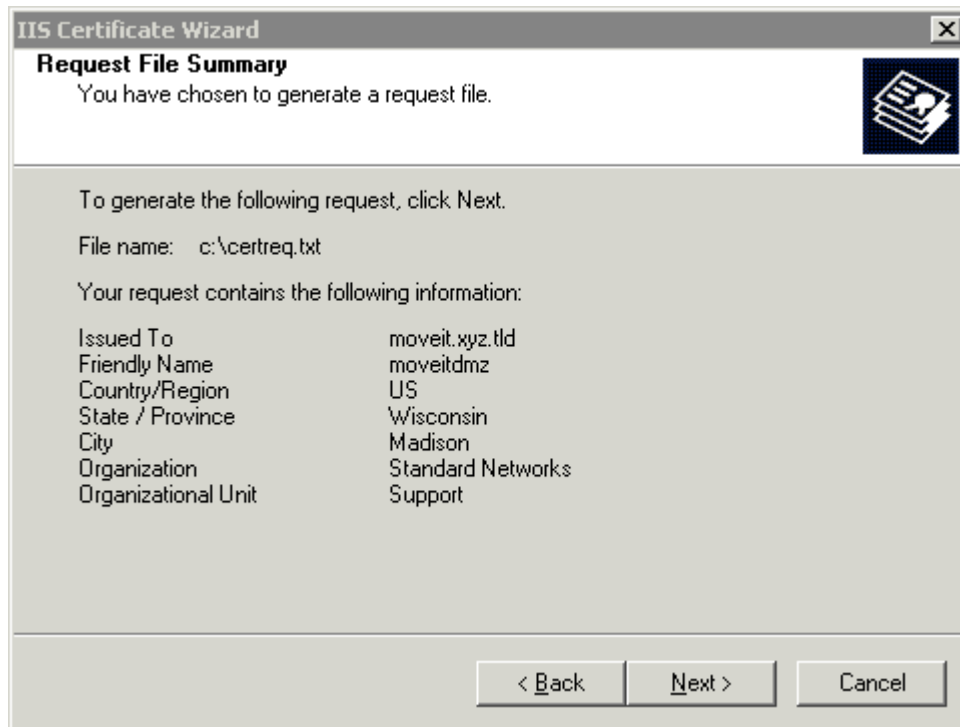
Your certificate request is saved as a text file with the file name you specify.

Enter a file name for the certificate request.

File name:
c:\certreq.txt Browse...

< Back Next > Cancel

Verify the certificate from the Summary information and click Next.



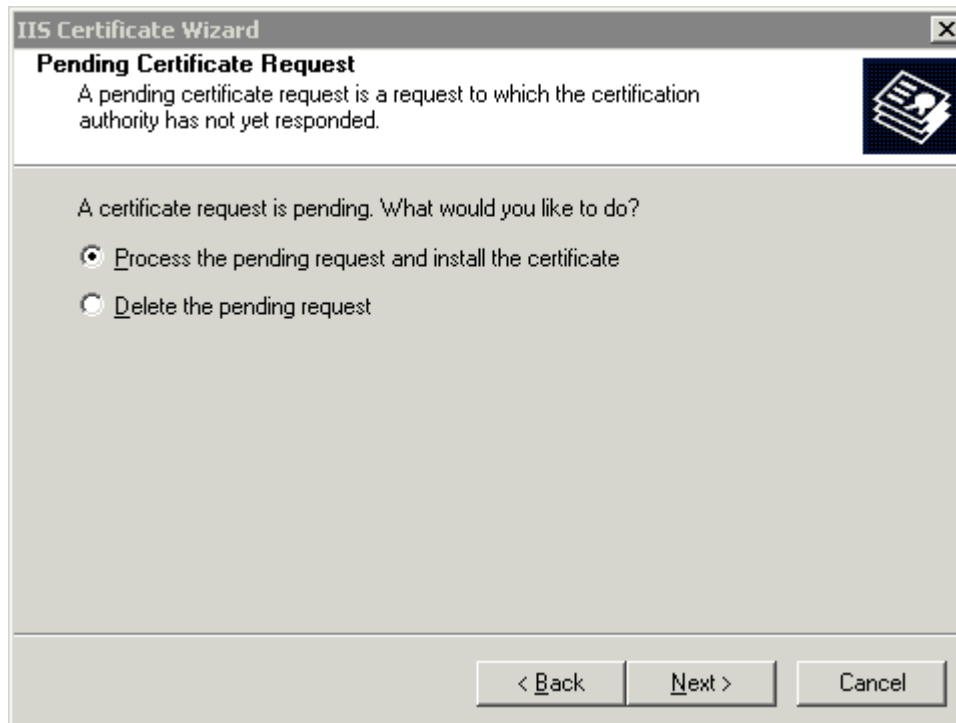
Click **Finish** to finalize your CSR. You will now need to send the CSR to a ***Certificate Authority of your choice*** (on page 182).

Installing the Certificate (after receiving the file from a CA)

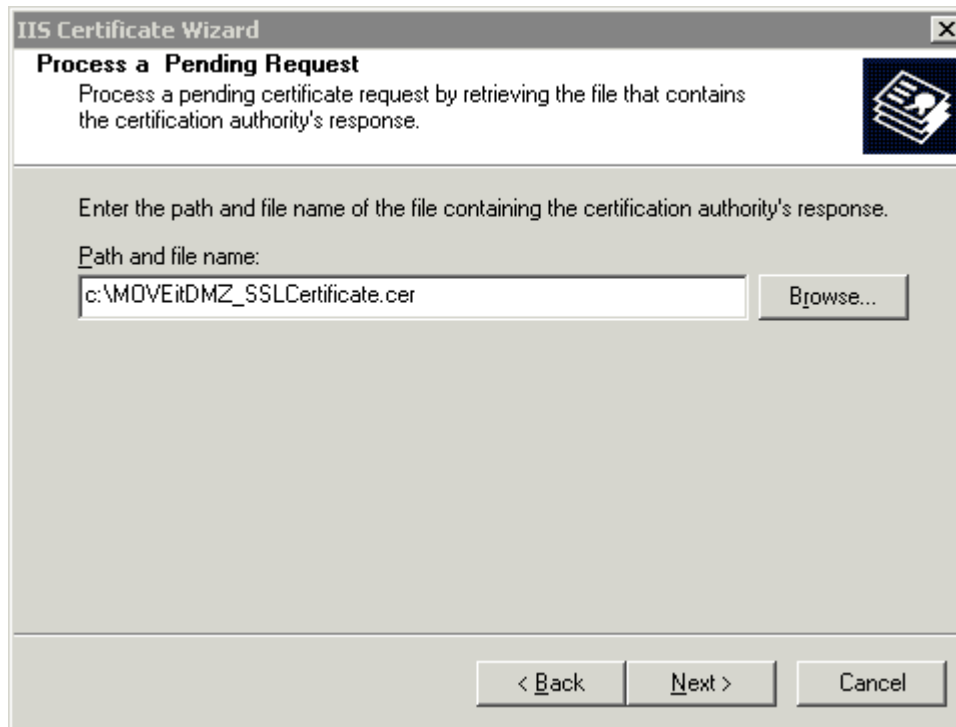
When you have received the certificate (typically several days later), then proceed to the next step.

Start with a server that has a pending request. Click **Start -> Programs -> Administrative Tools -> Internet Information Services Manager (IIS Manager)**. Select the web site you wish to work with and **Right-Click** then select **Properties**. Click on the **Directory Security** tab then click **Server Certificate....** This will start the Web Server Certificate Wizard.

Select **Process** the pending request and install certificate and click **Next**.



Select the path and filename of the response that was sent from the Certificate Authority.



Choose to install the certificate using **Port 443** and then click **Finish**.

Hint: If you performed this procedure on your default IIS site to because you were still using the MOVEit DMZ 90-day test certificate, you should now move your new cert over to your moveitdmz IIS site. First, go to the **Directory Security** tab on the default IIS site, click **Server Certificate...** and select the **Remove** action. Next, open the moveitdmz IIS site's properties, go to the **Directory Security** tab, click **Server Certificate...** and select the **Replace** (or **Assign**) action. Finally, select the certificate you requested and installed from the default IIS site.

The certificate now needs to be **assigned to the MOVEit DMZ FTP Server** (on page 215).

SSL - Server Certs - Import and Export

This topic covers the following tasks:

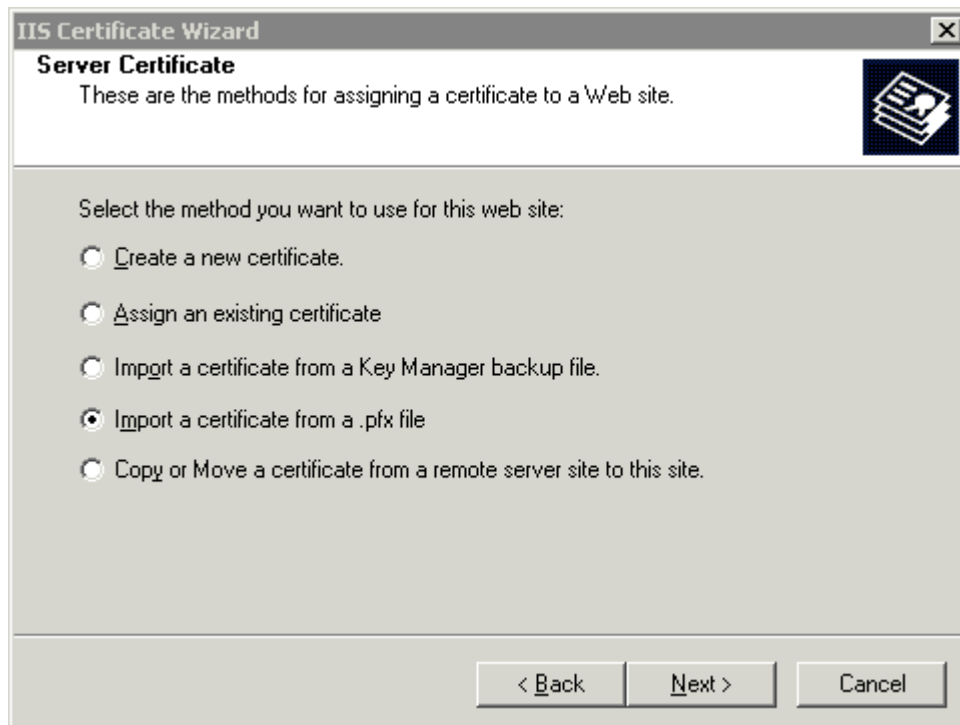
- Import an SSL certificate
 - Method 1 - Using the IIS Manager
 - Method 2 - Using the MMC Snap-in
- Export an SSL certificate
- Removing an SSL certificate from an IIS web site

Import an SSL certificate

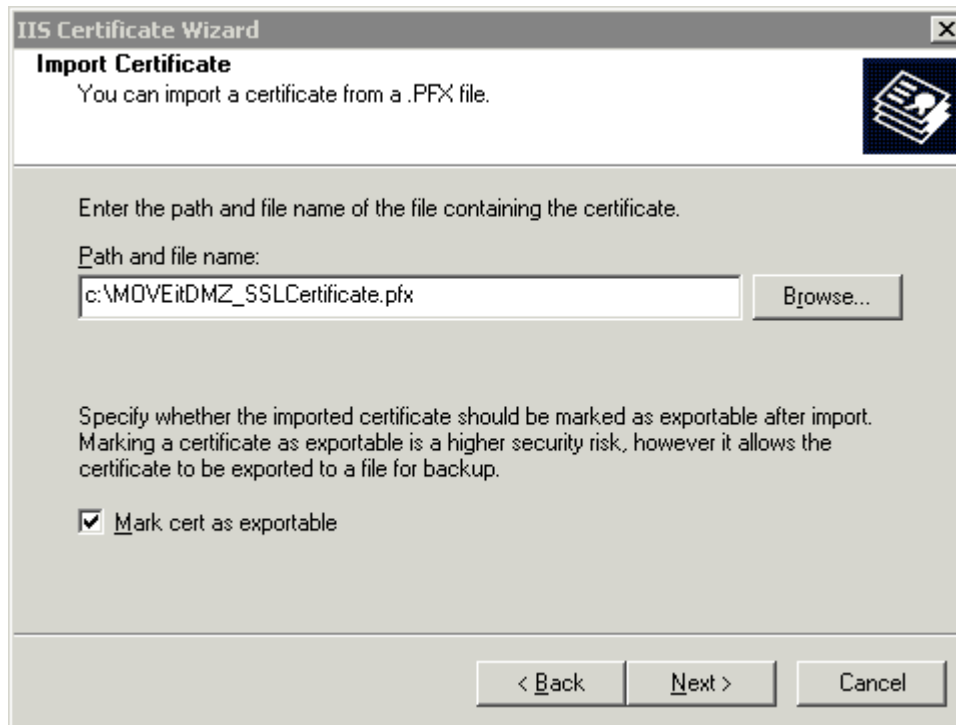
➤ *Method 1 - Using the IIS Manager*

Click Start -> Programs -> Administrative Tools -> Internet Information Services Manager (IIS Manager). Select the web site you wish to work with and Right-Click then select **Properties**. Click on the **Directory Security** tab then click **Server Certificate....** This will start the Web Server Certificate Wizard.

Select **import a certificate from a .pfx file**. PFX is a common format used to store both the public and private keys of an SSL Certificate.



Browse to the file and select **Mark this key as exportable** then click **Next**.



IIS Certificate Wizard

Import Certificate

You can import a certificate from a .PFX file.

Enter the path and file name of the file containing the certificate.

Path and file name:
c:\MOVEitDMZ_SSLSertificate.pfx

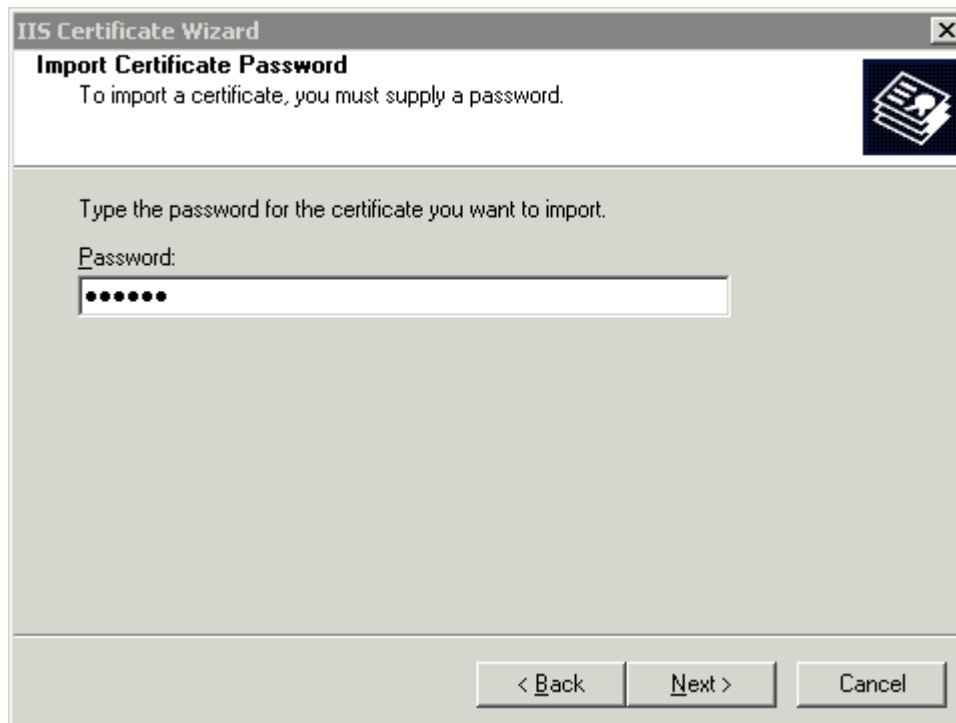
Browse...

Specify whether the imported certificate should be marked as exportable after import. Marking a certificate as exportable is a higher security risk, however it allows the certificate to be exported to a file for backup.

☒ **Mark cert as exportable**

< Back Next > Cancel

Type the password and click **Next**.



IIS Certificate Wizard

Import Certificate Password

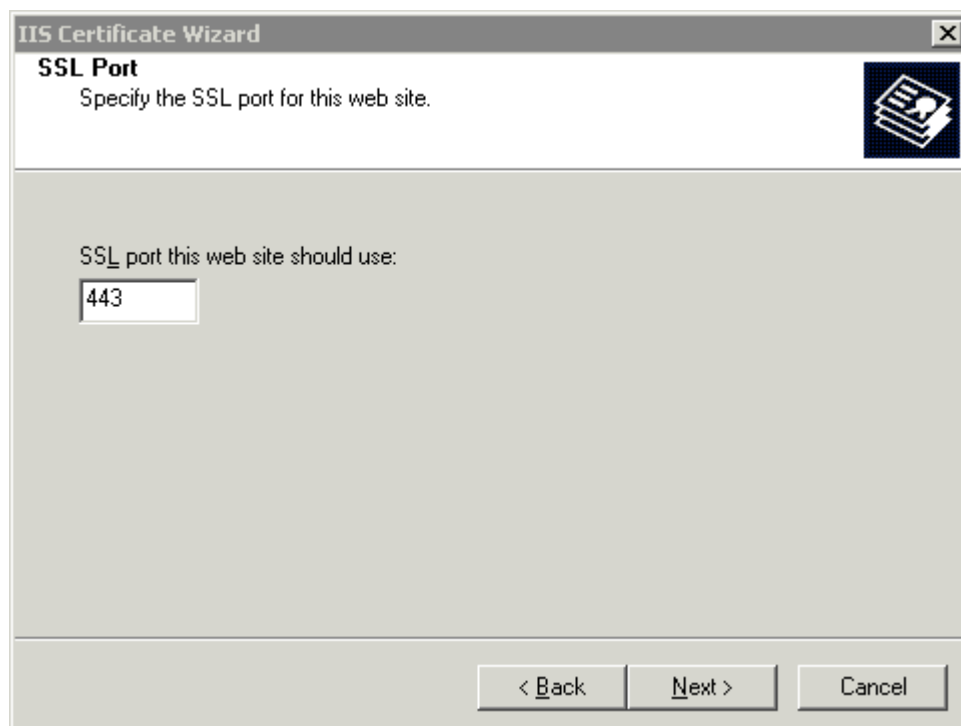
To import a certificate, you must supply a password.

Type the password for the certificate you want to import.

Password:
•••••

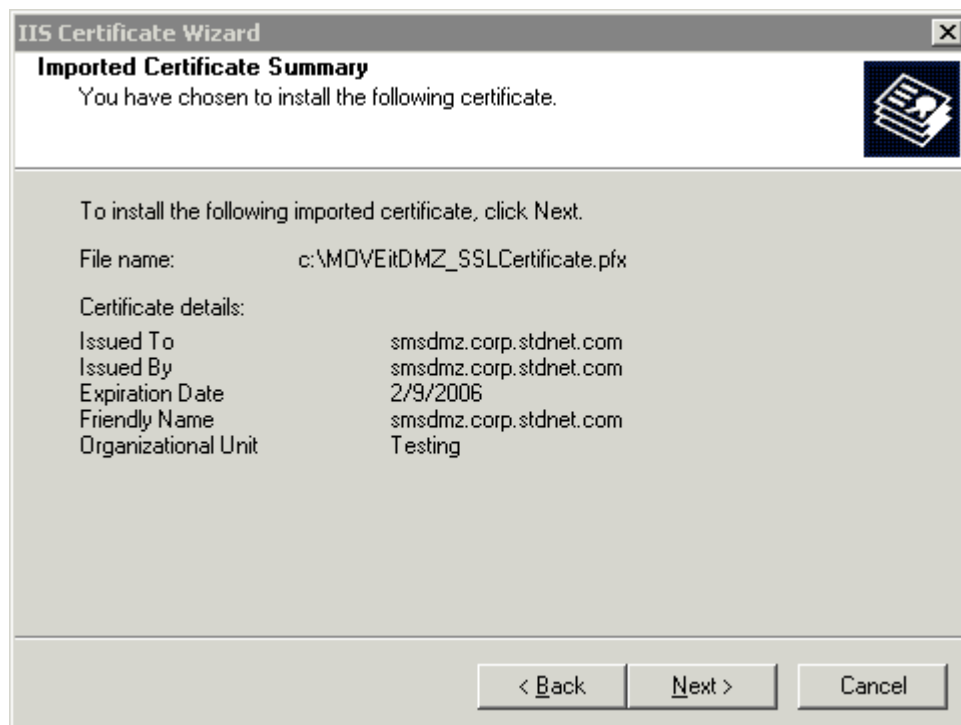
< Back Next > Cancel

Select port (almost always 443) to use click Next.



The screenshot shows the 'IIS Certificate Wizard' window, specifically the 'SSL Port' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'SSL Port' with the instruction 'Specify the SSL port for this web site.' Below this, a text box is labeled 'SSL port this web site should use:' and contains the number '443'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A small icon of a certificate is visible in the top right corner of the wizard area.

Verify the certificate summary and click Next.

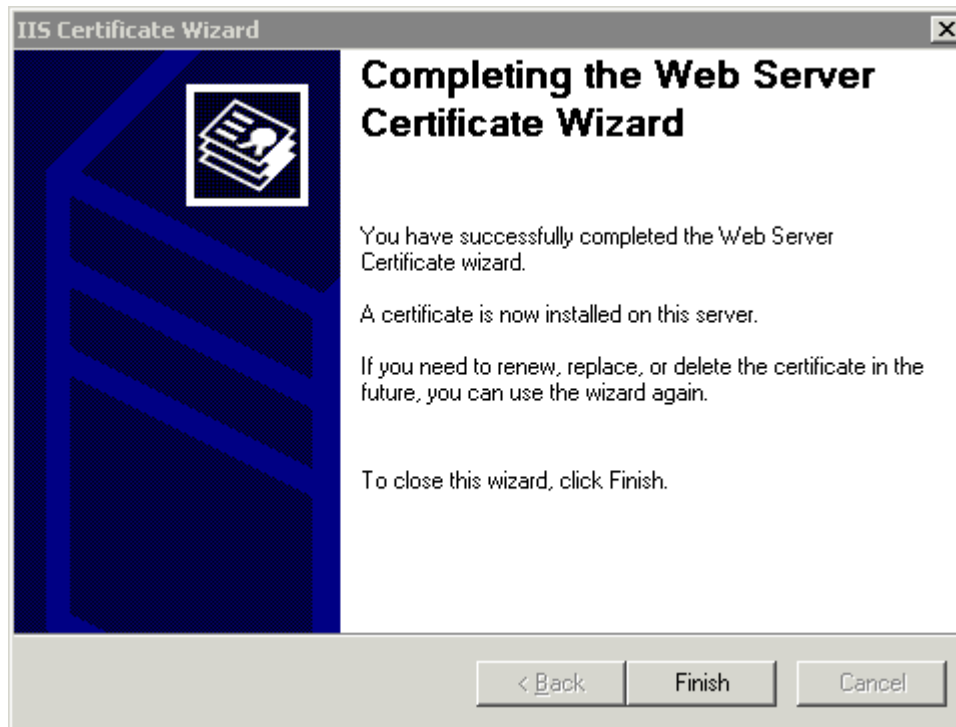


The screenshot shows the 'IIS Certificate Wizard' window, specifically the 'Imported Certificate Summary' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Imported Certificate Summary' with the instruction 'You have chosen to install the following certificate.' Below this, it says 'To install the following imported certificate, click Next.' The 'File name:' is listed as 'c:\MOVEitDMZ_SSLCertificate.pfx'. Under 'Certificate details:', the following information is displayed:

Issued To	smsdmz.corp.stdnet.com
Issued By	smsdmz.corp.stdnet.com
Expiration Date	2/9/2006
Friendly Name	smsdmz.corp.stdnet.com
Organizational Unit	Testing

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A small icon of a certificate is visible in the top right corner of the wizard area.

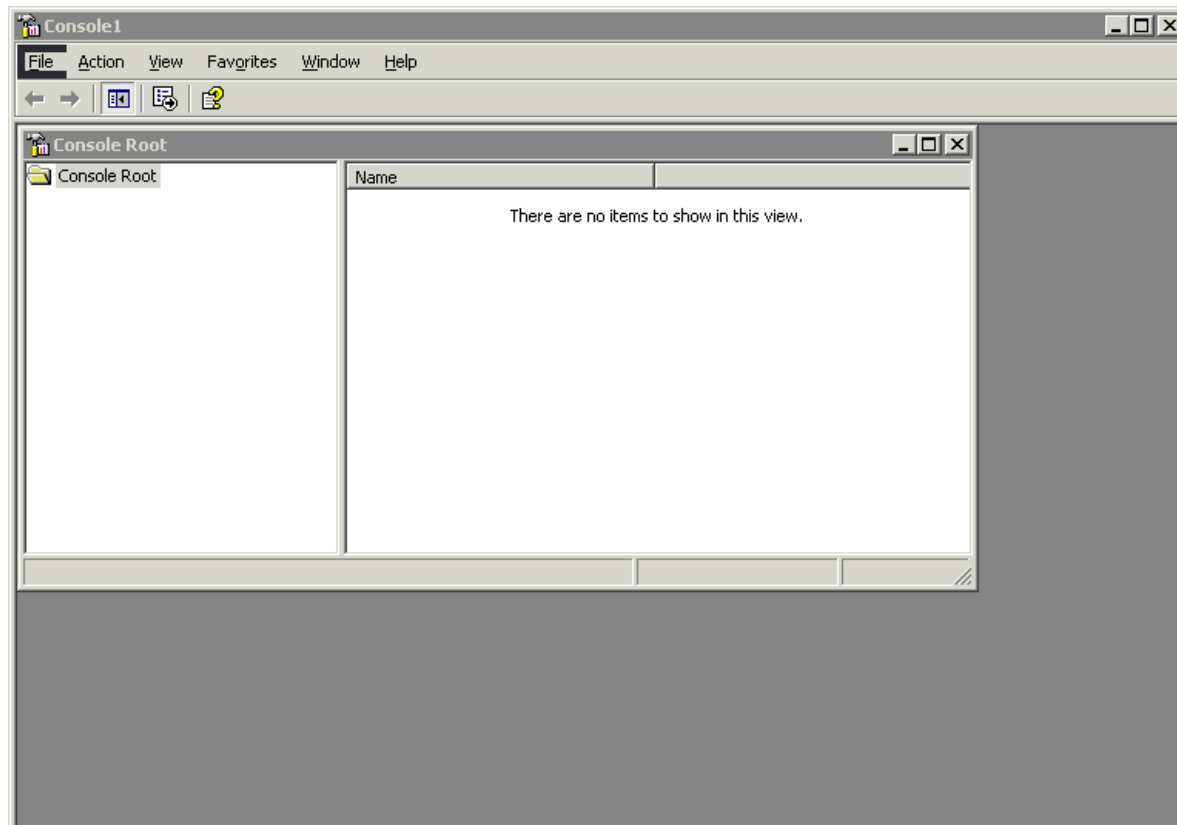
The certificate is now imported into IIS, click Finish.



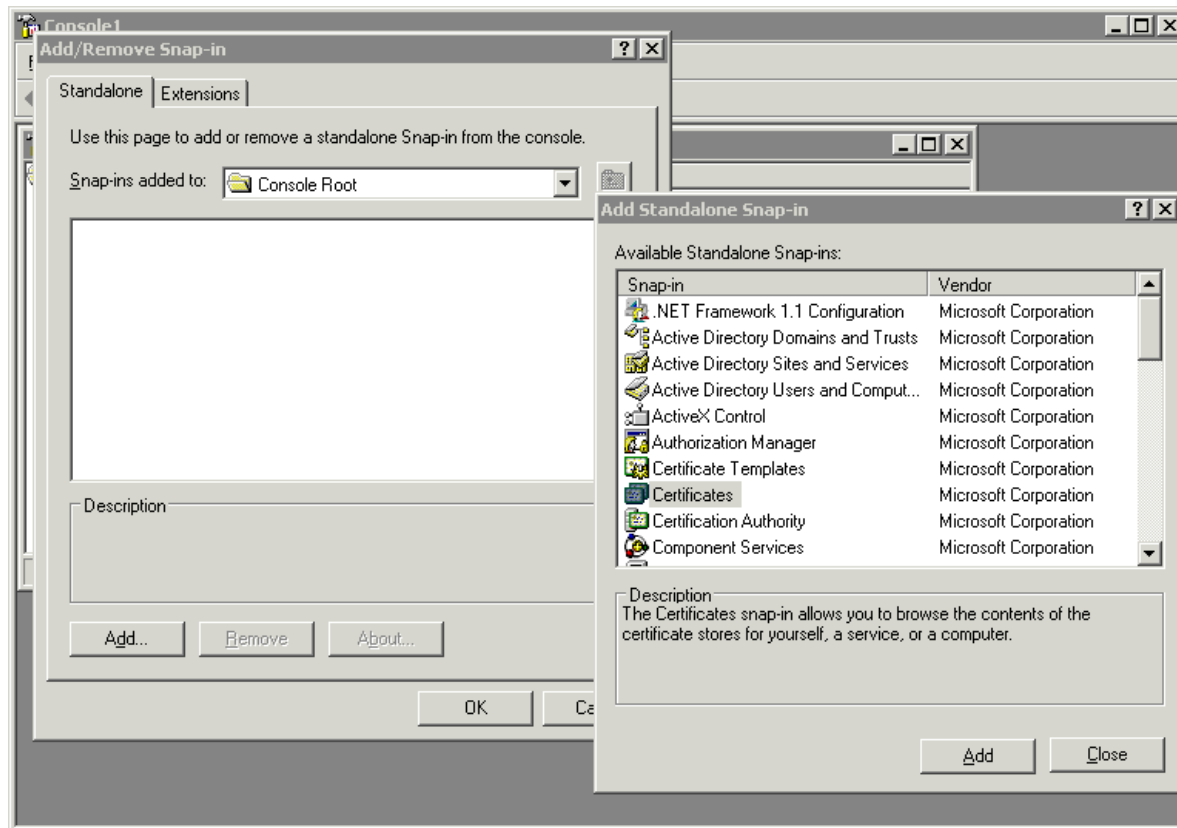
The certificate now needs to be ***assigned to the MOVEit DMZ FTP Server*** (on page 215).

➤ ***Method 2 - Using the MMC Snap-in***

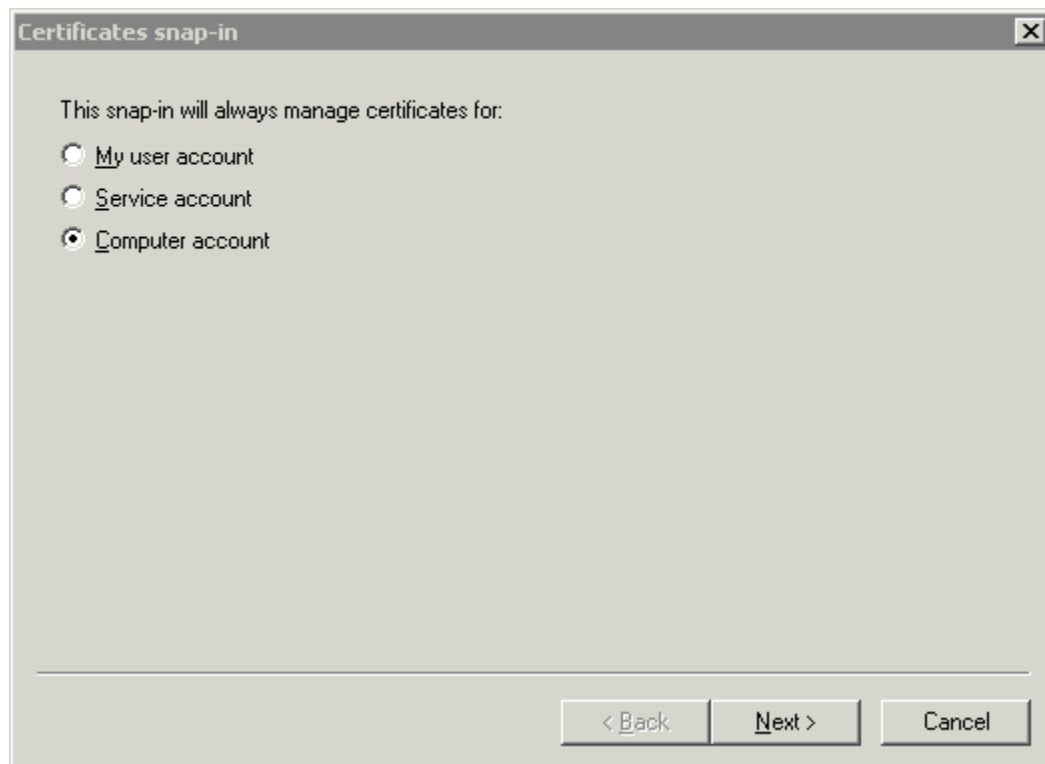
Click Start -> Run and type mmc.



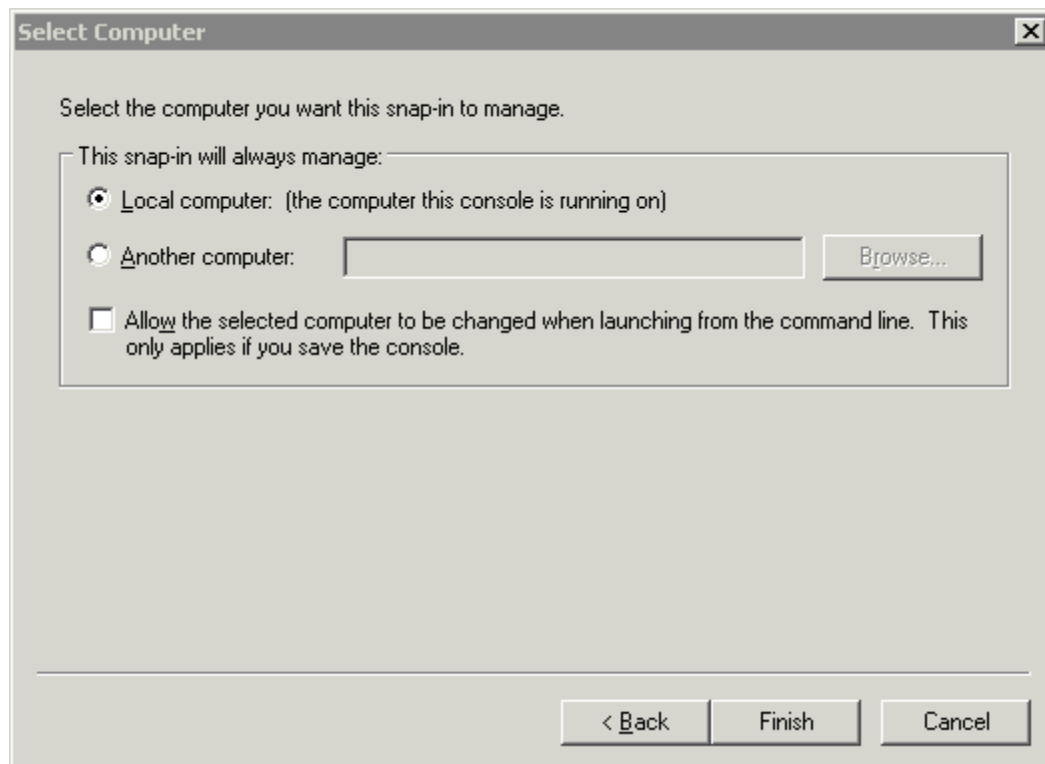
Click **File** then pick **Add/Remove Snap-ins** and select **Certificates** and click **Add**.



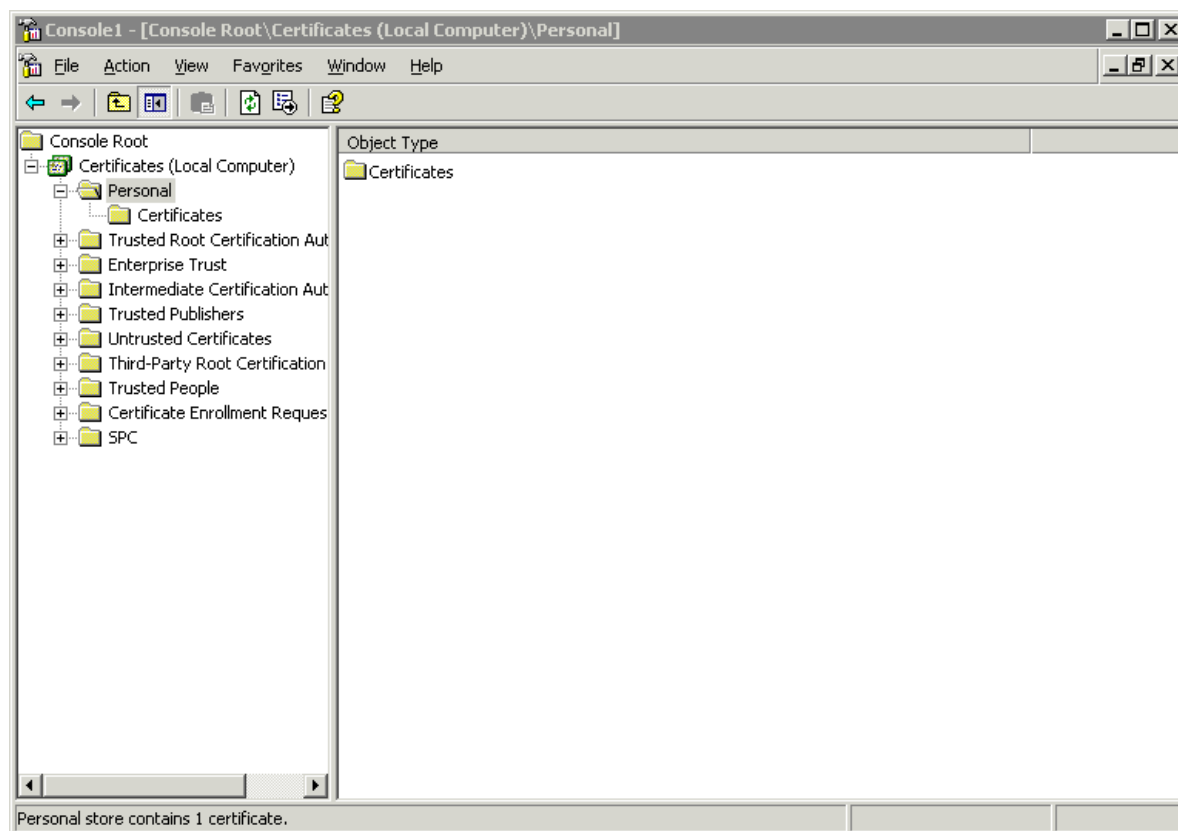
Select the Computer Account and click Next.



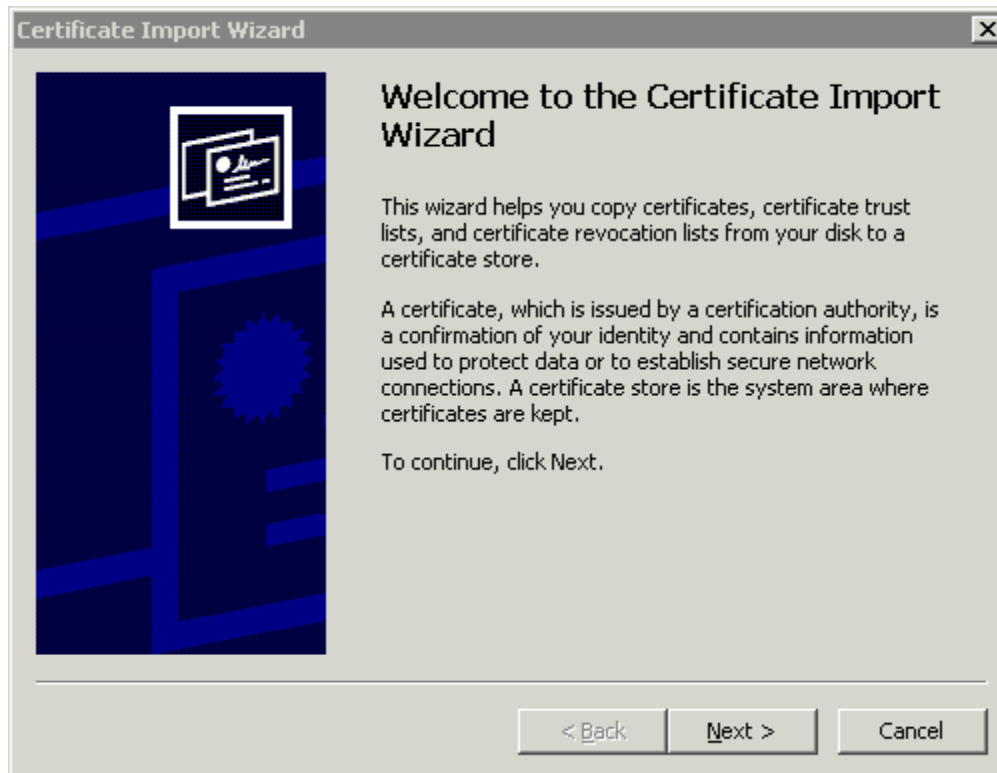
Select Local Computer and click Finish.



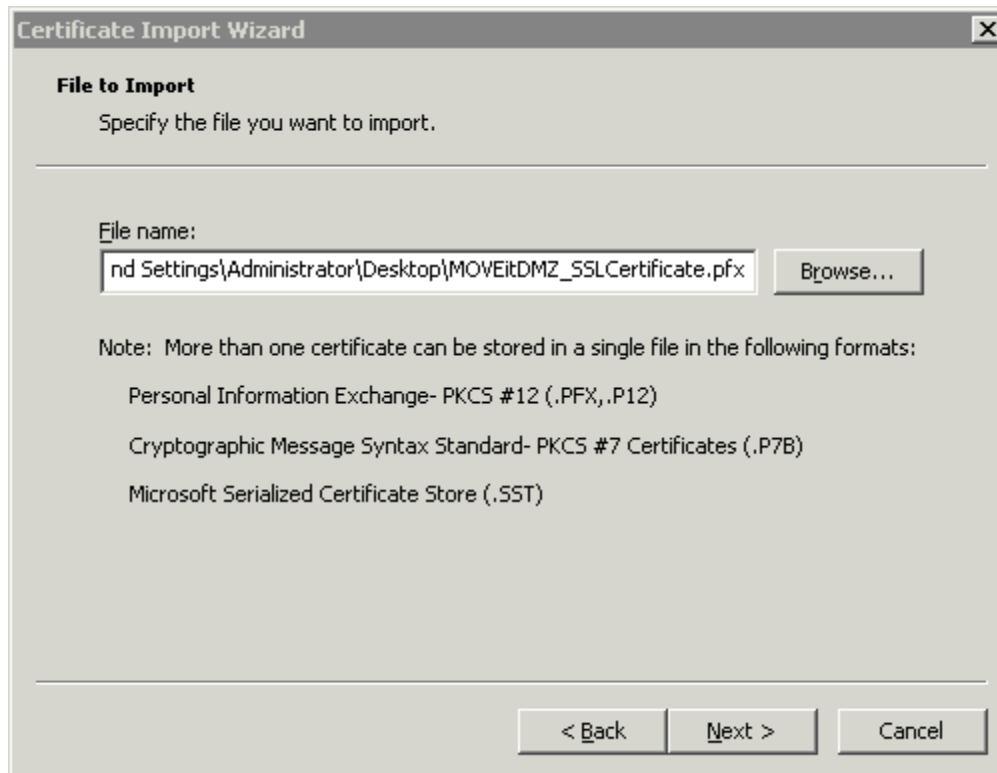
Now you have the Certificates Snap-in added. Select the **Personal** store and expand so you see Certificates. **Right-Click** on Certificates and select **All Tasks** and then pick **Import**. This will start the Import Wizard.



The Certificate Import Wizard, click Next.



Select the certificate you would like to import and click **Next**.



The image shows a Windows-style dialog box titled "Certificate Import Wizard". It has a standard title bar with a close button (X) in the top right corner. The main content area is titled "File to Import" and contains the instruction "Specify the file you want to import." Below this is a horizontal line. Underneath the line, there is a label "File name:" followed by a text input field containing the path "nd Settings\Administrator\Desktop\MOVEitDMZ_SSLCertificate.pfx". To the right of the input field is a "Browse..." button. Below the input field, there is a "Note:" followed by the text "More than one certificate can be stored in a single file in the following formats:". This is followed by three bulleted items: "Personal Information Exchange- PKCS #12 (.PFX,.P12)", "Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)", and "Microsoft Serialized Certificate Store (.SST)". At the bottom of the dialog box, there are three buttons: "< Back", "Next >", and "Cancel".

Certificate Import Wizard

File to Import

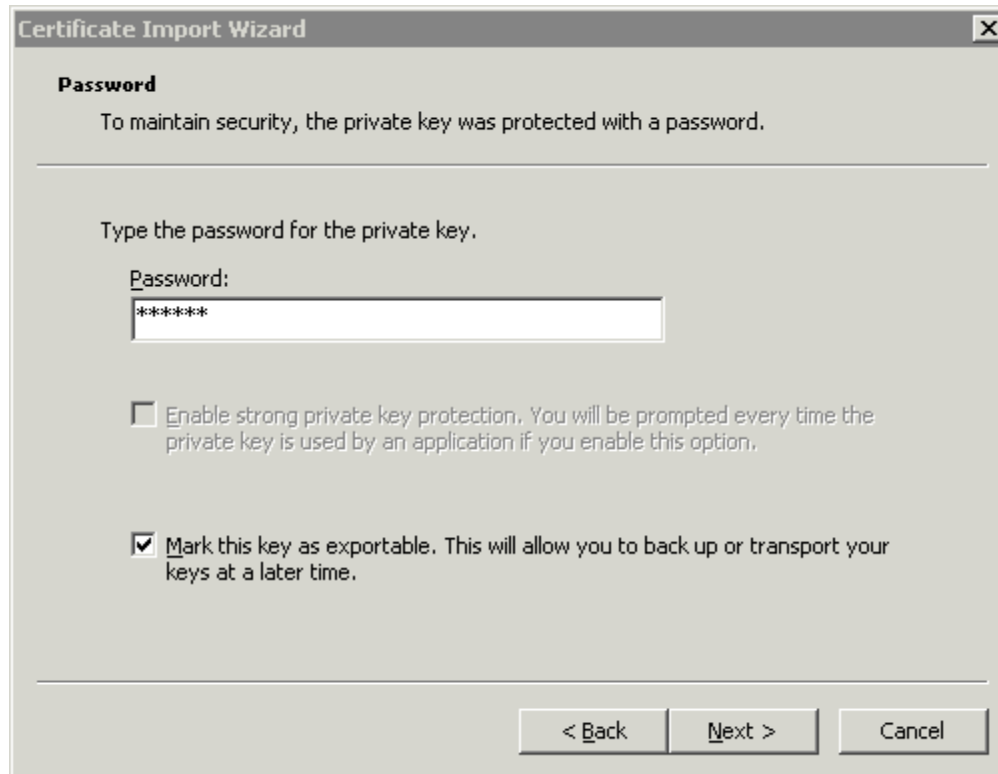
Specify the file you want to import.

File name:
nd Settings\Administrator\Desktop\MOVEitDMZ_SSLCertificate.pfx

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

If the certificate was exported with a password type the password and select Mark this key as exportable and click Next.



The image shows a Windows-style dialog box titled "Certificate Import Wizard". The window has a standard title bar with a close button (X) in the top right corner. The main content area is titled "Password" in bold. Below the title, there is a line of text: "To maintain security, the private key was protected with a password." A horizontal separator line follows. Below the separator, the text "Type the password for the private key." is displayed. Underneath this text is a label "Password:" followed by a text input field containing seven asterisks "*****". Below the input field, there are two checkboxes. The first checkbox is unchecked and is followed by the text "Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option." The second checkbox is checked and is followed by the text "Mark this key as exportable. This will allow you to back up or transport your keys at a later time." At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☒ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

< Back Next > Cancel

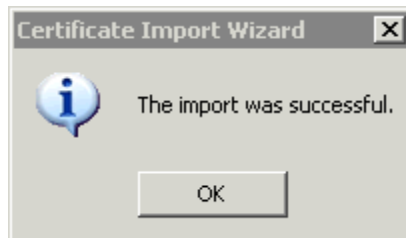
Place all certificates in the **Personal** store and click Next.



Verify the certificate import settings and click **Finish**.



If the import is successful a message similar to the one below should be displayed.

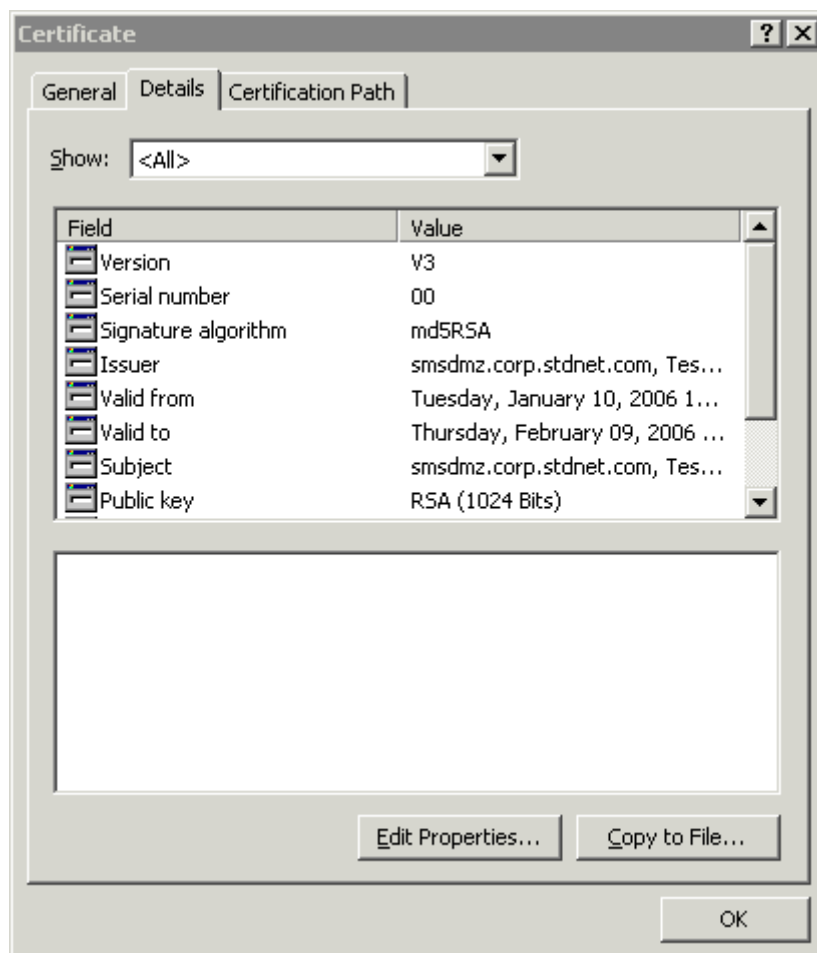


The certificate is now installed into the system and can be assigned to the DMZ Components.

Export an SSL certificate

Click Start -> Programs -> Administrative Tools -> Internet Information Services Manager (IIS Manager). Select the web site you wish to work with and Right-Click then select **Properties**. Click on the **Directory Security** tab then click **View Certificate...**

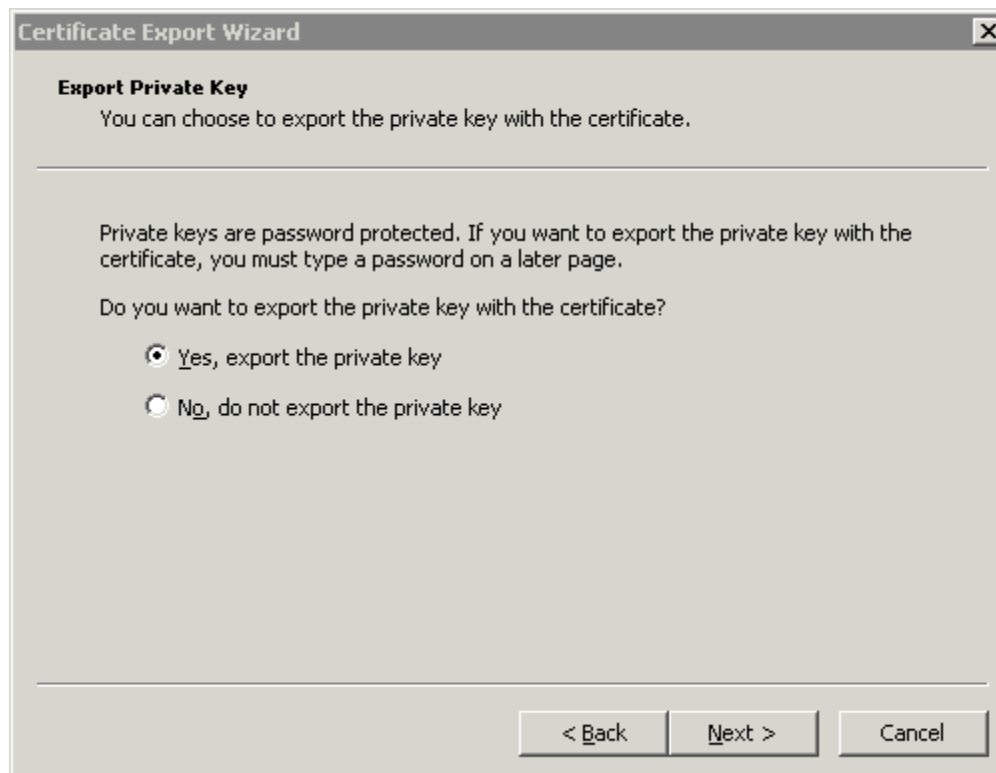
Click the **details** tab and select **Copy to File...**



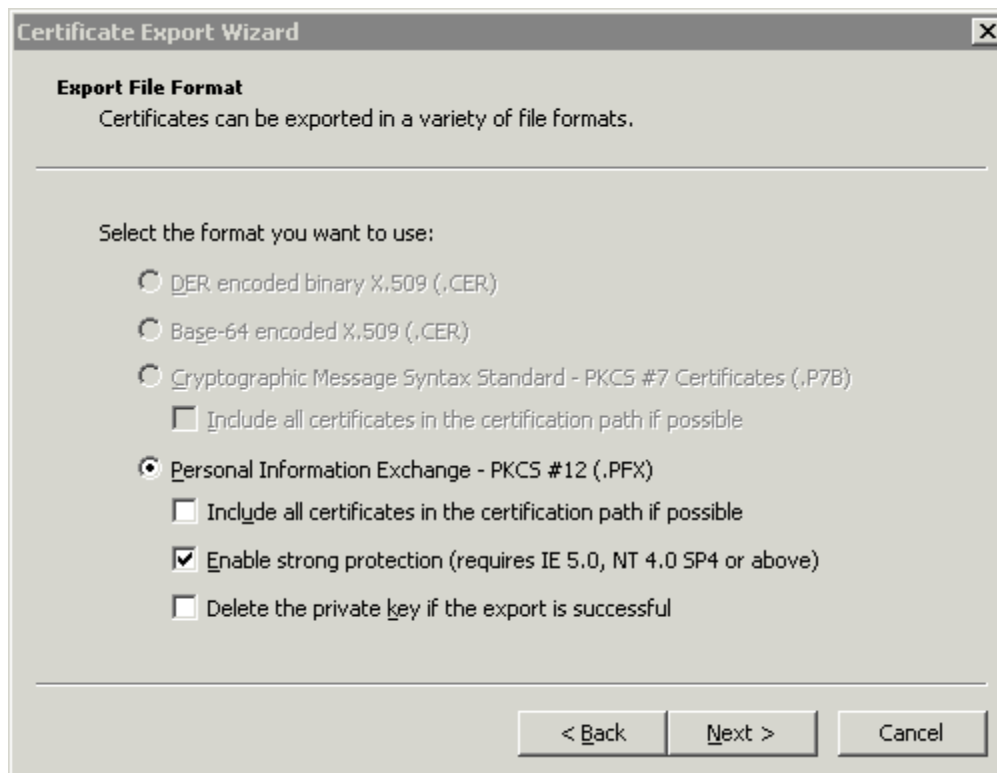
The Certificate Export Manager should be started, click Next.



Click **Yes** to Export the private key.



Select the .PFX format and check Strong Encryption then click Next.



Type in a password to secure the private key.



The image shows a Windows-style dialog box titled "Certificate Export Wizard" with a close button (X) in the top right corner. The dialog has a light gray background. At the top, the word "Password" is written in bold. Below it, a message states: "To maintain security, you must protect the private key by using a password." A horizontal line separates this message from the input area. The input area contains the text "Type and confirm a password." followed by two labels: "Password:" and "Confirm password:". Each label is followed by a text input field containing seven asterisks (*****). At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Password

To maintain security, you must protect the private key by using a password.

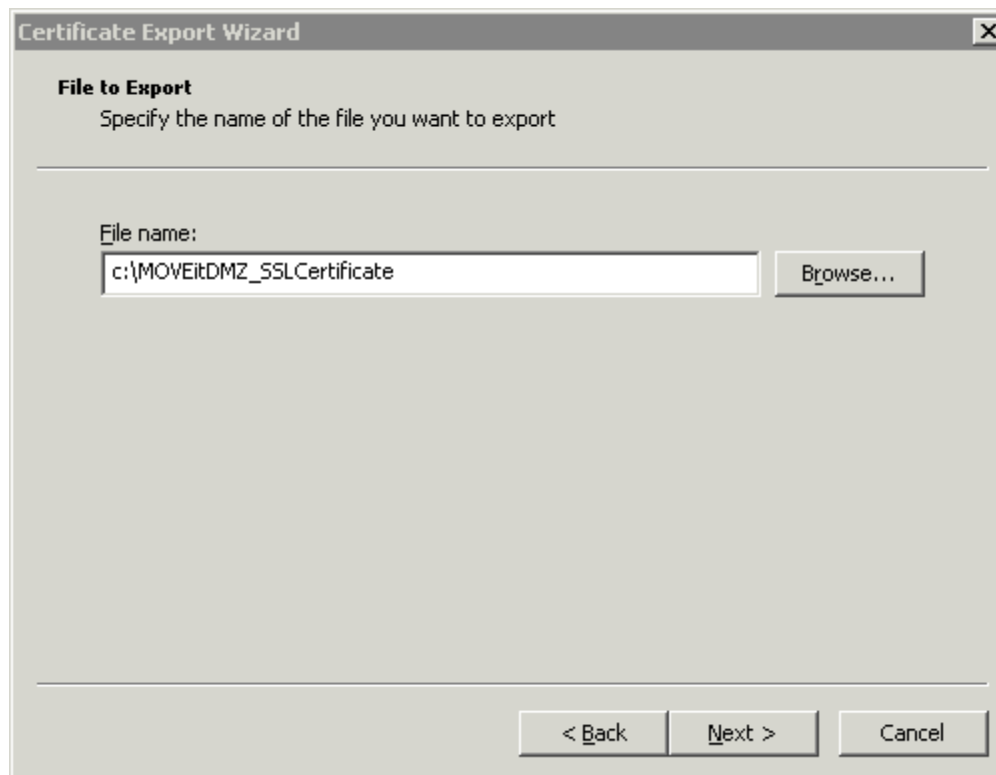
Type and confirm a password.

Password:

Confirm password:

< Back Next > Cancel

Specify a filename to save the certificate.



The image shows a Windows-style dialog box titled "Certificate Export Wizard". It has a standard title bar with a close button (X). The main area is titled "File to Export" and contains the instruction "Specify the name of the file you want to export". Below this is a horizontal line. Underneath the line, the text "File name:" is followed by a text input field containing the path "c:\\MOVEitDMZ_SSLCertificate". To the right of the input field is a "Browse..." button. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:

Verify the certificate export settings and click **Finish**.



If the export is successful a message similar to the one below should be displayed.

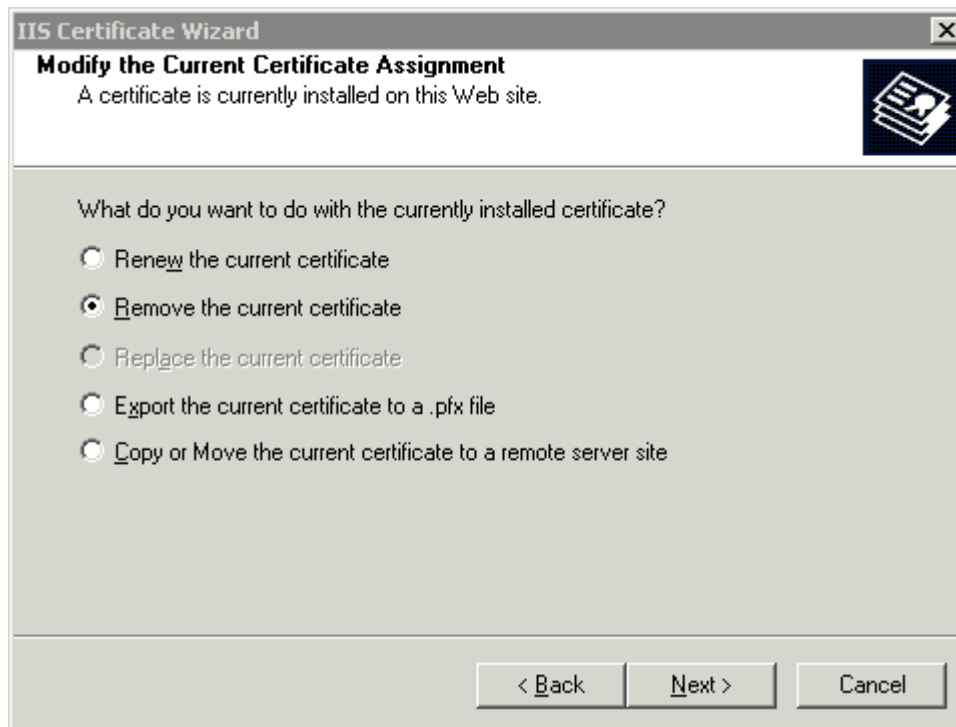


The certificate is now ready to be used or installed on another system.

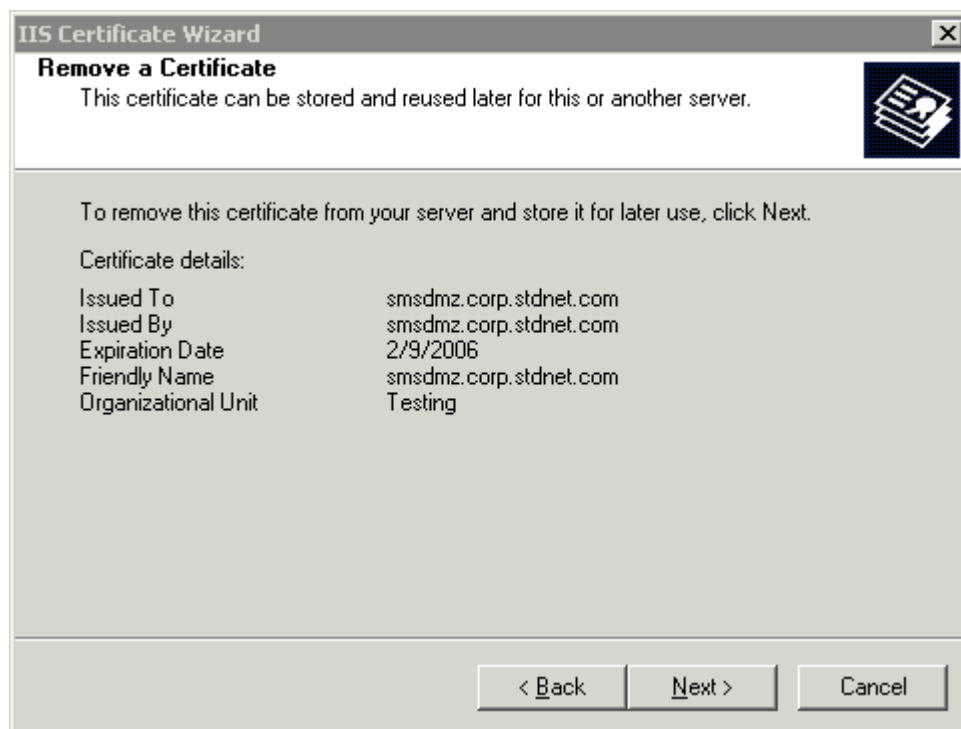
Removing an SSL certificate from an IIS web site

This assumes you already have an SSL certificate installed. Click Start -> Programs -> Administrative Tools -> Internet Information Services Manager (IIS Manager). Select the web site you wish to work with and Right-Click then select **Properties**. Click on the **Directory Security** tab then click **Server Certificate...**. This will start the Web Server Certificate Wizard, click **Next**.

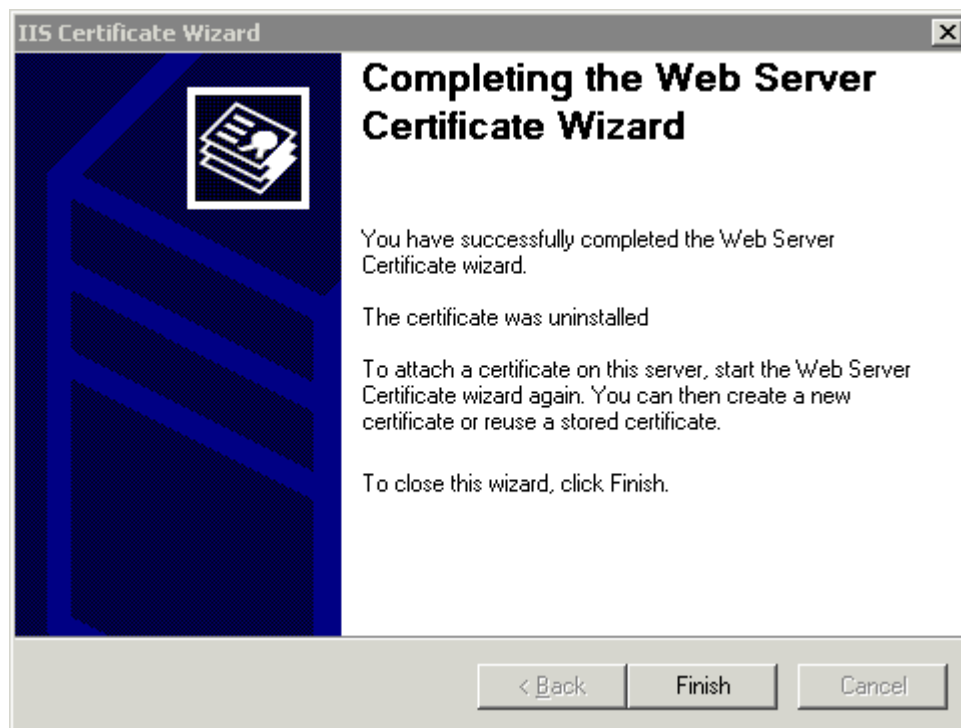
Select **Remove the current certificate** and click **Next**.



Verify the certificate that is about to be removed and click Next.



The certificate has been removed click Finish.



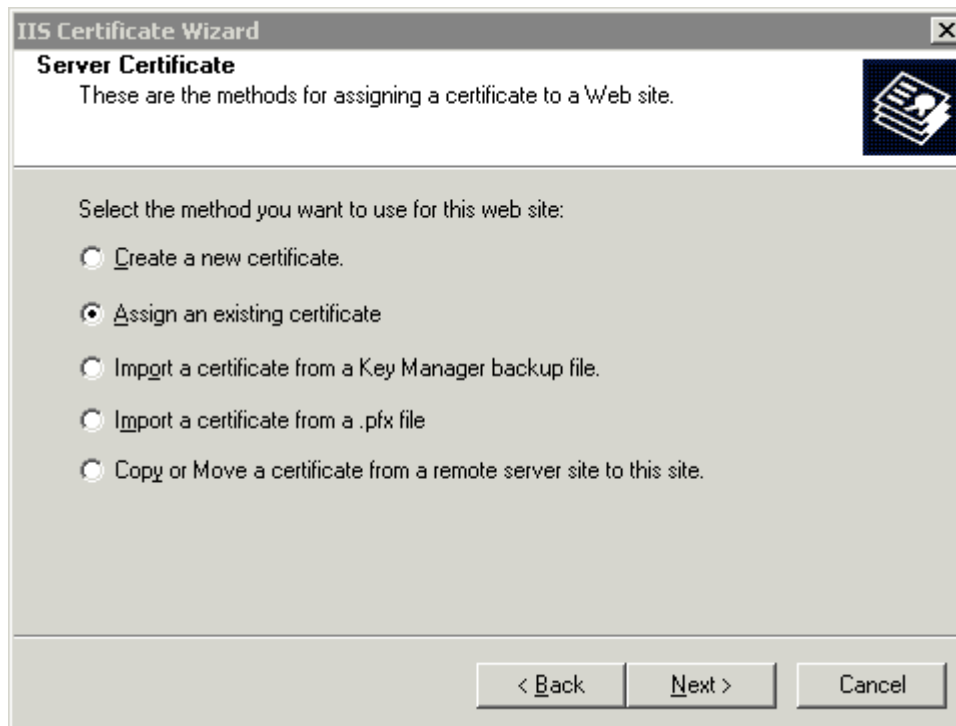
SSL - Server Certs - Assign to Components

Assign an SSL certificate to the MOVEitDMZ Web Site

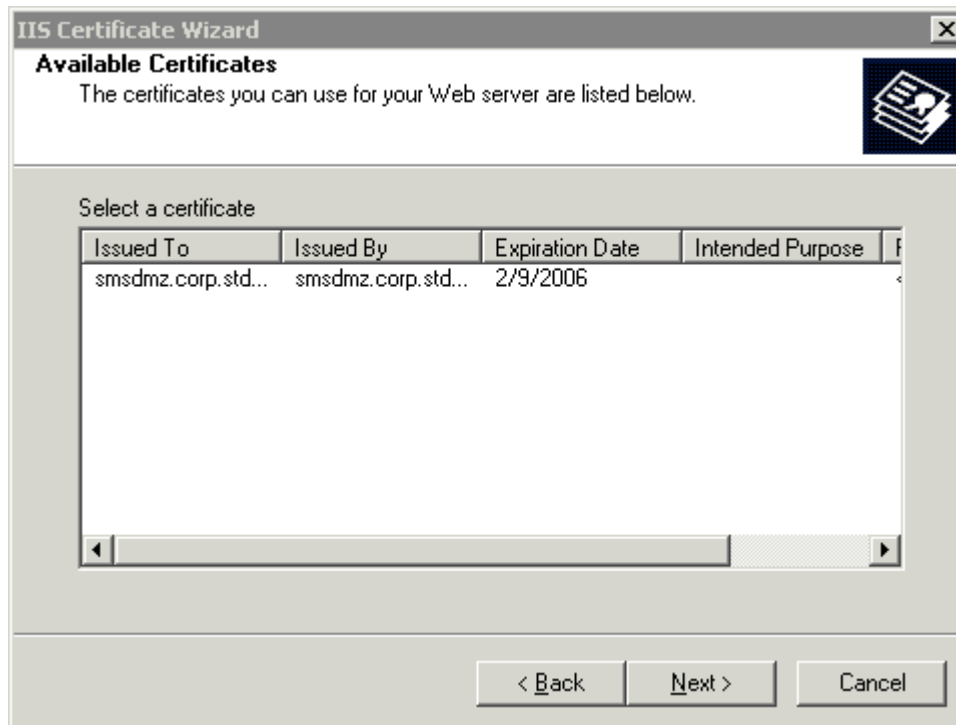
To perform these procedures please have your **SSL certificate(s) imported** (on page 191) already.

Click Start -> Programs -> Administrative Tools -> Internet Information Services Manager (IIS Manager). Select the web site you wish to work with and Right-Click then select **Properties**. Click on the **Directory Security** tab then click **Server Certificate....** This will start the Web Server Certificate Wizard.

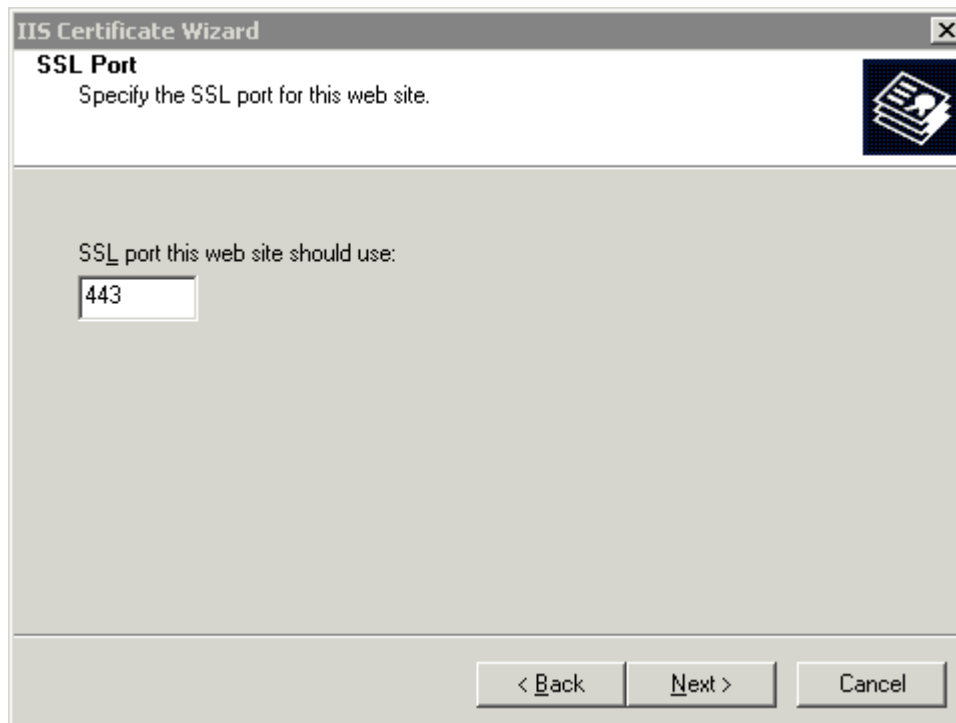
Select **Assign an existing certificate** and click **Next**.



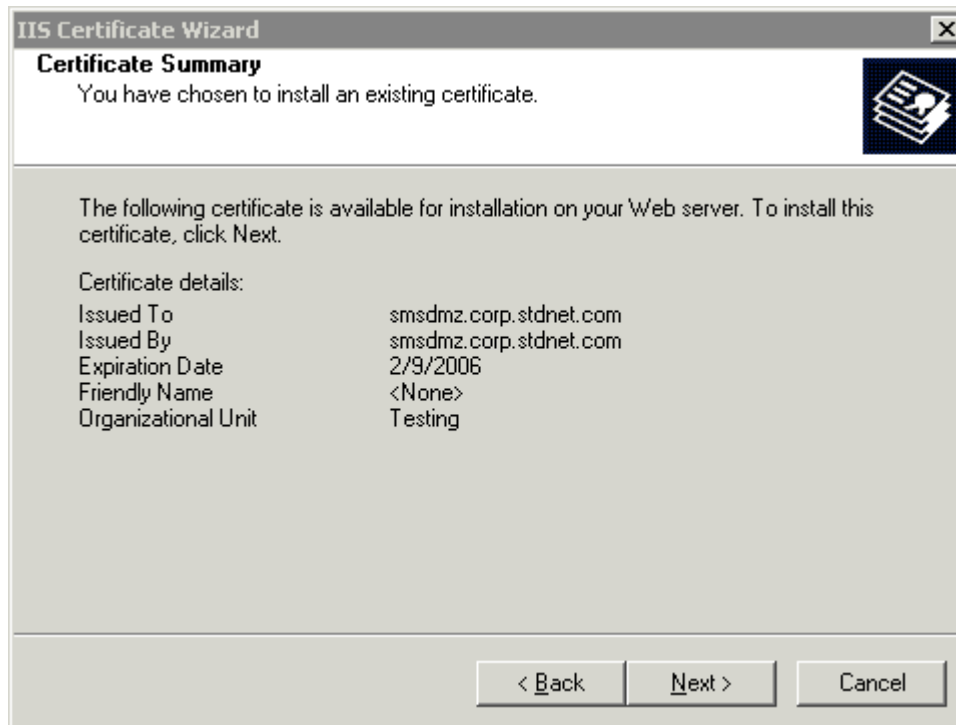
Select the correct certificate and click **Next**.



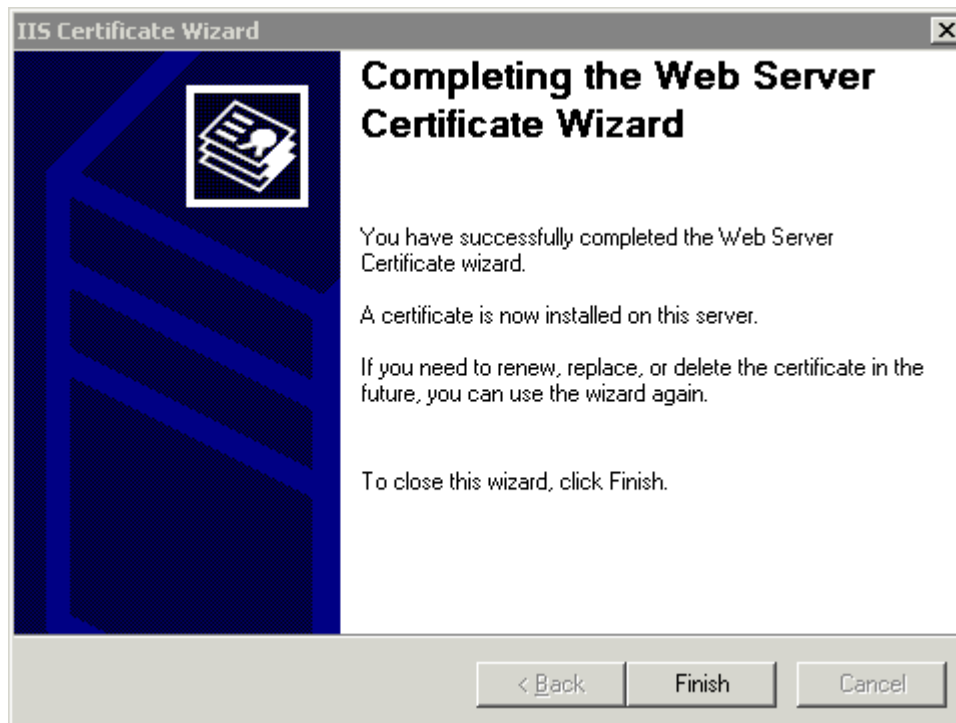
Select port (almost always 443) to use click **Next**.



Verify the certificate summary and click Next.



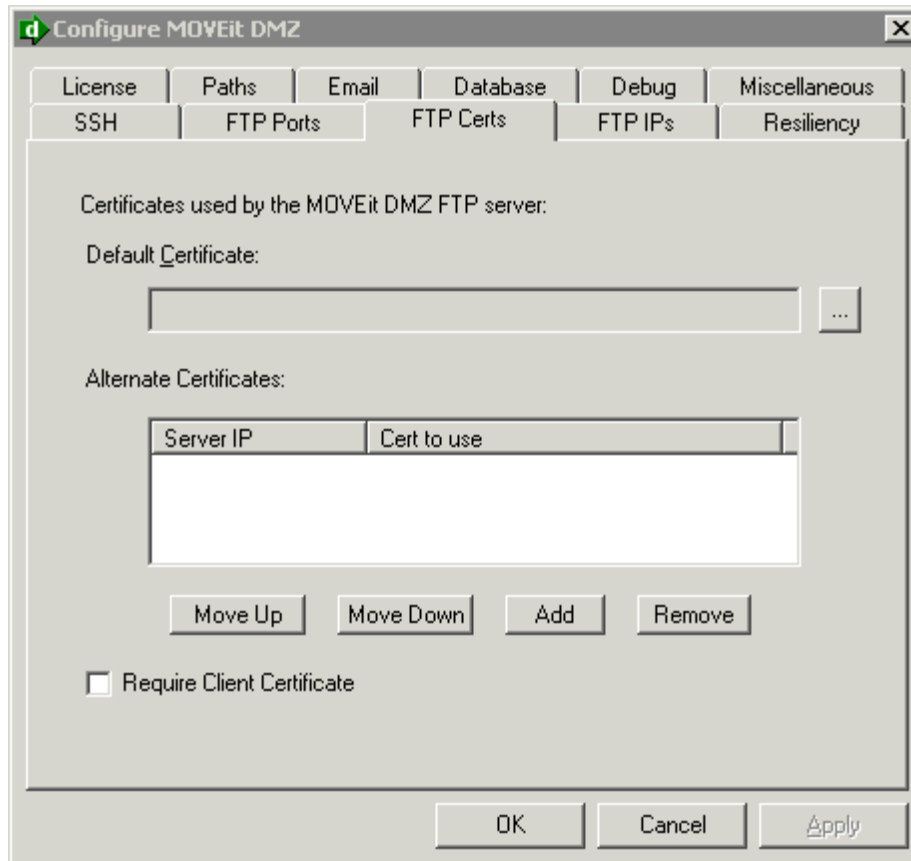
The certificate has now been assigned to the Web site, click Finish.



Assign an SSL certificate to the MOVEit DMZ FTP Server

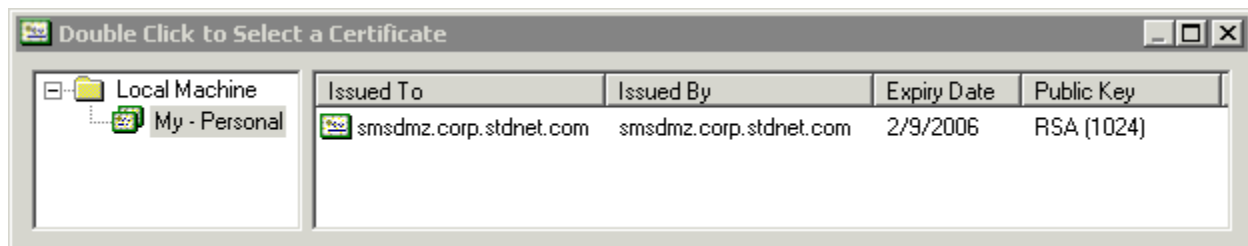
Remember to assign certificates to the FTP server when upgrading SSL certificates. This will cause FTP over SSL clients to fail if certificates are not updated.

Click Start -> Programs -> MOVEit DMZ -> MOVEit DMZ Config.

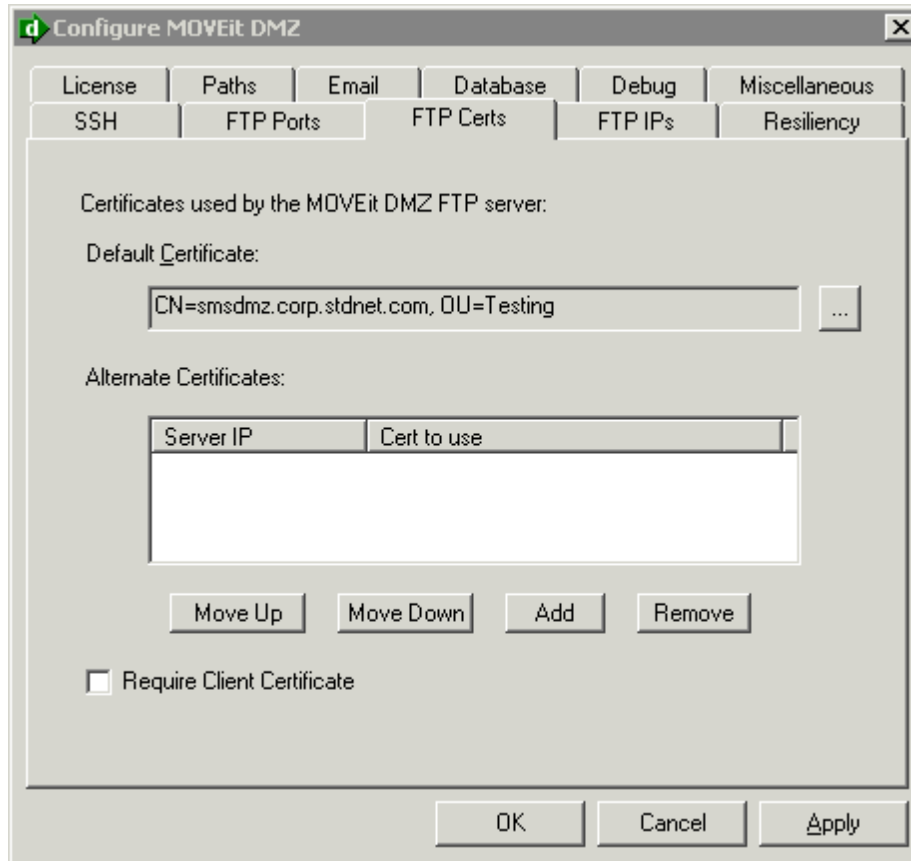


Select the FTP Certs tab and click the [...] box next to Default Certificate. This will open the Certificate Manager.

Click on My Personal under Current User or Local Machine (depending how the certificate was imported) and Double-Click the certificate that was used for MOVEit DMZ Web Site.



The Certificate selected should be selected and you can click Ok. The MOVEit DMZ FTP Server needs to be restarted for this to take effect.



To restart the MOVEit DMZ Service open a command prompt and type `net stop moveitdmzftp`. After the service has successfully stopped, type `net start moveitdmzftp`. The SSL certificate should now take effect in the MOVEit DMZ FTP server.

SSL - Server Certs - Backing Up

For backing up or replatforming a certificate, the easiest method is to use the ***MOVEit DMZ Backup and Restore utilities*** (on page 150), as these utilities handle the backing up and restoring of both server and client SSL certificates loaded on the system. Otherwise, if you need to export and import certificates manually, the following procedures are available to guide you.

Microsoft makes it easy to generate new certificates and replace existing certificates. However, exporting a certificate from one machine and importing it on another machine using the same Microsoft certificate facility is not as easy for two key reasons:

- By default, Microsoft tries to export keys without their private keys. While one could argue that this is good for security, many "next next next" administrators blow right by the configuration dialog where they should check the **export private key** box.
- Microsoft allows you to import server certificates without private keys. Although this feature is essential when defining obscure external certificates, the silent acceptance of these certificates often leads administrators to believe that they have successfully exported/imported a server certificate even though the private key was not moved.

There is one easy way to tell if you did an export/import procedure properly, however. If, when you try to import a certificate, you are prompted for a password, you probably did the procedure correctly. (A password is required to unlock the private key from an export file.)

If you are unsure why someone might export a server certificate in the first place, there are four general situations in which this occurs:

- You want a backup copy of the certificate so you can quickly restore the entire server if anything bad happens
- You are "replatforming" an existing secure server
- You do not have the funds to buy a certificate for a development or test box and you want to borrow a real certificate from your production box.
- You need to deliver the PUBLIC part of your certificate to a client for installation before that client will be allowed to connect (in this case, you do NOT export your private key)

Manual procedures to import and export SSL certificates are covered in ***SSL - Server Certs - Import and Export*** (on page 191).

- ***Telltale Errors*** (on page 220)
- ***Exporting MOVEit DMZ's SSL Server Certificate Without Private Key*** (on page 220)

Telltale Errors

You may have improperly exported/imported a server certificate (with a its private key) if you notice any of the following errors in your secure FTP server logs, secure web server logs or client displays:

- Your MOVEit DMZ FTP server logs report a "Not Loaded" certificate error.

- A locally installed copy of MOVEit Freely reports a "Handshake Error" when connecting to any valid FTP port on localhost.
- https:// connections to your web server are not logged in the IIS web logs.
- While running Internet Explorer on the same box as your web server, you get a "site not available" response when trying to connect to your web site via any https:// URL. (i.e. https://localhost/help.htm)

Exporting MOVEit DMZ's SSL Server Certificate Without Private Key (for import into various FTP clients)

Some FTPS (FTP/SSL) clients must import the MOVEit DMZ's SSL certificate, and possibly any root or intermediary CA certificates in the certification path, before the client can establish a FTPS connection with MOVEit DMZ. Since the same SSL certificate is used by both IIS (https) and MOVEit DMZ FTP (ftps), it is easy to export the certificates using Internet Explorer.

- *To export the MOVEit DMZ's host SSL certificate, perform the following steps:*
 1. Connect to the MOVEit DMZ using Internet Explorer (e.g., <https://moveit.stdnet.com>).
 2. Double-click the padlock in the status bar.
 3. Click the Details tab.
 4. Click the Copy to File button to start the Certificate Export Wizard.
 5. Follow the prompts to export the certificate in the desired format. If you're not sure which format, try Base-64.
- *To export the root CA and any intermediate CA certificates in the certification path, perform the following steps:*
 1. Connect to the MOVEit DMZ using Internet Explorer (e.g., <https://moveit.stdnet.com>).
 2. Double-click the padlock in the status bar.
 3. Click the Certification Path tab.
 4. Click the certificate you wish to export to select it.
 5. Click the View Certificate button. A second dialog will open.
 6. Click the Details tab.
 7. Click the Copy to File button to start the Certificate Export Wizard.
 8. Follow the prompts to export the certificate in the desired format.

Client Certs

This subsection describes SSL Client Certificates.

SSL - Client Certs - Overview

Just like the SSL server certificate is used to verify the identity of the server to the client, clients can also present SSL certificates to the server to help verify their identity. SSL certificates presented by a client to the server are called Client Certificates. While most SSL servers do not require clients to present their own certificates, more and more servers are starting to, as client certs provide an additional factor of authentication. MOVEit DMZ supports accepting or requiring client certs on both the FTP/SSL and HTTPS interfaces.

As is the case with almost any client key/certificate scheme, the higher security offered by cryptographic-quality client certificates is offset by additional administrative work. The SSL server must typically be configured to require client certificates or not (though IIS is able to accept client certificates if they are present, but still allow connections when they are not), and the client certificate must be trusted by the server for the connection to continue. Trusting a client certificate, like trusting a server certificate, requires either the certificate itself to be trusted, or the certificate be signed by a trusted Certificate Authority.

Client Certificate Connect/Authenticate Criteria

To use a client cert to authenticate a specific user to either the FTP/SSL or HTTPS interfaces, at least one of the following "CA" conditions and one of the following "credential" conditions must BOTH be true. Client certs must match one of the "CA" conditions in order to actually connect to MOVEit DMZ, while matching one of the "credential" conditions allows the client to authenticate to MOVEit DMZ.

- CA Conditions
 - The client cert itself must be installed in the Microsoft Trusted Root cert store.
 - The client cert must be signed by a CA cert which is trusted, either because the CA cert itself is installed in the Microsoft Trusted Root cert store, or a CA in the signing chain is installed in the Microsoft Trusted Root cert store.
- Credential Conditions
 - The client cert's thumbprint must be assigned to the specific user's profile.
 - The client cert's common name (CN) must be assigned to the specific user's profile AND the client cert's CA must be in the org-level list of approved CAs.
 - The client cert's common name (CN) must match the username or fullname of the specific user, the org-level **Match Cert CN to Username/Full Name** option must be enabled, AND the client cert's CA must be in the org-level list of approved CAs.

Client Certificate Connect/Authenticate Example - Fixed Cert, Flexible Criteria

To illustrate how these conditions would apply to a real certificate, consider a client certificate with the following characteristics.

- CN = "Frank"
- Thumbprint = "3D17 CFF3 E27B 127D 2753 A7F1 873E 2743 783B FBD2"
- Signed by CA cert with CN = "Chug and Ring"
- The CA cert has been signed by another CA cert with CN = "Toot"

To use this certificate to connect and authenticate a specific user, one of the following "CA" conditions and one of the following "credential" conditions must be true.

- To allow an SSL connection to occur, one of the following CA conditions must be true:
 - The "Frank" cert has been installed in the Microsoft Certificate Trusted Root cert store.
 - The "Chug and Ring" CA cert has been installed in the Microsoft Certificate Trusted Root cert store.
 - The "Toot" CA cert has been installed in the Microsoft Certificate Trusted Root cert store.
- To allow the client certificate to serve as a valid credential for a specific user, one of the following "credential" conditions must be true:
 - A thumbprint of "3D17 CFF3 E27B 127D 2753 A7F1 873E 2743 783B FBD2" has been assigned to the specific user's profile.
 - A CN of "Frank" has been assigned to the specific user's profile AND "Chug and Ring" has been added to the org-level list of approved CAs.
 - The specific user's username or full name is "Frank", the org-level Match Cert CN to Username/Full Name option has been enabled, AND "Chug and Ring" has been added to the org-level list of approved CAs.

Client Certificate Connect/Authenticate Example - Flexible Cert, Fixed Criteria

The following diagram provides an example in which the authentication criteria are fixed and a number of different client certs may be used for authentication. Please take a moment to find the following sections on the diagram:

- MOVEit DMZ Server: The three important stores of certification information and an important setting are pictured.
 - User Profile (Accepted Certs) of "Rich": Several thumbprints are listed here, as is the alternate CN of "Dick". ("Rich" is also an allowed CN because the Match CN to Username/Fullname option is checked.)
 - Trusted CAs: Certificates which present a CN for authentication must be signed by one of these CAs. Notice that one CA ("Verisign") is listed as trusted but certificates signed with this CA will fail to connect anyway because the CA is not installed in the Microsoft Trusted Root Certificate Store.

- Microsoft Trusted Root Certificate Store.: This is the only place client certificate information is installed (rather than referenced). All client certs must be signed by CA in this store (or be installed themselves) before any FTP/SSL connection will work.
- Match CN to Username/Fullname: See "User Profile..." above.
- Third-Party CAs: A selection of third-party CAs and some "reseller" CAs whose signing certificates have been signed by a "root-level" CAs.

Client Certs That Cannot Connect

(ANY) CA:Verisign	(ANY) CA:SwissKey	Th:CDGD	Dick	Rich

Client Certs That Connect OK But Cannot Authenticate

Dick CA:Comodo	Dick CA:Verisign	Dick CA:Thawte
Rich CA:Comodo	Rich CA:Verisign	Rich CA:Thawte
Th:3434 CA:Comodo	Th:3434 CA:Verisign	Th:3434 CA:Thawte

Client Certs That Connect OK And Authenticate OK

Dick CA:Comodo	Dick CA:Verisign
Rich CA:Comodo	Rich CA:Verisign
Th:5656 CA:Comodo	Th:5656 CA:Verisign

Th:ABAB

MOVEit DMZ Server

User Profile (Accepted Certs) of "Rich"

CN = Dick
Thumbprint (Th) = 5656
Thumbprint (Th) = ABAB

Trusted CAs

CN = TResell
CN = Verisign
CN = Comodo

☒ Match CN to Username/Fullname

Microsoft Trusted Root Certificate Store

Thawte

VResell
CA:Verisign

Comodo

Th:ABAB

Third-Party CAs

Thawte	Verisign	Comodo	SwissKey
TResell CA:Thawte	VResell CA:Verisign	CResell CA:Comodo	

Symbol Key

Sample	= Self-Signed Cert (CN="Sample")	Th:XXXX CA:Sample	= CA-Signed Cert (Thumbprint="XXXX", Signed by "Sample")

Given this configuration, various client certificates will connect and authenticate with various degrees of success, depending on the CN, Thumbprint and CA associated with each certificate. (Self-signed certificates are indicated by a large black bar where most other certificates list the name of their CA.)

- Client Certs That Cannot Connect: These client certs do not "chain up" to any certificate installed in MOVEit DMZ's Microsoft Trusted Root Certificate Store.
- Client Certs That Can Connect But Not Authenticate: All of these client certs "chain up" to a certificate installed in MOVEit DMZ's Microsoft Trusted Root Certificate Store. However, these certificates are not registered properly for authentication because:
 - The certificate has a matching CN but its CA is not a Trusted CA.
 - The certificate's thumbprint does not match a user profile thumbprint.

- **Client Certs That Can Connect And Authenticate:** All of these client certs "chain up" to a certificate installed in MOVEit DMZ's Microsoft Trusted Root Certificate Store. All of these certificates also authenticate properly because:
 - The certificate has a matching CN and has been signed by a Trusted CA.
 - The certificate's thumbprint matches a user profile thumbprint.

Client Certificate Administration

As said above, the tradeoff for the increased security of client certificates is increased administrative overhead, however MOVEit DMZ tries to make it as easy as possible to manage users with client certs. Administration of client certs is done via the Edit SSL Client Certificates page, which is accessible from the **User Profile** (on page 286). On the user profile page, click either the HTTP Policy or FTP Policy links...

User Authentication

Last Signon: 3/31/2014 1:15:04 PM

Account Status: Active - [Change Status](#)

Expiration Policy: No Policy Set - [Change Policy](#)

Authentication Source: MOVEit Only

Password: - [Change Password](#)

Credentials Required for Access: *(in addition to Username)*

HTTP Server:	Web Interface: Password Only with SSL	HTTP Policy
	HTTP Clients: Password Only with SSL	
FTP Server:	Secure (SSL): Password Only with SSL	FTP Policy
	Insecure: Not Allowed	
SSH Server:	SSH Client Key OR Password	SSH Policy
Mobile Interface:	Password, no caching allowed	Mobile Policy

Remote Access Policy:

IP/Hostname: Use Default Rules - [Select Ruleset](#) - [View Rules](#)

Multiple Signons: Allowed - [Change Multi Signons](#)

...then click on the Edit SSL Client Certificates link...

Edit HTTP Policy...

Press the "Change HTTP Policy" button to save changes to these settings.

Allow HTTPS Access via Web Interface:
☒ Yes
 ☐ No

Allow HTTPS Access via HTTP Clients:
☒ Yes
 ☐ No

SSL Client Cert Required:
☐ Yes
 ☒ No

Password also required with SSL Client Cert:
☒ Yes
 ☐ No

Change HTTP Policy

 **Edit SSL Client Certificates**

This will take you to the client certificate management page for the user.

User Profile (org1user1)

Current SSL Client Certificates...

Client Certificates in this list have been accepted as valid credentials for FTP and HTTP login.

Type	Data
There are no SSL Client Certificates registered	

Add (manually)
Import
Create New

[Trusted CAs](#)

Holding Tank...

SSL Client Certificates in this holding tank have been presented, but have not yet been accepted as valid credentials.

Type	Date and Time / Data
 SSL Thumb	4/11/2014 11:02:45 AM 669C5B9F800F1FD7FBFCBD93B393E369BBE8D7C
 SSL CN	4/11/2014 11:02:45 AM org1user1

Delete All Tank Certificates

~ OR ~ [Return to the full user profile](#)

From here, existing cert entries may be removed, new ones **added manually** (on page 227), **imported from a file** (on page 227) or **created from scratch** (on page 227). A "**Trusted CAs** (on page 235)" link also provides quick access to the list of trusted CAs and the **organizational CA** (on page 235) used to sign any client certificates created through the web interface. The section at the bottom of the page also allows any pending **Holding Tank** (on page 231) entries to be accepted or removed.

SSL - Client Certs - Importing/Creating

Importing Client Certificates

Often the easiest way to allow a user with an existing client cert to begin authenticating with that client cert is to have the user try signing on once and then accept the certificate entries that show up in the user and organization holding tanks (see the Holding Tank page for more information). However, sometimes a user will be able to present their certificate to administrators before they sign on for the first time. In this case, administrators may import that cert into MOVEit DMZ's stores, and potentially the Microsoft Trusted Root store if necessary.

Because of the way SSL certificates work, the only component administrators will need to import a user's client cert is the "public" portion. (The "private" portion of a client certificate must be kept by the user and should NOT be given out to anyone.) If the user is able to provide the public portion of their cert, it can be imported into MOVEit DMZ using the Import Existing Client Certificate page. To reach this page, go to the ***client cert administration*** (on page 222) page and click the **Import** link.

Import Existing Client Certificate.....

Select a *.cer file: No file selected.

When you click the "Import Certificate" button, one of the following things will occur:

If this certificate is self-signed, MOVEit DMZ will associate it with this user and trust it for use when establishing SSL connections.

If your certificate has been signed by a CA...

...trusted by this organization, the CN from this certificate will associate with this user.

...NOT trusted by this organization, an error will be returned instructing you to import and/or trust the CA cert first.

Once imported, MOVEit DMZ will be able to determine the nature of the certificate automatically. As mentioned on this page, if the cert is self-signed, DMZ will add the cert's thumbprint to the user record and import the cert into the Microsoft Trusted Root store, so that a user using the cert will be allowed to connect to the server. If the cert is signed by a CA, DMZ will check to see if that CA is trusted by the current organization first. If it is, DMZ will add the cert's CN to the user record. Otherwise, an error will be returned prompting the administrator to trust the CA before continuing.

Adding Client Certificates

If a user has an existing client certificate but is unable to provide administrators with the public portion directly, there is still a way to associate an element of that cert with the user's account, provided the user can give administrators specific information about the cert. If the user can provide either the thumbprint or CN of their client cert, administrators may add this information to the user record by going to the client cert administration page and clicking the **Add (manually)** link.

Add Client Certificate.....

To add a Client Certificate by hand, first enter the **New Certificate Data**:
Example SSL Cert SHA-1 Thumbprint: 7F51 3DCD A577 0923 0DD5 CF01 6EDE D8F3 7D6F F2EC
Example SSL Cert Common Name: John Q. Public

Certificate Data Type:

Then press the "Add Certificate" button:

Here, the administrator may add either the cert thumbprint or CN manually in the provided textbox, and then select which data type they are entering. Clicking the Add Certificate button will add the entered information to the user record.

Note: This method does not take care of any trust issues. In order for the user to connect to the server with their client cert, it must still be trusted, either by being in the Microsoft Trusted Root store if self-signed, or by being signed by a trusted CA.

Creating New Client Certificates

If a user does not have a client certificate, a certificate signed by the organization's CA can be generated by MOVEit DMZ. This cert will be automatically associated with the user account by thumbprint and provided to the administrator as a "[username].pfx" file so that the administrator can provide the cert to the user. The user must then import the new cert into their client cert store for whatever client they are using to connect to the server. (In most Windows environments, just opening a "*.pfx" client certificate file will launch a friendly client certificate import wizard.)

To create a new client cert for a particular user, go to a that user's SSL client cert administration page and click the **Create New** link. If you do not currently have an organizational CA to sign new client certificates, you will be provided with a link that will help you create one (if you are a full Admin). Otherwise, you will be taken to a form that asks for standard certificate information. Note that several fields, such as name, email address and organization will already be filled in with known values.

Create New CA-Signed Client Certificate.....

The following values should probably match those already found on this user's profile, but they do not need to match. Only the Name (CN) field is required:

Name (CN):

Email Address:

Organization:

The following optional fields are only related to this certificate; enter the most appropriate values or leave blank:

Country:

State/Province:

Organization Unit:

This information comes from the organization CA signing certificate:

Issuer: O=test, S=ma, C=test, E=test@ipswitch.com, CN=TestOrg

Set an appropriate valid date range for the certificate:

Valid Dates:

The following password will protect this certificate while resident on disk. You may choose to use the suggested password or pick one of your own. In either case be sure to record it. Your user will need this password in order to install the certificate.

Suggested Password: mb83ym

Password: ☒ Use Suggested Password ☐ Type Custom Password

Note: Be sure to remember the password either entered or selected. This password will need to be provided to the end user in order to successfully import the new cert.

Clicking the Create Certificate button will bring up a confirmation page, where the details of the new cert will be presented.

Create New CA-Signed Client Certificate.....

OK, you are about to generate a CA-signed client certificate with the following properties:

Version	V3
Serial number	(t.b.a.)
Signature algorithm	sha1RSA
Subject	CN = John Smith E = jsmith@stdnet.com C = US S = Wisconsin
Issuer	CN = TestOrg E = test@ipswitch.com C = test S = ma O = test
Valid from	3/31/2014 1:41:49 PM
Valid to	3/31/2015 1:41:49 PM
Public key	RSA (1024 Bits)

Press the button below to generate the certificate, link it to the current user and download the full certificate to you desktop (or other designated location). Only press this button once!

Create and Download Certificate

After you download the cert, you should find a way to securely pass it to your user (along with the password), confirm that they can import it (along with its private key) and delete the copy you have. If you did not record the password from the previous form, your user will not be able to import the certificate.

Upon clicking the Create and Download Certificate button, the certificate will be created, signed by the org CA, associated with the user, and presented to the administrator for download. The administrator will then be responsible for providing the new "*.pfx" cert file to the user so it can be imported, along with the password that was selected on the initial Create Client Certificate page.

The user should follow the procedures provided in the **Getting Started - SignOn** (on page 7) section to import their client cert into their browser.

SSL - Client Certs - Holding Tank

The client certificate holding tank holds certificates that have been presented by a user as authentication credentials but have not yet been accepted as valid credentials for that user. The holding tank is populated automatically whenever an SSL connection is established and a valid username is presented along with an invalid certificate. Holding tank entries will NOT be created if an SSL connection could not be established due to client cert trust issues.

The use of a holding tank in cert authentication situations makes it easy for administrators to accept specific certs for users without having to **manually add, import, or create** (on page 227) certificates into a user profile.

Walkthrough

The following procedure describes how an FTP/SSL client can connect with a new cert and leave the cert's fingerprint behind for an administrator to promote/accept into the user's profile at a later date. Any FTP/SSL user whose client has already installed an SSL client cert signed by a CA registered in MOVEit DMZ's Microsoft Trusted Root Certificate store should be able to use this procedure.

First, have the remote FTP/SSL client attempt to connect to MOVEit DMZ. This connection should fail. For example, the following MOVEit Freely session attempts to connect with a client key and fails.

```
C:\>ftps -ccn:lucy -e:on -a -user:moveitfreelydemo -password:a1s2d3 dotnet
```

```
220-Security Notice
```

```
220-You are about to access a secured resource. Ext Auth Mania reserves the
220 right to monitor and/or limit access to this resource at any time.
```

```
234 SSL enabled start the negotiation
```

```
Connected to dotnet.
```

```
530 Not logged in. Client Certificate is not registered.
```

```
ftp> quit
```

```
221 Goodbye
```

Next, sign on as an Admin to MOVEit DMZ and go to the **client cert administration** (on page 222) page of the user who just tried to authenticate. The second section on this page displays the Holding Tank entries for this user.

Notice that a single authentication attempt put TWO entries into the holding tank: one for the CN of the cert, and one for the thumbprint. Either may be accepted by clicking the Accept link for that entry.

If you accept the cert CN, you will avoid cert renewal issues if the end user gets an updated cert with the same CN but a different expiration date. However, you also run a risk of CN collision if any of this organization's Trusted CAs issue CNs with the same name to multiple people (e.g., Thawte Free Email certificates) or you have multiple trusted CA's.

If you accept the Thumbprint of the cert, you will encounter cert renewal issues if the end user gets an updated cert with the same CN but a different expiration date. However, you will avoid the risk of CN collision if any of this organization's Trusted CAs issue CNs with the same name to multiple people (e.g., Thawte Free Email certificates) or you have multiple trusted CA's.

As a rule of thumb, if you use a limited number of org-level Trusted CAs (e.g., your organization is its own CA), you should probably choose to accept CN's. If you use many Trusted CAs or you include CAs which issue certificates with the same CN to multiple people, you should probably choose to accept thumbprints. (Authentications using client cert thumbprints do not pay any attention to the list of Trusted CAs.)

In our example, we will accept the "SSL CN" of the client certificate because it was issued by a CA which never issues certificates with the same CN to different people.

After either the CN or Thumbprint is accepted, a confirmation screen will appear which contains several interesting pieces of information and a question. On the top of the page, there is a success message and a short display showing the accepted value (the CN, in this case). The question at the bottom of the page asks if you would like to get rid of the other holding tank entry the certificate created. You will usually want to click the DELETE option, but you could, technically, add both the CN and Thumbprint to a user record. (If you did this, the user would still only need to provide a cert with the correct CN or the correct Thumbprint - not both.)

FIX IMAGE - how to get something to display in holding tank?

User Profile (User)

Confirm Holding Tank Deletion

Type	Date and Time	Certificate
SSL Thumb	4/23/2014 12:53:08 PM	056251e9fe2569554e624731b6340d72ba33d107

Are you sure you want to delete this Holding Tank entry?

After electing to either delete or keep the other holding tank entries, you will be returned to the client cert administration page, where the newly accepted entry should now be present. At this point, it is time to try the FTP client sign on again.

```
C:\>ftps -ccn:lucy -e:on -a -user:moveitfreelydemo -password:a1s2d3 dotnet
```

```
220-Security Notice
```

```
220-You are about to access a secured resource. Ext Auth Mania reserves the  
220 right to monitor and/or limit access to this resource at any time.
```

```
234 SSL enabled start the negotiation Connected to dotnet.
```

```
331 Password required for moveitfreelydemo
```

```
230-Welcome to JGL Test Org. Enjoy your stay & have fun!
```

```
230 User moveitfreelydemo logged in.
```

```
200 PBSZ command successful
```

```
200 PROT command successful
```

```
215 Windows_NT version 5.0 (MOVEit DMZ FTP 3.1.8.6)
```

```
200 Integrity mode selected
```

```
ftp>
```

This time the sign on attempt worked.

Importing Certificates from the Organization-Wide Holding Tank

A complete list of all unassigned certs for all users in the organization may be viewed in the organization-wide holding tank. The organization-wide holding tank is accessible from the **Settings** page by following either the [Security | Interface Policy | FTP](#) or [Security | Interface Policy | HTTP](#) links. To assign specific certs, click into the complete list with the [View Tank Keys](#) link.

Trusted CAs...

A client certificate presented by a user must either have been signed by one of the CAs listed below or must match a specific thumbprint assigned to that user's profile before the certificate will be accepted as a valid user credential.

Type	Certificate
SSL CN	ORGANIZATION1

[Add CA \(manually\)...](#) [Import CA...](#) [Trust Microsoft CA...](#)

Client Cert CA Holding Tank...

Certificates in this holding tank have presented as CAs by incoming client certificates, but have not yet been accepted as a valid CA.

Type	Date-Time / Certificate
There are no client CA certs in the holding tank.	

User Client Certificate Holding Tank...

There are currently 2 client certificates in the holding tank.

[View Tank Certs...](#) [Delete All Tank Certs...](#)

The Holding Tank retention setting controls behavior on both the SSL (HTTP and FTP) and SSH interfaces.

Holding Tank retention: (days to keep holding tank certificates)

[Change Holding Tank Settings](#)

~ OR ~ [Return to the full organization settings](#)

Cert information is listed by username and then by type. Select the appropriate cert and click the **Accept** link next to it. After a cert has been accepted, the interface will return to the organization-wide holding tank so other keys may be assigned or deleted.

Settings (SSL Certs - Holding Tank)

Client Certificate Holding Tank...

Certificates in this holding tank have been presented by users, but have not yet been accepted as a valid credential.

Type	User / Certificate	Date and Time	Actions
SSL Thumb	org1user1 (org1user1) 669C5B9F800F1FD7FBFEFCBD93B393E369BBE8D7C	4/11/2014 11:02:45 AM	Delete - Accept
SSL CN	org1user1 (org1user1) org1user1	4/11/2014 11:02:45 AM	Delete - Accept

[Delete All Tank Certs](#)

~ OR ~ [Return to SSL Certificate Settings](#)

Cleaning Unassigned Certs Out of the Holding Tank

Unassigned certs will automatically be cleaned out the holding tank after a certain number of days. The exact number of days is a configurable option under the organization-wide SSL policy. (The same value applies to unassigned SSH client keys and untrusted CA certs in the holding tank.)

Unassigned certs may also be manually cleaned out an individual user's holding tank or the organization-wide holding tank using any of the provided **delete** or **delete all** links.

SSL - Client Certs - Trusted CAs

A client cert's SHA-1 Thumbprint provides a cryptographic-quality way to prove that a specific certificate is what it says it is. A client cert's CN, however, could be found on hundreds or thousands of other perfectly valid client certs. The way MOVEit DMZ avoids mix-ups and keeps track of certs which use CN authentication is to follow their CA chain and to only allow certs which have been signed by a short list of Trusted CAs to authenticate.

By definition, a Trusted CA is a CA that an organization trusts with providing properly (CN) named certificates to the correct users. If a CA issues certificates with the same CN to multiple users (e.g., "Thawte Personal Freemail CA"), then that CA should NOT be a Trusted CA. If your organization already maintains its own CA, then that CA should probably be in your list of Trusted CAs. Third-party organization CA's may or may not also be added as trusted CAs depending on how well you trust their ability to issue unique CN-named certificates to the correct users.

Trusted CA vs. Microsoft Trusted Root Certificate Store

The Microsoft Trusted Root Certificate Store contains installed certs of CAs. All client certs which connect to MOVEit DMZ must "chain up" to a cert installed in the Microsoft Trusted Root Certificate Store. Once an SSL connection is established, however, the Microsoft Trusted Root Certificate Store has no further role in authentication.

The Trusted CAs is a (CN) list of CAs; no certificates are actually installed here. Client certs which offer a CN for authentication must be signed by one of the CAs listed here, but CAs in this list do not actually need to be in the Microsoft Trusted Root Certificate Store too as long as each Trusted CA "chains up" to an entry in the Microsoft Trusted Root Certificate Store. The Trusted CA list is available on the org-level SSL settings page, which is accessible from the **Settings** page by following either the **Security | Interface Policy | FTP** or **Security | Interface Policy | HTTP** links.

Trusted CAs...

A client certificate presented by a user must either have been signed by one of the CAs listed below or must match a specific thumbprint assigned to that user's profile before the certificate will be accepted as a valid user credential.

Type	Certificate	
SSL CN	ORGANIZATION1	

Add CA (manually)...Import CA...Trust Microsoft CA...

Client Cert CA Holding Tank...

Certificates in this holding tank have presented as CAs by incoming client certificates, but have not yet been accepted as a valid CA.

Type	Date-Time / Certificate

There are no client CA certs in the holding tank.

User Client Certificate Holding Tank...

There are currently 2 client certificates in the holding tank.

View Tank Certs...Delete All Tank Certs...

The Holding Tank retention setting controls behavior on both the SSL (HTTP and FTP) and SSH interfaces.

Holding Tank retention: (days to keep holding tank certificates)

[Change Holding Tank Settings](#)

~ OR ~ [Return to the full organization settings](#)

Please also see the **Connect/Authenticate examples** (on page 222) on the Client Certs - Overview documentation page for an illustration of how the Trusted CA vs. Microsoft Trusted Root Certificate Store work together.

Trusted CA Holding Tank

The Trusted CA list has its own holding tank similar to the **client cert holding tank** (on page 231). To get a CA certificate entry in the Trusted CA holding tank, a user must connect with a client cert that "chains up" to a CA in the Microsoft Trusted Root Certificate Store and whose thumbprint does not match the related user profile.

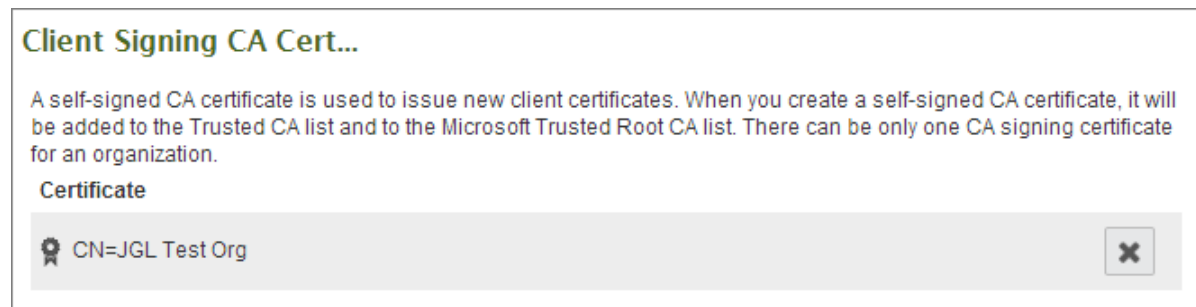
Trusted CA List Maintenance

There are two other ways to add Trusted CAs. One is to manually type the CN of a Trusted CA. The other is to scroll down and select any of the CA certs already installed in the Microsoft Trusted Root Certificate Store (or Microsoft Intermediate CAs Store).

When you delete a Trusted CA entry, you are only deleting a pointer, even if the Trusted CA is also installed in the Microsoft Trusted Root Certificate Store. (You must delete certificates directly from the Microsoft Trusted Root Certificate Store using the usual MMC console if that is the desired action.)

Organization Cert-Signing CA

Every organization on MOVEit DMZ can create and use a single CA certificate to sign any client certificates created through MOVEit DMZ's web interface. These CA certificates are "self-signed" but are automatically included in and installed through the "*.pfx" client certificate files created during the new client certification creation process.



Background: In version 4.0, MOVEit DMZ generated self-signed client certificates (i.e., certificates not signed by any CA) through a similar interface. However, in practice only about 100-200 self-signed client certificates can be supported under the default IIS configuration so client certificates created by MOVEit DMZ are now CA-signed to avoid this limit.

How and When to Create an Organization Cert-Signing CA

If you have been directed to create an organization CA to sign client certificates (after clicking a **Create New** link) or you see a **Client Signing CA Cert** section like the following section...

Client Signing CA Cert...

A self-signed CA certificate is used to issue new client certificates. When you create a self-signed CA certificate, it will be added to the Trusted CA list and to the Microsoft Trusted Root CA list. There can be only one CA signing certificate for an organization.

Certificate

There is no CA Certificate.

Create CA Certificate...

...you should create an organization client cert-signing CA certificate. To do so, click the **Create CA** link in this section and fill out the following form. This signing certificate will be visible on any client certificate you or any other administrator creates through MOVEit DMZ's web interface, so it is usually worth the time to provide meaningful answers to each question on the form. Also, the duration of this certificate should be **LONGER** than the duration of any particular client certificate you plan to issue now or in the future.

Create CA Certificate ...

Enter the the appropriate values. Only the Name (CN) field is required:

Name (CN):	MOVEitSample
Email Address:	techsupport@moveitdmz.com
Organization:	MOVEit Sample
Country:	USA
State/Province:	MA
Organization Unit:	Demonstrations

Set an appropriate valid date range for the certificate:

Valid Dates:

When you click the "Create CA Certificate" button, the selected certificate will be added to the Microsoft Trusted Root Certificate Store and also to the Trusted CA list.

Create CA Certificate

Once an organization's CA cert has been created, it is generally an invisible part of the client cert creation process; there is no CA cert drop-down or similar control to worry about.

SSL - Client Certs - Troubleshooting

Like other connection problems, such as with FTP connections, client certificate problems can be broken down by analyzing "how far did the client get." The following guide provides a quick overview of the client certificate troubleshooting process. Also make sure you familiarize yourself with the **CA and credential requirements** (on page 222) all clients need to meet to successfully connect and authenticate with a client cert.

Client cert-related connection issues are generally the result of one of three problems: failure to establish a TCP connection, failure to establish an SSL session, and failure to authenticate. All client cert troubleshooting should explore these factors in this order. For FTP connections, TCP connectivity is covered in the regular FTP/SSL Troubleshooting guide; the other two issues are covered here.

- Problem: Cannot Connect
 - Make sure firewall and other basic connectivity issues do not apply
 - Is the client configured to use a client certificate?
 - Is the client OK with the MOVEit DMZ server certificate?
 - Is the CA of the client certificate installed in the MOVEit DMZ Microsoft Trusted Root Certificate Store? (If not, is the client certificate itself installed here?)
- Problem: Cannot Authenticate
 - If you cannot connect, you don't need to worry about authentication issues yet.
 - Check the user profile.
 - Is a client certificate required? (If not, this is a password problem.)
 - If a password is required when a client certificate is required, did the client provide one?
 - If the org-level option to match cert CNs to usernames/realnames is enabled and the client certificate CN matches the username/realname of this user, is the CA of the client cert in the org-level list of Trusted CAs?
 - Otherwise, are there any entries in the user's client cert holding tank? (If so, accept the appropriate entry.)
 - Is the CN of the client cert listed as an accepted cert in the user profile? (If so, make sure the CA of the client cert is in the org-level list of Trusted CAs.)
 - Pull a user report for the user. Drill down into the log entries for additional clues.

Frequently Asked Questions

Q: I checked the "require certs" on my user profile but MOVEit DMZ is ignoring the client cert.

A: You also need to configure the **Client Cert ports** option on the **FTP Ports** tab of the **MOVEit DMZ Config** (on page 577) utility. Your FTP client will also need to connect to one of the two client cert ports rather than one of the two **non-cert** ports before client cert authentication will succeed.

Q: What's the best way to migrate my users to client certificates?

A: Turn on the **Client Cert ports** option on the **FTP Ports** tab of the MOVEit DMZ Config utility (and open the matching firewall ports) now. As each of your clients migrate to FTP client certificate authentication, instruct them to switch their connection parameters from a **non-cert** port to a client cert port.

Q: I generated a client certificate but when I try to connect it doesn't show up in the client certificate holding tank.

A: One of two things needs to occur before MOVEit DMZ will allow the client to establish an SSL connection using that client certificate. The self-generated client certificates either needs to be signed by a CA whose certificate is already in MOVEit DMZ's Microsoft Trusted Root Certificate Store, or the self-generated client certificate itself needs to be imported into MOVEit DMZ's Microsoft Trusted Root Certificate Store. Instructions to perform either operation are available from the **Client Certs - Importing and Creating** (on page 227) page.

Q: I accepted a client certificate CN as a valid credential for a particular user, but that user still gets a "certificate not registered" error when he tried to connect.

A: The client certificate's CA has probably not been assigned as a trusted CA within the organization. Check to see if the client certificate's CA is in the **Client Cert CA Holding Tank** (on page 235)

Additional Help

For additional help, you may want to consult the Knowledge Base on our support site at

http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ
(http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ).

SSL - Client Certs - IIS Configuration

MOVEit DMZ relies on Microsoft's IIS server to provide HTTPS connection services. Therefore, MOVEit DMZ must also rely on IIS to also provide **client certificate** functionality.

MOVEit DMZ users must use client certificates that are ultimately trusted or stored in the Microsoft Certificate Trusted Root store, but MOVEit DMZ's certificate management interface usually takes care of this requirement behind the scenes. This section focuses on the IIS settings that the MOVEit DMZ installation/upgrade toggles to turn on client certificate support (by default) and a second supported option.

IIS Set to Accept Client Certs on Some Files

MOVEit DMZ's web interface supports client certificate authentication as soon as it is installed or upgraded to version 4.0 or higher. No manual changes to IIS are required; the installation/upgrade program sets the necessary IIS settings behind the scenes.

Authentication requirement flags on individual user accounts control whether client certificates are required and what client certificates can be used for authentication. (See **Web Interface - Users - Profile** (on page 286) for more information about this.)

Advantages/Disadvantages

- Advantage: Requires no additional set up or administrative work.
- Advantage: Easy to use when migrating users to client certificate environment.
- Advantage: Backwards compatible with existing clients and processes.
- Disadvantage: Auditors may prefer the **Require client certificates** box on IIS is checked.

humancc.aspx and machinecc.aspx

By default, MOVEit DMZ sets the **Accept client certificates** flag on two files: **humancc.aspx** and **machinecc.aspx**. The "cc" in both files stands for "client certificate."

All web browser sessions must authenticate through **human.aspx** and all other clients must authenticate through **machine.aspx**. When a user attempts to authenticate through either **human.aspx** or **machine.aspx** and MOVEit DMZ notices that the user's account requires client certificate authentication, MOVEit DMZ will automatically redirect the user's session to **humancc.aspx** or **machinecc.aspx**. At this point the user will be prompted for client certificate credentials (if using a web browser) or client certificate credentials will be consumed (if using another client). No "second sign on page" is presented; from the user's perspective the entire sign on operation requires only a single submission.

No other files or folders are marked to "Accept client certificates". Access to MOVEit DMZ resources is only possible after a user authenticates with any required client certificates, so only the authentication gateways need to be marked to **Accept client certificates**.

Site-wide "Accept Client Certificates" Flag (Don't Set It!)

Do not set the site-wide **Accept client certificates** flag on your MOVEit DMZ IIS website. This configuration is not supported and is not necessary to require individual MOVEit DMZ users to use client certificates while authenticating.

Two signs that someone may have flipped the site-wide **Accept client certificates** on your moveitdmz IIS site are:

- Your IE users are prompted with a mysterious and empty dialog box when they connect to MOVEit DMZ. The empty box is IE's unusual way of telling the user that the site they just connected to has asked for a client certificate (that's what the IIS **Accept** flag does) but that the user doesn't have any client certificates that would work with the site.
- All file transfers stop working and all FTP and SSH signons are rejected.

IIS Set to Require Client Certs on Most Content

Setting the IIS site flag to **Require client certificates** is usually not necessary and is generally not recommended unless it is absolutely required. The large amount of work required by administrators, end users and operators of remote systems usually makes implementing a pure IIS "Require" environment harder than explaining to an auditor why MOVEit DMZ's application-level client certificates is a better choice.

Furthermore, the **Require client certificates** flag is only supported by MOVEit DMZ software under Windows Server 2003.

Advantages/Disadvantages

- Advantage: Auditors may like that the **Require client certificates** box on IIS is checked.
- Advantage: No one can sign on from a remote location without using a client certificate. (No exceptions.)
- Disadvantage: Admin users will lose remote access if they no longer have a valid client certificate.
- Disadvantage: Requires additional set up and administrative work.
- Disadvantage: Makes migrating users to client certificate environment tough.
- Disadvantage: Not backwards compatible with existing clients and processes.

Extra Localhost-Only IIS Site

MOVEit DMZ's FTP, SSH, ISAPI and related services often communicate with the core MOVEit DMZ application through HTTP/S-based XML transactions. To allow this conversation to continue in a **Require client certificates** environment, you must make a copy of the original moveitdmz IIS and set it to listen for localhost connections only.

To set up this extra site and configure MOVEit DMZ to use it in the context of setting the IIS site-wide **Require client certificates** flag, use the following procedure.

- 1** Open the IIS manager and **Export** the moveitdmz IIS site.

- Right-click your existing MOVEit DMZ site
 - Choose **All tasks** and then **Save configuration to file**
- 2** Import the site you just exported and click through the **duplicate name** warning. (This warning is harmless and will allow you to import the site anyway.)
- Right-click the **Web Sites** heading
 - Choose **New** and then **Web site from file**
 - Browse to the file created in step 1
 - Click on the **Read file** button, select the site name and click **OK**
- 3** Rename the new site. (The duplicate name situation will be harmful if you leave it.)
- 4** Open the new site and perform these steps in this order:
- Set client certificate requirements to **Ignore**
 - Uncheck the **128-bit SSL** requirement box, if checked.
 - Uncheck the **Require SSL**, if checked.
 - Remove any server certificates associated with the site.
 - Bind the site to 127.0.0.1 only (no host headers) and clear out the SSL port. Fill in the (non-SSL) port with a value of 80 if it is not currently populated.
- 5** Open the original `moveitdmz` site and make sure it is not explicitly bound to 127.0.0.1.
- 6** Open the MOVEit DMZ Configuration utility, go the **Paths** tab and set the machine URL to `http://localhost/machine.aspx`.
- 7** At this point you can turn on the **Require client certificates** option on the `moveitdmz` site. If you are prompted, you should override settings on all folders and files except those listed in the "Exceptions" section below. Make sure that the file security setting for `humancc.aspx` and `machinecc.aspx` is to require SSL and to require client certificates.
- 8** Make sure that both sites are started.
- 9** Test with the MOVEit DMZ Check utility (may skip some tests) and later with live client sessions to make sure everything still works.

Exceptions

Although the default client certificate property on your moveitdmz IIS site will be set to **Require...**, the following folders must always be marked **Ignore client certificates** to support the use of the Java Upload/Download Wizard.

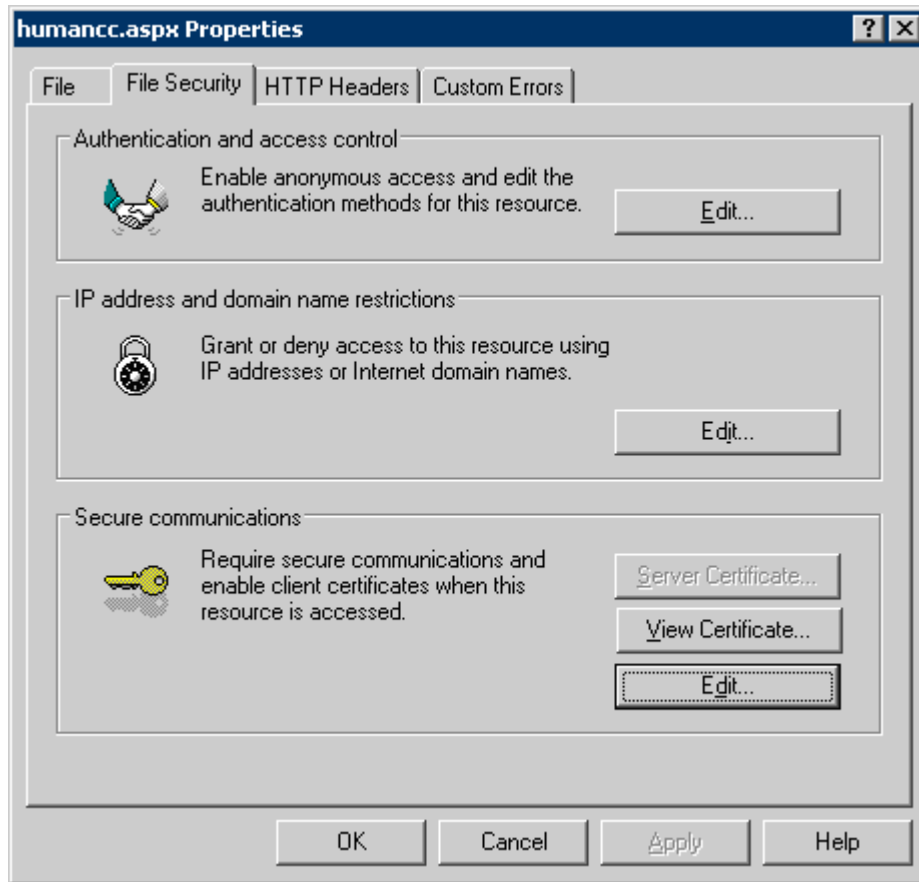
- **MOVEitISAPI:** The **Ignore client certificates** checkbox must be checked to avoid client certificate complications when using the Java Upload/Download Wizard. It is safe to do this because this file transfer facility will not grant access to files unless a session was previously authenticated
- **Java:** The **Ignore client certificates** checkbox must be checked to avoid client certificate complications when using the Java Upload/Download Wizard. This folder is the home of the Java Upload/Download Wizard applet that is downloaded and run by web browsers. It is safe to do this because the contents of this folder are publicly available from any other MOVEit DMZ server.
- **Images:** The **Ignore client certificates** checkbox must be checked to avoid client certificate complications when using the Java Upload/Download Wizard. This folder is the home of the images used in the Java Upload/Download Wizard applet. It is safe to do this because the contents of this folder are publicly available from any other MOVEit DMZ server or publicly available to anyone with access to the (public) MOVEit DMZ sign on page.

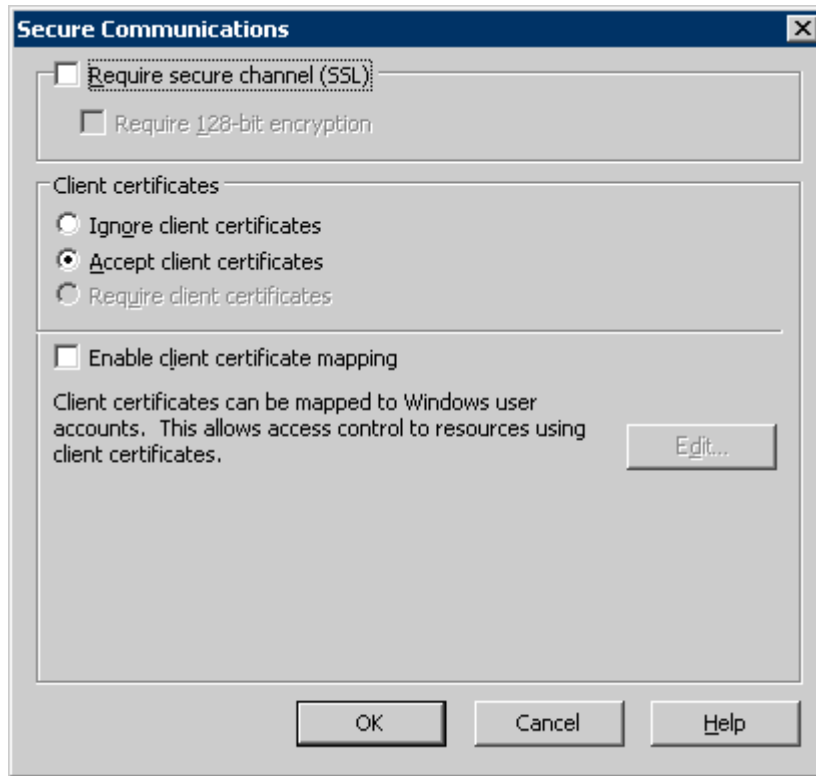
The MOVEit DMZ installation and upgrade programs will reset **Ignore client certificates** on these folders automatically when they are run. (However, **Repair** installation actions will not reset these parameters.)

Reverting from "Require..." to "Accept..."

To revert from **Require...** to **Accept...**, the easiest way to proceed is to set the IIS site-level client certificate requirement from **Require...** to **Ignore...** and then force a MOVEit DMZ upgrade (not just a "repair") to reset the appropriate properties on other elements in the IIS web site. (The latest procedure to force a complete MOVEit DMZ upgrade is available as an article in the Knowledge Base on the **MOVEit support site** (http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ).)

Otherwise, set the IIS site-level client certificate requirement from **Require...** to **Ignore...** (while choosing to override all subfolders) and then set the **Accept client certificates** flag on the **humancc_aspx** and **machinecc_aspx** files as shown here:





After completing either procedure, you may also wish to delete the extra localhost IIS site that setting the site-wide **Require...** flag requires. You may also need to change the **Machine URL** on the **Paths** tab of the DMZ Config Utility if your moveitdmz site is bound to a specific IP address.

SSL - Client Certs - Hardware Tokens - Overview

SSL certificates are often stored in memory or on disk as part of an operating system or other piece of software's configuration. However, SSL certificates may also be stored in a removable form of physical media such as a USB dongle or magnetic card.

Removable (and often, read-only) storage is most commonly associated with client certificates is because dongles and cards and other removable media can be carried by individual people; to forge a hardware-based credential, you need to be in possession of the hardware. Server certificates need to be continually available and are thus almost always tied into software. In fact, the use of removable storage with server certificates could make it easier for people to steal a server's private key as servers are frequently left unattended.

Regardless of how an SSL client certificate is stored, if an SSL-enabled web browser or FTP client can read that certificate, then it may be used to authenticate with MOVEit DMZ.

Not all hardware client certificates work the same way. Some require "phoning home" to a central authentication server before they can be used, while others (such as the Aladdin eToken described below) are "standalone". Some SSL clients (such as MOVEit Freely) can use hardware certificates that automatically tie into the operating system store, while other SSL clients will need their own direct access to the SSL hardware. Despite these variables, the bottom line is that MOVEit DMZ will be able to make use of an SSL hardware token as long as the CLIENT can obtain the appropriate credential from the SSL hardware token and pass it to MOVEit DMZ as part of the normal SSL negotiation.

SSL - Client Certs - Hardware Tokens - Aladdin eTokens

MOVEit DMZ supports the use of SSL client certificates, including certificates on hardware tokens, for authentication to MOVEit DMZ via its FTPS or HTTPS interfaces. This document discusses how to configure an Aladdin eToken Pro for use with MOVEit DMZ.

The eToken Pro is a small USB-based cryptographic device that can store client certificates. When an SSL-enabled FTP client or web browser attempts to use a client certificate that is stored on an eToken, the Aladdin software drivers obtain the certificate from the token and present it to the application. The token must be physically attached to the computer at the time the certificate is needed.

Installing the eToken

Before connecting the eToken to the computer, insert the Aladdin CD-ROM and choose **Install eToken RTE**. This will install the USB drivers and a simple "eToken Properties" utility. If you want to be able to copy certificates to a token, you must also choose **Install Utilities** from the CD.

Regarding the eToken Utilities: There need not be a separate administrative computer for managing eTokens: it is possible for end users to perform all eToken configuration themselves on their own computers. If you want end users to be able to manage the certificates on their eTokens themselves, then the eToken Utilities should be installed on each computer.

If an administrator will be doing certificate management for all eTokens on a single administrative computer, then the eToken Utilities don't need to be installed on the end user computers. However, in order for an administrator to be able to configure all eTokens from a single administrative computer, the individual client certificates must also be installed on that computer.

When the software has been installed, insert the USB token. (You do not need to reboot the computer.) The red light inside the token (visible from all sides) should light up.

Run Start | Programs | eToken | eToken Properties and change the token's password from the default of 1234567890.

Copying certificates to the eToken

Once you have **created and installed a certificate** (on page 227) on the computer, you can copy it to the eToken:

- Run Start | Programs | eToken | Utilities | eToken Certificate Converter.
- Choose an existing certificate name in the left pane.
- You should probably check the box **Delete original certificate and keys**. This will remove the key from the local certificate store after copying it to the token. If you don't choose **Delete original**, you'll want to do this later, perhaps by using Internet Explorer's Tools | Internet Options... | Content | Certificates... Otherwise, with the certificate's key residing both on the computer and on the token, there'd be little point in having the hardware token.
- Choose >> **Import to eToken** >>. You will be prompted for the password of the eToken connected to your machine.
- Enter the password. After several seconds, you'll see "The operation was successful."
- Choose OK. After you click OK, the window will now display the certificate in the right pane.
- Choose Exit.

If you move the hardware token to a different computer, you will not need to take any special actions (other than installing the eToken RTE) for the computer to be able to use the certificate.

You can run the "eToken Properties" program again to confirm that the certificate is now on the token. You can also use Internet Explorer to confirm that the certificate is available, by choosing Tools | Internet Options... | Content | Certificates... If you unplug the token, then subsequently the Microsoft Certificates applet will not show the certificate.

When you run an FTP client or web browser that uses the certificate, you'll get a eToken Base Cryptographic Provider dialog, asking for the token's password, each time the program runs.

SSH

This section describes SSH Server Keys and Client Keys.

SSH - Server Keys - Overview

Users of SSH clients know to trust specific machines because their keys will match publicly available SSH fingerprints. As part of the instructions you give your clients, you **SHOULD** be distributing the fingerprint of your MOVEit DMZ SSH server so your clients can confirm the identity of your server. (Without this protection, anyone could spoof this or any other SSH server!)

The following OpenSSH session shows this mechanism in action. Specifically, OpenSSH asks the end user if they want to trust the remote server after displaying the MD5 hash of the remote server's SSH server key.

```
d:\>sftp sshftpuser@moveit.myorg.com
```

```
Connecting to moveit.myorg.com...
```

```
The authenticity of host 'moveit.myorg.com (33.44.55.66)' can't be established.
```

```
RSA key fingerprint is b4:51:8a:9c:5d:7e:98:db:f0:88:08:52:31:b4:a0:1e.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
sshftpuser@moveit.myorg.com's password:
```

MOVEit DMZ's SSH key is automatically generated the first time the server is started and an associated fingerprint is created at the same time. To view your MOVEit DMZ SSH key fingerprint log into a Windows console on your MOVEit DMZ server. Open **Start -> All Programs -> MOVEit DMZ -> MOVEit DMZ Config** and navigate to the SSH tab to view your MOVEit DMZ's SSH key MD5 hash.

Configure MOVEit DMZ

License	Status	Paths	Email	Settings	Database
FTP Ports	FTP Certs	FTP IPs	SSL	SSH	SSH Ciphers

SSH Configuration

Server Key:

SSH Port: (default 22)

Bind to IP Address:
(0.0.0.0 = all available IP's)

Server Keys

Name	Fingerprint
(default)	b4:51:8a:9c:5d:7e:98:db:f0:88:08:52:31:b4:a0:1e

Alternate Bindings

Server IP	Server Key	Organization

Server Key Backup

The MOVEit DMZ SSH server key is stored encrypted in the registry under the `SSHServer\PrivKey` registry entry. Any registry backup, including the registry backup performed by the **MOVEit DMZ Backup Utility** (on page 150), will back up this key.

Server Key Export

To export MOVEit DMZ's public SSH server key in either OpenSSH or SSH2 format, see the related instructions in **SSH - Configuration** (on page 639).

Requirements

MOVEit DMZ only supports FTP over SSH (or SFTP) and SCP2. SCP (SCP1) and all Terminal sessions will be denied access.

MOVEit DMZ SSH Server uses SSH Protocol 2 only. A client will not be able to connect to the MOVEit DMZ server using only Protocol 1. MOVEit DMZ SSH Server recommends using the following encryption ciphers: AES, 3DES, and Blowfish. (An ever-expanding list of **compatible clients** (on page 793) and a **complete list of encryption options** (on page 639) is also included in this documentation.)

Troubleshooting

If the SSH user is connecting to MOVEit with the correct username but the administrator does not see any SSH public key entries in the audit logs, it is likely that the end user has NOT yet generated a public/private key pair for SSH. End users can often use the `ssh-keygen -t rsa` command to generate these keys, but they should be advised to NOT enter a passphrase when prompted during the key generation; if a passphrase is entered it will be asked for during each subsequent attempt to connect and will spoil attempts to automate the process.

SSH - Client Keys - Overview

The SSH specification allows for three different kinds of authentication. The first is standard username and password, which MOVEit DMZ obviously supports. The second is hostname only, which MOVEit DMZ does not support. The third authentication method is username and client key, which MOVEit DMZ also supports as described below.

As is the case with almost any client key/certificate scheme, the higher security offered by cryptographic-quality keys is offset by additional administrative work. Resetting a password is no longer enough to "let someone back in" when keys are used.

In SSH applications, client keys are almost always generated client-side. Because there is no central authority to vouch for SSH keys (if there was, SSH would be SSL), all SSH keys must be individually trusted by both client and server.

MOVEit DMZ supports the use of both DSS and RSA keys. The server key automatically generated by MOVEit DMZ's SSH server is an RSA key; no incompatibilities with any SSH clients regarding this key format have ever been encountered. Client keys may be of either type.

Generating SSH Client Keys

MOVEit DMZ is NOT an SSH client key generator. Almost all modern SSH clients already have a facility to generate client keys and these facilities should be used whenever possible. Some common SSH client's key generation facilities are briefly described below:

- *nix, OpenSSH: Use the `ssh-keygen -t rsa` command.
- Windows WS_FTP 9.0: From the main menu, select **Options | Tools** and use the **Create...** button under the **SSH | Client Keys** tree.

If you must generate and distribute SSH client keys, consider using the OpenSSH for Windows toolkit to generate these. See ***Specific Clients - OpenSSH for Windows*** (on page 652) for more information about this process.

Associating SSH Client Keys with Users

The facility which associates SSH client keys with specific users on MOVEit DMZ is available as part of the "SSH Policy" from any (web-based) User Profile. Rather than store the entire SSH key for a remote client, MOVEit DMZ simply records the cryptographically unique fingerprint (MD5) of a client key. Either the client or MOVEit DMZ itself can be used to generate and import the necessary fingerprint.

Generating and Importing SSH Client Keys

There are two ways to generate and import an SSH client key for a particular user.

- ***End user generates key, administrator imports key or fingerprint.*** (on page 255)
- ***End user attempts a connection, administrator accepts cached fingerprint from holding tank.*** (on page 259)

The second option is probably quicker and less error-prone if the end user and administrator are in near-real-time communication with each other.

SSH - Client Keys - Import

Some users may be able to provide their SSH key fingerprints in advance. For example, most *nix users may use the `ssh-keygen -l` command to display their SSH fingerprint.

```
sshenduser@slackwarelinux:~$ ssh-keygen -l
```

Enter file in which the key is (/home/sshenduser/.ssh/id_rsa):

```
2048 63:bd:cc:05:ba:41:63:67:b1:b8:b6:6e:98:1f:10:67
```

```
/home/sshenduser/.ssh/id_rsa.pub
```

In other cases, users may only provide the public key itself. To manually add MD5 fingerprints or public keys provided by an end user, go to the [User Profile](#) page and click on the [SSH Policy](#) link.

User Profile (kristina)

General Information

Username: kristina

Full Name: kristina

User ID: kristina23t5a3u1

Permission: Administrator

Notifications: via HTML-Format Email ([user@ipswitch.com](#)) + Administrative Alerts

Language: English

Created: 2/26/2014 12:43:53 PM by Default SysAdmin

 [Change Information](#)

 [View Home Folder \(/Home/kristina\)](#)

 [View Folder Access List](#)

 [View User Logs](#)

User Authentication

Last Signon: 4/1/2014 7:31:22 AM

Account Status: Active - [Change Status](#)

Expiration Policy: No Policy Set - [Change Policy](#)

Authentication Source: MOVEit Only

Password: - [Change Password](#)

Credentials Required for Access: *(in addition to Username)*

HTTP Server: Web Interface: Password Only with SSL [HTTP Policy](#)

HTTP Clients: Password Only with SSL

FTP Server: Secure (SSL): Password Only with SSL [FTP Policy](#)

Insecure: Not Allowed

SSH Server: SSH Client Key OR Password [SSH Policy](#)

Mobile Interface: Password, no caching allowed [Mobile Policy](#)

Then, scroll down to the Current SSH Keys section and click on Add (manually).

Current SSH Keys...

Keys in this list have been accepted as valid credentials for SSH login.

Type	Data	
SSH Key	abcdefghijklmnopqrstuvwxyz123456789012345678901	

[Add \(manually\)](#)

[Import](#)

Next type (or hopefully, paste) the fingerprint or the entire SSH client's key into the text box provided.

Add SSH Key...

To add an SSH Key by hand, first type (or paste) a **New SSH Fingerprint or Public Key**:

Example SSH Key Fingerprint:
0e:23:45:a1:fb:83:8f:30:70:0a:e0:0d:d7:77:3b:8b

OR

Example SSH Public Key:
--- BEGIN SSH2 PUBLIC KEY ---
Comment: "rsa-key-20041210"
AAAAB3NzaC1yc2EAAAABJQAAAIBwaiGcziMcaZNCYMDJqgwkBXfx/91Nng/SRA8
V4p00f6VVo1tpn3WkHwFDbYCe5LbITBi/HKoUhpneFSB3eKMEfx32n/IYGszK
yY4cVPTj/2uCc6zOpUI32JYFngu8JiJfurPb6BAVKkCPGY6hqhsIO18pQ0O1cAUk
QarJNQ==
--- END SSH2 PUBLIC KEY ---

OR

Example SSH Public Key:
ssh-dss
AAAAB3NzaC1yc2EAAAABJQAAAIBwaiGcziMcaZNCYMDJqgwkBXfx/91Nng/SRA8V4p0
0f6VVo1tpn3WkHwFDbYCe5LbITBi/HKoUhpneFSB3eKMEfx32n/IYGszKyY4cVPTj
/2uCc6zOpUI32JYFngu8JiJfurPb6BAVKkCPGY6hqhsIO18pQ0O1cAUkQarJNQ==

Then press the "Add SSH Key" button: **Add SSH Key**

If a valid key was provided, MOVEit DMZ will display a success message and list the key in the **Current SSH Keys** section. As you can see, a single user may be associated with multiple SSH keys; this is especially useful if a user may be using the same username from multiple machines.

Current SSH Keys...

Keys in this list have been accepted as valid credentials for SSH login.

Type	Data	
SSH Key	abcdefghijklmnopqrstuvwxyz123456789012345678901	
SSH Key	0e:23:45:a1:fb:83:8f:30:70:0a:e0:0d:d7:77:3b:8b	

Add (manually)
Import

As an alternative, if you have the SSH key in a file on your PC, you can upload it directly by clicking on **Import**. Enter or browse to the SSH key file and press the **Import SSH Key** button. A successful import will display in the **Current SSH Keys** section.

Import Existing SSH Key...

Select an SSH public key file: No file selected.

Import SSH Key

Finally, to make sure the key will be solicited from the SSH client and/or that the key will be a required credential, see the **Edit SSH Policy** section and check the boxes appropriately.

If you plan on using OpenSSH in batch mode, you should use the following settings (require_key = yes, require_pass_with_key = no). If you want to enforce "two-factor" authentication, enable all of the following settings (require_key = yes, require_pass_with_key = yes).

Default SSH Policy Settings...
These settings control the default values used for the user-level settings of the same name. These settings control behavior on the SSH interface only.

Allow SSH Access by Default:	☒ Yes	☐ No
SSH Key Required by Default:	☒ Yes	☐ No
Password also required with valid SSH Key by Default:	☐ Yes	☒ No

[Change Default SSH Policy](#)

For detailed information about configuring the SSH Keys policy, please also see the ***Interface Policy*** (on page 482) documentation page.

SSH - Client Keys - Holding Tank

The SSH Key holding tank holds keys that have been presented by various users as authentication credentials but have not yet been accepted as valid credentials for those users. The holding tank is populated automatically whenever a valid username is presented along with an invalid key AND the sign on fails (typically the signon fails because a key was required).

The use of a holding tank in key authentication situations makes it easy for administrators to "click-accept" specific keys for users without having to *manually copy or type keys into a user profile* (on page 255).

For detailed information about configuring the SSH Keys policy, please also see the *Interface Policy* (on page 482) documentation page.

Walkthrough

The following procedure describes how an SSH client can connect with a new key and leave the key's fingerprint behind for an administrator to promote/accept into the user's profile at a later date. Any SSH user whose client has already generated and installed an SSH client key should be able to use this procedure.

First, have the remote SSH client attempt to connect to MOVEit DMZ. This connection should fail. For example, the following OpenSSH for Windows session attempts to connect with a client key and fails.

```
D:\temp>sftp -oUserKnownHostsFile=c:\progra~1\OpenSSH\bin\ssh\known_hosts  
-oIdentityFile=c:\progra~1\OpenSSH\bin\ssh\id_rsa sshkeyboi@moveit.myorg.com
```

```
Connecting to moveit.myorg.com...
```

```
sshkeyboi@moveit.myorg.com's password:
```

```
Authenticated with partial success.
```

```
Permission denied (publickey).
```

```
Connection closed
```

Next, sign on as an Admin to MOVEit DMZ and go to the User Profile of the user which just tried to authenticate. Click the SSH Policy link. (Or, go to the *organization holding tank* (on page 482) under Settings | Security | Interface Policy | SSH...)

User Profile (kristina)

General Information

Username: kristina

Full Name: kristina

User ID: kristina23t5a3u1

Permission: Administrator

Notifications: via HTML-Format Email ([user@ipswitch.com](#)) + Administrative Alerts

Language: English

Created: 2/26/2014 12:43:53 PM by Default SysAdmin

 [Change Information](#)

 [View Home Folder \(/Home/kristina\)](#)

 [View Folder Access List](#)

 [View User Logs](#)

User Authentication

Last Signon: 4/1/2014 7:31:22 AM

Account Status: Active - [Change Status](#)

Expiration Policy: No Policy Set - [Change Policy](#)

Authentication Source: MOVEit Only

Password: - [Change Password](#)

Credentials Required for Access: *(in addition to Username)*

HTTP Server: Web Interface: Password Only with SSL [HTTP Policy](#)

HTTP Clients: Password Only with SSL

FTP Server: Secure (SSL): Password Only with SSL [FTP Policy](#)

Insecure: Not Allowed

SSH Server: SSH Client Key OR Password

[SSH Policy](#)

Mobile Interface: Password, no caching allowed

[Mobile Policy](#)

Double-check the fingerprint and especially the time of the key fingerprint you are about to add and then click the **Accept** link.

Warning: An administrator should accept a key from the holding tank only if there is good reason to believe that the connection attempt that resulted in the holding tank entry actually came from the authorized user.

Holding Tank...

Keys in this holding tank have been presented, but have not yet been accepted as valid credentials.

Type	Date and Time / Data	
SSH Key	4/18/2014 10:45:51 AM	2f:19:84:fe:cd:52:4e:af:7c:82:03:2c:2c:8c:81:bd X Accept

If a valid key was provided, MOVEit DMZ will display a success message and list the key in the **Current SSH Keys** section. As you can see, a single user may be associated with multiple SSH keys; this is especially useful if a user may be using the same username from multiple machines.

Current SSH Keys...

Keys in this list have been accepted as valid credentials for SSH login.

Type	Data	
SSH Key	abcdefghijklmnopqrstuvwxyz123456789012345678901	X
SSH Key	0e:23:45:a1:fb:83:8f:30:70:0a:e0:0d:d7:77:3b:8b	X

Finally, to make sure the key will be solicited from the SSH client and/or that the key will be a required credential, see the **Edit SSH Policy** section and check the boxes appropriately.

If you plan on using OpenSSH in batch mode, you should use the following settings (require_key = yes, require_pass_with_key = no). If you want to enforce "two-factor" authentication, enable all of the following settings (require_key = yes, require_pass_with_key = yes).

Default SSH Policy Settings...

These settings control the default values used for the user-level settings of the same name. These settings control behavior on the SSH interface only.

Allow SSH Access by Default: ☒ Yes ☐ No

SSH Key Required by Default: ☒ Yes ☐ No

Password also required with valid SSH Key by Default: ☐ Yes ☒ No

Importing Keys from the Organization-Wide Holding Tank

A complete list of all unassigned keys for all users in the organization may be viewed in the organization-wide holding tank. The organization-wide holding tank is accessible from the **Settings** page by following the **Security | Interface Policy | SSH** link. To assign specific keys, click into the complete list with the **View Tank Keys** link.

Default SSH Policy Settings...

These settings control the default values used for the user-level settings of the same name. These settings control behavior on the SSH interface only.

Allow SSH Access by Default:

☒ Yes
 ☐ No

SSH Key Required by Default:

☒ Yes
 ☐ No

Password also required with valid SSH Key by Default:

☒ Yes
 ☐ No

Change Default SSH Policy

User SSH Key Holding Tank...

There are currently 1 SSH keys in the holding tank.

[Delete All Tank Keys](#)
[View Tank Keys](#)

The Holding Tank retention setting controls behavior on both the SSL (HTTP and FTP) and SSH interfaces.

Holding Tank retention:

30

(days to keep holding tank certificates)

Change Holding Tank Settings

~ OR ~ [Return to the full organization settings](#)

Keys are listed by username. Select the appropriate key and click the **Accept** link next to it. After a key has been accepted, the interface will return to the organization-wide holding tank so other keys may be assigned or deleted.

SSH keys Holding Tank...

Keys in this holding tank have been presented by users, but have not yet been accepted as valid credentials.

Type	User / Certificate	Date and Time	
SSH Key	Test (test)	4/18/2014 10:45:51 AM	X Accept
	2f:19:84:fe:cd:52:4e:af:7c:82:03:2c:2c:8c:81:bd		

Delete All Tank Keys

Cleaning Unassigned Keys Out of the Holding Tank

Unassigned keys will automatically be cleaned out the holding tank after a certain number of days. The exact number of days is a configurable option under the organization-wide SSH policy. (The same value applies to unassigned SSL client certs and untrusted CA certs in the holding tank.)

Unassigned keys may also be manually cleaned out an individual user's holding tank or the organization-wide holding tank using any of the provided **delete all** links.

Web Interface

This section contains reference information describing the features and screens of the desktop-size web browser interface.

Home Page

Admin Only Features

The Home Page displays a few extra sections for administrators, including configuration hints, and a summary of currently active sessions. Within active sessions, you can view lists of currently signed on users, and lists of locked out users. This information is organization wide for regular administrators, and system wide for sysadmins.

Configuration Hints

Administrators of new organizations are shown several suggested configuration tasks to perform, including adding users and configuring access rules. These are items generally necessary for correct operation of a DMZ organization. Links are provided to take the administrator directly to the referenced pages.

Configuration Hints



You currently do not have any user accounts. You **MUST** have user accounts in your organization so people can work with MOVEit DMZ.

[Add Users](#)

Configuration Hints



You are currently signed on to the **SYSTEM** organization.

[Act as administrator in the Org 1 organization](#)

You are currently allowing administrative access from the console only. You should add additional addresses into your remote access policy to allow administrators to configure and transfer files with MOVEit DMZ from remote locations.

[Edit Administrator Remote Access Rules](#)

For SysAdmins of new DMZ installations, several system configuration hints are shown on the home page. These are items generally necessary for correct operation of a DMZ system. As with regular administrator hints, links are provided to take the SysAdmin directly to the referenced pages.

Configuration hints may also be shown for administrators of existing organizations, if a specific configuration item may require their attention. For example, if an organization's user count is approaching the Maximum User List Count value, administrators will receive a configuration hint regarding this, informing them that they may experience a change in behavior.

Another example is if an organization's user count is approaching the Maximum User Count value (within 10% of the configured maximum), administrators will receive a configuration hint regarding this.

Configuration Hints



You are within 10% of the maximum number of users for your organization. You should either remove unused user accounts or contact your system administrator to increase your maximum users.

[Manage Users](#)

Session Summary

The Session Summary section shows the number of active sessions by interface type, which is the interface to which the user is connected, such as Web, FTP, SSH). The summary also shows the number of unique users connected to the various interfaces, and the total number of current sessions.

Clicking the 'Session Manager' link shows the Active Sessions section.

Active Sessions

The Active Sessions section displays a list of currently signed on users. Information such as IP address, interface type, and time of last action are included in the list. Organization administrators see a list of all signed on users in their organization, while for sysadmins, the list includes all users throughout the entire DMZ system that are currently signed on. On web farm systems, the node number the user is signed on to is also displayed.

In the event of a large number of active sessions entries being present, the list will be limited to 1,000 entries for performance reasons. If this limit is reached, a note will be displayed indicating this fact.

The "timeout" listed indicates how many minutes are left before the session will expire. This value is the number of minutes an inactive session times out after (by default 20 minutes) minus the number of minutes it has been since the session was last active. Almost all sessions should use the same timeout value except for active file transfer sessions, which usually enjoy a longer session timeout.

Session Manager

Session Summary

By Interface: Web: 5

Totals: Unique Users: 1 Sessions: 5

Active Sessions

Full Name	Username	IP Address	Interface	Last Event (Timeout)	
kristina	kristina	127.0.0.1	Web	8:23:29 AM (9 min)	✕
james	james	127.0.0.1	Web	8:19:06 AM (5 min)	✕
sandra	sandra	192.168.150.233	Web	8:34:43 AM (20 min)	✕
william	william	127.0.0.1	Web	8:21:09 AM (7 min)	✕
kris	kris	127.0.0.1	Web	8:22:17 AM (8 min)	✕

Remove All Sessions

Individual sessions can be removed by clicking the Remove link and clicking Yes on the following confirmation page. All the current sessions can be removed at once by clicking the Remove All Sessions link at the bottom of the session list (this action will also require confirmation). Be aware that it is possible for the current user to remove their own session, either by clicking the Remove link for their session, or by clicking the Remove All Sessions link. If this is done, the current user will be returned to the signon screen immediately following the action.

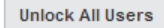
Locked Out Users List

The Locked Out Users section displays a list of currently locked out users. These are users who have attempted and failed to sign on to the system too many times in too short a timespan. (These values are controlled in the Username Lockouts settings page.) The time of their lockout is shown, along with links to unlock the account, delete the account, or unlock all locked out users. Also, if lockout expirations are configured, a message informing you of the lockout expiration setting is shown. As with the Active Sessions section, an organization administrator sees a list of all locked out users in their organization, while a sysadmin sees a list of all locked out users on the system.

Locked Out Users

The following accounts have been locked for security violations:

Username	Real Name	Lockout Date/Time	
 fred	Fred	4/7/2014 1:19:51 PM	 



Your policy will automatically unlock these accounts in 33 minute(s), but you may also choose to reactivate these accounts now.

Users

Overview

A user account allows a single person, organization or device to authenticate to MOVEit DMZ. Admins, SysAdmins and some GroupAdmins may add, delete and edit users.

Every account is guarded with a username and a password of a certain minimum strength. Frequently accounts are also guarded with IP/hostname restrictions, interface/protocol restrictions, or an SSH key or SSL certificate.

By default, any particular username is unique to one organization, so a username can be shared between organizations. The SysAdmin user, who has the ability to administer all organizations, can change this setting so that an individual username can be used only by one organization.

Users

Filter: All Users sorted by Username

Username	Full Name	Last Signon	Permission	
annie	Annie	4/1/2014 8:49:20 AM	User	
bobby	Bobby	4/1/2014 8:49:28 AM	User	
kristina	kristina	4/1/2014 8:49:32 AM	Admin	

Page 1 of 1 (Users 1 to 3 of 3 total @ 10 per page)

[Add User](#)

The main list of users has several columns:

- Username: The unique username of the user. People will use their username and their password to sign onto MOVEit DMZ. Clicking on the username will open the User Profile for that user.
- Full Name: The full name of the user.
- Last Signon: When this user last signed on.
- Organization: The name of the organization to which this user belongs. (SysAdmins only.)
- Permission: This user's base permission set (TempUser, User, FileAdmin, Admin, SysAdmin).
- Action:
 - Clone: Allows administrators to clone this user. When a user account is cloned, its settings, group memberships, folder permissions, and home folder structures are all copied to the new account. This action is useful in conjunction with "template" users for creating new accounts based on a pre-defined set of user parameters. Temporary users may not be cloned.

MOVEit DMZ will attempt to determine the best home folder path for the new user, based on the cloned user's existing home folder path, and provide that path as the default value. Administrators can change the home folder path as desired.

- **Delete:** Deletes this user (after confirmation)

An "add" link allows Admins to create new user accounts. (See "Adding a User" section below.)

Because there may be many users on the system, the list of users will be limited to a configurable number per page. Page navigation links will be provided if the number of users exceeds this limit. The value is configurable in the Account Options page.

User Filter

To make finding specific users easier, a filter section is provided to narrow down the list of users presented.

Filter Users:

Permission:

Status:

Sort by: ...Where Value Like:

Apply Filters

Pick a Letter: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

- **Permission:**
 - - Any -: All users
 - End User: Only end users
 - Admin: Only administrators
 - FileAdmin: Only file administrators
 - GroupAdmin: Only group administrators
 - TempUser: Only temporary users
 - SysAdmin: Only system administrators (only available to SysAdmins)
- **Status:**
 - - Any -: All users
 - Active: Only active users
 - Inactive: Only suspended or locked out users
 - Never Signed On: Only those users who have never signed on to the system

- Template: Only those users marked as "template" users
- In Group:
 - - Any -: All users
 - <Group Name>: Only users who are members of the selected group
- Sort By:
 - Username: Sort results by username
 - Full Name: Sort results by full name
 - Last Signon: Sort results by last signon time
- ...Where Value Like:
 - If not blank, only users whose field selected in the Sort By option value matches the provided search term

Adding a User

The Add a New User page is divided into four different sections.

Add a New User...

Assign a user account for each employee and/or customer with whom your organization must communicate securely.

Username:

Full Name:

Email Address(es):

Email Notifications: ☐ Off ☒ On ☐ On + Admin

Permission: ☒ User ☐ FileAdmin ☐ Admin

Language:

Authentication Method:

Password Delivery: *(Password must be manually delivered)*

Suggested Password: w4i9v5

Password Creation: ☒ Use Suggested Password ☐ Type Custom Password

☐ Force user to change password on first login
(WARNING: the password selected above will be short-lived)

Folder will be created if it does not already exist. You may use the macros [USERNAME], [FULLNAME], and [USERID] in the path.

Home Folder:

Notes:

Group Membership:
(Ctrl-Click to select multiple groups)

Administrators
East Coast
West Coast

The first section is the **general information section**. Here is where the username, full name, email address, notification setting, permission code, and language are entered. The notification setting determines if the user will receive email notifications from the system. Setting a blank email address will automatically set the notifications setting to "Off". Setting the notification setting to "On + Admin" will allow administrators and GroupAdmins to receive special admin notifications when certain events happen to users under their control, such as password and account expirations and user lockouts.

Each user must have a unique username, and a unique full name, both of which may contain any character in the ISO-Latin-1 (ISO/IEC 8859-1) character set, with one exception: the username cannot use the slash ("/") character as it is a special character used to add an organization identifier to the username. Email addresses do not need to be unique across users, and can even be left blank.

Note: These values may not begin with the characters "@!", for internal reasons.

The next section is the **authentication section**. This is where the password is set; the suggested password may be used, or a custom password can be entered. The clickable keyboard is available here for entering new passwords, to help thwart keystroke loggers.

Note: Maximum password length is 32 characters. Any new password created which exceeds the 32 character limit, will be truncated to the first 32 characters.

Also available in this section are the "Force user to change password on first login" and "Email new password to user" options. The latter will only appear if the organization allows sending new passwords by email. The "Force user to change password on first login" option will require the user to change their password when they first sign on with their account (a similar option is available when changing a user's password). The "Email new password to user" option will cause a plain-text email to be sent out to the user, assuming a valid email address has been supplied, and the notifications setting is enabled, containing the user's new account information, including the new password. (If an email address has not been set, or the notifications setting is off, a warning message will be displayed prompting for confirmation, and no email notification will be sent.)

When the current organization is operating in a "mixed" authentication mode (RADIUS then MOVEit or LDAP then MOVEit), another option will appear in the authentication section, called Authentication Method. This allows the administrator to select the authentication method for the user. The authentication method can be "MOVEit Only", "External Only", or "Both". When set to "External Only", MOVEit DMZ will not allow users who fail to authenticate against an external server to be signed onto the system. When set to "MOVEit Only", MOVEit DMZ will not attempt to authenticate a user using the external server; it will use its own user database to authenticate the user. When set to "Both", MOVEit DMZ will first try to authenticate the user using the external server, and if that fails, then attempt to authenticate the user using its own user database.

In the next section, you can specify a default folder to be the **user's home folder**. The default entry, `"/Home/[FULLNAME],"` creates a folder with the user's Full Name, which was entered at the top of this form. You can also set the folder name to use the USERNAME, again entered on this form, or the USER ID, which is an internal ID automatically generated when the user is created. This USER ID cannot be changed and will always remain the same for the life of the account.

A second option here is to specify a different folder in place of the /Home folder. For example, you could enter `"/Users/[FULLNAME]."` If the Users folder does not exist (in the Root folder), it will be created.

Other options for the user's home folder include: setting the user's home folder to any folder, provided it is not a restricted type, in the MOVEit DMZ organization; setting up a shared home folder for multiple users; or not setting a home folder for the user. An Administrator can change the home folder setting for an individual user, at any time, by selecting a user and going to the User Profile - User Settings options.

Note: If an expired user account is deleted, the user's home folder will also be automatically deleted, unless someone else has explicit permissions to that user home folder. For more information, see the ***Feature Focus - Expiration Policies topic***. (on page 76)

The final section is the miscellaneous section, which contains an optional **notes** field, and a list of **groups** to choose from to add the user to. Multiple groups may be selected by holding down the Ctrl key while clicking.

Permissions

There are seven different levels of access a user may possess in the MOVEit DMZ system. The seven levels in order of increasing privilege are Anonymous, Temporary User/Guest, User, GroupAdmin, FileAdmin, Admin and SysAdmin.

The following table summarizes what each class of user permission can and cannot do. ("Y" = yes, "*" = if allowed/configured) Anonymous users (i.e., users who have not signed on) may only submit Webposts and attempt to sign on to the system as an authenticated user.

Activity	SysAdmin	Admin	FileAdmin	GroupAdmin	User	TempUser
Manage Organizations	Y	-	-	-	-	-
Manage Schemes	Y	-	-	-	-	-
Set/Download Debug Logs	Y	-	-	-	-	-
Set IP Lockout Policy	Y	-	-	-	-	-
Set User Lockout Policy	Y	Y	-	-	-	-
Manage Organization-Wide Settings (e.g., Branding)	Y	Y	-	-	-	-
Configure and Run Reports	Y	Y	-	-	-	-
View Audit/Transfer Logs	Y	Y	Y	*	*	*
Manage Users and Groups	Y	Y	-	*	-	-
Manage Address Books	Y	Y	-	*	-	-
Create/Delete Folders	Y	Y	Y	*	*	-
Grant Permissions to Folders	Y	Y	Y	*	-	-
Manage Other Folder Settings	Y	Y	Y	*	*	-
Delete Files	Y	Y	Y	*	*	-
Upload/Download/Move/Copy Files	-	Y	Y	*	*	-

Send/Read Packages	-	Y	*	*	*	Y
See a Restricted View Because of Display Profiles	-	-	-	*	*	*

Hint: Permission to download or upload files from specific folders is controlled in the "Permissions and Settings" section of those folders. Permission to send packages to specific users is controlled by "Address Books." Users can also inherit various rights from the groups of which they are members.

Anonymous

By definition anyone who has not signed onto the system is an **anonymous user**. Anyone who has signed onto the system becomes an **authenticated user**. As expected, an anonymous user enjoys the narrowest set of rights on the MOVEit DMZ system.

File Rights: An anonymous user may submit web forms into specific MOVEit DMZ "webpost" folders. Anonymous users may not upload/download files or send/receive packages.

Administrative Rights: An anonymous user may view the login screen of any particular Organization. If the user provides a valid username and password on the sign on screen, the user will be granted additional rights. Anonymous users are also barred from seeing the current version number of product. (Authenticated users may see the version number.)

Example(s):

- Nancy notices an advertisement on Woodstock First Bank's web site for a CD with a great rate. She clicks on a "sign me up" link which displays a form the bank created. Nancy fills out the form and submits it. The form opens a secure connection across the internet into the MOVEit DMZ system and deposits whatever information Nancy provided into an encrypted file on the MOVEit DMZ system. Nancy never needed to sign onto the MOVEit DMZ system but she nonetheless took advantage of a MOVEit DMZ feature. Therefore, Nancy is an anonymous user.
- Melissa is an IS employee of Woodstock First Bank and has an account on the MOVEit DMZ system. She opens a browser bookmark on her local system which pops up the MOVEit DMZ system login page. As long as Melissa sees the login page, Melissa is an anonymous user. After she successfully logs in through this page Melissa will be an authenticated user.

Temporary User/Guest User

Temporary Users are an optional class of user that can be enabled and disabled per organization. They are only available in organizations where Ad Hoc Transfer is enabled. Temporary Users are user accounts that can be created by selected users on the DMZ system, and provide a minimal level of access to DMZ resources. Temporary Users are only allowed to participate in Ad Hoc Transfer; they do not have access to folders on the DMZ system and cannot upload and download files, except when those files are associated with packages. They are only allowed to sign in to DMZ through the web and API interfaces, not the FTP or SSH interfaces. Temporary users (like other users) can be configured to expire after a certain amount of time has passed. (See the **Expiration Policy** (on page 76) Feature Focus page for more information about expiration policies)

File Rights: A temporary user may view packages sent to them, download files from the package, and may send packages to users who they are authorized to send to. Temporary users may not participate in any other form of file transfer, and have no rights to any folders on the DMZ system.

Administrative Rights: A temporary user may change his or her password.

If the organization administrator configures Ad Hoc Transfer to create 'Temporary Users', when a registered user sends a package, the temporary-user recipients will receive a password for that package only. The temporary-user recipients will log on with that password, and can view a package, download files in it, and reply to the package. The Temporary User will have an account on the MOVEit DMZ system; the Temporary User suits limited-time use scenarios.

If the administrator enables Unregistered Senders along with 'Temporary Users', an unregistered user can self-register as a temporary-user sender. The temporary-user senders will either be automatically logged on after self-registering with a "Captcha" or they will manually log on with password using either a password or "password link" sent by email after they self-register. Then they can create a package, upload files to it, and send it.

Example(s):

- Mary is a registered Ad Hoc Transfer user. She is on the phone with Thomas, who is not a registered user, but she has a need to send a package and/or some files to Thomas. Normally, Mary would need to get her administrator to add Thomas to the system, but because temporary users have been enabled, Mary can send her package to an email address rather than someone in her drop-down address book of registered users. As part of the process of composing her new package, Mary is prompted for Thomas' email address, full name and a password; Mary gives Thomas that password over the phone.

Thomas is now set up as a temporary user. Thomas has limited access to Ad Hoc Transfer (he can only communicate with Mary) and his account will be automatically expired after 7 days of inactivity (or whatever Mary's administrator set the temporary user expiration settings to be).

In a few seconds Thomas will get an email message containing a link to the new package Mary posted for him. He can use his email address and the password Mary provided him over the phone to sign on, view the package, download files, and reply and send files to Mary.

- David is an unregistered user, but he has access to a MOVEit DMZ sign on page or equivalent that has been configured to enable self-registration as a temporary user. He has a need to send a package and/or some files to Mary, a registered Ad Hoc Transfer user. Normally, Mary would need to get her administrator to add David to the system, but because self-registration as a temporary user has been enabled, David can self-register and send Mary a package to her email address. Following the process of self-registering, as configured by the organization administrator, David enters Mary's email address, his email address, and the letters in the presented "Captcha" question (which shows distorted letters and requires correct entry). David is next asked to enter a password.

David has now been set up as a temporary user. For this package, he has limited access to Ad Hoc Transfer (he can only communicate with Mary) but he has been set up to have wider access (the ability to send to other users) until his account expires. His account will be automatically expired after 7 days of inactivity (or whatever Mary's administrator set the temporary user expiration settings to be).

In a few seconds Mary will get an email message containing a link to the new package David sent to her. She can use her email or DMZ account to view the package, download files, and reply and send files to David.

A Guest User has capabilities similar to a Temporary User, except that the Guest User is further restricted to viewing or sending a single package. If the administrator configures Ad Hoc Transfer to use 'Package Passwords', when a registered user sends a package, the guest-user recipients will receive a password for that package only. The guest user recipients will log on with that password, and can view a package, download files in it, and reply to the package. The Guest User will not have an account on the MOVEit DMZ system; the Guest User suits one-time use scenarios.

If the administrator enables Unregistered Senders along with 'Package Passwords', an unregistered user can self-register as a guest-user sender. The guest-user senders will either be automatically logged on after self-registering with a "Captcha" or they will manually log on with password using a password sent by email after they self-register. Then they can create a package, upload files to it, and send it.

User

User accounts provide a basic level of access to the clients, customers and partners of a particular organization. Every user account comes with a home directory into which users can upload files for the organization and into which the organization will copy files for the user. Through the use of secure sockets, an encrypted channel is used to transport sensitive files safely between a user's home folder and the user's local computer across the Internet.

Frequently users are granted additional privileges to read files from organizational distribution folder.

A user lacks the power to view the files or activities of other users, but a user does have online access to an extensive audit of every activity which took place against their files or account. In any active organization most MOVEit DMZ accounts will be user accounts.

File Rights: A user may transfer files between his or her local computer and his or her home folder. A user also frequently has the ability to read files from one or more distribution folders.

Administrative Rights: A user may track his or her files and may see when changes were made to his or her account details. A user may change his or her own password, contact information and email address.

Example(s):

- Max is an employee in the human resources department of Argyle Industries. Argyle Industries uses Woodstock First Bank to process its payroll. Max wants to send his highly sensitive payroll file in a secure fashion directly to Woodstock First Bank. Max should not be allowed to see the payroll files sent in by other companies. Max is an ideal candidate for a user account.
- Fred is a customer of Plaid Software, having purchased its award-winning Kilt software and related support. Plaid Software wishes to make the latest version of Kilt available to its customers at all times so it sets up a "Kilt" distribution folder and allows Kilt licensees to download files from this folders. Fred is an ideal candidate for a user account with additional rights to read from the Kilt distribution folder.

GroupAdmin

GroupAdmin permission is granted to Users on specific Groups. This class of permission will NOT appear in the "Permission" field of a user's record, but it will be indicated in the list of groups this user belongs to. GroupAdmin permission can mean different things depending on the specific group settings, but it generally means that a GroupAdmin has a limited ability to add/remove/modify other users in the GroupAdmin's group.

GroupAdmins are typically promoted to their position to allow remote administrators access control over a group of related users. For example, an insurance company may delegate GroupAdmin control to an IT staffer at a partner provider with twenty separate users on the insurance company's MOVEit DMZ. This would allow the IT staffer to control access by employees (or ex-employees!) of his own company. (This is particularly useful when dealing with companies with high turnover.)

See **Web Interface - Groups - GroupAdmins** (on page 277) for more information.

Hint: Add all users to an "All Users" group and make help desk Users GroupAdmins of the "All Users" group to allow your help desk to change passwords but not access the MOVEit filesystem.

FileAdmin

FileAdmin accounts allow selected people in the offices of a single MOVEit DMZ Organization to work with ALL files received from multiple Users and multiple anonymous web form submissions. Because of its relative power, the FileAdmin access level is an optional access level designed as a convenience for small organizations who wish to give a small group of trusted people complete access to any file which passes through their organization. (Larger organizations will find it useful to divide sections of file authority by assigning privileges to user groups.) One exception to this rule are accounts set up to allow MOVEit Central to connect; Central accounts are commonly FileAdmin accounts.

Hint: Use a FileAdmin account to connect MOVEit Central to MOVEit DMZ.

File Rights: A FileAdmin may view, edit, move, delete and download files from any folder in his or her Organization. A FileAdmin may create new folders or delete old folders. A FileAdmin may also upload files from his or her local computer into the MOVEit DMZ system.

Administrative Rights: A FileAdmin may track any files in his or her Organization including all files uploaded by his or her Organization's Users. A FileAdmin may see when changes were made to his or her account details. A FileAdmin may change his or her own password, contact information and email address.

Example(s):

- Erik is a corporate accounts specialist with Woodstock First Bank. Erik wants to pick the payroll files from Argyle Industries and several other customers off the MOVEit DMZ system. Erik should not have the power to change the corporate color scheme or add new users. Erik is an ideal candidate for an FileAdmin account.
- A corporation would like to set up an MOVEit Central inside their private network to automatically download and process files received from various customers. IT staff would like the MOVEit Central to browse and pull files from any folder on the MOVEit DMZ system. MOVEit Central will most likely require a FileAdmin account.

Admin

The most powerful account in any Organization is an Admin account. These accounts allow people in the office of a MOVEit DMZ Organization to control the appearance, users, groups and security settings of their particular Organization. An Administrator has the power to add and delete other users, change colors and specify who users should contact with problems or questions. There will normally be only one or two Administrators for each MOVEit DMZ organization.

File Rights: (same as FileAdmin) An Administrator may view, edit, move, delete and download files from any folder in his or her Organization. An Administrator may create new folders or delete old folders. An Administrator may also upload files from his or her local computer into the MOVEit DMZ system.

Administrative Rights: An Administrator may track any files in his or her Organization including all files uploaded by his or her Organization's Users. An Administrator may see when changes were made to any account in his or her Organization. An Administrator may add or delete Users, FileAdmins and Administrators and may change the password, contact information and email address of any user in his or her Organization. An Administrator may change Organizational settings such as colors, corporate logo, contact information and the "Message of the Day" displayed to everyone who signs onto his or her Organization.

Example(s):

- Linda is a trusted IT manager of Woodstock First Bank. Linda is in charge of adding and removing user accounts, matching the appearance of the MOVEit DMZ system with the Woodstock First Bank theme and occasionally needs to figure out what happened to a certain file. Linda is an ideal candidate for an Administrator account.

SysAdmin

The most powerful accounts on any MOVEit DMZ server are SysAdmin accounts. SysAdmin accounts allow people from the organization(s) hosting and/or sponsoring the MOVEit DMZ server itself to create, configure and remove Organizations. A SysAdmin also has the power to act as an Administrator of any particular Organization on the MOVEit DMZ system with one important exception: SysAdmins are not allowed to read or write files to or from any particular organization. This restriction not only enforces the privacy and confidentiality of each organization, but also ensures that the administrators of each system remain in control over those users who may work with the local filesystem.

Because of their great power, SysAdmin accounts should be protected carefully and used only to establish, configure or remove organizations or to change global settings which no other account can. (By default SysAdmins are allowed onto the system only if they are actually seated at the MOVEit DMZ console.)

Hint: Unless you run a data center with multiple MOVEit DMZ organizations, it is generally easier to do most of your administrative tasks (e.g., add/delete users) as an Admin in your default organization instead of as a SysAdmin.

File Rights: A SysAdmin may view, download and delete system-wide audit files. SysAdmins may NOT view, upload or download files to or from institutions, although SysAdmins certainly do have this power within their own restricted "Org #0".

Administrative Rights: A SysAdmin may track any significant errors which occurred on the system as well as any activities he or she or any other SysAdmin performed. A SysAdmin may enable or disable any file processing service and may add, modify or delete entire Organizations. (More power is available after assuming the role of Administrator for a particular Organization.)

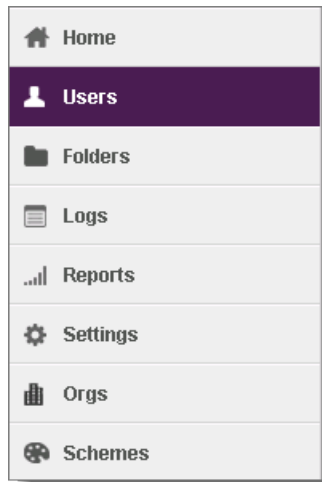
Special Abilities: A SysAdmin may assume the role of an Administrator for any Organization. When a SysAdmin "drills down" into an Organization, a SysAdmin temporarily loses the abilities of a SysAdmin and gains those of that Organization's Administrator, minus the ability to work with files. A SysAdmin may "pop up" into full SysAdmin mode by leaving that Organization.

Example(s):

- Standard Bank Services purchased MOVEit DMZ to provide secure data transport and collection services to three member banks. Jason is an employee of Standard Bank Services and has been given the task of setting up and maintaining Organizational accounts. As part of his duties Jason also provides help over the phone and he occasionally finds it useful to view Organizational settings. Jason is an ideal candidate for a SysAdmin account.

Navigation Links

The navigation links displayed on the left side of the screen are determined by the current user's permission.



The following table summarizes the relationship between permission and visible links. ("Y" = yes; "*" = if licensed and org-level option enabled)

Link	GuestUser	TempUser	User	GroupAdmin	FileAdmin	Admin	SysAdmin
Home	-	Y	Y	Y	Y	Y	Y
Users	-	-	-	Y	-	Y	Y
Groups	-	-	-	-	-	Y	Y
Folders	-	-	Y	Y	Y	Y	Y
Packages	Y	*	*	*	*	*	-
Logs	-	-	Y	Y	Y	Y	Y
Reports	-	-	-	-	-	Y	Y
Settings	-	-	-	-	-	Y	Y
Orgs	-	-	-	-	-	-	Y
Schemes	-	-	-	-	-	-	Y

Profile

The "user profile" page provides information about a single user and links to edit permissions, access rules and other attributes. The following sections are currently available on this page:

- General Information
- User Authentication
- User Settings
- Group Information
- Address Book Information

General Information

General Information

Username: kristina

Full Name: kristina

User ID: kristina9wla62c0

Permission: Administrator

Notifications: via HTML-Format Email ([name@ipswitch.com](#)) + Administrative Alerts

Language: English

Created: 4/1/2014 8:18:41 AM by Default SysAdmin

 [Change Information](#)

 [View Home Folder \(/Home/kristina\)](#)

 [View Folder Access List](#)

 [View User Logs](#)

"Change Information" Link

This link allows administrators to change the full name, email address, and other general properties of this user.

- **User ID:** An internal ID automatically generated when this user is created. This value cannot be changed, and will always be the same for the life of this account.
- **Username:** The login name of this account. If home folders derive their name from usernames ("from full name" is the default), then the user changing this value will be prompted to also change the user's home folder name. Changing the home folder name may affect automated transfers already in place.
- **Full Name:** The full name of this account. If home folders derive their name from full names ("from full name" is the default), then the user changing this value will be prompted to also change the user's home folder name. Changing the home folder name may affect automated transfers already in place.
- **Email Address(es):** The email address or addresses that notification emails for this user will be sent to if Email Notifications are enabled. Multiple email addresses may be entered by separating them with commas.
- **Email Notifications:** This option determines whether the user will receive email notifications of events such as new files or packages. Setting the option to "On+Admin" will cause the user to receive administrative notifications when other users expire or are locked out, or other such events, but only if the user is an Admin or a GroupAdmin.

Note: This option must be set to "On" or "On+Admin", AND a valid email address must be present for email notifications to be sent to this user.

- **Permission:** The user's permission can be changed here to an Admin, FileAdmin, or regular User. See the **Permissions** (on page 277) page for more information about the different permission classes.
- **Preferred Email Format:** This option allows an administrator to set the preferred email format for notifications sent to this user. Notifications may be in HTML form, or Text form.
- **Language:** End Users are normally allowed to change this option unless restricted by a display profile. The value of this option controls not only the language used by the end user in the Web and FTP Interfaces, it also controls the language in which notifications are sent.
- **Notes:** Changing this value will not have any affect on the system. This is the only place this information is used.

Hint: It is usually best to derive home folder names from usernames (which are usually changed less frequently) rather than full names if you anticipate several full name changes in a environment in which automated transfers are wide-spread.

Hint: DISABLE notifications on your automated users, especially any FileAdmin users used by MOVEit Central to connect to MOVEit DMZ. A blank email address will also be treated like a disabled notification.

If the user is a Temporary User, an option will be provided on this page to convert the account to a full End User. To do so, simply click the "Promote Temp User to End User" button. When this is done, a home folder is created for the user, and any limited group memberships the Temporary User has will be converted to normal memberships. The user will also be switched to use the default End User expiration profile, if one is currently assigned in the organization. For more information about the differences between Temporary Users and End Users, see the **User Permissions** (on page 277) page.

"View..." Links

There are four convenience links which may be displayed on a user profile:

- **View Home Folder** - Provides a direct link to the user's home folder. (This link will be hidden for temporary users.)
- **View Folder Access List** - Pulls up the User Folder Access Permissions page, which lists all the folders on the system that the user has access to, and the permission type that gives them that access. (This link will be hidden for temporary users.)
- **View User Logs** - Pulls up a pre-filled "user log" request.
- **Send Package** - Addresses a new package to this user. (Only available if Ad Hoc Transfer is enabled on this organization.)

User Authentication

User Authentication

Last Signon: 4/1/2014 9:36:44 AM

Account Status: Active - [Change Status](#)

Expiration Policy: No Policy Set - [Change Policy](#)

Authentication Source: MOVEit Only

Password: - [Change Password](#)

Credentials Required for Access: *(in addition to Username)*

HTTP Server: Web Interface: Password Only with SSL [HTTP Policy](#)

HTTP Clients: Password Only with SSL

FTP Server: Secure (SSL): Password Only with SSL [FTP Policy](#)

Insecure: Not Allowed

SSH Server: SSH Client Key OR Password [SSH Policy](#)

Mobile Interface: Password, no caching allowed [Mobile Policy](#)

Remote Access Policy:

IP/Hostname: Use Default Rules - [Select Ruleset](#) - [View Rules](#)

Multiple Signons: Allowed - [Change Multi Signons](#)

Last Signon

This line shows the date and time of the user's last successful signon.

Account Status

User accounts may be "Active", "Inactive", or "Template". Only when an account is "Active" will users be allowed to sign on to it. Clicking the "Change Status" link will allow an administrator to change the status of the user.

Change Account Status...

The account status indicates whether or not this account will be allowed to sign on, how notifications reach it and how expiration policies affect it.

- Active - Allowed to sign on; allowed to receive notifications; expiration policies will take effect.
- Inactive - Not allowed to sign on; not allowed to receive notifications; expiration policies will take effect.
- Template - Not allowed to sign on; not allowed to receive notifications; expiration policies will not take effect.

New accounts are marked "Active" by default. Accounts can be marked "Inactive" through this interface or may be locked out because of authentication violations. Accounts marked "Template" are typically cloned to create new and active users. (Account status is never cloned, but is instead always set to "Active".)

The optional "Remark" field provides a space to quickly explain status changes to the next administrator who checks this user's status.

Status:

New Status Remark:

[Change Account Status](#)

"Inactive" accounts are not allowed to sign on and do not receive email notifications. Accounts may be manually set to "Inactive", or they may be set "Inactive" automatically for one of several possible reasons, such as failure to change a password within a specified amount of time or too many attempts to guess an unknown password during login.

Administrators may either manually unlock an inactive account or, in the case of too many bad password attempts, simply wait for a timer to automatically unlock an account. (Accounts locked for security reasons are also visible on an administrator's home page; email notifications of such lockouts are also sent to all administrators with "admin notifications" turned on.)

"Template" accounts are also not able to sign on and do not receive email notifications. The difference between "Inactive" and "Template" accounts is that template accounts are not subject to account expiration, even if an expiration policy is set on the account. As a result, template accounts are typically used as a parent account for user cloning, both for manually created users, and for users created automatically (such as by an External Authentication source). In these cases, the resulting user will have the same expiration policy and other settings as the template account, but unlike the template account, will be subject to that expiration policy.

Expiration Policy

User accounts may be assigned expiration policies either by user class or individually. The expiration policy assigned to the user will be listed here, and an indication will be provided if the user is currently expired by that policy. Clicking the "Change Policy" link will allow an administrator to change the policy assigned to the user.

Change Expiration Policy...

Expiration Policy: Default TempUser Expiration Policy ▾ [Change Expiration Policy](#)

Current Policy Settings...

This account will expire...
on 4/8/2014 9:46:36 AM unless account is used again (7 day(s) after last signon) - [Reset Last Signon](#)

On this page, the current expiration policy assigned to the user will be shown, along with the details of when the user will be expired by each method enabled in the policy itself. If no policy is assigned, "- None -" will be shown. Selecting a different policy and clicking the Change Expiration Policy button will change the policy assigned to the user.

Note: If an expired user account is deleted, the user's home folder will also be automatically deleted, unless someone else has explicit permissions to that user home folder.

Under Current Policy Settings, an information string is displayed stating the details of when the user will be expired according to the current policy. As applicable, a link might be provided to enable reset. For example:

"This account will expire...

on 8/30/2012 1:06:53 PM unless account is either used again or receives a new package (7 day(s) after last signon or received package) - Reset Last Signon

Note that while users with a status of "Template" can have expiration policies assigned to them, they are not actually subject to the rules of that policy. However, users cloned from such an account will have the same expiration policy assigned initially and will be subject to the policy's rules.

Authentication Source

This line shows which authentication source the user is currently using. The possible authentication sources are:

- **External Only** - This value indicates that the user is being authenticated by an external source only. This value is automatically applied when the organization is set to only use external sources for authentication. This value may also be applied to the user when the organization is set to use both external sources and the internal user database for authentication.

Note: When a user is configured for External Only authentication, they will not be allowed to change their password through the Account Options page. All password changes will need to be done through the external authentication server itself.

- **External then MOVEit** - This value indicates that the user will first be authenticated by each active external source available to the organization. If all of those sources fail, the user will be authenticated against the internal user database using a cached copy of the most recently successful external authentication password. This value is only available when the organization is set to use both external sources and the internal user database for authentication.
- **MOVEit Only** - This value indicates that the user will only be authenticated by the internal user database. It is only available when the organization is set to use both external sources and the internal user database for authentication. Users created through the MOVEit DMZ web interface will default to this authentication source unless a different source is selected.

A link will also be shown when the organization is set to use both external sources and the internal user database for authentication, to allow an administrator to change the user's authentication method. Also available to change is the user's external authentication source affinity, which determines which external authentication source the user primarily authenticates with (for more information about external authentication, see the ***Authentication Method section of the Settings - Security - User Policy*** (on page 419) page).

For users created automatically by an external authentication signon, the authentication method and the authentication source affinity will be set automatically. The authentication method applied to users created in this manner can be configured for each external authentication source in the organization. The authentication source affinity is automatically set to the authentication source that the user was created from.

Set Authentication Method

By changing the Authentication Method, you place the responsibility of user security on another server. **If your authentication server is compromised, the data contained within MOVEit DMZ may be compromised as well.** When switching authentication methods to an external server only, remember that all users who are to sign on to MOVEit DMZ need to be configured on the authentication server.

Authentication Method: MOVEit DMZ ▼

Change Authentication Method

Password

The Password line shows the current status of the user's password. If password aging is enabled, it will show the number of days left until the password expires, and the number of days until the user will be warned of password expiration, if password expiration warning is enabled. The Change Password link opens the Change Password page, which allows the administrator to change the password and several password related settings for the user.

Change Password...

Enter Your Old Password:



Suggested Password:

6b747v

New Password:

☒ Use Suggested Password ☐ Type Custom Password

Now press the "Change Password" button:

Change Password

Change Password Aging Exemption

This user is exempt from password aging:

☐ Yes ☒ No

Change Password Aging Exemption

Admin may choose to use the suggested password, or enter their own password, by selecting the appropriate New Password option. If the Use Custom Password option is selected, a new password field, and a password confirmation field will appear for the admin to enter the new password. The clickable keyboard is available here for entering new passwords, to help thwart keystroke loggers.

Note: Maximum Password length is 32 characters. Any new password created which exceed the 32 character limit, will be truncated to first 32 characters.

The "Email password to user" checkbox, when checked, will cause an insecure plain-text email notification to be sent to the user with their new password. This feature is only available if the organization has allowed the sending of password notifications. Enabling this option will automatically turn on the "Force user to change password" option, for security reasons.

The "Force user to change password on next login" checkbox, when checked, will require the user to change their password on their next login. If the user is currently suspended because their password expired, another checkbox will appear allowing the administrator to re-activate the user at the same time their password is changed.

The "Change Password Aging Exemption" section allows an administrator to designate this user as exempt from the usual password aging restrictions which would normally force this user to change his or her password every X days. (Password complexity, password history and other password strength requirements remain in effect even if this option is checked.)

Hint: Consider exempting automated users from password changes, especially any FileAdmin users used by MOVEit Central to connect to MOVEit DMZ.

The "Change Password Permissions" section allows an administrator to prohibit a user from requesting an automatic password change, even if the current organization settings allow password change requests.

Credentials Required for Access

This section displays the various interfaces the user may use to access the MOVEit DMZ server, and which credentials are required to successfully authenticate. The username is required for all authentication methods, so is not listed. Each major interface type (HTTP, FTP, SSH, and Mobile) provides a link which allows administrators to edit the permissions and required credentials for each interface for the user (to override, for this user, the organization's default interface policy). (These settings will not be preserved if you change the default policy and apply changes to all existing users.)

SSL Client Certs are managed by clicking either the HTTP Policy link or the FTP Policy link, and SSH Client Keys are managed by clicking the SSH Policy link. In addition, if there are any pending SSL Client Certs or SSH Client Keys attached to the user which need to be accepted or denied, notes will appear under the HTTP Server, FTP Server, and/or SSH Server sections indicating the number of pending certs and/or keys.

- HTTP Server:
 - Web Interface: Web browser interface.

-
- No Access Allowed - The user is not allowed to use this interface.
 - SSL Client Cert OR Password - An SSL client certificate or a password are required.
 - SSL Client Cert AND Password - An SSL client certificate and password are required.
 - SSL Client Cert Only - Only an SSL client certificate is required.
 - Password Only with SSL - A password is required, with or without an SSL client certificate.
 - HTTP Clients: Non-browser HTTP interface, used by other MOVEit clients such as MOVEit Central and MOVEit DMZ API.
 - No Access Allowed - The user is not allowed to use this interface.
 - SSL Client Cert OR Password - An SSL client certificate or a password are required.
 - SSL Client Cert AND Password - An SSL client certificate and password are required.
 - SSL Client Cert Only - Only an SSL client certificate is required.
 - Password Only with SSL - A password is required, with or without an SSL client certificate.
 - FTP Server:
 - Secure (SSL): FTP/SSL interface.
 - No Access Allowed - The user is not allowed to use this interface.
 - SSL Client Cert OR Password - An SSL client certificate or a password are required.
 - SSL Client Cert AND Password - An SSL client certificate and password are required.
 - SSL Client Cert Only - Only an SSL client certificate is required.
 - Password Only with SSL - A password is required, with or without an SSL client certificate.
 - Insecure: Plain-text unencrypted FTP interface.
 - No Access Allowed - The user is not allowed to use this interface.
 - Password Only - A password is required. Requires Non-Secure FTP to be enabled and allowed for the IP addresses for the user. See the ***FTP Configuration*** (on page 577) doc page for more information.
 - SSH Server: FTP over SSH (SFTP) interface.
 - No Access Allowed - The user is not allowed to use this interface.
 - SSH Client Key OR Password - An SSH client key or a password are required.
 - SSH Client Key AND Password - An SSH client key and password are required.
 - SSH Client Key Only - Only an SSH client key is required.
 - Password Only - Only a password is required.

- **Mobile Interface:** Mobile App and Mobile Web interface.
 - No Access Allowed - The user is not allowed to use (sign in from) the Mobile App.
 - Password, no caching allowed - A password is required every time to sign in from the Mobile App; the password cannot be cached on the mobile device.
 - Password, optionally cached and protected by PIN code - A password is required; the password can be optionally cached on the mobile device (and if it is, it is required to be protected by PIN code).

Note: The required PIN length (that is, whether it is 4, 5, or 6 digits) is inherited from the Org default "Required PIN length" policy (set in **Web Interface - Settings - Security Policies - Interface** (on page 482)).

Remote Access Policy

Administrators have the ability to limit user access to particular IP and hostname addresses. By default, the IP and hostnames from which a particular user or administrator may access MOVEit DMZ are controlled by the organization's default remote access settings (available on the Settings page), but Administrators may specify custom access rules by selecting a CUSTOM ruleset and then defining that ruleset.

The "IP/Hostname" line displays the current remote access ruleset being used by the user, either Default Ruleset or Custom Ruleset. Also available are two links. Click "Select Ruleset" to choose either the Default Ruleset or a Custom Ruleset. Click the "View Rules" to either see how the default rules apply to this user or to change custom rules.

The "View Custom Rules" link will be present only after you select "Use Custom Rules."

Rule	Hostname/IP	Comment
Allow	198.0.0.0	
Allow	172.0.0.0	
Allow	(All IPs)	

Add Remote Access Rule

The interface for adding, editing, and deleting custom IP/Hostname rules is similar to the default IP/Hostname interface available through the organizational settings page.

Administrators may also prevent the user from signing on multiple times using the same interface from different client machines. The Multiple Signons line displays whether the user is allowed to do so, and also provides a link for changing the setting for the user.

When multiple signons are prohibited, a user will not be allowed to sign on from more than one IP address to the same interface. For example, a browser session for the "jsmith" user would be allowed from 192.168.1.1, but a second concurrent "jsmith" browser session from 192.168.2.2 would be refused. At the same time, however, "jsmith" could sign on using an FTP client from 192.168.2.2, because the web and FTP are two different interfaces.

User Settings

User Settings

Ad Hoc Quota: None - [Change Ad Hoc Quota](#)
Package Expiration: None - [Change Expiration](#)
Send To Unregistered: Allowed - [Change Unregistered Recipients](#)
Send Attachments: Allowed - [Change Attachment Settings](#)
Attachment Download Limits: None - [Change Download Limits](#)
Home Folder: /Home/kristin - [Change Home Folder](#)
Default Folder: /Home/kristin - [Change Default Folder](#)
Upload/Download Wizard: Prompt - [Change Wizard Status](#)
Sign On/Sign Off Logging: All - [Change Logging Status](#)
DLP Ruleset: None - [Change Ruleset](#)

Folder Quota

Administrators can set a quota for a user that will prevent the user from uploading more than a certain amount of bytes to the DMZ system. The quota may be configured in kilobytes or megabytes, and applies to files this user uploads or creates. For example, a user with a 5 megabyte quota could upload a 2 megabyte file and a 3 megabyte file, but not two 3 megabyte files. As files are deleted from the system (often by the processing organization), the user is allowed to upload additional files. For example, a user with a 5 megabyte quota could upload 4 megabyte files on Monday, Tuesday and Wednesday as long as the processing organization deleted them from MOVEit DMZ each night.

Hint: The file attachment quota for packages is set in the "Ad Hoc Quota" section.

Ad Hoc Quota

Administrators can set quotas on the amount of bytes a user can send in packages, which includes attached files and any notes. A quota can be set on the total number of bytes in packages sent within a given number of days. A quota can also be set on the number of bytes a user can send in any one package.

Package Expiration

Expire packages after: If users are allowed to set per package expiration values (see "Which users can set specific expirations on their packages?" under "Aging and Expiration" in **Web Interface - Settings - Ad Hoc Transfer - Maintenance** (on page 522)), then Administrators can set a personalized default value.

Note: The Mobile apps and web do not offer senders the per package option. The "default" set here becomes the absolute value always used to expire packages sent from this user from mobile. It overrides the organization's default setting, which also is used as an absolute value to expire packages sent from mobile. See "Which users can set specific expirations on their packages?" under "Aging and Expiration" in **Web Interface - Settings - Ad Hoc Transfer - Maintenance** (on page 522).

Expire packages after: Shows the default number of days, after which the package expires and files are no longer available to recipients. Administrators can set a custom value for a user.

Send to Unregistered

Normally, whether or not a user can send packages to unregistered users is governed by the settings of the organization, and possibly the settings of the groups that user is a member of. However, it can also be changed here, to deny a user from being able to send to unregistered users, even if that user would normally be allowed to. The current permissions for this user are shown here, and the user's 'Send to Unregistered' setting can be changed by clicking on the 'Change Prohibition' link.

Send Attachments

Whether or not a user can add file attachments to packages is governed by the settings of the organization, and possibly the settings of the groups that user is a member of, but administrators can use this setting to prohibit a user from adding files to packages.

Attachment Download Limits

Shows the default number of times recipients of a package can download a file. This is the total number of downloads for all recipients, so if the limit is 10 and one recipient downloads a file 10 times, then the file will no longer be available for download. Administrators can set a custom download limit for a user by setting a default value and maximum for downloads for the user.

Note: The Mobile apps and web do not offer senders the per package option. The "default" set here becomes an absolute value always used to limit downloads of packages sent from mobile. It overrides the org per user default setting and the , which will otherwise be used as the absolute value always used to limit downloads from mobile. See [Which users can set specific download limits on their packages?](#) under "Sending Files" in *Web Interface - Settings - Ad Hoc Transfer - Content* (on page 513).

Home Folder

A user's home folder is the folder to which the user gains automatic permissions, depending on the Default Home Folder Access organization setting. Normally, the home folder is also used as the default folder, meaning it is the folder the user gets to navigate to and upload to by default.

By default, when a new user is added, MOVEit DMZ creates a folder with the user's Full Name in the Home folder, for example: /Home/John Smith.

To change the home folder, select from the available folders, then click **Change Home Folder**. If you want to set the user to have no home folder, select None from the Home Folder list.

Default Folder

By default, a user's home folder is their initially selected choice when uploading a file to the DMZ system. A link is also provided on their Home page to go directly to their home folder. This setting allows an administrator to change the "default" folder for a user to any other folder on the system. When a user goes to upload a file, this folder will be the folder initially selected as the destination. A link will also appear on the user's Home page which takes them directly to the default folder. The default folder is also where the user will be placed when signing on to the DMZ system through the FTP or SSH servers.

The Edit Default Folder Settings section of this page contains settings related to the user's default folder:

- **Make Default Folder the Root Folder ("chroot") When Using FTPS or SFTP** - When enabled, the user's default folder will become their root folder when they sign on through the FTPS or SFTP interfaces. The only files and folders the user will be able to see will be those that are in or below the default folder, and the user will be prevented from navigating to a directory that is outside their default folder.

Shared Account

User accounts are typically used by a single user only, and have full access to the files that they upload, and the log entries that they have generated. Sometimes a single user account needs to be used by several users though, in which case each individual shouldn't necessarily be able to see the activities of other people using the account. The Shared Account setting should be enabled for such accounts. When enabled, this option will hide files uploaded to write-only folders by all people sharing the account. (Files uploaded to write-only folders are normally visible to the user that uploaded them.) It will also hide log entries created by the user, and prevent the user from altering account settings such as email address and password.

Upload/Download Wizard

This section determines whether or not a user will be prompted to install the Upload/Download Wizard if they do not already have it installed. When the Prompt to install Upload/Download Wizard setting is set to Yes, users who do not have the wizard installed will be prompted about it, and asked if they want to install it, after they sign on. When set to No, users will not be prompted about the wizard, though they will still be able to use the wizard if it is already installed. Users may also install the wizard from their Account Options page.

Sign On/Sign Off Logging

For automated user accounts that frequently access MOVEitDMZ via FTP/SSH to look for new files, you can turn off database logging of successful sign-on/sign-off events. This will prevent the performance issues and timeouts from excessive logging. The default logging setting is "All", meaning all events, both successes and failures, will be logged. The alternative logging setting is "Failures Only".

To turn off - or turn back on - successful Sign On/Sign Off logging for the user, click the **Change Logging Status** link. In the Edit Sign On/Sign Off Logging Status page, click Yes or No for the setting ("Suppress successful Sign On/Sign Off attempts from being logged to the database"). Click the "Change Logging Status" button. Then click "Return to the full user profile" link to return to the main user profile page.

DLP Ruleset

Administrators can set Data Loss Prevention (DLP) rules to monitor for sensitive information in data from file transfers and Ad Hoc transfers, including subject, note/body and attachment. File transfers that violate a DLP policy can be blocked, quarantined, or allowed. This setting shows whether any rulesets assigned to this user. Click **Change Ruleset** to change rulesets for the specific user, which overrides the ruleset assigned to the user class for that user.

Group Information

Group Information

Member of Groups: *(None)*

 [Join or Leave Groups](#)

This section allows an Admin and some GroupAdmins to add and remove this user to/from groups. If this user is a GroupAdmin or has another special relationship to a group, it will also be noted here.

Address Book Information

Address Book Information

Members of Address Book:

Annie (annie)

Bobby (bobby)

GROUP: East Coast

 [Edit Address Book for this User](#)

The address book for a user contains the list of users and groups this user will be able to send packages to if Ad Hoc Transfer is enabled.

Clicking on the "Edit Address Book for this User" link will bring up the Edit Address Book page for the user. Here, the list of users and groups that this user will be able to send packages to can be added to or modified.

User/Group	Allow Packages to Members	
GROUP: East Coast	No	X
Annie (annie)	-	X
Bobby (bobby)	-	X

Search: Fred (fred)

Select User or Group:
 (Ctrl-Click to select multiple users and/or groups)

☐ Allow Sending Packages to Individual Members of Group(s)
☒ Also Add kristina to Address Books of Selected Users/Groups
☐ Also allow kristina to upload files to home folders of selected USERS and visa versa
☐ Also allow selected GROUPS to upload files to home folder of kristina

Add Entries

The current list of users and groups in this user's address book is shown at the top of the page. The list has three columns:

- User/Group: The username or group name of the address book entry.
- Allow Msgs to Members: This property is only available for groups. When set to Yes, the members of that group will also be shown in this user's list of available recipients.
- Action:
 - Remove: Removes this entry from the address book

A list of users and groups who can be added to this user's address book is also shown. Selecting one or more users and/or groups from the list and then clicking the "Add Entries" button will add those users and groups to this user's address book. Multiple selection is possible by holding down the Control key when selecting entries. Additional options are available to modify the result of adding the new entry:

- Allow Packages to Individual Members of Group(s): The user will be able to see the members of the added group in their list of available recipients.
- Also Add (USER) to Address Books of Selected Users/Groups: Adds the current user to each of the selected users' and/or groups' address books.
- Also allow (USER) to upload files to home folders of selected USERS and visa versa: Gives the current user Write permissions to each selected users' home folder, and visa versa.
- Also allow selected GROUPS to upload files to home folder of (USER): Gives each selected group Write permissions to the current user's home folder.

Groups

Overview

A group organizes several users and makes assignment of permissions easier. For example, folder permissions and packages address book entries can be applied to groups rather than individual users.

Users who are normal Members of a group typically enjoy all the permissions enjoyed by that group.

GroupAdmins (on page 277) are users who have been "promoted" to assist with the management of the group (such as adding/deleting users) and Limited Members typically enjoy only a few of the group attributes. The complete list of group members can be viewed from a **Group Profile** (on page 306) or by using the **"In Group" drop-down filter** (on page 271) on the main "Users" page.

Display profiles (on page 306) and some default user settings can be applied to groups. A **custom announcement** (on page 306) that normally appears on members' Home pages and a **custom logo** (on page 306) that will appear on all members' pages can also be applied to groups. If the "External Authentication" feature has been enabled, MOVEit DMZ can automatically replicate some or all of its user group membership information from an associated LDAP server.

All Groups			
Name	Description	Members	
 East Coast	East Coast sales	2	 
 West Coast	West Coast Sales	2	 

Page 1 of 1 (Groups 1 to 2 of 2 total @ 10 per page)

Add Group

The main list of groups has several columns:

- Name: The name of the group. Clicking on the group name will open the group profile.
- Description: An optional description of the group.
- Members: A count of the current group members.
- You may also:
 - Clone: Allows you to clone this Group
 - Delete: Deletes this Group (after confirmation)

An "add" link allows Admins to create new groups.

Because there may be many groups on the system, the list of groups will be limited to a configurable number per page. Page navigation links will be provided if the number of groups exceeds this limit. The value is configurable in the Account Options page.

In addition, there are additional "helper" views available to find specific groups.

Filter Groups:

Pick a Selection: All Groups - Empty Groups - Groups w/o Perms

Pick a Letter: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

- Pick a Selection:
 - All Groups: Displays all groups
 - Empty Group: Displays only groups without any members
 - Groups w/o Perms: Displays only groups without any folder permissions
- Pick a Letter:
 - (Any Letter): Forwards to the page on which the first group associated with the letter appears. (e.g., "G" might send an Admin to page 4, which contained a "Germantown" group.)

GroupAdmins

GroupAdmins are **end users** (on page 277) who have been promoted by (organization-level) Admins or other GroupAdmins for the purpose of administering users in groups. These special users are generally responsible for adding new users to the group, removing users from the group, changing passwords and editing the various properties of users within the group.

GroupAdmins have less rights than full organization administrators, so are subject to various limitations when administering their groups. The specific rights GroupAdmins enjoy over any particular group are configured on group profiles in the "**GroupAdmin Settings**" *section* (on page 306).

GroupAdmins may also receive notifications about events that happen to the users they have control over, such as password expirations and user lockouts. In order to receive these notifications, GroupAdmin users must have their notifications setting set to "On+Admin". See the Web Interface - Users - Profile page for more information about this setting.

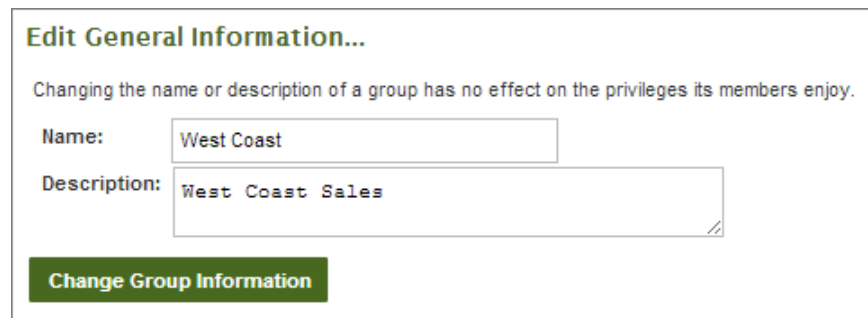
Profile

The group profile allows Admins to change the membership list of the group, as well as the name and description, and several other group-level settings. (Name changes are harmless because groups are tracked internally using a separate ID.) The following sections are currently available on this page:

- Change General Information
- Add Or Remove Members
- Change GroupAdmin Settings
- Change Member Settings
- Change Display Profile
- View Folder Permissions
- Address Book Information
- Group Custom Email Notifications
- Change Announcement
- Change Logo

Change General Information

The group name and description can be changed in the Change General Information section.



Edit General Information...

Changing the name or description of a group has no effect on the privileges its members enjoy.

Name:

Description:

Change Group Information

All characters in the ISO-Latin-1 (ISO/IEC 8859-1) set are allowed in group names.

Note: Group names may not begin with the characters "@!", for internal reasons.

Add Or Remove Members

This section is provided to add or remove users from this group and to change their membership class. The "Select User" drop-down only lists users who are not already members of the group. If there are many users in this organization, the "Select User" drop-down may be automatically replaced with a "Find User" dialog instead. Administrators (and authorized GroupAdmins) may designate certain members of the group as GroupAdmins. Click the "Make Admin" link to promote the given member as a GroupAdmin, and click the "Make Not Admin" link to remove GroupAdmin permissions from the related user.

Users who are normal Members of a group typically enjoy all the permissions enjoyed by that group. **GroupAdmins** (on page 277) are users who have been "promoted" to assist with the management of the group (such as adding/deleting users). Limited Members are subordinate users that typically enjoy only a few of the group attributes, such as being visible in the address books of full group Members.

Add or Remove Members...

Normal Members of this group enjoy all the privileges assigned to the group. GroupAdmins are given extra privileges in order to assist with the administration of the group (such as adding/deleting users) and Limited Members are typically temporary users who appear in the Ad Hoc Transfer address books of other group members. Membership type is indicated in the Class column. Use the "Remove" links to remove members. Use the "Make Admin" links to mark users as GroupAdmins, and the "Make Not Admin" links to de-mark users as GroupAdmins. Members can be added using the user list box.

Username	Full Name	Class	
 bobby	Bobby	Member	 
 fred	Fred	Member	 

Annie (annie)
kristina (kristina)

Select User:

(Ctrl-Click to select multiple users)

Add Member(s)

 Click to Compose (Insecure) Email Message to All Members
 Click to Compose Package to this Group

If entries appear or disappear mysteriously from this list, remember that if the "External Authentication" feature has been enabled, MOVEit DMZ can automatically replicate some or all of its user group membership information from an associated LDAP server. (External Authentication synchronization actions will be logged in the audit trail, so they should become less mysterious after some research.)

Also available at the bottom of the membership section are two links which can be used to message the members of the group. The first is a link which can be used to send an insecure email to all the members of the group that have email addresses. This is simply a "mailto" link, containing a comma-delimited list of all email addresses of the group members. The second is a link to compose and send a package to the group. Use this link instead of the first link if security is a priority, and if you want to send files to the group.

Change GroupAdmin Settings

Edit GroupAdmin Settings...

This group's GroupAdmins may:

- ☐ Change the logo and announcement for this group
- ☒ Add new users as group members and edit/delete existing group members
- ☐ List all users in the organization and add existing users as group members
- ☒ Change passwords of existing group members
- ☐ Enjoy following permissions on member home folders:
Read Write Delete List Notify Subs Admin
☐ ☐ ☐ ☐ ☐ ☐ ☒
- ☒ List and edit limited members added by group members

Set a member's file quota to any value up to: KB ▾

Set a member's ad hoc transfer quota to any value up to: KB ▾

Set a member's per-package attachment quota to any value up to: KB ▾

Change GroupAdmin Settings

These settings determine the authority GroupAdmins of this group will exercise over group members.

- Change the logo and announcement for this group: Determines whether GroupAdmins of this group will have the ability to change the logo and announcement for this group. If this option is enabled, GroupAdmins will be able to view the profile pages for their groups and will have access to the Edit Logo and Edit Announcement sections.
- Add new users as group members and edit/delete existing group members: Determines whether GroupAdmins of this group will have the ability to add, delete and modify details about the end user members of the group. If this option, or the Change Passwords of Existing Group Members option is enabled, GroupAdmins will be able to change the security status of end user group members as well.
- List all users in the organization and add existing users as group members: Determines whether GroupAdmins of this group will be able to list all end users in the organization, and add those users to their groups, thereby gaining any administrative authority they are granted by the group over those users.
- Change passwords of existing group members: Determines whether GroupAdmins of this group will have the ability to change passwords of the end user members of the group. If this option, or the Edit/Delete Existing Group Members option is enabled, GroupAdmins will be able to change the security status of end user group members as well.
- Enjoy following permissions on member home folders: Determines which permissions, if any, GroupAdmins in this group will enjoy on the home folders of end user members.
- List and edit temporary users added by group members: Determines whether GroupAdmins in this group will have administrative access to Limited Members of the group. Temporary users created by group members are automatically assigned to the group as a Limited Member. This option should be enabled if you want GroupAdmins to be able to see and control who the group's full time end users are communicating with.
- Set a member's file quota to any value up to: Used to set a limit to how high GroupAdmins can set the user quotas for individual end user members of this group. For example, if this value is set to 50 MB, a GroupAdmin may set an individual user quota to 1 MB or 25 MB but not 60 MB. A value of 0 KB or 0 MB indicates there is no restriction on the GroupAdmin's ability to set end user member file quotas in effect.
- Set a member's ad hoc transfer quota to any value up to: Used to set a limit on how high Group Admins can set the user Ad Hoc Quota setting for individual end user members of this group. For example, if this value is set to 50 MB, a GroupAdmin may set an individual Ad Hoc Quota to 10 MB or 20 MB but not 60 MB. A value of 0 KB or 0 MB indicates there is no restriction on the GroupAdmin's ability to set end user member ad hoc quotas in effect.
- Set a member's per-package attachment quota to any value up to: Used to set a limit on how high Group Admins can set the user Maximum Attachment Size setting for individual end user members of this group. For example, if this value is set to 5 MB, a GroupAdmin may set an individual user maximum attachment size to 1 MB or 2 MB but not 6 MB. A value of 0 KB or 0 MB indicates there is no restriction on the GroupAdmin's ability to set end user member attachment quotas in effect.

Change Member Settings

Edit Member Settings...

This group's members may:

- ☐ See limited members in their address book (if allowed to see individual group members)

Change Member Settings

These settings determine the privileges conferred on members of this group. The settings available here depend on the settings chosen on the 'Web Interface - Settings - Ad Hoc Transfer - Registered Users page'.

- **Send packages:** Determines whether end user members of this group can send packages. This setting is only available when the organization-level Registered Users setting is set to "Members of groups that grant Ad Hoc Transfer access".
- **Send packages to registered users not listed in their address books:** Determines whether end user members of this group can send packages to registered users who are not in their address book. This setting is only available when the organization-level address book setting is set to "Members of groups that grant this permission".
- **Send packages to recipients who are not currently registered users:** Determines whether end user members of this group can send packages to unregistered users. This setting is only available when the organization-level setting is set to "Members of groups that grant this permission".
- **See limited members in their address book (if allowed to see individual group members):** This option determines whether temporary users will show up in the address books of all the normal members of a group (specifically, those users who have this group in their address book with the 'Allow Packages to Individual Members of Group(s)' setting applied). Note that temporary users created as an unregistered recipient of - or unregistered sender to - a normal member, will always show up in the address book of that one member. The question settled by this option is, should they also be included in the address books of the other group members? For example, Group A has three registered users, Member 1, Member 2 and Member 3. If Member 1 sends a package to Temp 1. With this option selected, Temp 1 will show up in the address books of Member 2 and Member 3, as well as that of Member 1. Similarly, if Temp 2 self-registers to send a package to Member 2, Temp 2 will appear in the address books of Member 1 and Member 3, as well as that of Member 2. (With the option not selected, Temp 1 would only appear in Member 1's address book, and Temp 2 would only appear in Member 2's address book.) Select this option if all members of a group should be able to communicate with any temporary user that is created for an Ad Hoc Transfer with any normal group member.

Change Display Profile

The Change Display Profile section allows an administrator to change the display profiles that will be used to create the look and feel of the web interface for GroupAdmins and regular members of this group. Display profiles can be independently set for these two user types. This allows group members to be assigned a basic profile, while GroupAdmins get a more advanced profile.

Change Display Profile...

Group Display Profiles customize the web interface seen by GroupAdmins and members of this group. If the value is set to "(None)", the associated members will use the display profile defined for their user permission level (e.g. "Temp Users"), if any, instead.

GroupAdmin Display Profile: (None) ▼

Member Display Profile: (None) ▼ [Edit Display Profiles](#)

[Change Display Profiles](#)

When set to "(None)", the associated members will use the display profile configured for their user class. Otherwise, they will use the selected profile. If a user is a member of more than one group, each with their own selected display profiles, the user will use a display profile which combines the settings of the individual display profiles that would normally apply to the user.

View Folder Permissions

View Folder Permissions...

All members of this group enjoy the following permissions on the listed folders.

Name	Read	Write	Delete	List	Notify	Subs	Admin
 / Archive	X			X			
 / WebPosts	X			X	X		

This section displays folder permissions which have been explicitly assigned to this group. To add, delete or change these permissions, follow the links to the folders and use the "change permission" links on the various folders.

Address Book Information

Address Book Information**Members of Address Book:**

[Fred \(fred\)](#)

[GROUP: East Coast \(Allow Msgs to Members\)](#)

 [Edit Address Book for this Group](#)

The address book for the group contains the list of users and groups any member of this group will be able to send packages to if Ad Hoc Transfer is enabled on the DMZ system.

Edit Group Address Book

User/Group	Allow Msgs to Members	
GROUP: East Coast	Yes	
Fred (fred)	-	

Select User or Group:
(Ctrl-Click to select multiple users and/or groups)

Annie (annie)

Bobby (bobby)

kristina (kristina)

GROUP: Administrators

GROUP: West Coast

☐ Allow Packages to Individual Members of Group(s)
☐ Also Add Administrators to Address Books of Selected Users/Groups

Add Entries

The current list of users and groups in this group's address book is shown at the top of the page. The list has three columns:

- User/Group: The username or group name of the address book entry.
- Allow Packages to Individual Members of Group(s): This property is only available for groups. When set to Yes, the members of that group will also be shown in this group's list of available recipients.
- Remove: Removes this entry from the address book

A list of users and groups who can be added to this group's address book is also shown. Selecting one or more users and/or groups from the list and then clicking the "Add Entries" button will add those users and groups to this group's address book. Select the "Allow Packages to Individual Members of Group(s)" checkbox if you want the members of this group to be able to see the members of the added group in their list of available recipients. Select the "Also Add..." checkbox if you want to add the current group to each of the selected users' and/or groups' address books. Multiple selection is possible by holding down the Control key when selecting entries.

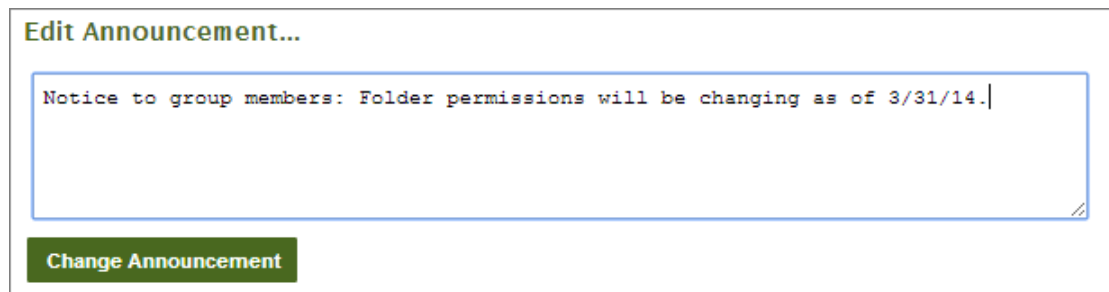
Hint: To permit all members of a group to send packages to all other members of their group, add the group to its own address book and make sure the Allow Packages to Individual Members of Group(s) option is enabled.

Group Custom Email Notifications

If custom email notifications have been created, the groupadmin can make them available to users. For information about custom email notifications, see *Web Interface _Settings - Appearance - Custom Notifications* (on page 373).

Change Announcement

A group announcement, if present, will appear in the Announcements section of the Home page of all members of the group. If a user is a member of multiple groups that have configured group announcements, he or she will see all associated announcements at the top of his or her page.



Edit Announcement...

Notice to group members: Folder permissions will be changing as of 3/31/14.

Change Announcement

Change Logo

A group logo, if present, will be placed at the top of the content section of the MOVEit DMZ web page for all members of the group. Images must be in GIF format and must be less than 100,000 bytes. If a user is a member of multiple groups that have configured group logos, he or she will see all associated logos at the top of his or her page.

Edit Logo...

The following logo will be displayed for all group members at the top of the content section of every page.

Current Logo: None

To change this logo, select a new banner logo ("GIF" format only) from your local computer with the "Browse" button below, and then press the "Upload Group Logo" button to upload it as your new banner logo. To clear the current logo, leave the New Logo field blank and press the "Upload Group Logo" button.

New Logo: mountains.jpeg

(Recommended width is 340 to 620 pixels. 580 pixels is ideal with a 800-pixel organization logo.)

Logs

Overview

Clicking on the Logs link in the left-hand navigation will display the "Edit Filter" page.

The "Edit Filter" page allows users to select the content displayed in the advanced file view. The selections entered here will be remembered through the current session. Once a user signs out, or the session expires, the selections are forgotten.

Filter Logs...

Date: ☒ Display only log entries within this date range:
Start Date/Time: 2014 ▾ Apr ▾ 1 ▾ 12 ▾ 00 ▾ AM ▾
End Date/Time: 2014 ▾ Apr ▾ 1 ▾ 11 ▾ 59 ▾ PM ▾ All Day
Action: (Any) ▾
User: By Username: (Any) ▾
By Full Name: (Any) ▾
(Deleted users are indicated by italic font)
Username Contains:
File: FileID Contains:
FileName Contains:
Size: Comparison: (Any) ▾ Size (kb):
Folder: FolderPath Contains:
IP Address: Contains:
Agent Brand: Contains:
Success/Failure: (Any) ▾
Apply Filters

- **Date:** Allows the user to select entries between any two date/times. The "All Day" link, if present, will set the start time to 12:00 AM, and the end time to 11:59 PM. (Remember to check the box to apply date settings.)
- **Action:** Allows the user to select general action types. (i.e. "Administration", "File Transfer", "Uploads", etc.)
- **User:** Allows the user to specify a username, full name, or enter a partial username.
- **File:** Allows the user to specify either a file ID or a file name. (File transfers only - wildcards accepted for file name.)
- **Size:** Allows the user to specify a file size. (i.e. "Greater than", "Less than" - file transfers only.)
- **Folder:** Allows the user to specify a folder.
- **IP Address:** Allows the user to specify an IP address from which actions were initiated. (Wildcards accepted.)
- **Agent Brand:** Allows the user to specify an agent name (for example: "Mozilla" or "MOVEit Central").
- **Success/Failure:** Allows the user to note whether all entries, only failed entries or only successful entries should be displayed.

Logs Page

The logs page provides an easy way to look up file transfers, sign ons, password changes and other audited activities from an online interface. The columns and content of this view are entirely customizable through the "Customize View" (columns) and "Edit Filter" (content) links. Pre-defined filters, both built-in and custom, can be accessed by clicking the "Favorite Filters" link, and custom views can be saved by clicking the "Save Current View to Favorites" link. Finally, navigation links ("Go to Page") allow users to page through log entries.

Note: To conform with Payment Card Industry (PCI) requirements, MOVEit DMZ creates an audit log record every time the audit log is viewed. A "View Audit Log" record is written every time a list of log records is viewed, including every run of any report that accesses the audit log. A "View Audit Log Entry" record is written every time the details of an individual audit log record are viewed. For users who find these records distracting, a new "Suppress Log Views" option is available in the existing Customize View options. This option defaults to off, thus displaying log view audit records.

Logs

[Customize View](#)[Edit Filter](#)[Favorite Filters](#)[Save Current View To Favorites](#)

Current Filter(s): Date is between 4/1/2014 12:00:00 AM and 4/1/2014 11:59:00 PM

Log Entries

Date and Time ▾	Action	User Full Name	File Name	File ID	Folder Name	IP Address
4/1/2014 1:46:09 PM	Add Entry to Group Address Book	kristina				192.168.150.233
4/1/2014 1:46:09 PM	Add Entry to Group Address Book	kristina				192.168.150.233
4/1/2014 1:46:06 PM	Add Entry to Group Address Book	kristina				192.168.150.233
4/1/2014 1:45:07 PM	Add Permission for a Group to Folder	kristina			/WebPosts	192.168.150.233
4/1/2014 1:44:56 PM	Add Permission for a Group to Folder	kristina			/Archive	192.168.150.233
4/1/2014 1:44:41 PM	Add Group	kristina				192.168.150.233
4/1/2014 1:43:46 PM	Add Permission for a Group to Folder	kristina			/Home/February	192.168.150.233
4/1/2014 1:43:39 PM	Disable Inherit Permissions From Parent for Folder	kristina			/Home/February	192.168.150.233
4/1/2014 1:42:43 PM	Add Folder	kristina			/Home/February	192.168.150.233
4/1/2014 1:42:34 PM	Add Folder	kristina			/Home/January	192.168.150.233
4/1/2014 1:34:45 PM	Add Group Member	kristina				192.168.150.233
4/1/2014 1:34:40 PM	Add Group Member	kristina				192.168.150.233

Page 1 of 5 (Log Entries 1 to 12 of 56 total)

Go to Page: First | Prev | Go | Next | Last

[Customize View](#)[Edit Filter](#)[Favorite Filters](#)[Save Current View To Favorites](#)

Users, files, and folders that are referenced by log entries can usually be clicked on to view the information page for that item. The date/time value of each log entry can be clicked on to view the details for that particular entry. A certificate icon next to the date/time value indicates that this log entry contains client certificate information, meaning the user who did the action was signed on with a client certificate at the time. The details of the client certificate will be displayed on the log entry page.

Log Entry

Clicking on the Date/Time link for a specific entry in the list of log entries brings up the Log Entry page for that entry.

Log Entry

Date/Time	4/1/2014 1:44:56 PM
User	Username: kristina Real Name: kristina IP Address: 192.168.150.233 Agent:  Chrome Browser 33.0.1750.154
Folder	Path: /Archive ID: 985615576
Description	Add Permission for Group Administrators to Folder /Archive
Technical	Error Code: 0 Message: Allowed 'list, read' access to the 'Administrators' group.

This page contains all the information available about the entry including when the entry was added, who was responsible for the action, a description of the action that took place, the success or failure code of the action, and any notes and/or further details about the action. A link to return to the main Logs page is also available, which will return the user to the same Logs page they arrived from.

View User Logs

Each user profile has a "View User Logs" link which administrators can use to define a log filter that returns log information about just that user.

User Profile (kristina)

General Information

Username: kristina

Full Name: kristina

User ID: kristinm7dr0a965

Permission: Administrator

Notifications: via HTML-Format Email ([name@ipswitch.com](#))

Language: English

Created: 4/1/2014 9:54:19 AM by kristina

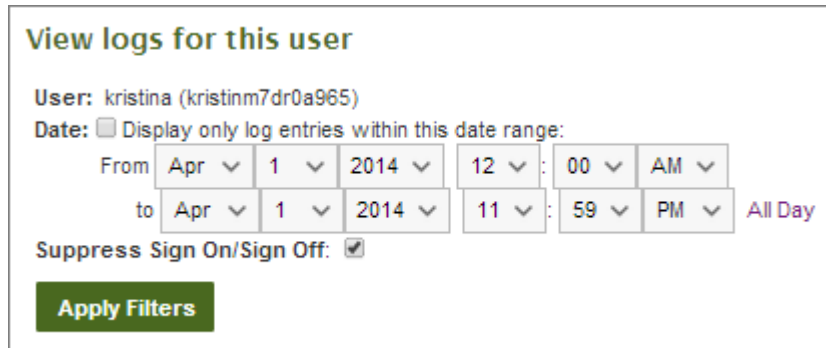
 [Change Information](#)

 [View Home Folder \(/Home/kristin\)](#)

 [View Folder Access List](#)

 [View User Logs](#)

Clicking the link leads to a filter specification page, which allows the admin to select a user to view log information about. Clicking on the Apply Filters button will execute the user filter and show the log entries associated with the selected user.



View logs for this user

User: kristina (kristinm7dr0a965)

Date: ☐ Display only log entries within this date range:

From Apr 1 2014 12 : 00 AM

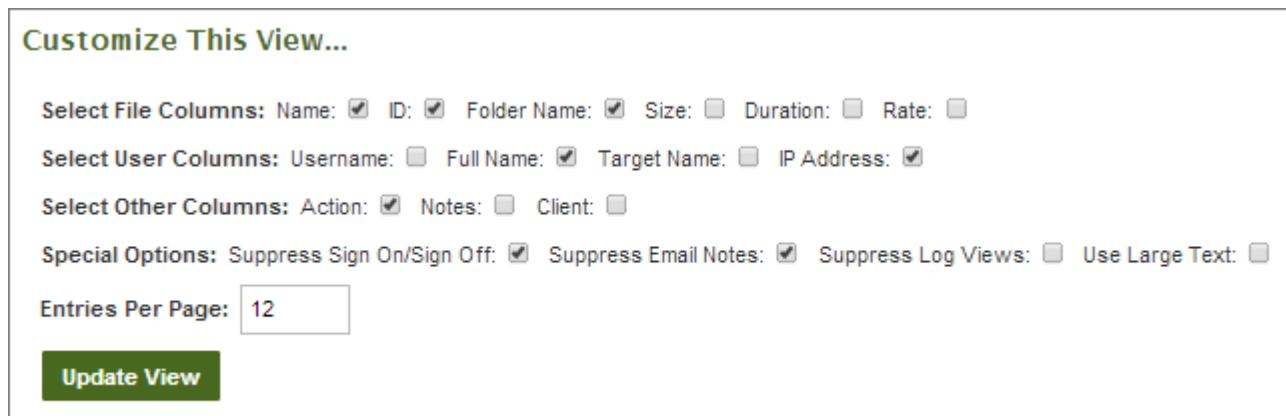
to Apr 1 2014 11 : 59 PM All Day

Suppress Sign On/Sign Off: ☒

Apply Filters

Customize View

The "Customize View" link will bring up a form which allows users to select the columns displayed in the advanced file view. Changes to these selections will be saved and pre-filled during future log page visits, even between sessions. At least one column must be selected here, or an error will be displayed.



Customize This View...

Select File Columns: Name: ☒ ID: ☒ Folder Name: ☒ Size: ☐ Duration: ☐ Rate: ☐

Select User Columns: Username: ☐ Full Name: ☒ Target Name: ☐ IP Address: ☒

Select Other Columns: Action: ☒ Notes: ☐ Client: ☐

Special Options: Suppress Sign On/Sign Off: ☒ Suppress Email Notes: ☒ Suppress Log Views: ☐ Use Large Text: ☐

Entries Per Page:

Update View

File Columns:

- **Name:** The original name of the file
- **ID:** The seven-digit ID of the file
- **Folder Name:** The name of the MOVEit DMZ folder in which this file is currently stored
- **Size:** The size (in bytes) of the file or secure message
- **Duration:** The length of time (in seconds) it took to transfer the file
- **Rate:** The data transfer rate of the file transfer (in bytes/second)

User Columns:

- **Username:** The username of the user (i.e. "fsmith") who performed this action
- **Full Name:** The full name of the user (i.e. "Fred Smith") who performed this action
- **Target Name:** The full name of the user this action affected
- **IP Address:** The IP address from which this action was initiated

Other Columns:

- **Action:** The action performed
- **Notes:** Additional notes regarding this action
- **Client:** The client type and version from which this action was performed. Icons will be displayed for known client types, and unknown client types will have their full agent identification string displayed.

Special Options:

- **Suppress Sign On/Sign Off:** Used to hide or show sign on or sign off entries in the log. (Often people are only interested in specific actions users performed rather than the times they were signed on.)
- **Suppress Email Notes:** Used to hide or show email notification entries in the log.
- **Suppress Log Views:** Do not display log view records. (To conform with PCI requirements, a record is created each time the audit log, or an audit log entry is viewed.)
- **Use Large Text:** Increases the font size used in the table of entries

Entries per Page:

- Sets the number of entries displayed on each page.

Edit Filter

The "Edit Filter" allows users to select the content displayed in the advanced file view.

Favorite Filters

The "Favorite Filters" link will bring up a page which allows users to select a saved custom view, or one of several commonly requested filters involving file transfers, administration, or all activities. The "Define Advanced Filter" link will pop up the Edit Filter form described above.

Favorite Filters
To add a new favorite filter, set the desired filter and view settings from the log entries page, then click the Save Current View To Favorites link.
Filter
Sunday Uploads ▶ ✕
Wednesday Uploads ▶ ✕

Select a Filter...
Daily File Transfer: Today - Yesterday - Pick a Date
Daily Administration: Today - Yesterday - Pick a Date
Custom Filter: Define Advanced Filter

Save Current View to Favorites

Favorite views (combinations of column and record count preferences and filter options) can be saved to the Favorite Filters page by setting up the view using the "Customize View" and "Edit Filter" links, then clicking the "Save Current View to Favorites" link. The user will be prompted to enter a name for the new view, or use the name of the currently selected view, if they would like to update it. Once a custom view has been saved, it can be loaded again from the Favorite Filters page.

Add a Favorite Filter

To save the current log viewing settings and filters as a Favorite Filter, enter a name below, then click the Add Favorite Filter button.

Filter Name:

Add Favorite Filter

Current Filter Settings

Show Columns:	File Name, File ID, Folder Name, User Full Name, IP Address, Action	
View Options:	Suppress Sign On/Sign Off, Suppress Email Notes Display 12 entries per page	
Sort by:	Date and Time Descending	
Filter Options:	Use Date/Time Range:	Yes
	Start Date/Time:	4/1/2014 12:00:00 AM
	End Date/Time:	4/1/2014 11:59:00 PM
	Action Filter:	File Transfer
	Success/Failure Filter:	Successful

Reports

Overview

The Reports page provides access to MOVEit DMZ's reporting capabilities. Here, automated reports can be added, edited, executed, and deleted. Additionally, access to the quick Statistics page is provided. See the **Statistics** (on page 345) page for more details.

Reports

Statistics

 [Go to Quick Statistics](#) (previously known as "Stats")

Reports

Name	Category	
Default Report Settings	Report Template	
Content Scanning Report 1	Content Scanning	  
Locked Out IP Addresses	File Transfer	  
Performance Report 1	Performance	  
Storage Report 1	Storage	  
User Maintenance Report 1	User Maintenance	  

Add Report...

Select a report category and click the "Continue" button to continue to configure a new report.

Report Category:

[Continue](#)

Reports

Reports are MOVEit DMZ's method for providing easy access to the large amount of performance and status data that DMZ gathers about itself. A report is a set of instructions for executing a data query, formatting the results, and saving the resulting report to a specific location. Reports can be created either with one of the built-in categories and types, or the Custom category, which allows administrators to enter their own query parameters or import specialized reports. For more information about defining Custom reports, see the Custom Reports page.

Adding or Editing a Report

To add a report, select the category of report you wish to create, and click the Continue button. This will bring up the Add Report page (for a list of report categories, and the report types available in each category, see the **Report Types** (on page 334) page). To edit an existing report, click on the name of the report in the report list, or click the Edit link associated with the report.

Edit Report...

Please specify the name, type and format of the report.

Name:

Report Category: Performance

Report Type:

Format:

Created: 4/1/2014 2:11:47 PM by kristina

Last Modified: 4/1/2014 2:11:47 PM

The following options determine when this report will be created and where it will be saved. You may use macros such as "[yyyy]" (year) in your folder and file names to datestamp your reports. Scheduled reports will be run by the nightly scheduled task. By default, this task runs at 1am.

Run On Days:

Examples: "All", "4,7,8", "Mon,Tue" - blank means "not scheduled"

Save In Folder:

Save As File:

If no value is entered, the report title will be used

☒ Overwrite Existing File

Except where indicated, the following report parameters are optional.

Start Date:

End Date:

Format: YYYY-MM-DD

Macros Allowed: [yyyy], [mm], [dd]

Examples: 2005-06-04, [yyyy]-[mm]-[dd], [yyyy]-[mm-3]-01

Size Units: Required

Update Report

Name

Each report must have a name, which will be listed on the reports page. The name for the new report should be chosen to convey the category and type of the given report. Names such as "Total File Transfer Report" or "Memory Usage for the Last Month" are good choices. Names such as "Report 1" or "My Report" are less desirable. The report name can be changed after creation without affecting the operation of the report.

Report Type

The type of report to execute is selected from this drop-down menu. Each report category has several report types to choose from. Most report categories have Total reports, which provide aggregated information, as well as By Month, By Week, and By Day reports, which break the aggregated information into the selected timespans. A complete list of report categories and the types available in each can be found on the **Report Types** (on page 334) page.

Format

The format of the report is selected here. This defines how the report information will be presented. Available formats are:

- XML - Information will be presented in an XML document. This format is ideal for loading into external applications for post-processing. The report document will have the following schema:

```
<DMZReport>
  <ReportRow>
    <Column_Name>Value</Column_Name>
    <Column_Name>Value</Column_Name>
    ...
  </ReportRow>
  ...
</DMZReport>
```
- CSV - Information will be presented in a text document in comma-separated-value format. This format is ideal for loading into spreadsheet programs such as Excel. When this format is selected, two additional options become available:
 - Value Delimiter - This character will be used as the delimiter character in the report document. By default, this is a comma (,).
 - Text Qualifier - This character will be used to surround each column and value. Set to a blank string to not use any qualifier character. By default, this is a double-quote (").

- Bare HTML - Information will be presented in an HTML file with very basic formatting.
- Styled HTML - Information will be presented in an HTML file styled with the organization's stylesheet rules. This format is ideal for presenting the report content in a professional manner.

Run On Days

Reports may be scheduled to run on specific days of the week, or days of the month. Enter the days you wish the report to run in this field, or "All" to have it run every day. Scheduled reports will be run during the nightly scheduled task on the days configured. By default, this task runs at 1am. You may also leave this field blank if you do not want reports to run automatically.

Some examples of values which may be entered in this field and how those values would be interpreted may help.

- 1,2,5 - Run on the first, second and fifth day of the month
- Tue, Sat - Run on every Tuesday and Saturday
- 3, 4, Wed - Run on the third and fourth day of the month and every Wednesday
- 3, 4, Wed, All - Run everyday

Save In Folder, Save As File

These fields determine where the resulting report document will be saved. The Save In Folder value should be a MOVEit DMZ folder path, and will be where the report document will be saved on the system. The value does not need to be an existing folder, as MOVEit DMZ will create the folder if it does not exist. Date macros may also be used to create date-specific folders. For example:

"Distribution/Reports_[yyyy][mm]" would save reports to a folder named "Distribution/Reports_200510" during the month of October, 2005.

The Save As File value defines the name of the file which the report document will be saved to. As with the Save In Folder value, date macros can be used to create date-specific filenames. For example:

"Total_File_Transfers_[yyyy][mm][dd].txt" would save a report to a file named "Total_File_Transfers_20051020.txt" on October 20, 2005.

If the Overwrite Existing File option is checked, the report generator will attempt to delete a file that has the same name as the new report, if such a file exists. This is especially useful for reports with static names, as errors could occur if the destination folder is not configured to allow file overwrites.

Report Parameters

The rest of the configuration of a report deals with setting the available parameters for the report type. These parameters can narrow down the scope of report, as well as define the output of a report. To see which parameters are available for each report category, see the **Report Types** (on page 334) page.

Available parameters are:

- **Start Date** - Defines a date before which data will be ignored when creating a report. Use this along with the End Date parameter to narrow down the timespan that a report will cover. This parameter can accept date macros. Dates MUST be expressed in YYYY-MM-DD format (e.g., "2005-03-04").
- **End Date** - Defines a date after which data will be ignored when creating a report. Use this along with the Start Date parameter to narrow down the timespan that a report will cover. This parameter can accept date macros. Dates MUST be expressed in YYYY-MM-DD format (e.g., "2005-03-04").
- **Size Units** - Defines the size units a report will return bytecounts in. Available options are Kilobytes, Megabytes, and Gigabytes.
- **Attempt Threshold** - For the "Suspicious Usernames - Many Attempts" and "Suspicious IPs - Many Attempts" reports in the Security category, this parameter defines the number of failed attempts a username or IP address needs to have made to register in these reports.
- **IP Threshold** - For the "Suspicious Usernames - Many IPs" report in the Security category, this parameter defines the number of failed attempts an IP address needs to have made to register in this report.
- **Username Threshold** - For the "Suspicious IPs - Many Usernames" report in the Security category, this parameter defines the number of failed attempts a username needs to have made to register in this report.

Date and Time Macros

Date and time macros provide a powerful way to define dates, times and date-and-time ranges relative to the current date and time. The six basic elements of date and time macros are:

- [YYYY] - Year (4 digits)
- [MM] - Month (2 digits)
- [DD] - Day-of-Month (2 digits)
- [HH] - Hour (2 digits)
- [TT] - Minute (2 digits)
- [SS] - Second (2 digits)

To express relative dates and times, plus (+) and minus (-) modifiers are used within the square brackets of the macros. For example, "[DD-2]" represents two days ago. Date and time macro modifiers affect the entire macro expression. Some examples of this behavior may help explain it.

- Today is Sep 14, 2005. "[YYYY]-[MM]-[DD-3]" will be interpreted as "2005-09-11"
- Today is Oct 15, 2005. "[YYYY]-[MM-1]-01" will be interpreted as "2005-09-01"
- Today is Nov 16, 2005. "[YYYY+5]-[MM+3]-[DD]" will be interpreted as "2011-02-16"
- Today is Jan 1, 2006. "[YYYY]-[MM]-[DD-1]" will be interpreted as "2005-12-31"

Schedule and Date Macro HINTS:

- To get an "end-of-month" report, schedule a report to run on "1" (first day of month), set the Start Date to "[YYYY]-[MM-1]-01" and set the End Date to "[YYYY]-[MM]-[DD-1]"

- To get an "end-of-week" (ending on Saturday) report, schedule a report to run on "Sunday", set the Start Date to "[YYYY]-[MM]-[DD-7]" and set the End Date to "[YYYY]-[MM]-[DD-1]"
- To get "daily" reports that cover "yesterday's" activity, schedule a report to run on "All", set the Start Date to "[YYYY]-[MM]-[DD-1]" and set the End Date to "[YYYY]-[MM]-[DD-1]"

Other Parameters

The rest of the configuration of a report deals with setting the available parameters for the report type. These parameters can narrow down the scope of report, as well as define the output of a report. To see which parameters are available for each report category, see the **Report Types** (on page 334) page. Available parameters are:

Running Reports

Scheduled reports will be run during the nightly scheduled task on the days configured in the Run On Days field. However, reports may also be run manually using one of two buttons in the Run Report section.

Run Report

You can run this report by clicking one of the two buttons below. The "Run Report and Download" button will run the report and return it directly to your browser as a file you can download and save to your local system. The "Run Report and Save" button will run the report and save the file to the target folder configured in the report.

Run Report and Download

Run Report and Save

Clicking the "Run Report and Download" button will cause the report to be created and sent directly to the browser. At this point, the browser should prompt to save or open the file. Clicking the "Run Report and Save" button will cause the report to be created and saved just as scheduled reports would be, in the folder specified by the Save In Folder value, with the filename specified by the Save As File value.

Additionally, an administrator may click the Run link for a report in the report list on the main Reports page. This link will perform the same action as the "Run Report and Download" button above.

Default Report Settings

The Default Report Settings entry exists in order to save administrators from having to enter similar configuration information into each report they add. Configuration information entered in this report entry will be automatically provided when adding new reports. Therefore, settings that many reports will have in common (Format, Schedule, etc) should be configured here.

Since the Default Report Settings entry is not a real report, it is not runnable, nor is it deletable. Editing the entry, however, works just like editing any other report. Note that changes made to the Default Report Settings entry will NOT be applied to existing reports, only to new reports.

Altering the Styled HTML Format

The layout of Styled HTML format reports is controlled by a template file called "reporttemplate.htm" A copy of this file can be found in your "(webroot)\templates\en" folder (e.g., "d:\moveitdmz\wwwroot\templates\en") Do not change this file; it will be overwritten every time you upgrade. Instead, follow one of these two brief procedures:

To change the Styled HTML format for all organizations:

- 1 Create a "templates\en" subfolder named "custom" if one does not already exist.
- 2 Copy "templates\en\reporttemplate.htm" into the "templates\en\custom" subfolder if it does not already exist there.
- 3 Make changes to the "templates\en\custom\reporttemplate.htm" as desired.

To change the Styled HTML format for a particular organization:

- 1 Create a "templates\en" subfolder named "custom" if one does not already exist.
- 2 Create a "templates\en\custom" subfolder named after the ID of the particular organization if one does not already exist. (For example, if the "Contractor" organization has an ID of "1234", create a subfolder named "1234".)
- 3 Copy "templates\en\reporttemplate.htm" into the "templates\en\custom\[OrgID]" subfolder if it does not already exist there.
- 4 Make changes to the "templates\en\custom\[OrgID]\reporttemplate.htm" as desired.

Note that changes made to this file will be applied immediately to new reports. However, changes made to this file will not affect any reports already created. If you have custom versions of reporttemplate.htm in both an organization-specific subfolder and the main "custom" subfolder, the organization-specific version will apply.

Macros Used in "reporttemplate.htm"

The following macros may be used in reporttemplate.htm.

- (Report Date Macros) - For example, "[YYYY]-[MM]-[DD] [HH]:[TT]:[SS]" could be interpreted as "2005-10-11 12:34:56"
- [InlineCSS] - This will be replaced by an inline copy of this organization's CSS stylesheet (set as part of an organization's Scheme).
- [OrgName] - The name of the organization.
- [ReportName] - The name of the report, as calculated from selections made in the report category drop-down and report type drop-down while defining the report.
- [ReportTitle] - The name of the report definition, as typed in by the creator.
- [Filter] - A description of the current filter (if any) used with the report.
- [ReportContent] - This will be replaced by a <TABLE> containing the actual report content.
- [ReportCreateMS] - The number of milliseconds it took to generate the report.
- [OrgLogRetain] - The number of days of audit log entries available to this report.
- [SysStatRetain] - The number of days of performance statistics available to this report.
- [MachineName] - The name of the machine on which this report was created.
- [ReportSQL] - The exact SQL statement(s) used to generate this report.

Report Types

Below is a list of the various built-in report categories, and the report types available under each category, along with the options available in each category.

Note: Typically, reports may contain up to 30 days of online audit records and 30 days of online performance statistics, depending on how you run the scheduled cleanup tasks that archive the older data.

File Transfer

These reports all summarize secure file transfer activity based on entries stored in the logs. All reports break out uploads and downloads separately.

Report Types

- Total
- By Month
- By Week
- By Day
- By User
- By User, By Month
- By User, By Week
- By User, By Day
- By Group
- By Group, By Month
- By Group, By Week
- By Group, By Day
- By IP
- By IP, By Month
- By IP, By Week
- By IP, By Day
- By Interface
- By Interface, By Month
- By Interface, By Week
- By Interface, By Day

Options

- Start Date
- End Date
- Size Units

Ad Hoc Transfer

These reports all summarize Ad Hoc Transfer activity based on entries stored in the logs. All reports break out sends and reads separately.

Report Types

- User Snapshot
- Total
- By Month
- By Week
- By Day
- By User
- By Month, By User
- By Week, By User
- By Day, By User
- By Group
- By Month, By Group
- By Week, By Group
- By Day, By Group

Options

- Start Date
- End Date
- Size Units

Storage

These reports display how many files, messages and archived logs are currently stored on MOVEit DMZ and how much space those items currently consume.

Report Types

- Total
- By Folder
- By Folder, Including Subfolders
- By User
- By Group

Options

- Size Units

User Maintenance

These reports all summarize user maintenance activity based on entries stored in the logs.

Report Types

- Total
- By Month
- By Week
- By Day
- By Activity
- By Activity, By Month
- By Activity, By Week
- By Activity, By Day

Options

- Start Date
- End Date

User Status

These reports list users (and groups) on the system, their current status and the permissions they enjoy.

Report Types

- Folder Quota, Any
- Folder Quota, Defined

- Folder Quota, Near or Above
- Package Quota, Any
- Package Quota, Defined
- Package Quota, Near or Above
- Active Users
- Inactive Users
- Password About To Expire
- Group Summary
- Group Membership
- User List For Auditors
- Default Home Folder Permissions
- Folder Permissions
- Address Books

Options

None

Security

These reports highlight suspicious signon attempts performed against a MOVEit DMZ server.

Report Types

- Suspicious Usernames - Many Attempts
- Suspicious Usernames - Many IPs
- Suspicious IPs - Many Attempts
- Suspicious IPs - Many Usernames
- Locked Out IPs - Current
- Locked Out IPs - Historical
- Locked Out Users - Current
- Locked Out Users - Historical

Options

- Start Date
- End Date
- Attempt Threshold

- IP Threshold
- Username Threshold

Performance

These reports examine the statistics gathered by the MOVEit SysStat service on MOVEit DMZ. (This service typically captures performance statistics to the MOVEit database about 12 times an hour.)

Several of these reports are always broken down into additional categories. Typical breakdowns include Maximum, Minimum and Average values, and TotalSystem, DMZCore, DMZISAPI, IIS, MySQL, DMZFTP, DMZSSH, DMZScheduler, and Central application break-outs. There are some exceptions, however.

- Sessions reports always list Active and All sessions separately.
- Memory reports always list Virtual and (Regular) memory separately.
- Disk reports always list space available on the various drives.
- Summary reports go across performance statistics rather than break them down by application. Summary reports contain a summary of active sessions, CPU, free disk, handles and memory usage.

Report Types

- CPU - All
- CPU - By Hour
- CPU - By Day
- Disk - All
- Disk - By Hour
- Disk - By Day
- Handles - All
- Handles - By Hour
- Handles - By Day
- Memory Usage - All
- Memory Usage - By Hour
- Memory Usage - By Day
- Virtual Memory - All
- Virtual Memory - By Hour
- Virtual Memory - By Day
- Processes - All
- Processes - By Hour
- Processes - By Day

- Sessions - All
- Sessions - By Hour
- Sessions - By Day
- Threads - All
- Threads - By Hour
- Threads - By Day
- Summary - All
- Summary - By Hour
- Summary - By Day

Options

- Start Date
- End Date
- Size Units

Content Scanning

These reports show various types of content scanning activity. Two reports give specific information about scan results: *Violations Blocked* and *DLP Violations (Allowed and Blocked)*. The remaining reports are maintenance reports that show aggregate counts.

If you are logged in as an organization administrator, the report shows scan results for your organization. If you are logged in as a system administrator, the report can show multiple organizations.

Report Types

- Violations Blocked
 - Includes both anti-virus (AV) detections and Data Loss Prevention (DLP) violations

- DLP Violations (Allowed and Blocked)
- Maintenance - Total
- Maintenance - By Month
- Maintenance - By Week
- Maintenance - By Day
- Maintenance - By Activity
- Maintenance - By Activity, By Month
- Maintenance - By Activity, By Week
- Maintenance - By Activity, By Day

Options

- Start Date
- End Date

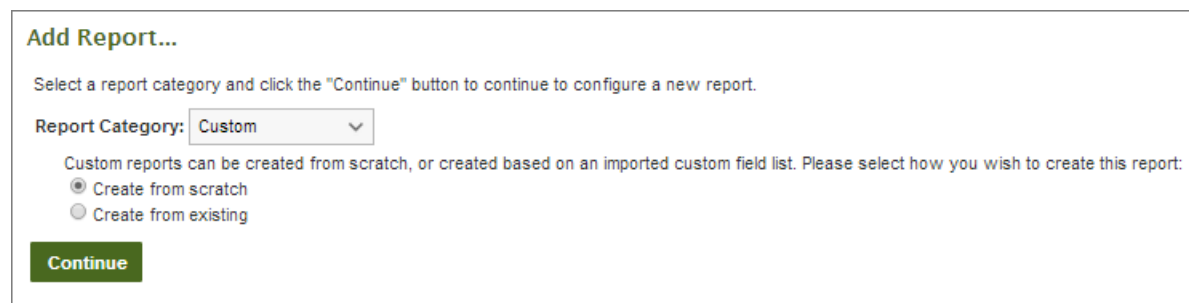
Custom Reports

Custom reports are similar to other reports in that they are sets of instructions for querying MOVEit DMZ's performance and status data, formatting the results, and saving the resulting report. Where other report categories and types execute pre-defined queries, however, custom reports provide the ability to define a custom query, allowing reports of any type to be created based on the data available. Knowing what data is available and how to request it is obviously a requisite to constructing useful custom reports. Knowledge of the SQL data querying language is also important. For information about the database schemas available to MOVEit DMZ, see the **Database Schema** (on page 680) page.

Managing custom reports is mostly the same as managing other reports. Custom reports may be added, edited, executed, and deleted. For more information about basic management of reports, see the **Reports Overview** (on page 325) page.

Adding a Custom Report

In addition to basic management, custom reports may also be exported and imported. This allows custom reports to be easily shared between systems, and between DMZ administrators and MOVEit support personnel. As a result, the process for adding a custom report looks slightly different than other report types. Upon choosing to add a custom report, additional options will be displayed asking if the new report should be created from scratch, or imported from an existing report file.



The screenshot shows a web form titled "Add Report...". Below the title is a instruction: "Select a report category and click the 'Continue' button to continue to configure a new report." There is a "Report Category:" label followed by a dropdown menu currently showing "Custom". Below this, a text line reads: "Custom reports can be created from scratch, or created based on an imported custom field list. Please select how you wish to create this report:". There are two radio button options: "Create from scratch" (which is selected) and "Create from existing". At the bottom left of the form is a green "Continue" button.

Electing to create a new report from scratch will lead to the Add Report page, as with other report types. Electing to create from an existing report file will cause a file browse box to be displayed. Use this to select the report file to import. A successful import will lead to the Edit Report page, where additional options may be configured.

Editing a Custom Report

Edit Report...

Please specify the name, type and format of the report.

Name:

Report Category: Performance

Report Type:

Format:

Created: 4/1/2014 2:11:47 PM by kristina
Last Modified: 4/1/2014 2:11:47 PM

The following options determine when this report will be created and where it will be saved. You may use macros such as "[yyyy]" (year) in your folder and file names to timestamp your reports. Scheduled reports will be run by the nightly scheduled task. By default, this task runs at 1am.

Run On Days:

Examples: "All", "4,7,8", "Mon,Tue" - blank means "not scheduled"

Save In Folder:

Save As File:

If no value is entered, the report title will be used

☒ Overwrite Existing File

Except where indicated, the following report parameters are optional.

Start Date:

End Date:

Format: YYYY-MM-DD
Macros Allowed: [yyyy], [mm], [dd]
Examples: 2005-06-04, [yyyy]-[mm]-[dd], [yyyy]-[mm-3]-01

Size Units: Required

Update Report

Most configuration options are the same for both built-in reports and custom reports. The Name, Format, Run On Days, Save In Folder, and Save As File options work the same way, as well as the CSV-specific options. The report parameters, however, are quite different from those available to built-in reports. The six available parameters define the data query that will be performed against MOVEit DMZ's database in order to gather the desired information for the report:

- **Fields** - Determines which fields will be requested during the query. If a report will be querying data from more than one database table, each field should be prefixed by its table name. For example, "Users.Username" or "Files.FolderID". Multiple fields should be separated by commas. This parameter is required.
- **Tables** - Determines which database tables will be queried, and how those tables should be joined to each other in order to get the proper results. For example, to get the RealName field for a user account that uploaded a file, use "Files LEFT JOIN Users ON Files.UploadUsername=Users.Username". This parameter is required.
- **Criteria** - Determines which data rows will be returned by the query. This is analogous to the "WHERE" clause in an SQL query. For example, to only return users who are not marked as deleted, use "Users.Deleted=0". Multiple criteria statements should be separated by the "AND" keyword.
- **Grouping** - Determines how results should be grouped, if desired. This is analogous to the "GROUP BY" clause in an SQL query. For example, to group by account usernames, use "Users.Username".
- **Order** - Determines the order in which the results will be returned. This is analogous to the "ORDER BY" clause in an SQL query. Use the "ASC" keyword to order in an ascending fashion, and the "DESC" keyword to order in a descending fashion. For example, to order by account usernames alphabetically in an ascending fashion, use "Users.Username ASC".
- **Limit** - Limits the number of results to the specified number. If blank, all results will be returned.

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 single-quotes or double-quotes to delimit phrases. For example, if today is currently July 5, 2007, a macro of:

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

Exporting a Custom Report

In addition to the Run Report section, the Export Report section will also be shown on the Edit Report page for custom reports. This allows the current report definition to be exported to a file, which can then be imported via the process above. Pressing the Export Report button will cause an export file to be generated and sent to the browser, from where it can be downloaded to a local file.

Export Report

You can export the custom fields of this report to an XML file by clicking the "Export Report" button below. The export file can be imported into other MOVEit DMZ servers to create similar reports on those systems.

Export Report

Note: Only the name and custom query definition fields are exported. Information such as format, run times, and folder to save to are not included in export files, as they are generally unique to the system.

Statistics

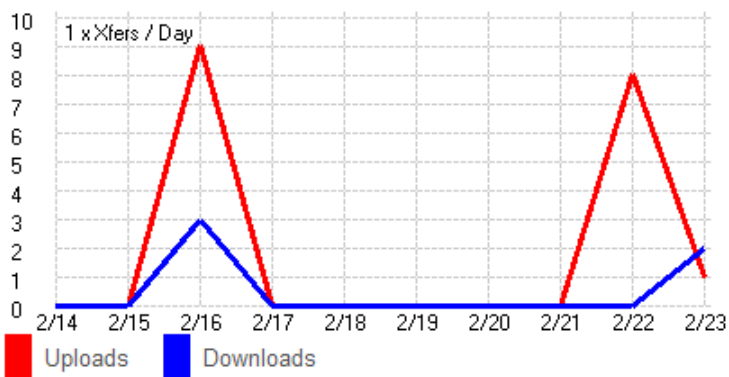
The Statistics page in the Reports section provides quick access to summaries of organization information such as file transfers and folder sizes. For sysadmins, this information encompasses the entire system.

Reports

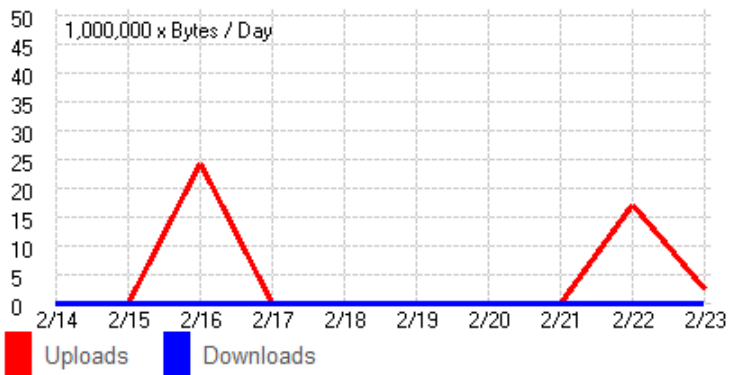
Statistics

 [Go to Quick Statistics](#) (previously known as "Stats")

Transfer Count



Bytes Transferred



Transfer Count

The Transfer Count display shows a summary of the number of uploads and downloads performed during the last 10 days. Uploads are shown in red, while downloads are shown in blue. The display will automatically scale to show all values. The scale of the display can be found in the upper left hand corner.

Bytes Transferred

The Bytes Transferred display shows a summary of the total number of bytes uploaded and downloaded during the last 10 days. As with the Transfer Count display, uploads are shown in red, while downloads are shown in blue. The display will automatically scale to show all values. The scale of the display can be found in the upper left hand corner.

Ten Largest Folders

/Messages/Global Messaging (35,263,443 bytes)

/Home/John Smith (10,867,656 bytes)

/FT Tools/PermTemp (10,864,103 bytes)

/FT Tools/Software (3,876,720 bytes)

/Home/Freddy Masterson (2,390,777 bytes)

/FT Tools/Images (2,337,788 bytes)

/Home/Helga Finlayson (27,497 bytes)

/Home/fred (365 bytes)

Five Largest Uploaders

fred (38,966,817 bytes)

Helga Finlayson (24,155,970 bytes)

Freddy Masterson (4,794,560 bytes)

John Smith (36,977 bytes)

Five Largest Downloaders

John Smith (103,184 bytes)

Helga Finlayson (57,742 bytes)

Freddy Masterson (52,473 bytes)

Ten Largest Folders

The Ten Largest Folders display shows a bar graph of the 10 largest folders in the organization. Size is measured by the total byte count of all the files contained in the folder. The relative sizes of the top 10 folders are shown as green bars. The actual byte counts of each folder, along with their full path name, are also shown.

Five Largest Uploaders

The Five Largest Uploaders display shows a bar graph of the 5 users in the organization who have uploaded the most bytes, according to the current set of audit logs. The relative upload byte counts of the top 5 users are shown as red bars. The actual upload byte counts, along with each user's real name, are also shown.

Five Largest Downloaders

The Five Largest Downloaders display shows a bar graph of the 5 users in the organization who have downloaded the most bytes, according to the current set of audit logs. The relative download byte counts of the top 5 users are shown as blue bars. The actual download byte counts, along with each user's real name, are also shown.

Settings

Overview

The settings page allows Admins to configure global options for their organizations.

Settings

Appearance

Info:	Announcement - Welcome Message - Tech Support - Sign On Banner
Brand:	Logo & Layout - Bullet - Color Scheme - Wizard - Mobile - "External" URL
Display:	Regulatory Compliance - Custom Help - Display Profiles - Max List Counts - Wizard
Notification:	Return Address - Items Displayed - Signature - Format - Custom
Folders:	Default Home Folder Path - Default Sort Order
International:	Languages - Interface

Security Policies

Password:	Length & Complexity - Aging & History - Permissions
User Auth:	Lockouts - Auth Method - Multi Signons - Expiration - Single Signon
User Settings:	Folder Quotas - Default Folder - Unique Full Names
Group:	Default Permissions
Remote Access:	Default Rules - IP Lockouts - IP Switching
Interface:	HTTP - FTP - SSH - Mobile
Folder:	Home Folder Permissions - Copy/Move
Content Scanning:	Anti-Virus - Data Loss Prevention (DLP)

Ad Hoc Transfer

Access:	Registered Senders - Unregistered Recipients - Unregistered Senders
Content:	Sending Files - Package Quotas - Package Notifications
Maintenance:	Aging & Expiration

Miscellaneous

Aging:	Audit Logs
Tamper Detection:	View/Reset

Hint: "Root folder" properties such as **Allow Overwrite on Home folders** are NOT configured through this Settings page. Instead, these properties are configured through the **Folder Settings** link available on each of the root folders.

SysAdmins will see a subset of these items plus an additional **System Settings** on the Settings page.

Settings

Appearance

As a "SysAdmin", changing these settings will only affect the (System) Organization, or act as defaults when you add a new Organization.

Info:	Announcement - Welcome Message - Tech Support - Sign On Banner
Brand:	Logo & Layout - Bullet - Color Scheme - Wizard - Mobile - "External" URL
Display:	Regulatory Compliance - Custom Help - Display Profiles - Max List Counts - Wizard
Notification:	Return Address - Items Displayed - Signature - Format - Custom
Folders:	Default Home Folder Path - Default Sort Order

Security Policies

As a "SysAdmin", changing these settings will only affect the (System) Organization, or act as defaults when you add a new Organization.

Password:	Length & Complexity - Aging & History
User Auth:	Lockouts - Multi Signons - Expiration
Remote Access:	IP Lockouts - IP Switching
Interface:	HTTP - FTP - SSH - Mobile
Folder:	Copy/Move

Miscellaneous

As a "SysAdmin", changing these settings will only affect the (System) Organization, or act as defaults when you add a new Organization.

Aging:	Audit Logs
Tamper Detection:	View/Reset
File Viewing:	Prevent View In Browser

System

As a "SysAdmin", you have exclusive access to these system-wide settings.

Debug Logs:	Configure & Download
Auditing:	Event Log - Syslog - Error Display - Failed Signons
User Authentication:	SiteMinder - Unique Usernames
Remote Access:	SysAdmin & Trusted Hosts - IP Lockout Policy
Notification:	Default Return Address - "Base" URL
Miscellaneous:	Default Organization - Wizard - Meta Refresh
Tamper Detection:	Reset All Orgs - Configure

Appearance

Appearance - Info

Announcement

The announcement is a brief message all users will see on their home page. This section is often used to warn about upcoming outages, point to new documentation or post additional legal notices to signed on users. This section should NOT be used to welcome users just signing on - use the **Welcome Message** field for this purpose instead. By default, the Announcement is blank. If the Announcement is left blank, there will be no Announcement section displayed on the home page.

This field supports *intra-string language tags* (on page 57).

Welcome Message

The welcome message appears in a banner at the top of the page whenever a user signs on successfully to the MOVEit DMZ system and in a console message when a user signs in via the FTP interface. The phrase [ORGNAME] will be replaced by the name of the current organization when the message is displayed. By default, this message is **Welcome to [OrgName]! Please watch this area for important messages.** If this message is left blank, then no welcome message will be displayed to users.

This field supports *intra-string language tags* (on page 57).

Tech Support

This section controls the information that users will see if they click their **Tech Support** links. This information includes a contact name, a phone number and an email address. (If the name is left blank, **Technical Support** will be used as the name. If the phone number or email address is left blank, no information will be found in their places.)

Optional Information and Contact webpages can be set here as well. Name and URL fields are available for both. If the Information link is specified, it will appear at the bottom of the Information section of the Tech Support page. If the Contact link is specified, it will appear at the bottom of the Contact section of the Tech Support page.

An optional **information** field may also be used to provide information about hours of service, additional contacts, etc.

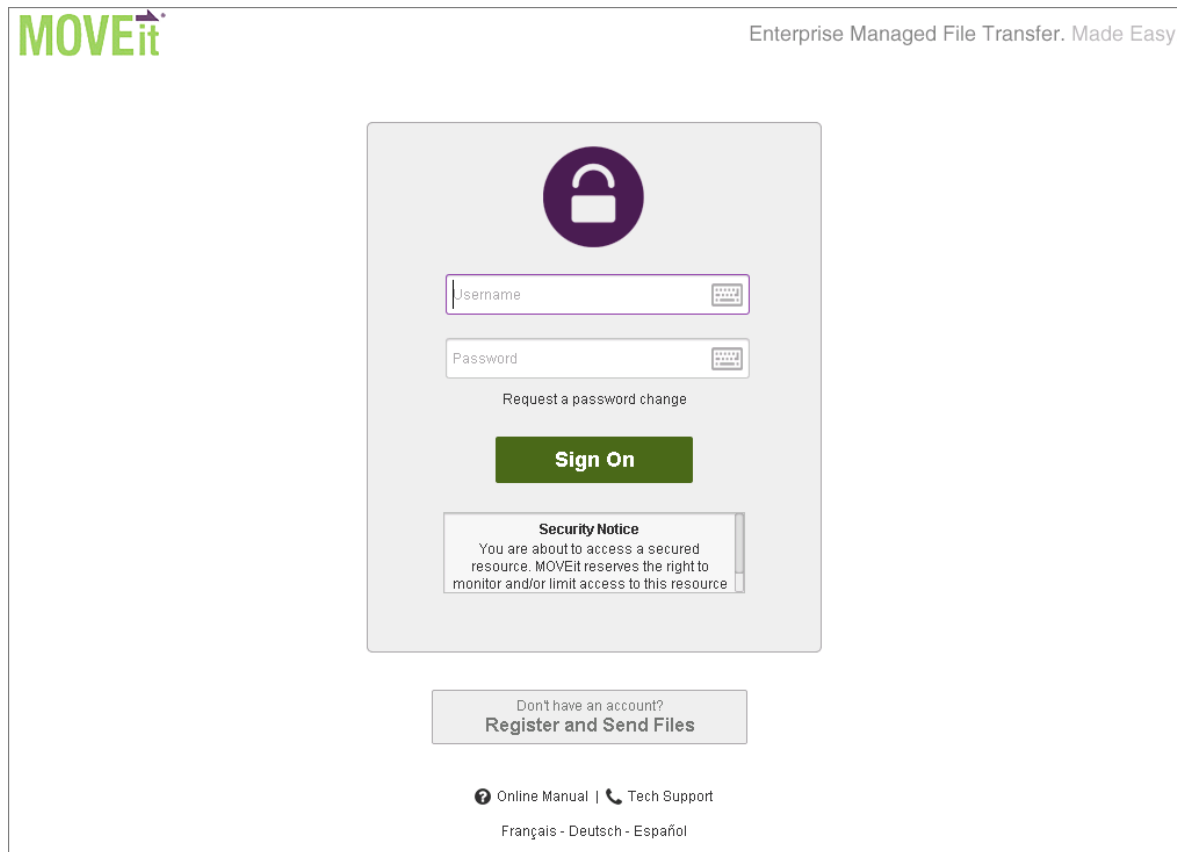
All Tech Support fields support *intra-string language tags* (on page 57).

Hint: Use MOVEit DMZ's WebPost feature to securely collect new account requests, password change requests and other support requests from your own custom web page.

Sign On Banner

The sign on banner and notice are displayed to users before they sign onto the web site or when a user connects to the FTP interface. The banner is typically something like "Security Notice" or "WARNING: Secure Resource".

In the example below, the banner is "Security Notice". The notice itself is the text that appears below the banner. It typically describes the secured resource and its intended purpose.



The screenshot displays the MOVEit web interface for sign-on. At the top left is the MOVEit logo, and at the top right is the tagline "Enterprise Managed File Transfer. Made Easy." The central area features a sign-on form with a purple padlock icon at the top. Below the icon are input fields for "Username" and "Password", each with a "Show/Hide" toggle. A link "Request a password change" is positioned below the password field. A prominent green "Sign On" button is centered below the form. Underneath the button is a "Security Notice" box containing the text: "You are about to access a secured resource. MOVEit reserves the right to monitor and/or limit access to this resource". At the bottom of the form area is a button labeled "Don't have an account? Register and Send Files". The footer contains links for "Online Manual" and "Tech Support", along with language options: "Français - Deutsch - Español".

Both the **Banner** and **Notice** fields support *intra-string language tags* (on page 57).

The fields for entering the banner and notice are blank by default. The system defaults displayed for the banner and notice (when you leave these fields blank) are **Security Notice** and **You are about to access a secured resource. [ORGNAME] reserves the right to monitor and/or limit access to this resource at any time.**

Edit the Sign On Banner and Notice...

The following banner and notice are presented to visitors before signing on to the web and FTP interfaces.

Banner:

Security Notice

Notice:

You are about to access a secured resource. Org 1 reserves the right to monitor and/or limit access to this resource at any time.

This setting determines when the banner and notice will be shown to users of the mobile interface.

Mobile Interface Visibility Requirement: Required When New

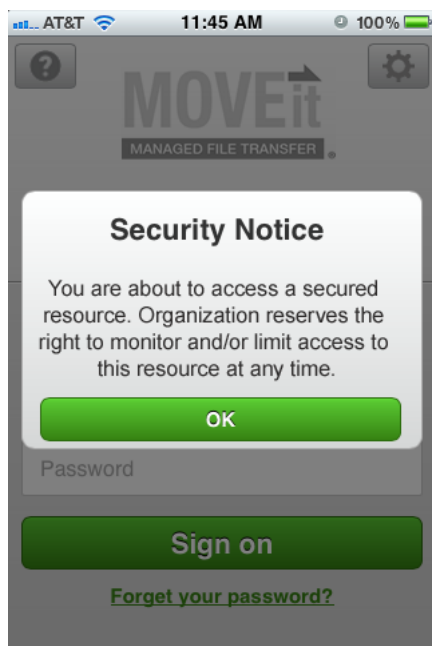
Save

Cancel

Note: For Banner text, do not exceed 30 characters, because, if you do, mobile displays only the default "Security Notice".

The **Mobile Interface Visibility Requirement** is the policy for displaying the banner and security notice on mobile devices when users access the MOVEit Mobile app or web.

Due to the limited screen area on typical mobile devices, the banner and notice are implemented on mobile devices as a pop up dialog box when the user accesses the mobile **Sign on** screen. The dialog box requires the user to tap OK to close.



Choose how frequently to show this dialog box, either: never, just when it has been changed, or every time the **Sign on** screen is accessed.

Note: If you change the banner and/or notice, they will not be refreshed on a mobile app until the user closes the app (that is, manually stops the running app process). Signing out does not refresh the banner and notice.

Your choice will depend on the specifics of your organization's notice, your regulatory compliance requirements, and practical ease-of-use considerations.

- **Not Required:** Never show the security notice box.
- **Required When New:** Show the security notice box any time that the user has freshly launched the mobile app or web and the mobile banner or notice has changed since the last time the user user saw the dialog box.
- **Always Required:** Show the security notice box every time a user accesses the mobile **Sign on** page.

Web Interface - Settings - Appearance - Brand

Logo & Layout

Admins should upload a custom logo (often the same one used on their main web site) soon after signing on for the first time. All users will be able to see this image. The logo is usually set to appear on the top left-side of the page. Admins can also set a custom logo, or tag line image, to display at the top right-side of the page. A header background image can be set to enhance the display of the logo.

Images can be in .gif, .jpg, or .png format.

For example, the default style for MOVEit DMZ shows a left-side logo with a right-side tag line and includes a header background image.

Note: The logo file that you upload here is not used for mobile. To upload a corresponding logo for use in the mobile app and web, use the Mobile link from Web Interface - Settings - Appearance - Brand.

Left-Side Logo

Current left-side logo (scaled):



Upload a new left-side logo:

Browse...

(gif, jpg, and png supported)

Upload**Right-Side Logo** (optional)

Current right-side logo (scaled):

Enterprise Managed File Transfer. Made Easy.

Upload a new right-side logo:

Browse...

(gif, jpg, and png supported)

Upload~ Or ~ [Remove this logo image](#)**Header Background Image** (optional)

Current background image (scaled):

Upload a new background image:

Browse...

(gif, jpg, and png supported)

Upload~ Or ~ [Remove this logo image](#)

If the width of logo is more than 600 pixels, the width of the page will stretch to match the new logo. (600 pixels will fill a browser on a screen with a resolution of 640x480.) A width of 660 pixels is recommended to fit the current page on a standard printed page. A width of 720 pixels is recommended to fill up a floating browser on a screen with a resolution of 800x600. A width of 760 pixels is recommended to fill up a full-screen browser on a screen with a resolution of 800x600.

Note: After changing the logo image, the new image might not display due to browser caching. Hold down the Control key and click your browser's Refresh button to reload the page without cached images.

Page Layout

Administrators can also set the page layout width and alignment. Select an option and click Save to see how the change affects the layout. Note that alignment applies only if you select less than 100% width.

Bullet

Bullets are turned off by default, but you may opt to have a custom bullet appear next to the green sub-titles on each page.

To turn on bullets:

- 1 Log on as an administrator.
- 2 Go to Settings > Appearance > Bullet.

- 3** Select a stock bullet or upload your own small *.gif image.

Select or Upload a Bullet...

The following bullet is used throughout the site.

Current Bullet: *(actual size)*

You may either select a "stock" bullet, or upload your own custom bullet. **Custom bullet images must be in the "GIF" format, and can be no larger than 100,000 bytes.**

NOTE: If the bullet image does not appear to change after you have chosen a new bullet or uploaded a new file, your browser is most likely caching the old image. To force the browser to refresh the image, click on the Home link in the left-hand navigation, then hold down the Control key on your keyboard and click the Refresh button in your browser.

Select a stock bullet:

To select a stock bullet, check the bullet desired below and then press the "select stock bullet" bullet to save your selection.

☐ No Bullet

☐  ☐ 

☐  ☐ 

☐  ☐ 

☐  ☐ 

☐  ☐ 

☐  ☐ 

Select Stock Bullet

~ OR ~ Upload a custom bullet:

To upload a custom bullet from your local computer, select your bullet with the "browse" button below, and then press the "upload custom bullet" button to upload it.

Browse...

Upload Custom Bullet

Note: Images are limited to 256 colors, however, they can be transparent and/or animated. Custom bullet images should be no more than 16 pixels by 16 pixels.

- 4 On the server where MOVEit is installed, open `c:\MOVEitDMZ\wwwroot\templates\stylesheet_MOVEit_2014.css`.
- 5 Locate the line that contains `.bulletimage`.

```
.pageheadingimage, .bulletimage { display:none; }
```

- 6** Change this line to:

```
.pageheadingimage { display:none; }
```

Important: Remember to remove the comma after `.pageheadingimage`.

- 7** Save the CSS file.

- 8 In your browser, click the Refresh button to see the bullets appear.

⇒ Select or Upload a Bullet...

The following bullet is used throughout the site.

Current Bullet: ⇒ *(actual size)*

You may either select a "stock" bullet, or upload your own custom bullet. **Custom bullet images must be in the "GIF" format, and can be no larger than 100,000 bytes.**

NOTE: If the bullet image does not appear to change after you have chosen a new bullet or uploaded a new file, your browser is most likely caching the old image. To force the browser to refresh the image, click on the Home link in the left-hand navigation, then hold down the Control key on your keyboard and click the Refresh button in your browser.

Select a stock bullet:

To select a stock bullet, check the bullet desired below and then press the "select stock bullet" button to save your selection.

☐ No Bullet



Select Stock Bullet

To remove the bullets, simply change the same line of code back to its original state below, and then refresh your browser window.

```
.pageheadingimage, .bulletimage { display:none; }
```

Color Scheme

Admins may preview or pick from one of the available color schemes. If a custom scheme is desired, SysAdmins have the ability to create and upload a (CSS) stylesheet template to fit your brand.

Change Color Scheme...

Select a color scheme from the list below.

Color Scheme: [Preview Color Scheme](#)

Hint: If you need a new custom scheme to match your current corporate scheme, ask moveitsales@ipswitch.com (<mailto:moveitsales@ipswitch.com>). We may have created one for your organization during your evaluation period.

Wizard

Admins may also change the name and the look of the MOVEit Wizard (ActiveX or Java version). The names entered in the top section of this page will appear in the title bar of the Upload and Download Wizards respectively. They will also be recorded as the Agent Name in audit log entries of Wizard file transfers. Set the values to blank strings if you'd like to use the default names. The bitmap image entered in the bottom section will be shown in place of the usual Wizard logo in the upper left corner of the Wizard. To set this back to the default logo, click the Upload Custom Wizard Logo button without selecting a file.

Set Custom Name For Wizard...

You can enter custom names for the Upload and Download Wizards. If you leave these empty, the standard names (*MOVEit Upload Wizard* and *MOVEit Download Wizard*) will be used.

Upload name:

Download name:

Set Wizard Names

Set Custom Wizard Logo...

To upload a custom Wizard logo from your local computer, select a 75 x 42 pixel .BMP file with the "browse" button below, and then press the "Upload Custom Wizard Logo" button to upload it. To disable a custom wizard logo, leave the filename empty and press the button.

Custom Wizard logo is currently **DISABLED**.

No file chosen

Upload Custom Wizard Logo

Set Custom Wizard Upload Zip File Name...

You can enter a custom default filename used by the Upload Wizard when the zip option is chosen. You can use the macros [username] and [fullname]. A value of [default] causes a language-specific default to be used.

Default Upload Zipfile Name:

Set Upload Zipfile Name

You can also set a file name to be used by the Upload Wizard when the zip files option is selected. This option compresses files into one file with a .zip extension and will use the file name you enter here. You can enter a custom default filename that will be used by the Upload Wizard when the zip option is chosen. You can use the macros [username] and [fullname]. A value of [default] causes a language-specific default to be used (the default English version is **upload.zip**.) If you want to prompt the user to enter a zip file name, leave the Default Upload Zipfile Name field blank.

Mobile

Administrators can upload a custom logo that will appear in the **Sign on** page for all mobile users. The logo will be displayed as shown in the Mockup diagram of the configuration page. (A user needs to sign on and off one time before the custom logo will be displayed.)

The image you upload should be a *.png file, 400 x 180 pixels, preferably with a transparent background. The logo will be automatically scaled down into medium (80%) and small (40%) formats for use in mobile as needed.

Example custom logo:



➤ **To upload the custom mobile logo:**

1. Click **Browse**.
2. Select the *.png image.
3. Click **Upload**.

A success message says **Changed organization mobile logo OK**.

Note: After changing the logo image, the new image might not display due to browser caching. Hold down the Control key and click your browser's Refresh button to reload the page without cached images.

Mobile Interface Logo

Customize the MOVEit DMZ Mobile interface with your logo.

Mobile Logo

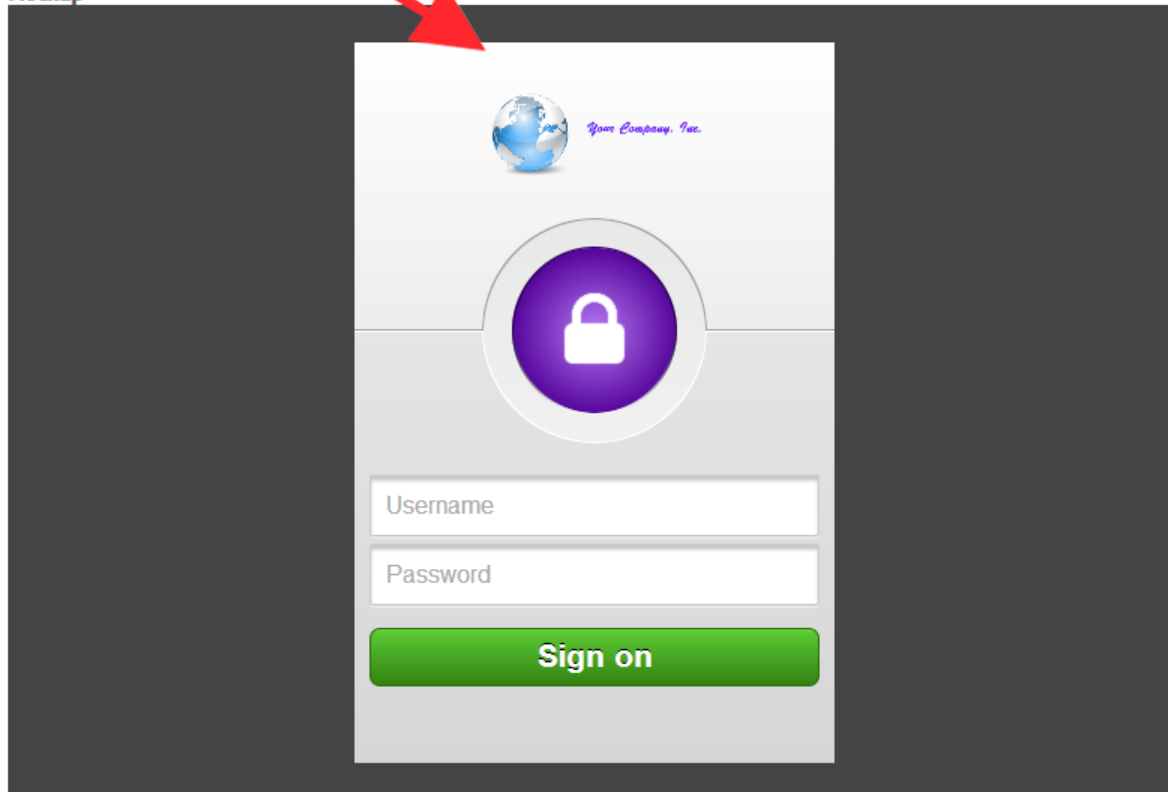
Current mobile logo (scaled):



Upload a new mobile logo. Logo must be a PNG image, and should be 400 x 180 pixels in size. The image should have a transparent background.

(.png only)

Mockup



External URL

This value is the URL to which users will be sent if they click on your organization's logo. By default, the **External URL** is blank. When the **External URL** is blank, a click on your organization's logo will act like a click on the **Home** navigation link.

This value is NOT the URL to which users are sent in their notifications; that value is called the **Base URL** and may only be set by a SysAdmin. A system-wide **Base URL** normally applies equally to all organizations, but individual values may be set on each organization. (If your MOVEit DMZ system supports multiple, licensed organizations and each one uses its own IIS site and SSL server certificate, you should be using different **Base URL** values for each organization.)

Appearance - Display

Regulatory Compliance

This section provides the options to display various sections that bring the DMZ system up to compliance with both ADA and FDA regulations. Included are the **skip repetitive navigation** link for ADA compliance, and the **GMT timezone offset statement** section for FDA compliance. Also available is an option to turn on and off the display of a **Powered By MOVEit** link at the bottom of the left-hand navigation column.

Custom Help

In addition to the Online Manual and Tech Support links available to users in the left-hand navigation column, the Custom Help section allows the organization administrator to provide a third link of their choice. This section allows the admin to enter a link name, and a link URL, which will appear below the Online Manual and Tech Support links. If a user clicks this link, the appropriate page will be launched in a separate window.

Both the link and name fields support *intra-string language tags* (on page 57).

Display Profiles

Display profiles allow the administrator of an organization to fine tune the look and feel of the MOVEit DMZ web interface for different classes of users. The admin first creates a display profile, selecting the sections to show and the options to provide. That profile can then be assigned to one or more of the five user classes available: Ad Hoc Transfer Only, Guest/Anonymous User, Power User, Temporary User and User. For more information about creating and assigning display profiles, see the **Display Profiles** (on page 67) Feature Focus page.

Max List Counts

The more users or folders there are on a MOVEit DMZ system, the longer it will take both DMZ and the client web browser to render pages that contain lists of those users or folders. For this reason, the Max List Counts option is provided, which causes search boxes to replace drop-down selection menus when the number of users or folders in the drop-down would exceed the specified values. The search boxes allow the user to enter a search term, and pick from a selection of users or folders that match the search term. While the process of selecting a user or folder does become slightly more complicated, the loading times for the associated DMZ web pages is greatly reduced, allowing more users to use the system simultaneously.

Note that the max list values are only applied to the number of users or folders that would be in a given list, not to the total number of users or folders on the system. So, if a given user has only two other users in her address book, she will see both those users in a drop-down menu when composing a secure message, even if there are thousands of other users on the system.

When the number of users or folders is near the limit (above or below) a special configuration hint will be displayed on Admin's home page to remind them that this setting will soon or has just caused a change to the user interface.

Wizard

This section determines whether or not users will be prompted to install the Upload/Download Wizard if they do not already have it installed. The setting value is applied when creating new users, and can be applied to existing users as well. It is overridden at the user level by per-user values of the setting.

When the Prompt to install Upload/Download Wizard setting is set to Yes, users who do not have the wizard installed will by default be prompted about it, and asked if they want to install it, after they sign on. When set to No, users will by default not be prompted about the wizard, though they will still be able to use the wizard if it is already installed. Users will still be able to install the wizard from their My Account page.

Overview

Overview

The notification settings allow you to control the format and appearance of email notifications sent out by MOVEit DMZ.

Return Address

The return address is the address from which notification messages will appear to come. (e.g., automation@stdnet.com)

Hint: Set this value to a real email address if you would like to be notified of email notifications which cannot be delivered. (Delivery failure messages will be sent back to this return address.)

Signature

This setting allows an Admin to configure the signature string that appears at the end of notification emails from this organization. Instances of the macro text [ORGNAME] will be replaced by the organization name. By default, the Signature is [ORGNAME] Notification Service. Normally the signature will be preceded by the phrase Regards,

This field supports *intra-string language tags* (on page 57).

Format

This setting determines the default email notification format which will be applied to new users created in the organization. The available formats are HTML and Text. When the value of this setting is changed, the administrator will also have the option of applying the change to all existing users in the organization.

HTML-formatted notifications contain stylesheet references and inline images to help match their appearance with the DMZ web interface. These references are taken from the settings of the organization that originated them, meaning organization color schemes, icons, and font information are all maintained in the emails that end users receive.

However, some email servers consider inline images an indication of spam, and block emails that contain them. The Text-format option is provided for those whose email servers prevent the receiving of HTML messages.

Customization

The content of email notifications can be customized in two ways. A set of check-box options called **Items Displayed** can be used to set a broad policy for what information is sent over clear-text email. See the **Web Interface - Settings - Appearance - Notification - Items Displayed** (on page 371) page for more information.

For finer control over the content of email notifications, you can create and edit custom notifications through the DMZ web interface. Custom versions of the email notifications can be assigned to an entire organization, in a multi-org system, or can be limited to specific User Groups within an organization. See the **Web Interface - Settings - Appearance - Notification - Custom** (on page 373) page for more information.

Appearance - Notification - Items Displayed

Items Displayed

Items displayed refers to the different sections of information available in the notification emails that are sent out for various reasons. These items can be switched on and off independently, allowing the administrator to determine what information is sent over clear-text email. Configurable items include basic information, comments, non-repudiation information, and a direct link to the notification subject.

Here is a sample notification with all the options turned on:

Example Email Notification Message



New File Notification

A new file from Joe User has arrived into the "/ Distribution / MyParent / MyFolder" folder.

Name: Example.txt
Tracking ID: 1234567
Original Size: 1,234 bytes
Uploaded By: Joe User (joe@user.com)
Comments: This file is called example.txt.

☒ For non-repudiation purposes, it has been confirmed that the file received by MOVEit DMZ is IDENTICAL to the file uploaded by Joe User.

Please use the following URL and your username/password to DOWNLOAD or view the current status of this file, including its full upload and download history.

(<https://KEaston-08R2DOC.FTQA.com/human.aspx?OrgID=9999&Arg12=fileview&Arg07=1234567&Arg06=123456&username=janeuser>)

Regards,
Org 1 Notification Service

- **Basic File Information:** This includes file information such as name, size, tracking ID, and the name of the user who uploaded the file.

Name: Example.txt
Tracking ID: 1234567
Original Size: 1,234 bytes
Uploaded By: Joe User (joe@user.com)
Comments: This file is called example.txt.

- **Uploader/Sender:** This determines whether the name of the user who uploaded the file or sent the package is shown in notification emails.

Name: Example.txt
Tracking ID: 1234567
Original Size: 1,234 bytes
Uploaded By: Joe User (joe@user.com)
Comments: This file is called example.txt.

- **Comment Field:** This determines whether any comments included with the file upload are shown.

Name: Example.txt
Tracking ID: 1234567
Original Size: 1,234 bytes
Uploaded By: Joe User (joe@user.com)
Comments: This file is called example.txt.

Note: Comment Field also determines whether the subject of a package is shown in package notification emails, but only when Secure the Note is set for the package. See **Web Interface - Settings - Ad Hoc Transfer - Content** (on page 513).

- **Non-repudiation Information:** This includes information regarding whether MOVEit DMZ can verify that the uploaded or downloaded file was unchanged during transit.

☒ For non-repudiation purposes, it has been confirmed that the file received by MOVEit DMZ is IDENTICAL to the file uploaded by Joe User.

- **Direct Fileview Link:** This determines whether a direct link to the subject file or package is provided in the email. If it is, clicking on that link will take a user directly to the file or package, after logging on.

Please use the following URL and your username/password to DOWNLOAD or view the current status of this file, including its full upload and download history.

(<https://KEaston-08R2DOC.FTQA.com/human.aspx?OrgID=9999&Arg12=fileview&Arg07=1234567&Arg06=123456&username=janeuser>)

- **Prefill Username:** This determines, in most cases, whether the username will be prefilled on the signon page when the user follows the link in a notification email. This option has no effect if the Direct Fileview Link option is disabled. In addition, this option generally has no effect when the package is sent from Outlook (having no effect for New Package Notifications and for Credentials Notifications to Guest users). Note, however, that it does affect Credentials Notifications to Temporary users.

Appearance - Notification - Custom

Appearance - Custom Notifications

Whereas the Items Displayed settings allow you to turn on and off specific components of a notification, they do not let you control the actual text. The Custom Notifications feature allows you override the standard template with a customized version for all users within an organization, or for just a specific group.

List of all defined Custom Notifications

By clicking on the Settings | Appearance | Notification: Custom link, you get to a master list of custom notifications you have defined for your organization. From here you can create new notifications, clone notifications you have already created, edit the content of notifications, and enable or disable notifications for use within your organization.

Edit Custom Email Notifications...

Email notifications are used for many situations:

1. File, webpost and package notifications, including upload confirmations, new file notifications, delivery notifications, and delete notifications. These are sent to end-users who are interested in the status of files.
2. User notifications including password and user expirations, password changes, new user and temp user notifications. These are sent to users to tell them about the status of their account.
3. Admin notifications about user status changes. These are sent to admins responsible for end-users.

Notifications may be viewed and edited by clicking the "Edit" link.

Name	Template	Apply	Lang	
Custom Notification 1	New File Upload Notification		en	  

Add Custom Notification

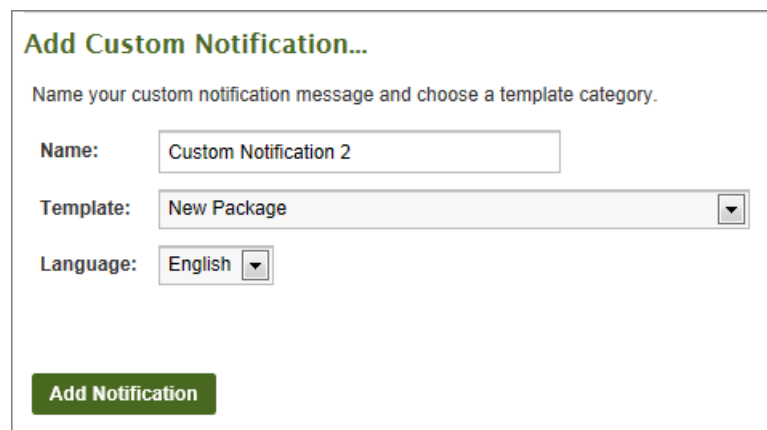
The main list of notifications has several columns:

- **Name:** The unique name for this notification. This is your helpful-hint as to what purpose you have for this notification.
- **Template:** The system-defined notification template that this one overrides. The list of system templates can be found below in the Adding a Notification section. See the **Web Interface - Settings - Appearance - Custom Notification - Templates** (on page 380) page for the complete list of templates.
- **Apply:** This is a flag that says whether the custom notification is has been turned on or applied to the organization. If the column displays the word Org, then the notification has been enabled for the entire organization. If it is blank, the custom notification is still in draft stage or has been applied to a specific group.
- **Language:** This column which identifies the language for which the notification is used. You can customize email notifications for each supported language.
- **Action:**
 - **Clone:** Allows you to clone a notification as a starting point for a new one.
 - **Edit:** Takes you to the editor for changing the content of the notification. You can do the same thing by clicking on the Name field.
 - **Delete:** Deletes this notification (after confirmation.)

An add link allows you to create new notifications based on standard templates.

Adding a Notification

To add a new custom notification, click on the **add** link at the bottom of the custom notification list.



The screenshot shows a web form titled "Add Custom Notification...". Below the title is a subtitle: "Name your custom notification message and choose a template category." The form contains three input fields: "Name:" with the text "Custom Notification 2", "Template:" with a dropdown menu showing "New Package", and "Language:" with a dropdown menu showing "English". At the bottom of the form is a green button labeled "Add Notification".

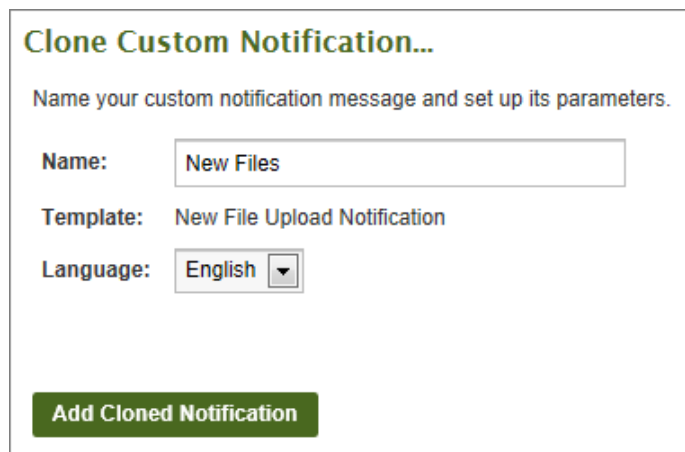
- **Name:** Name your custom notification here. Names have to be unique, and they can be used to describe your purpose for the notification, for example: Dept password change.
- **Template:** Choose one of the standard templates from the drop-down list. See the **Web Interface - Settings - Appearance - Custom Notification - Templates** (on page 380) page for details on all the templates.

Press the Add Notification button to advance to the editing screen.

When you add a new notification, a standard template notification is built and presented for editing. At the time you add the notification, the **Items Displayed** settings currently in effect will be used to select the features enabled in the custom notification. For example, if the Comment Field option is set in the **Items Displayed** settings when you add a file or message notification, the new notification will include the comment.

Cloning a Notification

Once you have a working custom notification, you may want to create a slightly different version without starting from scratch, and without changing the original. You can select an existing custom notification from the list and click on the Clone link.

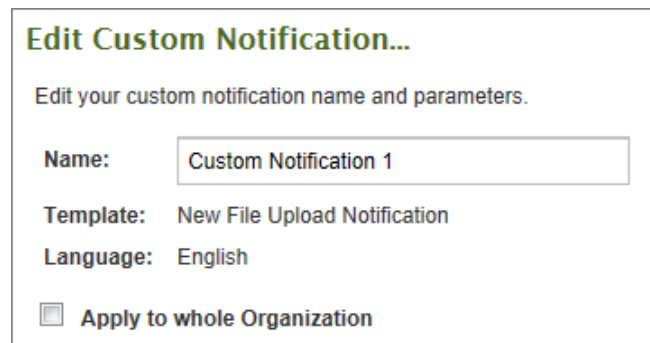


The screenshot shows a web form titled "Clone Custom Notification...". Below the title is a subtitle: "Name your custom notification message and set up its parameters." The form contains three fields: "Name:" with a text input field containing "New Files"; "Template:" with a text input field containing "New File Upload Notification"; and "Language:" with a dropdown menu showing "English". At the bottom of the form is a green button labeled "Add Cloned Notification".

This is very similar to **Adding a Notification**, but notice that the template is fixed, you only get a field for specifying the name of the new notification. After you press the **Add Cloned Notification** button, you are presented with the edit screen containing a copy of the original notification.

Editing a Notification

Immediately after adding or cloning a new notification, or if you click on the **Edit** link in the notification list, you get the editing display. The screen is broken up here and each part is described separately.



Edit Custom Notification...

Edit your custom notification name and parameters.

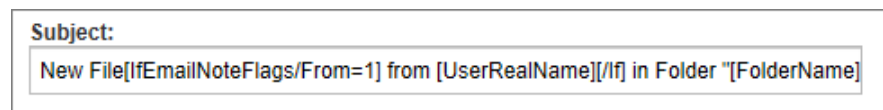
Name:

Template: New File Upload Notification

Language: English

☐ **Apply to whole Organization**

- **Name:** You may change the descriptive name of the notification.
- **Template:** Once you have added a notification, you may not change the template type. It is displayed here for reference.
- **Apply to whole Organization:** When you are ready to activate a custom notification you can check this box and the custom notification will be used for all emails of the template type. This toggles on the Org tag in the Notification list screen.



Subject:

- **Subject:** This is the subject line of the email sent out with the custom notification. You may edit the text of the subject line, including the use of macros as described below.

Body:

```
[Class=textbig][IconFile]New File Notification

A new file[IfEmailNoteFlags/From=1] from [UserRealName][If] has arrived into
the "[FolderPathURL]" folder.
[Wrap][IfEmailNoteFlags/Basic=1][Or][IfEmailNoteFlags/Comments=1]
[Class=listrow2][b]Name:[/b] [OriginalFileName]
[b]Tracking ID:[/b] [FileID]
[b]Original Size:[/b] [NiceFileSize] bytes
[IfEmailNoteFlags/From=1][b]Uploaded By:[/b] [UserRealName] ([UserEmail])
[/If][IfEmailNoteFlags/Comments=1][And][IfUploadComment!=][b]Comments:[/b]
[UploadComment]
[/If][/Class][Wrap][Wrap][IfEmailNoteFlags/NonRepudiation=1]
[i][IconIntegrity][IfIntegrityChecked=1]For non-repudiation purposes, it has
been confirmed that the file received by MOVEit DMZ is IDENTICAL to the file
uploaded by [UserRealName].
[Otherwise]For non-repudiation purposes, it cannot be confirmed that the file
received by MOVEit DMZ is identical to the file uploaded by [UserRealName]
because the client used to upload this file ([UploadAgent]) either does not
support integrity checking, or doesn't have its integrity checking option
enabled. If you believe the client used to upload the file supports integrity
checking, please assume that the integrity checking option is enabled in future
```

Update Notification

- **Body:** This is the body of the email sent out with the custom notification. It contains text that is included verbatim that you may change as it suits your specific needs. It also contains three types of macros enclosed in square brackets, ([]). Some macros are direct inserts of information available at the time of the notification, for example, [Username], or [FileID]. Other macros are used to provide a rudimentary meta-language for creating if-then-else decisions and for-loop structures. Some macros are available for controlling the appearance, usually of HTML-formatted emails. Macros are discussed in depth on the **Web Interface - Settings - Appearance - Custom Notification - Macros** (on page 386) page.
- **Update Notification button:** Any changes to the header, subject or body of a notification are saved when you press the Update button.

Example Email Notification Message

Subject: New File from Joe User in Folder "MyFolder"



New File Notification

A new file from Joe User has arrived into the "/ Distribution / MyParent / MyFolder" folder.

Name: Example.txt

Tracking ID: 1234567

Original Size: 1,234 bytes

Uploaded By: Joe User (joe@user.com)

Comments: This file is called example.txt.

☒ For non-repudiation purposes, it has been confirmed that the file received by MOVEit DMZ is IDENTICAL to the file uploaded by Joe User.

Please use the following URL and your username/password to view this package over a secure connection. After viewing this package, you may also download any associated attachments or compose a reply using your favorite web browser.

(<https://KEaston-08R2DOC.FTQA.com/human.aspx?OrgID=9999&Arg12=fileview&Arg07=1234567&Arg06=123456&username=janeuser>)

Regards,
Org 1 Notification Service

[Send Test Email to Me](#)

An example of the last-saved version of your custom notification is displayed as it would appear when sent as an email in HTML format. The subject is displayed separately from the body of the email. Generic sample data is filled into the message to show how the macro fields would be processed. A **Send Test Email to Me** button lets you send an actual email to yourself with the sample data. The email subject of the test email will always be prefixed with the words **TEST EMAIL:**. Every time you make a change to the subject or body of the custom notification and press the **Update Notification** button, the display will refresh to show you the results of your changes.

Example TEXT Email Notification Message

Subject: New File from Joe User in Folder "MyFolder"

New File Notification

A new file from Joe User has arrived into the "/ Distribution / MyParent / MyFolder" folder.

Name: Example.txt
Tracking ID: 1234567
Original Size: 1,234 bytes
Uploaded By: Joe User (joe@user.com)
Comments: This file is called example.txt.

For non-repudiation purposes, it has been confirmed that the file received by MOVEit DMZ is IDENTICAL to the file uploaded by Joe User.

Please use the following URL and your username/password to view this package over a secure connection. After viewing this package, you may also download any associated attachments or compose a reply using your favorite web browser.

(<https://KEaston-08R2DOC.FTQA.com/human.aspx?OrgID=9999&Arg12=fileview&Arg07=1234567&Arg06=123456&username=janeuser>)

Regards,
Org 1 Notification Service

Send Test TEXT Email to Me

An example of the same notification as it would appear sent as an email in TEXT format is also displayed. For the Summary File Notifications, which have completely different HTML and TEXT versions, only one or the other is displayed. A similar **Send Test TEXT Email to Me** button can be used to send a sample in text mode to your email address.

Appearance - Custom Notification - Templates

Appearance - Custom Notification - Templates

Custom Notifications are used to override standard templates for emails sent out to users and administrators. This is the list of system templates and their use.

Template	Description
Immediate File Notifications	
New File Upload Notification	Sent to users with Notify rights to the uploaded file's parent folder, informing them of the arrival of the new file. This New File Notification is be sent individually (immediately after a file has arrived), The File Upload List template below is used for a delayed batch message listing all the files that have arrived within a configurable time frame.
File Delivery Receipt	Sent to the uploader of a file when another user downloads that file. File Delivery Receipts are only sent out individually, as soon as the download action has occurred.
File Non-Delivery Receipt	Sent to the uploader of a file when another user deletes it before downloading it. File Non-Delivery Receipts are only sent out individually, as soon as the delete action has occurred.
File Upload Confirmation	Sent to the uploader of a new file informing them that the file has arrived and that the appropriate users have been notified of its arrival. This is the immediate notification. The batch-mode notification is below.
Package Notifications	
New Package	Sent to recipients of packages informing them that a new package has been posted for them to view.
New Temp User Package (with password)	Sent to temp user recipients of packages informing them that a new package has been posted for them to view and includes account information for the new user, including a password.
New Temp User Package	Sent to temp user recipients of packages informing them that a new

(with password link)	package has been posted for them to view and includes account information for the new user, including a link to where the user can set a password.
New Guest Package	Sent to guest user recipients of packages informing them that a new package has been posted for them to view and includes a package password for the guest user.
Package Password Notification	Sent to guest user recipients of packages to provide a password for the guest user to view the package. This is sent if package passwords are configured to be sent separately from the New Guest Package notification.
Package Delivery Receipt	Sent to the sender of a package when a recipient views the package. Package Delivery Receipts are only sent if the sender of the package enables the Delivery Receipt(s) setting on an individual package before sending it.
Package Download Receipt	Sent to the sender of a package when a recipient downloads a file from the package. Package Download Receipts are only sent if the sender of the package enables the Delivery Receipt(s) setting on an individual package before sending it.
Package Deleted By User	Sent to the sender of a package when a recipient deletes the package notification before viewing it. Package Non-Delivery Receipts are only sent if the sender of the package enables the Delivery Receipt(s) setting on an individual package before sending it.
Package User Was Deleted	Sent to the sender of a package when a recipient is deleted before viewing the package.
Package Expiration	Sent to the sender of a package when the package expires. A package expires when it meets either the package expiration number of days, or the maximum downloads specified in the individual package options (if available), or otherwise set by the administrator in the Ad Hoc Transfer - Package Quotas.
Package Delayed Delivery Receipt TEXT Package Delayed Delivery Receipt HTML	For bulk notification of package delivery events. Sent to the sender of a package to provide bulk notification of when a recipient views the package. Package Delivery Receipts are only sent if the sender of the package enables the Delivery Receipt(s) setting on an individual package before sending it. One template is used for text-formatted

	notification and the other is used for HTML formatted notification.
Webpost Notifications	
New Webpost Upload Notification	Sent to users with Notify rights to the Webpost's folder, informing them of the arrival of the new post.
Webpost Confirmation	Sent to the poster informing them that the Webpost has arrived and that the appropriate users have been notified of its arrival. This confirmation includes a "Thank You" message configurable on the Webpost folder.
User/Password Notifications	
New User Welcome (with password)	Informs a new user that their account has been created on the system. Includes the account username, and the account password.
New User Welcome (with password link)	Informs a new user that their account has been created on the system. Includes the account username, and a link to where the user can set a password.
Guest Self Registration Welcome	Sent to self-registering guest users when the emailed password option is being used. The notification includes a URL link and a password. It explains that they can sign in and then send the package.
Temp User Self Registration Welcome	Sent to self-registering temporary users who self-register using the reCAPTCHA option. It confirms creation of their new temporary user account.
Temp Self Registration Welcome (with password)	Sent to self-registering temporary users when an emailed password is being used. The notification includes the account username, a password, and a URL link. It explains that a new account has been created and that they can use the link to sign in.
Temp Self Registration Welcome (with password link)	Sent to self-registering temporary users when an emailed password request link is being used. The notification includes the account username and a URL link. It explains that a new account has been created and that they can use the link to begin using the account.
New Password Notification (with password)	Sent to a user informing them that their password has been changed by an administrator, and includes the new password. These messages are only available if the proper Permissions are set in an organization's Password Policy (on page 415).

New Password Notification (with password link)	Sent to a user informing them that they must change their password, and includes a link to where the user can set the password. These messages are only available if the proper Permissions are set in an organization's Password Policy (on page 415)
Password Change Request Confirmation	Sent to a user who requests a password change from the signon screen (this feature must be turned on for the organization). The link on the email must be used to complete the password change process.
Password Change Request Error	Sent to a user who requests a password change from the signon screen when he has been configured to not allow password change.
New User Password Request Confirmation	Sent to a new user who received a password link notification and sets a password successfully.
New User Password Request Error	Sent to a new user who received a password link notification and sets a password that does not meet the password rules.
Password Expiration Warning	Sent to a user informing them that their password expiration time is approaching. Users still have time to log on and change their password before their account is locked out.
Password Expiration	Sent to a user informing them that their password expiration time has run out. Users are directed to their administrator for reinstatement.
User Account Expiration Warning	Sent to a user informing them that their account expiration time is approaching. Account expiration can be based on inactivity, a fixed number of signons, or a specific date. For more information about creating and assigning expiration policies, see the Feature Focus - Expiration Policies (on page 76) page.
User Account Expiration	Sent to a user informing them that their account has expired and is no longer accessible.
Administrator Notifications	
Admin User Expired Notice	Administrator alerts inform interested administrators of various important user events in an organization. This notification tells Admins when a user is inactivated because of expiration policy. The notification happens when a user attempts to signon but is found to have been expired. The Admin has the option of reactivating the user.

Admin User Locked Out Notice	Sent to Admins when a user is locked out for signon violations.
Admin User Expired List	Sent to Admins during the overnight processing when a group of users is marked as expired, or notified of impending expiration.
Admin User Password Notice	Sent to Admins during the overnight processing when a group of users is marked as inactive, or warned, because of password expiration, or impending expiration. If users are allowed to change their own password by configuration option, the user notification goes out at the same time.
Admin IP Lockout Notice	Sent to Admins when an IP address is locked out for attempted signon violations.
Admin User Counts Notice	Sent to Admins when the number of users is approaching the licensed or configured maximums.
Summary File Notifications - TEXT	
File Upload List Notification TEXT	This and the following templates are for bulk notification of file events. The first three are used for TEXT format notification and the last three for HTML format. This notification is sent to users with Notify rights to the uploaded file's parent folder, informing them of the arrival of new files. It is a delayed batch message listing all the files that have arrived within a configurable time frame.
File Upload List Confirmation TEXT	This is the corresponding batch notification listing all files uploaded by a user within a configurable time frame.
File Not Downloaded List TEXT	This batch notification list files for which a configurable time frame has expired without anyone downloading the files.
Summary File Notifications - HTML	
File Upload List Notification HTML	These next three templates are the HTML format versions. While the TEXT versions list each folder and the newly uploaded files in each folder as a block of text information, the HTML notifications use an HTML table format for the list. This notification lists all the files that have arrived for an interested user within the time frame.

File Upload List Confirmation HTML	This HTML message is the corresponding batch notification confirming all files uploaded by a user within a configurable time frame.
File Not Downloaded List HTML	This HTML batch notification is returned to a user who uploaded files for which a configurable time frame has expired without anyone downloading them.

Appearance - Notification - Macros

Overview

Custom Notifications use a special macro language to embed into the text helpful hints about how to modify the content for display. There are three types of macros, ones that are simple insertions of data fields, ones that change the appearance, such as bold face, and ones that provide a control structure for conditions and loops. Each group of macros are listed below.

Most of the macros that change appearance or establish controls automatically expire at the end of a paragraph, indicated by a blank line in the text. So, for example, if you use an [i] to start italic text, it reverts back to standard text at the next paragraph. In this case, a closing [/i] macro is optional.

A Note about Usernames

Starting in version 5.5, Usernames have been changed to be unique User IDs, separate from the actual User login names used to sign onto MOVEit DMZ. A new LoginName field has been added to the user table. For compatibility, upgrades to version 5.5 will copy the Username to the LoginName for existing users. All new users will be created with a Username that is built from the first 8 characters of the LoginName and 8 random alphanumeric characters to make a unique User ID. For custom notifications, in the table below, references to the [Username] or [xxxx/Username] or [MyUsername] fields will return the unique User ID, and [UserLoginName] or [xxxx/LoginName] or [MyLoginName] will return the actual login.

Appearance Macros

Macro	Description
[i][i]	Start and end italic text.
[b][b]	Start and end bold text.
[hr]	Insert a horizontal rule.
[br]	Insert a line break.
[p]	Paragraph - force a blank line in HTML or text.
[class=xxx]	Establish (and ends) a text change. Classes are based on the organization style-sheet.

<code>[/class]</code>	Some classes that are used are: ▪ <code>[class=textbig]</code> - Larger than average size text ▪ <code>[class=textsmall]</code> - Normal text size ▪ <code>[class=texttiny]</code> - Smaller than normal text ▪ <code>[class=listrow1]</code> - Text with a shaded background ▪ <code>[class=listrow2]</code> - Darker shaded background
<code>[style=xxx]</code> <code>[/style]</code>	Establish (and ends) a style change.

Control Macros

Macro	Description
<code>[Ifxxxxx=y]</code> <code>[Ifxxxxx!=y]</code>	Include the following text if field "xxxxx" has a value equal to y (or not equal to y). You may choose among a number of cases by a series of <code>[if]</code> macros.
<code>[and]</code>	Use the <code>[and]</code> macro to logically combine two or more <code>[if]</code> statements with an "and" boolean operator. Example: <code>[IfMyValue=1][and][IfYourValue=1]... [/If]</code>
<code>[or]</code>	Use the <code>[or]</code> macro to logically combine two or more <code>[if]</code> statements with an "or" boolean operator. Example: <code>[IfMyValue=1][or][IfYourValue=1]... [/If]</code>
<code>[wrap]</code>	Use the <code>[wrap]</code> macro directly before an <code>[if]</code> if you want to nest additional <code>[if]</code> macros within the "wrapped" <code>[if]</code> . Example: <code>[Wrap][IfMyValue!=1]... [IfMyValue=2]... [/If]... [/Wrap]</code>
<code>[otherwise]</code>	Include the following text if no other previous <code>[if]</code> applies.
<code>[/if]</code>	Ends the conditional <code>[if]</code> within a paragraph. If there is no <code>[/if]</code> the condition ends at the end of the paragraph.
<code>[ForEachFolder]</code> <code>[ForEachFile]</code> <code>[ForEachuser]</code>	Creates a loop through each element of a list. For example, to list all attachments to a package within the New Package Notification (corresponding to the <code>[Attachment/Name]</code> macro), you would enter: <code>[ForEachAttachment][Name][BR][/For]</code> In this example, immediately following <code>[ForEach]</code>, enter the parent element of the list then terminate with the <code>]</code>. The parent is what precedes the forward-slash in the macro; for example in the <code>Attachment/Name</code> macro, the parent is "Attachment."

	Inside your ForEach loop, specify the child element(s) without the preceding parent and forward slash.
[/For]	Ends the loop [ForEachxxx] or else it expires at the end of a paragraph.
[URL] [/URL]	Creates a URL link within an HTML-formatted notification. Between the beginning and ending tags are two parts. Everything following the [URL] start up to a SPACE character is the hyperlink. Everything after the SPACE up to the closing [/URL] is the linked text.
[FolderPathURL] [FileViewURL] [FileViewURL] [MessageURL] [MsgHistoryURL] [WebPostListURL]] [LogonURL] [PasswordURL] [UserEditURL] [LockIPURL] [ListFileViewURL]] [ListFolderLinkURL] [ListFileLinkURL]]	These are all "shortcut" URL macros that contain all the hyperlink information to create each of the commonly used links within the standard templates..
[table xxx] [/table]	Starts (and ends) an HTML table. This and the following formats are only used in the three HTML-format bulk file notifications. Attributes "xxx" following the table tag are included.
[tr xxx] [/tr]	Starts a table row, passing the "xxx" attributes.
[td xxx] [/td]	Starts a table column, passing the "xxx" attributes..
[trdata] [/trdata]	Starts a data row (with alternate background shading).

Field Macros

Field macros are used to insert run-time variables into the text of emails. Each template has its own set of field macros that are available to it. There is also a group of common field macros available in all templates.

Common to all templates

Macro	Description
[EmailNoteFlags/Basic]	Flags from the Items Displayed settings: Basic File Information
[EmailNoteFlags/Comments]	Comment Field
[EmailNoteFlags/NonRepudiation]	Non-repudiation Messages
[EmailNoteFlags/DirectLink]	Direct Fileview Link
[EmailNoteFlags/From]	Uploader/Sender
[EmailNoteFlags/PrefillUsername]	Prefill User Login
[TechName]	Organization Tech contact name
[TechPhone]	Organization Tech contact phone
[TechEmail]	Organization Tech contact
[NoteSig]	Organization Signature with [ORGNAME] replaced
[BaseURL]	The Organization Base URL for constructing HTTP links

New File Upload Notification File Upload Confirmation

Macro	Description

[InstitutionName]	Name of the Organization
[Username]	User ID who uploaded the file
[UserLoginName]	Login name of the user who uploaded the file
[UserRealName]	Real name of the user who uploaded the file
[UserEmail]	Email of the user who uploaded the file
[OriginalFileName]	File name that was uploaded
[UploadComment]	Comment associated with the file when uploaded
[FileID]	File Tracking ID
[FolderID]	ID of the folder containing the file
[FolderName]	Name of the folder containing the file
[FolderPath]	Full path of the folder containing the file
[FileSize]	Size of the file
[NiceFileSize]	FileSize with commas added for easier reading
[InstID]	ID number of the Organization
[UploadAgent]	The browser or program that uploaded the file, name plus version
[IntegrityChecked]	1=File was uploaded with integrity, 0=Not
[UploadWizardName]	MOVEit Wizard or Org-configured wizard name
[MyUsername]	User ID to whom we are sending the email
[MyLoginName]	User Login to whom we are sending the email
[FolderPathURL]	HTTP link for viewing the folder on DMZ
[FileViewURL]	HTTP link for viewing the file on DMZ

[IconFile]	Large file icon
[IconIntegrity]	Small Integrity icon if Integrity Checked, or small Exclamation if not
[CScanName]	The user-configured scanner name specified in the Content Scanning settings, for example: Anti-Virus
[CScanID]	The "name/version/virus-definition" string provided by the content scanner.
[DLPViolation]	If not blank, the name of the DLP violation(s) found when scanning the file.

File Delivery Receipt

File Non-Delivery Receipt

Macro	Description
[File/ID]	These are all attributes of the file that was delivered (or not.) This is the ID number of the file
[File/InstID]	Ord ID for the file
[File/FolderID]	Folder ID containing the file
[File/FolderName]	Folder name containing the file
[File/OriginalFileTypeID]	File type (numeric) when file was created.
[File/CurrentFileTypeID]	File type (numeric) for file.
[File/Deleted]	1=File is marked for deletion (or in upload process)
[File/OriginalFilename]	File name as uploaded
[File/DisplayOriginalFilename]	HTML displayable file name
[File/FileSize]	File size
[File/UploadUsername]	User ID that uploaded the file
[File/UploadUserLoginName]	Login name of user that uploaded the file

[File/UploadUserRealName]	Real name of user that uploaded the file
[File/UploadIP]	IP address file was uploaded from
[File/UploadComment]	Comment associated with the file
[File/UploadStamp]	Date/Time the file was uploaded
[File/UploadAgentBrand]	Browser or program name that uploaded the file
[File/UploadAgentVersion]	Version of the Agent
[File/DownloadCount]	Number of times the file has been downloaded
[File/Thumbnail]	1=Indicates a thumbnail file is present
[File/UploadIntegrity]	1=Indicates the file was uploaded with integrity checking
[EventType]	1=File was downloaded w/o integrity checking 2=File was deleted without downloading 3=File was downloaded with integrity checking 5=User was deleted before downloading the file
[UploadAgent]	Agent brand and version that uploaded the file
[Download/Realname]	User real name that downloaded the file
[Download/Username]	User ID that downloaded the file
[Download/LoginName]	User login name that downloaded the file
[Download/Agent]	Agent brand and version that downloaded the file
[Download/FolderPath]	Folder path of the file
[Download/Stamp]	Date/Time of download
[InstID]	ID number
[InstitutionName]	Organization name
[UploadWizardName]	MOVEit Wizard or Org-configured wizard name

[DownloadWizardName]	MOVEit Wizard or Org-configured wizard name
[FileViewURL]	HTTP link for viewing the file
[IconFile]	Large file icon
[IconIntegrity]	Small Integrity icon if both upload and download integrity, or small Exclamation if not
[File/CScanName]	The user-configured scanner name specified in the Content Scanning settings, for example: Anti-Virus
[File/CScanID]	The "name/version/virus-definition" string provided by the content scanner.
[File/DLPViolation]	If not blank, the name of the DLP violation(s) found when scanning the file

New Package

New Package Secure Attach

New Temp User Package (with password)

New Temp User Package (with password) Secure Attach

New Temp User Package (with password link)

New Temp User Package (with password link) Secure Attach

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[From]	User ID of package sender
[FromLoginName]	User login name of package sender
[FromRealName]	User real name of package sender
[GuestDisplayName]	Display name of package sender (if sender is a guest user)

[MessageID]	Tracking ID of the package
[Subject]	Subject of the package
[ParentID]	Tracking ID of parent package (RE:/FW:)
[Attachment/ID]	ID number of attachment file (list)
[Attachment/Name]	Name of attachment file (list)
[Recipient/Username]	User ID of package recipient
[Recipient/LoginName]	User login name of recipient
[Recipient/RealName]	User real name of recipient
[Recipient/Email]	Email of recipient
[Recipient/EmailFormat]	Email format (1=HTML) for recipient
[Recipient/Permission]	Permissions (user type) of recipient
[Recipient/LastLoginStamp]	Last logon date/time.
[Recipient/LangUser]	Language code for recipient
[IconPackage]	Large package icon
[AttachmentCount]	Number of attachments
[DLPViolation]	If not blank, the name of the DLP violation(s) found when scanning the subject/note of the package
[DLPBlocked]	1 = The subject/note should be suppressed for this recipient
New Package New Package Secure Attach	
[MessageURL]	HTTP link for viewing the package on DMZ
New Temp User Package (with password) New Temp User Package (with password) Secure Attach	

[SendTempUserCredentials]	1=Organization allows sending passwords in notifications
[Recipient/DecryptedTempPassword]	Password (decrypted) for new temp user
[MessageURL]	HTTP link for viewing the package on DMZ
New Temp User Package (with password link) New Temp User Package (with password link) Secure Attach	
[NewTempUserPassURL]	HTTP link to set password for new temp user account and then immediately take the temp user to the new package.
New Package Secure Attach New Temp User Package (with password) Secure Attach New Temp User Package (with password link) Secure Attach	
[Attachment/AttDLPViolation]	If not blank, the name of the DLP violation(s) found when scanning the file
[Attachment/AttDLPMetaData]	1=DLP violation in file metadata
[Attachment/FileSize]	File size of the attachment
[Note]	The Note (body) of the package when "secure the note" is not set

New Guest Package

New Guest Package Secure Attach

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[From]	User ID of package sender
[FromLoginName]	User login name of package sender
[FromRealName]	User real name of package sender

[MessageID]	Tracking ID of the package
[Subject]	Subject of the package
[ParentID]	Tracking ID of parent package (RE:/FW:)
[Attachment/ID]	ID number of attachment file (list)
[Attachment/Name]	Name of attachment file (list)
[AccessCode]	Unique identifier linking to a specific package
[SendGuestPassword]	1=Include guest user password in the notification
[Password]	Password for guest access
[GuestAccessURL]	HTML link for guest access to the package
[IconPackage]	Large package icon
New Guest Package Secure Attach	
[Attachment/AttDLPViolation]	If not blank, the name of the DLP violation(s) found when scanning the file
[Attachment/AttDLPMetaData]	1=DLP violation in file metadata
[Attachment/FileSize]	File size of the attachment
[Note]	The Note (body) of the package when "secure the note" is not set

Package Password Notification

Guest Self Registration Welcome

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[Hostname]	Hostname of the Organization (obtained from URL)

[MessageID]	Tracking ID of the package
[Subject]	Subject of the package
[Password]	Password for guest access
[IconPackage]	Large package icon
[AccessCode]	Unique identifier linking to a specific package to be composed and sent
[SelfProvAccessURL]]	HTML link for guest sender access to the package

Package Delivery Receipt
 Package Download Receipt
 Package Deleted By User
 Package User Was Deleted

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[Username]	User ID who sent the package
[UserLoginName]	User login name who sent the package
[UserRealName]	User real name who sent the package
[Msg/ID]	Tracking ID of the package
[Msg/Subject]	Subject of the message
[Msg/SendStamp]	Date/Time of the package
[Download/Username]	User ID who read/deleted the package
[Download/LoginName]	User login name who read/deleted the package

[Download/Realname]	User real name who read/deleted the package
[Download/GuestDisplayName]	Display name who read/deleted the package (if it was guest user)
[Download/Agent]	Browser or program name and version that downloaded the package
[Download/Stamp]	Date/Time of download
[MsgHistoryURL]	HTTP link for viewing the package history on DMZ
[IconPackage]	Large package icon
[Msg/DLPViolation]	If not blank, the name of the DLP violation(s) found when scanning the subject/note of the message
Package Delivery Receipt, Package Deleted By User, Package User Was Deleted	
[EventType]	1=Package was read 2=Package was deleted before reading 5=User was delete before reading package
Package Download Receipt	
[Download/AttachmentID]	ID number of the attachment file that was downloaded
[Download/AttachmentName]	Name of the attachment file that was downloaded
[Download/AttachmentFolderID]	ID number of the folder containing the attachment file that was downloaded
[Download/AttDLPMetaData]	1=DLP violation in file metadata

Package Expiration

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[ID]	Tracking ID of the package

[UploadUsername]	User ID that sent the package
[UploadUserLoginName]	User login name that sent the package
[UploadUserRealname]	User real name that sent the package
[UploadComment]	Subject of the package
[Owner/Username]	User ID of mailbox owner who did not read package before it expired
[Owner/LoginName]	User login name of mailbox owner who did not read package before it expired
[Owner/RealName]	User real name of mailbox owner who did not read package before it expired
[IconPackage]	Large package icon

Package Delayed Delivery Receipt TEXT

Package Delayed Delivery Receipt HTML

Macro	Description
[InstID]	ID number of the Organization
[InstName]	Name of the Organization
[MyUsername]	User ID who sent the package
[MyLoginName]	User login name who sent the package
[MyRealName]	User real name who sent the package
[ListPackageLinkURL]	HTTP link for viewing the package list on DMZ
[ListAttachmentLinkURL]	HTTP link for viewing the attachment list on DMZ
[Package/ID]	Tracking ID of the package

[Package/Subject]	Subject of the package
[Package/SendStamp]	Date/Time the package was sent
[Package/Events/Event/Type]	Event type: read or download
[Package/Events/Event/Stamp]	Date/Time of the event
[Package/Events/Event/Recipient/Username]	User ID of recipient of the package for the event
[Package/Events/Event/Recipient/Realname]	User real name of recipient of the package for the event
[Package/Events/Event/Attachment/ID]	ID number of attachment file for the event
[Package/Events/Event/Attachment/OriginalFilename]	Original filename when uploaded of attachment file for the event
[Package/Events/Event/Attachment/FileSize]	Size of the attachment file for the event
[Package/Events/Event/Attachment/NiceFileSize]	Size - with commas added for easier reading - of the attachment file for the event
[Package/Events/Event/Attachment/DownloadIntegrity]	Download integrity for the attachment file for the event
[Package/Events/Event/Attachment/AttDLPMetadata]	1=DLP violation in file metadata

New Webpost Upload Notification Webpost Confirmation

Macro	Description
[Folder/ID]	Folder ID number
[Folder/Name]	Folder name
[Folder/FolderPath]	Folder path

[CurrentUser/Username]	UserID
[CurrentUser/LoginName]	User login name
[CurrentUser/RealName]	User real name
[CurrentUser/Email]	User email
[CurrentUser/EmailFormat]	User email format
[CurrentUser/HistChunk]	User hist chunk flag
[CurrentUser/UseCustomHostPermits]	User use custom host permissions flag
[CurrentUser/UserListLength]	User user list length
[CurrentUser/FileListLength]	User file list length
[CurrentUser/LangUser]	User language
[CurrentUser/AuthMethod]	User authentication method
[CurrentUser/InstID]	Organization ID
[CurrentUser/InstName]	Organization Name
[CurrentUser/InstUseCustomHeader]	Custom header flag
[CurrentUser/InstMOTD]	Organization Message-of-the-day
[CurrentUser/InstMOTDRealName]	Name of last user to change the organization message of the day
[CurrentUser/InstMOTDStamp]	Timestamp of last change of the organization message of the day
[CurrentUser/InstStylesheetID]	Organization stylesheet ID
[CurrentUser/InstStylesheetName]	Name of organization stylesheet
[CurrentUser/InstStylesheetFile]	File of organization stylesheet
[CurrentUser/InstHistoryTime]	Log retention

[CurrentUser/InstFormResponsePath]	Org "external" URL
[CurrentUser/InstTechInfo]	Tech contact info
[CurrentUser/InstFormResponseEmail]	Default from email address
[CurrentUser/InstSecBanner]	Security banner
[CurrentUser/InstSecNotice]	Security notice
[CurrentUser/InstMessaging]	Package flag
[CurrentUser/InstShowSkipLink]	Skip link enabled flag
[CurrentUser/InstShowGMTOffset]	GMT Offset display flag
[CurrentUser/InstShowMOVEitLink]	MOVEit display flag
[CurrentUser/SysAdmin]	Sysadmin flag
[CurrentUser/Permission]	User permissions
[CurrentUser/ExemptFromPasswordAging]	Exempt user from password aging
[CurrentUser/InstAuthMethod]	User authentication method
[CurrentUser/InstNoUserXPassword]	User not allowed to change password
[CurrentUser/InstTemporaryUsers]	Temporary users allowed
[CurrentUser/InstDefaultFilelistSortOrder]	Default sort order
[CurrentUser/InstCustomHelpLink]	Custom help link
[CurrentUser/InstCustomHelpName]	Custom help name
[CurrentUser/InstInformationLink]	Information link
[CurrentUser/InstInformationLinkName]	Information link name
[CurrentUser/InstContactLink]	Contact link
[CurrentUser/InstContactLinkName]	Contact link name

[CurrentUser/InstDefaultUseOrigUploader]	Flag for use original uploader
[CurrentUser/InstArchiveMessages]	Archive messages flag
[CurrentUser/InstAllowSelfAddressBooks]	Allow address books flag
[CurrentUser/InstAllowSendToUnregREcip]	Allow sending packages to unregistered recipients flag
[CurrentUser/InstAllowAttachments]	Allow package attachments flag
[CurrentUser/InstCustomWizardNameUpload]	Upload wizard brand name
[CurrentUser/InstCustomWizardNameDownload]	Download wizard brand name
[CurrentUser/InstCustomWizardLogoEnabled]	Custom wizard logo flag
[CurrentUser/InstCustomWizardZipName]	Custom wizard zip name
[CurrentUser/InstCustomWizardZipNameParsed]	Custom wizard zip name parsed flag
[CurrentUser/InstShowSelectLangPage]	Show language options on signon
[CurrentUser/InstMaxUsersInDropDown]	User list maximum
[CurrentUser/InstMaxFoldersInDropDown]	Folder list maximum
[CurrentUser/InstAllowSendPasswordByEmail]	Flag to allow passwords by email
[CurrentUser/InstAllowPassChangeRequests]	Flag to allow password change requests
[CurrentUser/InstPassChangeRequestMaxAge]	Time to allow for password change request
[CurrentUser/InstIPSwitchingMask]	IP Switching flag
[CurrentUser/InstLayoutWidth]	Display layout width
[CurrentUser/InstLayoutWidthUnit]	Display layout width unit
[CurrentUser/InstLayoutAlignment]	Display layout alignment
[CurrentUser/DisplayProfile]	Display profile

[CurrentUser/MessagingSignature]	Package signature
[CurrentUser/DefaultMsgDelivRcpt]	Default for package delivery receipts
[CurrentUser/SharedAccount]	Shared account flag
[CurrentUser/JavascriptEnabled]	Javascript enabled flag
[CurrentUser/CanSendAdHocPackages]	Can send ad hoc transfer packages flag
[CurrentUser/CanAddAttachments]	Can add attachments flag
[CurrentUser/CanAddToAddressBook]	Can add to address book flag
[CurrentUser/IsGroupAdmin]	User is group administrator
[CurrentUser/InstAllowUsernameFromClientCert]	Allow username from client cert flag
[CurrentUser/InstDefaultHomeFolderPath]	Default home folder path
[CurrentUser/DefaultCustomMsgExpiration]	Default custom expiration value for packages
[CurrentUser/MaxCustomMsgExpiration]	Maximum custom expiration value for packages
[CurrentUser/DefaultCustomDownloadLimit]	Default custom attachment download limit value for packages
[CurrentUser/MaxCustomDownloadLimit]	Maximum custom attachment download limit value for packages
[CurrentUser/AllowSendToUnregRecip]	User is allowed to send to unregistered recipients
[Post/xxxxx]	Data fields contained in webpost
[MyThankYouMessage]	Thank You message for webposts
[WebPostListURL]	HTTP link for viewing the webpost folder on DMZ
[IconFile]	Large file icon
New Webpost Upload Notification	

[MyUsername]	UserID of webpost recipient
[MyLoginName]	User login name of webpost recipient

New User Welcome (with password)

New User Welcome (with password link)

Temp User Self Registration Welcome

Temp Self Registration Welcome (with password)

Temp Self Registration Welcome (with password link)

New Password Notification (with password)

New Password Notification (with password link)

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[Hostname]	Name of host from URL
[Username]	New User ID
[UserLoginName]	New user login name
[UserRealName]	New user real name
[NewPassword]	Initial password for new user
[LogonURL]	HTTP link for logging onto DMZ
[IconInfo]	Large Info icon

Password Change Confirmation

Password Change Error

New User Password Request Confirmation

New User Password Request Error

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[UserLoginName]	User Login requesting password
[InstPassChangeRequestMaxAge]	Time to allow for password change request
[ConfirmCode]	Confirmation code for password change
[PasswordURL]	HTTP link for logging onto DMZ with confirmation code
[IconInfo]	Large Info icon (for confirmation)
[IconWarning]	Large Warning icon (for error)

Password Expiration Warning

Password Expiration

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[PasswordAgeTime]	Maximum password time
[PasswordWarnTime]	Password warning time
[PasswordAgeTimeWarnTime]	Password change interval
[UserName]	User ID
[UserLoginName]	User login name

[RealName]	User real name
[MyUsername]	User ID
[MyLoginName]	User login name
[LogonURL]	HTTP link for logging onto DMZ
[IconInfo]	Large Info icon
Password Expiration Warning	
[PasswordDaysLeft]	Number of days until password expires

User Account Expiration Warning

User Account Expiration

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[Username]	User ID
[UserLoginName]	User login name
[RealName]	User real name
[TimeString]	Current time
[DateString]	Current date
[IconInfo]	Large Info icon
User Account Expiration Warning	
[ExpirationWarnTime]	Number of days in advance to warn user about account expiration
User Account Expiration	

[ExpirationType]	0=Expire X days after creation 1=Expire X days after last activity (signon) 7=Expire after X successful signons 8=Expire on a given date

Admin User Expired Notice

Admin User Locked Out Notice

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[Username]	User ID that was expired
[LoginName]	User login name that was expired
[RealName]	User real name that was expired
[TimeString]	Current time
[DateString]	Current date
[MyUsername]	User ID of Admin
[MyLoginName]	User Login of Admin
[UserEditURL]	HTTP link for viewing user on DMZ
[IconInfo]	Large Info icon
Admin User Expired Notice	
[DeleteAfterExpireDelay]	Time before expired user deleted from system
Admin User Locked Out Notice	
[UserLockoutExpireTime]	Time before locked out user automatically reinstated

Admin User Expired List

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[user/Username]	User ID that was expired (list)
[user/LoginName]	User login name that was expired (list)
[user/RealName]	User real name that was expired (list)
[user/Permission]	User type (enduser/group admin) that was expired (list)
[user/Notified]	10=Deleted, 20=Warned (list)
[user/ExpirationType]	0=Expire X days after creation 1=Expire X days after last activity (signon) 7=Expire after X successful signons 8=Expire on a given date
[user/NotifiedType]	notify + expiration)
[IconInfo]	Large Info icon

Admin User Password Notice

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[PasswordAgeTime]	Maximum password time
[PasswordWarnTime]	Password warning time
[PasswordAgeTimeWarnTime]	Password change interval
[user/UserName]	User ID (list)

[user/LoginName]	User login name (list)
[user/RealName]	User real name (list)
[user/Notified]	User was 0=Suspended, 1=Warned
[MyUsername]	User ID of Admin
[MyLoginName]	User Login of Admin
[RealName]	User real name of Admin
[IconInfo]	Large Info icon

Admin IP Lockout Notice

Macro	Description
[InstID]	ID number of the Organization
[IPAddress]	Locked IP address
[Hostname]	Reverse DNS lookup of locked IP
[TimeString]	Current time
[DateString]	Current date
[IPLockoutExpireTime]	IP Lockout expiration time
[MyUsername]	User ID of Admin
[MyLoginName]	User Login of Admin
[LockIPURL]	HTTP link for viewing IP lockouts on DMZ
[IconInfo]	Large Info icon

Admin User Counts Notice

[Realname]	User real name of Admin

[UserCount/WhatUser]	User, End User, Temp User
[UserCount/HowManyNow]	Current value (user count)
[UserCount/WhichLimit]	System or Organization
[UserCount/HowMany]	The limit that it is within 10% of

File Upload List Notification TEXT/HTML

File Upload List Confirmation TEXT/HTML

File Not Downloaded List TEXT/HTML

Macro	Description
[InstID]	ID number of the Organization
[InstitutionName]	Name of the Organization
[MyUsername]	User ID of email recipient
[MyLoginName]	User Login of email recipient
[NewFileCount]	Count of new files
[Folder/@ID]	Folder ID (list)
[Folder/@Path]	Folder Path
[Folder/File/ID]	File ID (list)
[Folder/File/OriginalFileName]	File Original file name (or WebPost) (list)
[Folder/File/UploadUserRealName]	File Original uploader Real Name (or Anonymous if WebPost) (list)
[Folder/File/FileSize]	File size (list)
[Folder/File/NiceFileSize]	File size with commas (list)

[Folder/File/UploadStamp]	File upload timestamp (list)
[Folder/File/UploadComment]	File upload comment (list)
[Folder/File/UploadIntegrity]	File upload integrity flag (list)
[Folder/File/FolderID]	File upload Folder ID (list)
[Folder/File/FolderPath]	File upload Folder Path (list)
[ListFileViewURL]	For TEXT versions HTTP link for viewing file on DMZ
[ListFolderLinkURL]	For HTML versions HTTP link for viewing folder on DMZ
[ListFileLinkURL]	For HTML versions HTTP link for viewing file on DMZ
[IconFile]	Large File icon (All icons for HTML versions)
[IconFolder]	Small Folder icon
[IconFile1]	Small File icon
[IconIntegrity]	Small Integrity icon
[Folder/File/UploadCScanName]	The user-configured scanner name specified in the Content Scanning settings, for example: Anti-Virus
[Folder/File/UploadCScanID]	The "name/version/virus-definition" string provided by the content scanner.
[Folder/File/DLPViolation]	If not blank, the name of the DLP violation(s) found when scanning the file

Appearance - Folders

Edit Default Home Folder Path

This setting determines how user home folders will be named. When set to **[FULLNAME]**, a newly created user's home folder name will match the new user's full name (for example, John Smith). When set to **[USERNAME]**, the home folder name will match the new user's username (for example, jsmith). When set to **[USERID]**, the home folder name will match the user's autogenerated userid

This setting will also affect home folder renaming when a user's full name or username is changed. If a user's full name or username is changed while this setting is set to the equivalent value, the user making the change will be prompted to also change the name of the home folder to match the new full name or username.

Default Sort Order

This setting determines the default order in which files and subfolders will be sorted when displayed in folder contents lists. The admin can select from many different items of information, such as Upload IP Address and Size/Contents, but the two most common are Name and Created. The available options are:

- Name - Sort folder contents by name in ascending order.
- Created - Sort folder contents by creation timestamp in descending order.
- ID - Sort folder contents by ID in ascending order.
- Size/Contents - Sort folder contents by size (files) or contents (subfolders) in ascending order.
- Upload IP Address - Sort folder contents by the IP address of the uploader in ascending order.
- Creator - Sort folder contents by creator username in ascending order.
- Download Count - Sort files in folder by number of times downloaded in descending order.

Hint: Many more folder properties are configured through the **Folder Settings** links available from each folder.

Appearance - International

Languages

Organization Default Language...

The default language will be used on the signon page for first-time viewers, and will be applied to newly created users with no other language selection.

Default language: English ▼

[Change Default Language](#)

This page allows an administrator to select the default language for the organization. Four possible languages are always available for use by the end users in the organization: English, Français, Deutsch, and Español (that is, French, German, and Spanish). Users arriving at the organization **Sign on** screen for the first time will see the page in the default language.

The default system organization language is English. It is the language users arriving at the system for the first time will see if there is no default organization currently configured.

Interface

Edit Language Interface...

When the "Show Pre-Signon Language Select Page" option is set to On, a greeting page will appear to all users who access the site without a specified language in their cookie, or the URL. This page will ask the user to choose the language they would like to use.

Show Pre-Signon Language Select Page: ☐ On ☒ Off

[Change Language Interface](#)

This page provides configuration options for displaying multi-language related interfaces. Currently, the only option available is the **Show Pre-Signon Language Select Page** option. The default is **On**.

When set to **On**, a simple language selection page will be shown to users who arrive at the application without a pre-existing language selection cookie. The page will offer a choice of languages to continue with, including all available languages in the organization. Clicking a language link will take the user to the signon screen, displayed in their selected language.

Security Policies

Security Policies - Password

This topic describes the options you have for setting and managing passwords. To access these settings, select **Settings**, go to the Security Policies section, and select any of the options associated with Password.

The Password requirements set here will be displayed in the web interface where a user, or administrator, is asked to enter a password. For example, if the user is required to enter a password when sending a package, the password requirements will be listed:

Package

Provide Password

Please select or enter a password for recipient someone@domain.com. The password will be automatically emailed to the recipient.

☐ Use Suggested Password: 13z5hn

☒ Type Custom Password

Requirements:

- Must be at least 6 characters.
- Must not contain or resemble Username.
- Must contain at least one letter and one number.
- Must not contain dictionary words.

Password: 

Again: 

OK

Length & Complexity

This section controls the minimum password complexity and length requirements for the DMZ system.

Minimum Length: Password of this length and longer are the only passwords allowed. (Passwords can never be blank.) The minimum acceptable value is 4, and the default value is 6.

Complexity Strength: Controls what package of complexity rules are applied to passwords. The default complexity is Minimal.

- None - A "test" level (not available on the settings tab) which puts NO restrictions on the password other than it cannot be blank. (ALL other levels respect the minimum length and history requirements.) - Legal Passwords: a, linda, hello, linda67, lin67, hello67, lda67, LdA67 - Illegal Passwords:
- Almost None - The password cannot MATCH the username. (Case-insensitive comparisons are conducted when considering password rules even though the passwords themselves are case-sensitive.) Also, minimum length and history requirements are respected. - Legal Passwords: hello, linda67, lin67, hello67, lda67, LdA67 - Illegal Passwords: a, linda
- Weak - The password cannot CONTAIN the username, nor can it be an short version of the username. Also, minimum length and history requirements are respected. - Legal Passwords: hello, lin67, hello67, lda67, LdA67 - Illegal Passwords: a, linda, linda67
- Minimal - The password cannot RESEMBLE the username, nor visa versa. (The first three characters of both the username and the password are used to check for abbreviations.) In addition, every password must contain at least one letter and one number. Also, minimum length and history requirements are respected. - Legal Passwords: hello67, lda67, LdA67 - Illegal Passwords: a, linda, hello, linda67, lin67
- Sturdy - The password cannot RESEMBLE the username, nor visa versa. In addition, every password must contain at least one letter and one number. More importantly, passwords containing "dictionary words" (as defined in the passdict.txt file) are not allowed. Also, minimum length and history requirements are respected. - Legal Passwords: lda67, LdA67 - Illegal Passwords: a, linda, hello, linda67, lin67, hello67
- Tough - The password cannot RESEMBLE the username, nor visa versa. In addition, every password must contain at least one letter and one number, and there must be a mix of upper and lower case letters. More importantly, passwords containing "dictionary words" (as defined in the passdict.txt file) are not allowed. Also, minimum length and history requirements are respected. - Legal Passwords: LdA67 - Illegal Passwords: a, linda, hello, linda67, lin67, hello67, lda67

- **Very Tough** - The password cannot RESEMBLE the username, nor visa versa. In addition, every password must contain at least one letter, one number, and one special character, and there must be a mix of upper and lower case letters. More importantly, passwords containing "dictionary words" (as defined in the passdict.txt file) are not allowed. Also, minimum length and history requirements are respected - Legal Passwords: LdA6\$7 - Illegal Passwords: a, linda, hello, linda67, lin67, hello67, lda67, Lda67

The passdict.txt file which contains the full password dictionary is located in your d:\moveitdmz or similar folder. (It is not in "Program Files") This file is NOT encrypted and may be modified by any text editor.

Aging & History

This section controls the length of time a password is valid, and how many old passwords to remember.

Password History: Allows Admins the ability to prevent users from reusing passwords. Default value is 0, and the maximum allowed value is 99. Password histories are built as people change their passwords. In other words password histories will not magically appear as soon as an Admin changes his history setting from 0 to 5.

Password Aging: Turns password aging on and off. If enabled, passwords will EXPIRE after the configured number of days. Once a password has expired, the user will be locked out until an administrator can reenable their account. A notification of the password expiration will also be sent to interested administrators and GroupAdmins. Default value is OFF.

Lock out user if password older than: Passwords older than this number of days EXPIRE and will cause their users to be locked out until an administrator can reenable their account. Default value is 120 days, the minimum allowed value is 1, and the maximum allowed value is 9999.

Warn and force password change in advance: When enabled, MOVEit DMZ will EMAIL password expiration notices to the user in advance of their password becoming expired. An email notification will also be sent to interested administrators and GroupAdmins indicating that the user has been informed of the pending expiration of their password. Also, when a user's password is within the configured number of days, the user will automatically be forced to change their password the next time they signon.

How many days in advance: Controls how many days in advance of the password becoming expired a warning will be sent. Also controls how many days in advance of the password becoming expired MOVEit DMZ will begin forcing the user to change their password the next time they sign on. Default value is 10 days, the minimum allowed value is 0, and the value must be less than or equal to the value for the Lock out if older than setting.

When changes to the password aging options are made, the system will check to see if any current users will have their passwords marked as Expired due to the new settings. If any such users are found, a second page will appear asking the administrator if they wish to reset those users' password change stamps to the current time. Doing so will not change the passwords of the users. Instead, it will merely change the internal timestamp associated with each user's password, preventing the passwords from being considered old. If this prompt is declined, affected users will have their passwords marked as Expired during the next nightly scheduled task run.

Permissions

This section determines what abilities users have regarding passwords.

Allow Users to Change Own Password: When set to Yes, users will be able to change their own passwords. When set to No, users will be prevented from changing their own passwords. Default value is Yes.

Allow Admins to Email New Passwords to Users: When set to Yes, administrators will be provided with an option to email new passwords to users when adding a new user or changing an existing user's password. These notifications go out over insecure plain-text email. When set to No, the option will not be provided. Default value is No.

Allow Users to Request Automatic Password Change: When set to Yes, users will be allowed to request a password change from the signon screen. This allows users to reset their own passwords without having to talk to the site's technical support staff. Default value is No. If set to Yes, individual users may still be denied password change requests by enabling the **Prohibit user from requesting automatic password changes** setting on the user's profile. See the **Password section** (on page 286) of the User Profile documentation for more details.

Upon clicking the **Request password change** link on the signon page, the user will be prompted to enter their username. Once they have done so, an email address will be sent to that account's registered email address, if there is one, either with a link to continue the password change request, or a notice that the request was denied. If the link is provided, the user will have a limited amount of time to click the link, which will log them in to the MOVEit DMZ server and force them to change their password.

The length of time a password change request link is active is determined by the *Password request codes should expire after* setting. Each password change request is issued a unique ID code which identifies it to the server. That ID code is provided in the link sent to the user's email address. If that ID code is not used within the time specified by this setting, it will expire and will no longer be able to be used to reset the user's password.

Security Policies - User Authentication

This topic describes the options you have for configuring and managing user authentication. To access these settings, select **Settings**, go to the Security Policies section, and select any of the options associated with User Authentication.

Lockouts

Setting up a username lockout policy will allow this site to lock out usernames against which several bad password tries have been made. (This prevents someone from guessing the password of a valid username.) Once User Lockouts have been enabled and configured, a user who attempts to sign on with an incorrect password will be locked out following a specific number of failed attempts in a certain amount of time. Lockouts can also be set to expire after a configurable amount of time has elapsed.

Edit Username Lockout Policy...

Setting up a username lockout policy will allow this site to lock out usernames against which several bad password tries have been made. (This prevents someone from guessing the password of a valid username.) Press the "Change Lockout Policy" button to save changes to the username lockout policy.

Enable Username Lockout: Yes: ☐ No: ☒

Lock Out Users After Tries in Minutes

Expire Lockouts After Minutes
Set to 0 to disable lockout expiration.

Change Lockout Policy

Auth Method (Authentication Method)

MOVEit supports the following authentication methods:

- MOVEit DMZ - The built-in table of usernames and passwords.
- EXTERNAL Then MOVEit - Use the configured external authentication sources first. If the user fails to authenticate to these sources, fall back on the built-in table of usernames and passwords.
- EXTERNAL Only - Use only the configured external authentication sources.

Set Authentication Method

By changing the Authentication Method, you place the responsibility of user security on another server. **If your authentication server is compromised, the data contained within MOVEit DMZ may be compromised as well.** When switching authentication methods to an external server only, remember that all users who are to sign on to MOVEit DMZ need to be configured on the authentication server.

Authentication Method:

Change Authentication Method

Note: The Change password on next signon checks will not be enforced in any mode other than MOVEit DMZ.

Authentication Sources

When the organization's Auth Method is set to EXTERNAL Then MOVEit, or EXTERNAL Only, the Authentication Source list becomes available. Here, an administrator may add, edit, remove, and change the priority of the external authentication sources configured for this organization. When a user signs on to the organization for the first time, each active authentication source will be tried, in the order they are listed here. If a user successfully authenticates to one of the sources, that source is recorded in the user's profile, so that they will be immediately authenticated against it the next time they sign on (see the Authentication Source Affinity section of the *User Profile* (on page 286) page for more details).

Add/Edit External Authentication Sources...

You may add and/or edit your authentication sources below. Priority begins at the top of the list, meaning that when a new user signs on to the system, DMZ will try to authenticate the user using the top entry, and work its way down. However, once a user has already successfully signed on, DMZ will use the last successful authentication source first for that user's subsequent signons.

Enabled	Type	Name			
No	LDAP	LDAP	▼		
Yes ✓	LDAP	LDAP Basic	▲ ▼		
No	LDAP	RADIUS	▲		

Add Authentication Source...

The up and down arrows in the Actions column allow you to change the order in which the authentication sources are queried.

For more information about adding and configuring external authentication sources, see the ***External Authentication*** (on page 444) documentation in this section.

Multi Signons (Multiple Signons)

This section lets an administrator edit the default Deny Multiple Signons setting for the organization. New users will be created with the default setting, and when changed, an option is provided to set all current users with the new setting value. When Deny Multiple Signons is enabled, users will not be allowed to signon to the system using the same interface from different IP addresses. For example, a user WILL be allowed to sign on to the web interface from one machine, and the FTP interface from another, but will NOT be allowed to sign on to the web interface from two different machines.

Expiration

This section is where administrators may list, add, edit, delete, and assign Expiration Policies. These policies govern how accounts that are assigned the policy will be considered expired and removed from the system. For more information about creating and assigning expiration policies, see the ***Expiration Policies*** (on page 76) Feature Focus page.

Single Signon

The Single Signon feature allows MOVEit Server to authenticate a user without requiring sign on, provided that user is already signed on to a third-party user directory (like Microsoft Active Directory) using their network or corporate account. This section is where administrators can set up MOVEit as a service provider and configure one or more identity providers. For information on configuring Single Signon, see the ***User Authentication - Single Signon*** (on page 422) page. For information on general requirements, supported functionality, and how to deploy single signon to users, see the ***Single Signon*** (on page 87) Feature Focus page.

User Authentication - Single Signon

Single Signon allows your users to connect to MOVEit from their web browser, Ad Hoc Transfer for Outlook plug-in, or MOVEit Sync clients without having to enter a username and password each time.

MOVEit Server can use a third-party user directory (for example, Active Directory) to authenticate users. The Single Signon feature allows MOVEit Server to authenticate a user without requiring sign on, provided that user is already signed on (to the third-party user directory) using their network or corporate account.

MOVEit Server uses SAML (Security Assertion Markup Language) to exchange the authentication information with the user database.

This topic describes:

- How to set up MOVEit Server as the Local Service Provider/Relying Party to communicate with the user database (the SAML Identity Provider).
- How to add a Federated Identity Provider, which provides the user authentication information. You can add multiple Identity Providers. An identity provider can be used for SAML signon from a web browser, and also for **WS-Trust authentication** (on page 466), if set up as an external authentication source. WS-Trust can be used to extend Single Signon to other types of clients, such as the Outlook plug-in or Sync clients.

See **Feature Focus - Single Signon** (on page 87) for information about the requirements, a description of terms such as Service Provider and Identity Provider, and an overview of the process of configuring Single Signon.

For notes from our own testing with different identity providers, see **SAML Single Signon Configuration Notes** (on page 434)

For notes on troubleshooting common setup errors, see **Troubleshooting Single Signon Issues** (on page 442).

Configure Local Service Provider/Relying Party Settings

These settings are used to identify the MOVEit Server and organization as the Service Provider, secure the SAML communications, and to determine how MOVEit will receive responses from the Identity Provider.

Configure Local Service Provider/Relying Party Settings

Signing Certificate
The private portion of this certificate is used to sign authentication requests issued from MOVEit DMZ to the SAML Identity Provider. The Identity Provider uses the public portion to verify the signature.

🔑 CN=FT Documentation SAML Signing Certificate, O=FT Documentation

[Replace Certificate...](#) [Delete Certificate...](#)

Encryption Certificate
The public portion of this certificate is used by the SAML Identity Provider to encrypt authentication assertions sent to MOVEit DMZ. MOVEit DMZ uses the private portion to decrypt the assertions.

🔑 CN=FT Documentation SAML Encryption Certificate, O=FT Documentation

[Replace Certificate...](#) [Delete Certificate...](#)

Assertion Consumer Interfaces
These interfaces are responsible for receiving SAML assertions from the Identity Provider. Select which interfaces you wish to make available, and in what order.

Enabled	Interface	Location		
Yes ☒	HTTP-Post	https://doc-hemingway.ftqa.com/6685/SAML/SSO/HTTP-Post	▼	Disable
No	HTTP-Artifact	https://doc-hemingway.ftqa.com/6685/SAML/SSO/HTTP-Artifact	▲	Enable

Single Logout Interfaces
These interfaces are responsible for receiving SAML single logout requests and responses from the Identity Provider. Select which interfaces you wish to make available.

Enabled	Interface	Location	
Yes ☒	HTTP-Post	https://doc-hemingway.ftqa.com/6685/SAML/SLO/HTTP-Post	Disable
Yes ☒	HTTP-Redirect	https://doc-hemingway.ftqa.com/6685/SAML/SLO/HTTP-Redirect	Disable

Service Provider Metadata URL
This metadata XML file contains the Service Provider settings for this organization, and should be provided to the various Identity Providers this system should interact with.
Metadata: <https://DOC-HEMINGWAYFTQA.com/6685/SAML/Metadata.xml>

1 Create a Signing Certificate.

The MOVEit Server (Service Provider) sends a request to the Identity Provider. The private portion of the Signing Certificate assures that the request is from the MOVEit Server. The Identity Provider uses the public portion to verify the signature.

Click **Create Certificate** to open the Signing Certificate page. Enter the appropriate values, then click **Create Certificate**. Only the Common Name (CN) is required.

The new certificate is shown in the list.

You always have the options of replacing or deleting an existing certificate.

Note: While most servers require a Service Provider to have a signing certificate to sign requests, the encryption certificate is optional, though highly recommended for security.

2 Create an Encryption Certificate.

The Identity Provider sends an "authentication assertion" or other response to the MOVEit Server. The public portion of the Encryption Certificate is used to encrypt the assertion. MOVEit uses the private portion to decrypt the assertion.

Click **Create Certificate** to open the Encryption Certificate page. Enter the appropriate values, then click **Create Certificate**. Only the Common Name (CN) is required.

The new certificate is shown in the list.

You always have the options of replacing or deleting an existing certificate.

3 Set the appropriate Assertion Consumer Interfaces.

This interface determines how MOVEit will receive the response (the user authentication) from the identity provider. You can enable multiple interfaces, in which case the identity provider will use the first interface listed whose binding it supports.

- **HTTP-Post:** The HTTP-Post binding means that MOVEit will receive the security assertion from the identity provider through the client browser using an HTTP POST request. This is the most frequently used and most widely supported binding for assertion consumer interfaces. This is enabled by default.
- **HTTP-Artifact:** The HTTP-Artifact binding means that MOVEit will receive a reference to the security assertion (this reference is called an "artifact") from the identity provider through the client browser using an HTTP GET request, rather than the assertion itself. MOVEit will then contact the identity provider directly via SOAP in order to request the actual assertion, using the provided artifact.

HTTP-Post is more widely supported, and is good enough for most situations, but is less secure than HTTP-Artifact because the assertion data passes through the client browser, giving that browser an opportunity to access data that may not be appropriate for the client to see. This can be compensated for by using an encryption certificate, but only if the identity provider supports encrypting response messages.

HTTP-Artifact is more secure, since the assertion data never passes through the client browser – only the reference "artifact" does. However, it is less widely supported, and also requires a direct connection between MOVEit and the identity provider, which some firewall rules may not allow from the DMZ network segment.

4 Set the appropriate Single Logout Interfaces.

This interface determines how the identity provider sends a logout response or request to MOVEit. You can enable multiple interfaces, in which case the identity provider will use the first interface listed whose binding it supports.

Note: Shibboleth does not have sufficient support for single logout and Ipswitch does not recommend or support that feature with Shibboleth. It is not enabled by default in the Shibboleth Identity Provider, so MOVEit will not show the logout feature in the administrator interface. If it is enabled in the Identity Provider, we recommend you disable it here by clearing the **Enabled** option for all Single Logout interfaces.

- **HTTP-Post:** The HTTP-Post binding means that MOVEit will receive the logout request or response from the identity provider through the client browser using an HTTP POST request. This is enabled by default.
- **HTTP-Redirect:** The HTTP-Redirect binding means that MOVEit will receive the logout request or response from the identity provider through the client browser using an HTTP GET request.

- 5 You must provide the identity provider with the service provider metadata file that establishes your MOVEit Server organization as the service provider. Identity providers can access this file by the Service Provider Metadata URL.

When configuring the Identity Provider, you can provide this URL directly to the identity provider in the configuration settings. This requires that the identity provider has direct internet access to the MOVEit Server. If that's not the case, you can download the file and then upload it to the identity provider.

Note: This metadata file is updated when you change settings for a certificate, Assertion Consumer Interface, or Single Logout Interface. Make sure your identity provider is updated with the new file.

Add Federated Identity Providers

These settings add the identity providers (for example, an Active Directory Federated Services (ADFS) server) to which MOVEit Server can send an authentication request. The identity provider can be configured to offer two types of service: SAML single signon (available from the web browser), and WS-Trust (available as an external authentication method to other types of clients).

Note: If you are already using an external source for user authentication, we recommend that you use the same user store as your identity provider.

The Single Signon settings page shows the list of identity providers available (if any) to this organization.

- 1 To add a new provider, click **Add Identity Provider**. The Add SAML Identity Provider page opens.

Add SAML Identity Provider

SAML Identity Providers are added by supplying the provider's metadata file. You can do this either by uploading a copy from your local computer, or by providing the URL location of the metadata file to have MOVEit DMZ download it. Note that having MOVEit DMZ download the metadata file requires network access between MOVEit DMZ and the Identity Provider.

Upload metadata file: No file selected.

Or...

Enter metadata URL:

[Return to SAML Settings](#)

Identity providers that support SAML and WS-Trust authentication will provide a metadata file or URL that is used to configure them as a provider.

- 2 Click **Browse** to find and upload the metadata file for the provider; then click **Add Identity Provider**.
Or
Enter a URL for the providers's metadata, then click **Add Identity Provider**.
- 3 Click **Save** to save your changes.

The entry for the identity provider is created and added to list of identity providers on the Settings (Single Signon) page.

Editing an Identity Provider

You can edit an identity provider entry to make changes to some of the settings, to select whether to use Single Signon or WS-Trust services, and to define whether and how a user account in the identity provider is created as a user in MOVEit.

To edit an identity provider, click the **Edit** action to the right of the entry.

Edit Federated Identity Provider settings.

These settings identify the identity provider and configure how it will communicate with the service provider (MOVEit). The settings you need to use will depend in large part on your third-part identity provider. See your identity provider's documentation for requirements. For notes from our own testing with different identity providers, see **SAML Single Signon Configuration Notes** (on page 434).

Edit Federated Identity Provider Settings...

Below you can view and edit the general settings for this Federated Identity Provider, including name, enabled status, and allowed time skew.

Name:

Entity ID: http://DOC-MarkTwain.FTQA.com/adfs/services/trust

Enabled: ☐ Yes ☒ No

Time Condition Skew Allowance

If the clocks on your MOVEit DMZ server and Identity Provider server are not synced, you may end up with authentication failures due to the assertion valid time conditions not matching the server time. This value allows for some variation between the two clocks. It can be set to any value between 0 and 600 seconds (10 minutes).

seconds

Direct User Signon Link

If you would like your end users to go directly to the SAML signon process for this Identity Provider, you may provide them with the following link. After using this link and successfully signing on via SAML, cookies will be stored on the user's browser that will take them directly to the SAML signon process for this Identity Provider any time they visit the MOVEit DMZ application.

Link: <https://DOC-HEMINGWAY/FTQA.com/saml/signon.aspx?orgid=6685&idpid=5343&idpidstore=1>

Name: Enter a descriptive name. This name will be shown on the sign on page if you have multiple identity providers for an organization. Users can choose among the providers.

Entity ID: The URL for the identity provider. This comes from the metadata file; it cannot be modified here.

Enabled: A newly added identity provider is disabled by default. If you want to enable it, click **Yes**.

Time Condition Skew Allowance: This setting can prevent unnecessary authentication failures by allowing for some variation between the MOVEit Server clock setting and the identity provider's clock setting. By default, this is set to 60 seconds.

Direct User Signon Link: The URL link shown here provides direct access to the SAML Signon page. If you provide users with this link, they can skip the step of accessing the standard Sign on page, and having to then select an identity provider. After successful signon using this link, cookies stored on the user's browser will take them directly to the SAML Signon page on subsequent access.

Note: After the initial signon, if a user is already authenticated to the identity provider, they will not need to sign on when accessing MOVEit.

Select Federated Identity Provider Services

These settings let you select which of the available services you want to use with this organization, including SAML Single Signon and WS-Trust Secure Token Authentication.

SAML Single Signon Service

The identity provider provides single signon services using the SAML 2.0 protocol. These services are for single signon from a browser.

Select Federated Identity Provider Services...

Below you can select the various Federated Identity services available via this Identity Provider, including SAML Single Signon, and WS-Trust Secure Token authentication.

SAML Single Signon Services

This Identity Provider provides single signon services using the SAML 2.0 protocol. Select which Single Signon and Single Logout service bindings you wish to use, or disable SAML support if you do not wish to use it.

☒ Enable SAML Support

Signing Certificate

 CN=ADFS Signing - DOC-MarkTwain.FTQA.com

Encryption Certificate

 CN=ADFS Encryption - DOC-MarkTwain.FTQA.com

Single Signon Services

Interface	Location
☐ HTTP-Redirect	https://doc-marktwain.ftqa.com/adfs/ls/
☒ HTTP-Post	https://doc-marktwain.ftqa.com/adfs/ls/

Single Logout Services

Interface	Location
☐ HTTP-Redirect	https://doc-marktwain.ftqa.com/adfs/ls/
☒ HTTP-Post	https://doc-marktwain.ftqa.com/adfs/ls/

Save

Cancel

Enable SAML Support: Enable SAML single signon for this organization.

Signing Certificate: The certificate used to authorize responses from the identity provider. This comes from the metadata file; it cannot be modified here.

Encryption Certificate: The certificate used to encrypt responses from the identity provider. This comes from the metadata file; it cannot be modified here.

Single Signon Services: Sets the service that MOVEit Server uses to send authentication requests through the client browser.

Single Logout Services: Sets the type of service that MOVEit Server uses to send a logout request through the browser.

Note: The binding types for Single Signon and Single Logout services are essentially the same as those used in the Service Provider assertion consumer and single logout interfaces, though in this case, MOVEit Server is the sender and the identity provider is the receiver.

WS-Trust Security Token Service

Shows the WS-Trust external authentication sources, if any, that are configured to use this identity provider. WS-Trust service can request authentication tokens using provided username and password credentials. In this way, WS-Trust can provide external authentication from a client, for example, an FTP or SSH client.

Enabled: External authentication using WS-Trust is enabled for this organization.

Name: The name given to the WS-Trust authentication source when it was configured in MOVEit.

Edit: Click this button (to the right of the entry) to view or change the settings for this authentication source.

Add WS-Trust Authentication Source: Click this button to create a new WS-Trust source.

For information about creating or editing a WS-Trust source, see the ***External Authentication > WS-Trust (Authentication Only)*** (on page 466) page.

Edit Federated Identity Provider User settings

These settings configure how MOVEit will use the user information from the identity provider to create or modify the user account in MOVEit.

These settings will depend on which user attributes are available from your Identity Provider. You need to coordinate with the Identity Provider administrator. Note that the SAML Name ID attribute is always available from the Identity Provider.

Note: All newly created SAML Authentication accounts are provided a randomly generated password. The user or administrator can change this password, and the account can also be used to log into MOVEit through MOVEit authentication. If you are using Active Directory to do External Authentication, we recommend setting up LDAP against the same active directory ADFS uses. This will allow SAML and LDAP authentication to use the same credentials. We recommend setting up a mirroring external authentication source for FTP and SSH users because those interfaces cannot use SAML authentication.

Edit Federated Identity Provider User Settings

Below you can edit Identity Provider user settings, including the mappings between the Identity Provider attributes and the MOVEit DMZ user properties. If attributes are advertised in the provider's metadata file, they will be selectable via the drop-down menus using their friendly names. Otherwise, raw attribute names may be entered manually using the provided text boxes.

Login name: <i>Required</i>	Windows account name	Attribute name:	http://schemas.microsoft.com/ws/2008/06/identity/
Full name:	Common Name	Attribute name:	http://schemas.xmlsoap.org/claims/CommonNam
Email:	E-Mail Address	Attribute name:	http://schemas.xmlsoap.org/ws/2005/05/identity/cl

Auto-create account on signon: ☒ Yes ☐ No

☐ **Create user as a clone of**

The Login name, Full name, and Email template settings determine what values will be used for the new user's login name, full name, and email address fields if they are added to the MOVEit user account.

Attribute name: The mapping of Identity Provider attributes to MOVEit DMZ user properties is done by selecting an attribute advertised by the Identity Provider in its metadata file. If an Identity Provider does not advertise the available attributes in the metadata file, you can use the **Attribute name** box to manually enter an attribute name in the user settings. The value to use in the attribute name is dependent on the Identity Provider. ADFS provides a schema based on URIs (for example, for Full name, use: <http://schemas.xmlsoap.org/claims/CommonName>). Shibboleth provides a schema based on the urn oid (for example, for Full name, use: urn:oid:2.5.4.3). Refer to the Identity Provider documentation for the appropriate schema and values to use.

Auto-create account on signon: By default, when a new user successfully signs on, an account will be created in MOVEit. If you want to disable it, click No

Create user as a clone of: Lets you (the administrator) select an existing user as a template for users created by this authentication source. When this setting is enabled, the selected user will be cloned to create the new user account.

Edit Federated Identity Provider Group settings

These settings configure how MOVEit will use group information from the identity provider to add a group setting for the new MOVEit user.

Edit Federated Identity Provider Group Settings

Below you can edit Identity Provider group settings.

Group membership behavior: Report differences ▼

Group membership attribute: Select an attribute... ▼ **Attribute name:**

Group Mask:

☒ Include all groups except...
☐ Ignore all groups except...

Group Check Mask:

☒ Allow all users regardless of group membership
☐ Deny users in groups except...
☐ Allow users in groups except...

Group membership behavior: This setting determines how group memberships will be dealt with. When set to **Ignore Differences**, identity provider group memberships will be ignored, except in the case of the **Group Check Mask** setting. When set to **Report Differences**, differences between MOVEit group memberships and identity provider group memberships will be reported in the log. When set to **Correct Differences**, differences between MOVEit group memberships and identity provider group memberships will be corrected, if possible. MOVEit groups will NOT be added automatically, only group memberships. Groups existing on the identity provider but not on the MOVEit server will be noted as errors.

Group membership attribute: Select from the list of object properties to set the name of the group, if a group exists on the identity provider.

Attribute name: As with the user settings, if an Identity Provider does not advertise the available group attributes in the metadata file, you can use the **Attribute name** box to manually enter an attribute name for the group settings. Refer to the Identity Provider documentation for the appropriate schema and values to use.

Group Mask: These settings determine which groups will be included when syncing identity provider and MOVEit group memberships. The rule can be set to include groups except those matching one or more of the masks, or ignore groups except those matching one or more of the masks. The mask list can be one or more group name masks, separated by commas. Group name masks may contain the multiple-character wildcard *, and/or the single-character wildcard ?.

Group Check Mask: These settings operate similarly to the **Group Mask** settings, but determine the group memberships used by the system to determine if a user should be allowed to sign on or be automatically created (or mentioned in the error reports if the source is configured to not do auto-creation of users). By default, this setting is set to allow all users regardless of group memberships. The rule can also be set to deny users except those in groups matching one or more of the masks, or to allow users except those in groups matching one or more of the masks. As with the **Group Mask** setting, the mask list can be one or more group name masks, separated by commas. Group name masks may contain the multiple-character wildcard *, and/or the single-character wildcard ?.

Click **Save** to make your changes to the identity provider.

Update Federated Identity Provider Settings From Metadata

Similar to when you first add an identity provider using the metadata file, you can update the identity provider settings using this feature.

- 1 Click **Browse** to find and upload the metadata file for the provider; then click **Update Identity Provider**.
Or
Enter a URL for the providers's metadata, then click **Update Identity Provider**.
- 2 Click **Save** to save your changes.

The entry for the identity provider is updated using the information in the metadata file.

Update Federated Identity Provider Security Token Service Endpoints from Metadata

When you create a WS-Trust authentication source, you add the security token service information using the metadata file from your identity provider. If the information on the token service changes (on the identity provider), you can update the settings using this feature, so that MOVEit will have the new token service information.

- 1 Click **Browse** to find and upload the metadata file for the security token service; then click **Update Identity Provider**.

Or

Enter a URL for the providers's metadata, then click **Update Identity Provider**.

- 2 Click **Save** to save your changes.

The entry for the identity provider is updated using the information in the metadata file.

SAML Single Signon Configuration Notes

This topic documents some notes from our testing of SAML Single Signon with the supported Identity Providers. These may be of help to you in configuring and testing your implementation.

Note: Your organization may have Identity Provider requirements beyond those needed for the MOVEit configuration. Because of this, it is not possible for us to give a complete step-by-step procedure for configuring the Identity Provider. Refer to your Identity Provider's documentation for detailed configuration information.

See the ***User Authentication - Single Signon*** (on page 422) page for information about the MOVEit settings needed to support SAML Single Signon.

Note: If you want to use client certificates you must configure the Identity Provider to handle them. The SAML Single Signon process in MOVEit DMZ does not support client certificates. In MOVEit DMZ, in the User Profile for SAML users, the SSL Client Certificate Required option must be set to No.

Active Directory Federated Services (ADFS) Notes

These are notes from our test configurations using ADFS as the identity provider. The notes assume that you have ADFS connected to an Active Directory server.

Notes on the Identity Provider Installation/Configuration

- You need an ADFS server with access to an existing Active Directory system (on the same network domain).
- If you need to use the HTTP-Artifact binding, the ADFS server will need to store its configuration and the artifact database in a SQL Server. An existing ADFS server can be converted to use SQL Server.
- Once the ADFS server is installed, the web interfaces of the server (through IIS) should be secured with an SSL certificate. Additionally, MOVEit DMZ will have an SSL certificate protecting its IIS web interface. To support direct requests between the MOVEit DMZ and ADFS servers for direct downloading of metadata files, and artifact resolution requests, each server should be configured to trust the SSL certificate of the other server. This can be done by installing the public portion of each server's SSL certificate on the local computer's Trusted Authority certificate list.

Set up the Service Provider

Configure the MOVEit settings required by ADFS.

- **Certificates:** SAML requests and responses should generally be signed. OASIS also recommends that encryption be used to enhance security. To support both signing and encryption of SAML messages, create both a Signing Certificate and an Encryption Certificate.

- Assertion consumer interface: By default, MOVEit DMZ enables only the HTTP-Post interface for receiving and consuming SAML assertions from the Identity Provider. If you want to use the HTTP-Artifact interface, enable that interface and move it to the top of the Assertion Consumer Interfaces list.

Register MOVEit as the Service Provider/Relying Party

The SAML Service Provider and Identity Provider must register each other, in order to properly trust the requests and assertions that flow between the two servers. This is typically done by exchanging metadata files, which contain XML descriptions of the services, endpoints, and certificates of the server.

Register MOVEit as a Relying Party in ADFS. You can use the ADFS 2.0 Management Console to add a Relying Party Trust. This is where you can provide the URL for the Service Provider (MOVEit) metadata file, or provide a copy of the metadata file.

Set User Attributes

The settings for User Attributes are made in the both the Identity Provider's configuration and in the MOVEit settings. These settings determine which user information (such as Account Name, Common Name, Email Address), will be sent to MOVEit DMZ in authentication assertions.

You set the User Attributes, known as "claims" in ADFS, by using the Add Claim Rules dialog (in the ADFS 2.0 Management Console).

We set the following attributes:

- Add transient session ID claim: These rules required specific settings as described here.
 - On the Issuance Transform Rules tab, click the **Add Rule** button.
 - Select **Send Claims Using a Custom Rule**.
 - Enter a rule name like "Create transient session ID"
 - Enter the following rule text:


```
c1:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
    && c2:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant"]
    => add(store = "_OpaqueIdStore",
types = ("http://ipswitch.com/transientsessionid"),
query = "{0};{1};{2};{3};{4}",
param = "useEntropy",
param = c1.Value,
param = c1.OriginalIssuer,
```

```
param = "",  
param = c2.Value);
```

Click **Finish** to add the rule.

Click the **Add Rule** button again.

Select **Transform an Incoming Claim**.

Enter a rule name like "Send transient session ID as NameID".

As the Incoming claim type, enter: `http://ipswitch.com/transientsessionid`

Select **Name ID** as the Outgoing claim type.

Select **Transient Identifier** as the Outgoing name ID format.

Click **Finish** to add the rule.

- Add Active Directory attributes as claims: You can choose to supply whatever attributes required by your organization, but we set the claims to supply: Windows account name, Common name, Email address, and Group list, as these are the attributes we wanted to use in MOVEit.

In the (MOVEit) Single Signon settings, select to edit the Identity Provider, then in the User Settings, set the following:

- Login name: Windows account name (This is the only required setting.)
- Full name: Common Name
- Email: Email Address

Set other user or group settings as desired.

Additional ADFS Configuration

SHA-256: Currently, MOVEit DMZ does not support SHA-256 hashing in XML signatures, so ADFS must be configured to not use SHA-256 with the Service Provider. In the Relying Party Trust entry for MOVEit DMZ, in the Advanced tab, change Secure hash algorithm to SHA-1.

Register ADFS as the Identity Provider

Now that MOVEit DMZ is registered with the ADFS server, the reverse needs to happen as well. Again, you may either download the ADFS server's metadata (the ADFS server's metadata location is typically "<ADFS Server URL>/FederationMetadata/2007-06/FederationMetadata.xml"), or provide the metadata URL to MOVEit DMZ as part of the Identity Provider configuration.

Test Authentication using SAML

To test the configuration, sign on to MOVEit as an Org admin, copy the Direct User Signon Link from the Edit Federated Identity Provider Settings page (for the configured Identity Provider). Sign off from MOVEit, then paste that URL in the Address Bar of your browser. If configured properly, the Identity Provider will authenticate you and then return you to MOVEit DMZ, where you will be signed on. (The Identity Provider may or may not prompt for credentials, depending on the configuration.)

Note: The login prompt is not the MOVEit Signon page. The login prompt is from the Identity Provider (ADFS uses a browser default credential input window).

See the ***Troubleshooting Single Signon*** (on page 442) page for common configuration issues.

Shibboleth Notes

These are notes from our test configurations using Shibboleth as the identity provider. The notes assume that you have Shibboleth set up as the user store, or connected to an Active Directory server.

Notes on the Identity Provider Installation/Configuration

- Test the Tomcat server used by Shibboleth to make sure it can accept SSL/TLS connections and that it can access the Shibboleth Identity Provider. After installing Shibboleth, to test the Tomcat server, open: C:\Program Files (x86)\Internet2\Shib2IdP\conf\ReadMe.html. The Next Steps section of this document has several links to tests that you can run.
- Verify that the Identity Provider attempts to contact LDAP using TLS. LDAP must be configured to accept SSL/TLS connections. To verify, Go to C:\Program Files (x86)\Internet2\CaptiveTomcat 6.0\conf, then check the setting in attribute-resolver.xml: **UseStartTLS** should be set to "false". In the same directory, in login.config, the value **tls** should be set to "false."
- Restart Tomcat6 service.
- To verify that the Identity Provider can contact LDAP\Active Directory, launch the ReadMe.html file and select the **Test the IDP Status page here** link.
- Once the Shibboleth server is installed, the web interfaces of the server (through IIS) should be secured with an SSL certificate. Additionally, MOVEit DMZ will have an SSL certificate protecting its IIS web interface. To support direct requests between the MOVEit DMZ and Shibboleth servers for direct downloading of metadata files, and artifact resolution requests, each server should be configured to trust the SSL certificate of the other server. This can be done by installing the public portion of each server's SSL certificate on the local computer's Trusted Authority certificate list.

Set up the Service Provider

Configure the MOVEit settings required by Shibboleth.

- **Certificates:** SAML requests and responses should generally be signed. OASIS also recommends that encryption be used to enhance security. To support both signing and encryption of SAML messages, create both a Signing Certificate and an Encryption Certificate.
- **Assertion consumer interface:** By default, MOVEit DMZ enables only the HTTP-Post interface for receiving and consuming SAML assertions from the Identity Provider. If you want to use the HTTP-Artifact interface, enable that interface and move it to the top of the Assertion Consumer Interfaces list.

Note: If you use self-signed certificates, when you configure the Identity Provider, you will have to copy the metadata file from MOVEit, instead of using the URL for the metadata.

Register MOVEit as the Service Provider/Relying Party

The SAML Service Provider and Identity Provider must register each other, in order to properly trust the requests and assertions that flow between the two servers. This is typically done by exchanging metadata files, which contain XML descriptions of the services, endpoints, and certificates of the server.

- From the Service Provider settings in MOVEit, copy the metadata file (right-click the Service Provider Metadata URL, and save the target as DMZ-Metadata.xml), then copy the file to the Shibboleth system and paste it in the directory:
C:\Program Files (x86)\Internet2\Shib2IdP\metadata\ ; then restart the Tomcat6 service on the Shibboleth system.

- On the Shibboleth system, register MOVEit as the Service Provider/Relying Party. To do this, edit the relying-party.xml file, then add the metadata location in the Metadata Configuration section, for example:

```
<metadata:MetadataProvider id="DMZTestOrg"
xsi:type="metadata:FileBackedHTTPMetadataProvider"
metadataURL=https://<dmz-server>/<org-ID>/SAML/Metadata.xml
disregardSslCertificate="true"
backingFile="C:\Program Files (x86)\Internet2\Shib2Idp\metadata\DMZ-Metadata.xml" />
```

Note: Currently, Shibboleth cannot download the Service Provider metadata file from MOVEit DMZ, so it is necessary to copy the file as shown in the first step.

- Also, if you are using the HTTP-Artifact method for the Assertion Consumer Interface (set in MOVEit configuration), then Client Cert Auth needs to be disabled on Shibboleth. To do this: Edit C:\Program Files\Internet2\CaptiveTomcat 6.0\conf\server.xml, and under <Connector port="8443"> change clientAuth="TRUE" to clientAuth="FALSE". Save changes and restart Tomcat.

Set User Attributes

The settings for User Attributes are made in both the Identity Provider's configuration and in the MOVEit settings. These settings determine which user information (such as Account Name, Common Name, Email Address), will be sent to MOVEit DMZ in authentication assertions.

- In Shibboleth, set the User Attributes that will be sent to MOVEit in authentication assertions. To configure the attribute settings, go to C:\Program Files\Internet2\Shib2IdP\conf\ and edit the attribute-resolver.xml file.
- Release the attributes to MOVEit DMZ. To do this, edit the attribute-filter.xml settings.
- Publish the attributes in the Identity Provider's metadata.xml file. To do this, edit the idp-metadata.xml settings.
- In the (MOVEit) Single Signon settings, select to edit the Identity Provider, then in the User Settings, set the following:
 - Login name: Account name (This is the only required setting.)
 - Full name: Common Name
 - Email: Email Address
 Set other user or group settings as desired.

Register Shibboleth as the Identity Provider

Now that MOVEit DMZ is registered with the Shibboleth server, the reverse needs to happen as well. Again, you can either download the Shibboleth server's metadata, or provide the metadata URL to MOVEit DMZ as part of the Identity Provider configuration.

You can either select a local copy of the Identity Provider's metadata file [C:\[folder]\Metadata.xml], or copy the URL from `https://<idp-machine>:<port>/idp/shibboleth`, then select to add an Identity Provider, then paste the URL into the Identity Provider Metadata URL box.

Test Authentication using SAML

To test the configuration, sign on to MOVEit as an Org admin, copy the Direct User Signon Link from the Edit Federated Identity Provider Settings page (for the configured Identity Provider). Sign off from MOVEit, then paste that URL in the Address Bar of your browser. If configured properly, the Identity Provider will authenticate you and then return you to MOVEit DMZ, where you will be signed on. (The Identity Provider may or may not prompt for credentials, depending on the configuration.)

Note: The login prompt is not the MOVEit Signon page. The login prompts is from the Identity Provider (Shibboleth uses a Shibboleth splash screen,).

See the ***Troubleshooting Single Signon*** (on page 442) page for common configuration issues.

OneLogin Notes

These are notes from our test configurations using OneLogin as the identity provider. The notes assume that you have OneLogin setup as the user store, or connected to an Active Directory server.

Notes on the Identity Provider Installation/Configuration

- Once the OneLogin server is installed, the web interfaces of the server (through IIS) should be secured with an SSL certificate. Additionally, MOVEit DMZ will have an SSL certificate protecting its IIS web interface. To support direct requests between the MOVEit DMZ and OneLogin servers for direct downloading of metadata files, and artifact resolution requests, each server should be configured to trust the SSL certificate of the other server. This can be done by installing the public portion of each server's SSL certificate on the local computer's Trusted Authority certificate list.

Set up the Service Provider

Configure the Service Provider settings required by OneLogin.

- **Certificates:** SAML requests and responses should generally be signed. OASIS also recommends that encryption be used to enhance security. To support both signing and encryption of SAML messages, create both a Signing Certificate and an Encryption Certificate.

- **Assertion consumer interface:** By default, MOVEit DMZ enables only the HTTP-Post interface for receiving and consuming SAML assertions from the Identity Provider. If you want to use the HTTP-Artifact interface, enable that interface and move it to the top of the Assertion Consumer Interfaces list.

Register MOVEit as the Service Provider/Relying Party

The SAML Service Provider and Identity Provider must register each other, in order to properly trust the requests and assertions that flow between the two servers. This is typically done by exchanging metadata files, which contain XML descriptions of the services, endpoints, and certificates of the server.

From the Service Provider settings in MOVEit, open the Service Provider Metadata file and copy the entityID for the MOVEit DMZ organization. Then, open the OneLogin > Configuration page, and paste the entityID into the **SAML Audience** box.

From the Service Provider settings in MOVEit, copy the URL for the Assertion Consumer Interface, then open the OneLogin > Configuration page, and paste the URL into the **SAML Consumer URL** and also into the **SAML Recipient** box.

From the Service Provider settings in MOVEit, copy the URL for the Single Logout Interface (Redirect method), then open the OneLogin > Configuration page, and paste the URL into the **SAML Single Logout URL** box. For the Single Logout setting, OneLogin currently supports only the Redirect method.

We left the RelayState box empty.

Set User Attributes

The settings for User Attributes are made in the Identity Provider settings in MOVEit and in the OneLogin configuration. These settings determine which user information (such as Account Name, Common Name, Email Address), will be sent to MOVEit DMZ in authentication assertions.

In the (MOVEit) Single Signon settings, select to edit the Identity Provider, then in the User Settings, set the **Login name** to SAML NameID. This is the only required setting. Set other user or group settings as desired.

In OneLogin, select the Access Control tab and select to use the **Default role**.

Register OneLogin as the Identity Provider

Now that MOVEit DMZ is registered with the OneLogin server, the reverse needs to happen as well. You need to provide the metadata URL to MOVEit DMZ as part of the Identity Provider configuration.

From the OneLogin Configuration page, copy the Single Signon > Issuer URL, then go to the MOVEit settings, Single Signon, select to add an Identity Provider, then paste the URL into the Identity Provider Metadata URL field.

Test Authentication using SAML

To test the configuration, sign on to MOVEit as an Org admin, then copy the Direct Link URL from your Identity Provider configuration. Sign off from MOVEit, then paste the URL into the Address Bar of your browser. If configured properly, the Identity Provider will authenticate you and then return you to MOVEit DMZ, where you will be signed on. (The Identity Provider may or may not prompt for credentials, depending on the configuration.)

Note: The login prompt is not the MOVEit Signon page. The login prompt is from the Identity Provider.

See the ***Troubleshooting Single Signon*** (on page 442) page for common configuration issues.

Troubleshooting Single Signon Issues

This topic documents a troubleshooting process for common Single Signon failures.

When "SSL Client Cert Required" is enabled, the user cannot authenticate using SAML Single Signon

In the User Profile in MOVEit DMZ, if **SSL Client Cert Required** is set to **Yes**, the user will not be authenticated. You need to set this option to **No**. (Note that this type of failed signon attempt is not audit logged.) If you want to use a client certificate, you need to use the Identity Provider to handle the certificate.

Authentication error on MOVEit Signon page

If Single Signon authentication fails, the user may see the following notification on the MOVEit DMZ Sign On page:

Unable to authenticate with Identity Provider or not allowed to sign on from this location.

Here is a process that can help you assess and fix the problem:

- 1** The first step is to confirm your settings.
 - Ensure you have an Assertion Consumer Interface enabled that is compatible with your Identity Provider.
 - Ensure your Identity Provider is using the latest version of your MOVEit DMZ metadata file, and ensure your MOVEit server is using the latest version of the Identity Provider's metadata file.
 - Ensure the MOVEit Identity Provider settings have a sufficient Skew Allowance.
 - Ensure the MOVEit Identity Provider settings allow the creation of new users if you are trying to authenticate with a new user.
 - Ensure the MOVEit Identity Provider user and group settings are configured correctly.

For MOVEit settings, see the ***User Authentication - Single Signon*** (on page 422) page. For Identity Provider specific settings, please consult your Identity Provider documentation.

- 2 If all the settings appear to be correct, the next step in troubleshooting this error is to look in the DMZ_Web.log located at <DMZ_Install_Dir>\Logs (for example: C:\MOVEitDMZ\Logs). Depending on your Diagnostic Log Settings, the error may or may not be located in these logs. To check your current log settings, go to **Start Menu -> Programs -> MOVEit DMZ -> MOVEit DMZ Config -> Status Tab**. To view authentication issues, the "User Error" setting is sufficient. For complete debug information, use "All Debug".
- 3 After you have confirmed the log settings, look through the latest log entries. If necessary, if you had to change the log settings, have the user attempt to signon again so you can see the log information. Log errors you may see include:

Error in authentication response from Identity Provider

The following error indicates a problem that originates from your Identity Provider:

```
BindingHandler.AuthenticateSAMLResponse: Authentication not
successful: Code:urn:oasis:names:tc:SAML:2.0:status:Responder
SILUser.ExecuteAuthenticators: User '' failed to authenticate with
authenticator: SAML Assertion Authenticator
```

Additionally, some Identity Providers report errors in the Windows Event Log or in their own logs. If you see this error in the MOVEit logs, return to your Identity Provider machine and see if there are any Windows Event Logs entries or logs that indicate why the Identity Provider failed to perform Authentication.

Error in MOVEit Single Signon configuration: authentication request

The following error indicates a problem that originates from your MOVEit DMZ Server.

Authentication not successful:

```
Code:urn:oasis:names:tc:SAML:2.0:status:Requester
```

See the **User Authentication - Single Signon** (on page 422) page to confirm your configurations. If you need further assistance, please contact MOVEit Support.

Error in MOVEit Single Signon configuration: Skew Allowance

The following error indicates a problem with your "Skew Allowance" setting:

```
SAMLAuthenticator.AllowedByConditions: Current time
(2013-12-18T20:23:01.3936301Z) is outside
of assertion valid time range (2013-12-18T20:23:01.756Z to
2013-12-18T21:23:01.756Z) with skew
allowance 00:00:00 SILUser.ExecuteAuthenticators: User 'user1' failed
to authenticate with
authenticator: SAML Assertion Authenticator
```

Revisit your MOVEit Identity Provider's Skew Allowance setting and adjust this value to ensure this error does not continue to occur.

Security Policies - External Authentication - Overview

The primary configuration element for MOVEit DMZ's External Authentication feature is the Authentication Source. These sources define the type of server (LDAP, RADIUS, or WS-Trust) being used for authentication, the settings for accessing that server, and the settings for dealing with users who successfully authenticate to the server. Each Authentication Source is listed on the Auth Method page of the **User Policy** (on page 419) settings section in the order they will be checked if presented with new credentials. Links are provided for editing and deleting existing sources and changing their priorities, as well as for adding new sources.

For more information on how External Authentication works at a higher level, please see **Feature Focus - User Authentication** (on page 80).

Adding an Authentication Source

To add an authentication source, go to **Settings** page, then in the Security Policies section, in User Auth, select **Auth Method**.

Clicking **Add Authentication Source** will bring up the Add Authentication Source page. Here, a new authentication source can be created, and its basic settings defined.

Add Authentication Source...

Provide a name for this new authentication source, then select the authentication source type and the priority.

Source Name:

Source Type: LDAP (Lookup + Authentication) ▼

LDAP Server Type (LDAP Only) : Microsoft Active Directory ▼

Priority: Highest ▼

Add New Source

The basic settings for each new authentication source are:

- **Source Name** - The "friendly" name which will identify this source. The name will be listed in the authentication source list, as well as each user's source affinity selection page.
- **Source Type** - Identifies the type of authentication server this source will be defining. The following authentication source types are available:
 - **LDAP (Lookup + Authentication)** (on page 454) - Incoming usernames and passwords will be tried against a remote LDAP server. If authentication is successful, a new user may be created on the fly as a clone of an existing template user. However, user attributes such as email address and group memberships will be carried over from the LDAP server.

-
- **LDAP (Authentication Only)** (on page 451) - Incoming usernames and passwords will be tried against a remote LDAP server. If authentication is successful, a new user may be created on the fly as a clone of an existing template user.
 - **RADIUS (Authentication Only)** (on page 448) - Incoming usernames and passwords will be tried against a remote RADIUS server. If authentication is successful, a new user may be created on the fly as a clone of an existing template user.
 - **WS-Trust (Authentication Only)** (on page 466) - Incoming usernames and passwords will be tried against a remote WS-Trust server. If authentication is successful, a new user may be created on the fly as a clone of an existing template user.
 - **LDAP Server Type (LDAP Only)** - Identifies the type of LDAP server this authentication source will be querying. Based on this value, default settings will be prefilled in several fields for the newly created authentication source, and configuration hints appropriate to the server type will be displayed. Available server types are Microsoft Active Directory, Sun iPlanet, Novell eDirectory, and IBM Domino. Selecting **Other** will cause no default settings or configuration hints to be shown.
 - **WS-Trust Identity Provider (WS-Trust Only)** - Identifies the WS-Trust server this authentication source will be querying. In SAML terminology, the server is called an Identity Provider. You may have already set up an Identity Provider for the Single Signon feature. The **Add New Federated Identity Provider** link opens the page where you can configure a new identity provider. For information about adding an identity provider, see the **User Authentication - Single Signon** (on page 422) topic.

Note: If you have set up the Single Signon feature, you want to use the same identity provider that you use for browser-based single signon. This will allow users to use the same credentials to do both single signon through the browser (web interface), and username/password authentication through FTP and SSH clients.

- **Priority** - Determines where in the current authentication source list this new source should be placed. Select **Highest** to make this new source the first source on the list. Select **Lowest** to make this new source the last source on the list. Select **Middle** to place this new source in the middle of the list.

Once the new authentication source is added, a link will be provided at the top of the page, allowing the administrator to go directly to the settings page for the new source.

Editing an Authentication Source

An authentication source can be configured by clicking the Edit link for it in the authentication source list. Basic settings for the authentication source can be changed in the Edit Authentication Source Settings section, which is common to all authentication source types. Other settings appear based on the type of the source.

Common Settings

The Edit Authentication Source Settings section is common to all authentication source types. Here, the friendly name of the source can be changed, along with the Enabled status.

Edit Authentication Source Settings...
Below you can edit the generic settings for this authentication source, including name and enabled status.

Source Name:

Enabled: ☐ Yes ☒ No

Change Authentication Source Settings

- **Enabled** - Select the Yes option to make the authentication source immediately available for use as soon as it is added. Otherwise, select the No option to add the source to the list as temporarily disabled, so you can fine tune the source settings before making it available.

Specific Settings

Specific settings for each of the various types of external authentication sources can be found in their own documents in this section.

- ***Web Interface - Settings - Security Policies - External Authentication - RADIUS (Auth Only)*** (on page 448)
- ***Web Interface - Settings - Security Policies - External Authentication - LDAP Auth Only*** (on page 451)
- ***Web Interface - Settings - Security Policies - External Authentication - LDAP Lookup*** (on page 454)
- ***Web Interface - Settings - Security Policies - External Authentication - WS-Trust (Auth Only)*** (on page 466)

Security Policies - External Authentication - Radius (Authentication Only)

The Edit RADIUS Authentication Settings section determines the primary and backup server host, port, and shared secret to be used for this source. The primary fields are required to be present, though the primary shared secret can be blank. The backup fields are optional. The default port for RADIUS servers is 1645, and will normally be prefilled.

Edit RADIUS Authentication Settings...

The server specified here will be queried for authentication on user signon. You may optionally define a backup server; in the event that the primary server is unreachable, the backup server will be queried, if it is defined. If the RADIUS server does not reply to the signon query, MOVEit will try signing on again, until the number of signon attempts reaches the Authentication Retries parameter below.

Primary Server (Required)

Host:

Port:

Shared Secret:

[Test Primary Radius Connection](#) *(Requires JavaScript)*

Backup Server (Optional)

Host:

Port:

Shared Secret:

[Test Backup Radius Connection](#) *(Requires JavaScript)*

RADIUS Max Retries:

RADIUS Query Timeout:

Change RADIUS Settings

Also available in this section are the Max Retries and Timeout settings. Max Retries determines how many additional times the authentication source will be queried if a query has an error. Timeout determines how many seconds the system will wait for a response before considering a query to be failed.

Finally, both the primary and backup RADIUS server sections have **Test Connection** links which can be used to test the authentication settings. Clicking either link will open a test window prompting for a username and password to attempt authentication with. Once these are provided, the RADIUS Connection Test Results window will appear, which will list the parameters of the test, the result of the test, and any diagnostic information collected during the test.

The RADIUS Authenticated User Template section determines how a user authenticated by this source will be handled. The settings affect only users who successfully authenticate to the RADIUS server, but don't yet exist on the DMZ server.

RADIUS-Authenticated User Template...

If a user signs on successfully with a username that MOVEit DMZ has never encountered before, MOVEit DMZ will create a new account on the DMZ system, based upon the username and the "template" user you configure below.

Auto-create account on signon: ☒ Yes ☐ No

Use the [USERNAME] template to represent the username of the authenticating user. If the full name template is left blank, the username template will be used.

FullName Template:

Email Template:

Notes:

Added by RADIUS

The following settings determine how new users authenticated by this authentication source will be created. The Default User Authentication Method determines whether the users should be authenticated by EXTERNAL AUTHENTICATION only, or also by MOVEit DMZ's internal user database, if the external authentication should fail. Administrators may also elect to use an existing user as a template for authenticated users by enabling the Create User As Clone Of feature, and selecting the appropriate template user.

Default User Authentication Method:

☐ **Create user as a clone of**

Change RADIUS User Settings

The Auto-Create Account on Signon setting determines whether a new user will be automatically added to DMZ when they successfully authenticate. The Fullname, Email, and Notes template fields determine what values will be used for the new user's full name, email address, and notes fields if they are added. The macro [USERNAME] can be used to represent the username of the user. The Default Authentication Method setting determines whether the user will authenticate using both the external authentication sources and MOVEit DMZ's internal database, or just the external sources. This value will default to External Only for newly created authentication sources. The Create User As Clone Of setting allows the administrator to select an existing user as a template for users created by this authentication source. When this setting is enabled, the selected user will be cloned to create the new user account. If JavaScript is enabled on the browser and one or more template users exist in the organization, only template users will be shown in the dropdown menu by default. The **Show All Users** link will cause all users to be listed again.

If you plan on cloning users with preconfigured expiration policies (such as "expire after 30 days of inactivity"), you must use a "template user" (i.e. a user with a status of **template** rather than **active** or **inactive**). Cloning a template user allows MOVEit DMZ to carry an expiration policy from user to user, but template users are not themselves affected by expiration policies.

RADIUS-ODBC (Database) Authentication

Complete information about the optional RADIUS-ODBC authentication service can be found in the *Advanced Topics - RADIUS-ODBC Authentication* (on page 724) documentation.

Security Policies - External Authentication - LDAP Authentication Only

The Authentication Only mode for LDAP authentication operates similarly to RADIUS authentication. Primary and backup server and login information is configured, and DMZ uses these settings to simply authenticate the user. The [USERNAME] macro is the only one available, so users can only be authenticated from a single organizational unit or domain on the LDAP server.

Edit LDAP Authentication Settings

The Edit LDAP Authentication Settings section determines the primary and backup server URL and login template to be used for this source. The primary fields are required to be present. The backup fields are optional. The macro [USERNAME] can be used in the login templates to represent the username of the user.

The use of "LDAP://..." vs. "LDAPS://..." in the path fields determines whether or not LDAP over SSL will be used. The use of LDAP over SSL is strongly recommended to protect the transmission of credentials and other user information between MOVEit DMZ and any LDAP servers. Most modern LDAP servers support this.

Edit LDAP Authentication Settings...

The LDAP server specified here will be used for authentication when the user attempts to sign on. You may define an optional backup LDAP server; it need not be of the same type as the primary LDAP server. LDAP over SSL can be used by setting the protocol section of the server path to LDAPS://.

Microsoft Active Directory (AD) Configuration:

Path: LDAP://<HostName>

Example: LDAP://main.mycorp.com

Login Template: User Distinguished Name template

Example: MyDomain\[USERNAME]

Primary Server (Required)

Path: LDAP://monica.corp.stdnet.com/DC=corp,DC=stdn

User Login Template: CORP\[USERNAME]

[Test Primary Ldap Connection](#) (Requires JavaScript)

Backup Server (Optional)

Path:

User Login Template: MyDomain\[USERNAME]

[Test Backup Ldap Connection](#) (Requires JavaScript)

LDAP Max Authentication Retries: 3

[Change LDAP Settings](#)

Also available in this section is the Max Retries setting. Max Retries determines how many additional times the authentication source will be queried if a query has an error.

Finally, both the primary and backup LDAP server sections have **Test Connection** links which can be used to test the authentication settings. Clicking either link will open a test window prompting for a username and password to attempt authentication with. Once these are provided, the LDAP Connection Test Results window will appear, which will list the parameters of the test, the result of the test, and any diagnostic information collected during the test.

Edit LDAP User Settings

The Edit LDAP User Settings section determines how a user authenticated by this source will be handled. The settings effect only users who successfully authenticate to the LDAP server, but don't yet exist on the DMZ server.

Edit LDAP User Settings...

If a user signs on successfully with a username that MOVEit DMZ has never encountered before, MOVEit DMZ can create a new account on the DMZ system, based upon the username and template information you configure below.

Auto-create account on signon: ☒ Yes ☐ No

Use the [USERNAME] template to represent the username of the authenticating user. If the full name template is left blank, the username template will be used.

FullName Template:

Email Template:

Notes:

Added by LDAP

The following settings determine how new users authenticated by this authentication source will be created. The Default User Authentication Method determines whether the users should be authenticated by EXTERNAL AUTHENTICATION only, or also by MOVEit DMZ's internal user database, if the external authentication should fail. Administrators may also elect to use an existing user as a template for authenticated users by enabling the Create User As Clone Of feature, and selecting the appropriate template user.

Default User Authentication Method:

☐ **Create user as a clone of**

Change LDAP User Settings

The Auto-Create Account on Signon setting determines whether a new user will be automatically added to DMZ when they successfully authenticate. The Fullname, Email, and Notes template fields determine what values will be used for the new user's full name, email address, and notes fields if they are added. The macro [USERNAME] can be used to represent the username of the user. The Default Authentication Method setting determines whether the user will authenticate using both the external authentication sources and MOVEit DMZ's internal database, or just the external sources. This value will default to External Only for newly created authentication sources. The Create User As Clone Of setting allows the administrator to select an existing user as a template for users created by this authentication source. When this setting is enabled, the selected user will be cloned to create the new user account. If JavaScript is enabled on the browser and one or more template users exist in the organization, only template users will be shown in the dropdown menu by default. The **Show All Users** link will cause all users to be listed again.

If you plan on cloning users with preconfigured expiration policies (such as "expire after 30 days of inactivity"), you must use a "template user" (i.e. a user with a status of **template** rather than **active** or **inactive**). Cloning a template user allows MOVEit DMZ to carry an expiration policy from user to user, but template users are not themselves affected by expiration policies.

Security Policies - External Authentication - LDAP Lookup

The Lookup + Authentication mode for LDAP authentication offers much more flexibility than the Authentication Only mode. When this mode is set, DMZ will query the LDAP server for information about the incoming user and then use that information to build a login string. This querying allows DMZ to authenticate users from several different organizational units or domains. It also allows DMZ to use fields from the user's LDAP entry when building new user accounts, and even allows group memberships to be synchronized between the LDAP server and DMZ.

Edit LDAP Authentication Settings

The Edit LDAP Authentication Settings section determines the primary and backup server URL, administrator login and password, and login template to be used for this source. The primary URL and login template are required to be present. All other fields are optional.

The use of "LDAP://..." vs. "LDAPS://..." in the path fields determines whether or not LDAP over SSL will be used. The use of LDAP over SSL is strongly recommended to protect the transmission of credentials and other user information between MOVEit DMZ and any LDAP servers. Most modern LDAP servers support this.

Edit LDAP Authentication Settings...

The LDAP server specified here will be queried for information about a user when the account is generated, and then for authentication when the user attempts to sign on. You may define an optional backup LDAP server; it need not be of the same type as the primary LDAP server. LDAP over SSL can be used by setting the protocol section of the server path to LDAPS://. The special macro [mi:dn] will be replaced by the distinguished name of the user.

Microsoft Active Directory (AD) Configuration:

Path: LDAP://<HostName>/<SearchPath>,dc=<Domain>

Example: LDAP://main.mycorp.com/ou=Employees,dc=main,dc=mycorp,dc=com

Login Template: User Distinguished Name template

Example: [distinguishedName]

Admin Login: Administrator's Login String

Example: cn=Administrator,cn=Users,dc=mydomain,dc=mycorp,dc=com

Example: cn=Admin,ou=Operations,dc=mydomain,dc=mycorp,dc=com

Example: administrator@mydomain.mycorp.com

Primary Server (Required)

Path:	LDAPS://directoryserver/dc=corp,dc=stdnet,dc=com
User Login Template:	[distinguishedName]
Admin Login:	cn=Administrators,cn=Users,dc=stdnet,dc=corp,dc=com
Admin Login Password:	••••••••

[Test Primary Ldap Connection](#) (Requires JavaScript)

Backup Server (Optional)

Path:	LDAPS://directoryserver-backup/dc=stdnet,dc=corp,dc=cor
User Login Template:	[distinguishedName]
Admin Login:	cn=Administrators,cn=Users,dc=stdnet,dc=corp,dc=com
Admin Login Password:	••••••••

[Test Backup Ldap Connection](#) (Requires JavaScript)

Maximum LDAP Authentication Retries:

[Change LDAP Settings](#)

In addition to the base LDAP URL, the Path setting should also be provided with the base LDAP path in which users should be searched for. For example, if only users in the FileTransfer organizational unit should be allowed to sign on to DMZ, the path might be set to

"LDAPS://server.company.com/ou=FileTransfer,dc=server,dc=company,dc=com". The use of "LDAP://..." vs. "LDAPS://..." determines whether or not LDAP over SSL will be used. (The use of LDAP over SSL is encouraged to protect the transmission of credentials and other user information between MOVEit DMZ and any LDAP servers.)

Macros can be used in the Login Template to construct the appropriate login string for the user. Any field in the LDAP user entry can be used by simply surrounding the field name with square brackets ([]). For example, if you wish to use the value of the LDAP field `distinguishedName` for the user's login string, simply set the Login Template setting to `[distinguishedName]`. The special macro `[mi:dn]` will be interpreted by DMZ to be the LDAP distinguished name of the user.

The Administrator Login String and Password settings determine the account that DMZ will use to login to the LDAP server to find information about incoming users. It is also the account that will be used by the overnight scheduler to synchronize user information between DMZ and the LDAP server.

As with the Authentication Only mode, the Max Retries setting is also available. Max Retries determines how many additional times the authentication source will be queried if a query has an error. This setting only applies to the authentication of the user, not the querying for user information.

Finally, both the primary and backup LDAP server sections have **Test Connection** links which can be used to test the authentication settings. Clicking either link will open the LDAP Connection Test Results window, which will list the parameters of the test, the result of the test, and any diagnostic information collected during the test.

Edit LDAP User Settings

The Edit LDAP User Settings section determines how a user authenticated by this source will be handled. In addition to determining the values used to create new users, many of the various templates are also used during subsequent signons, and by the nightly LDAP synchronization task to make sure the user account remains synced with the user's LDAP entry.

Edit LDAP User Settings...

If a user signs on successfully with a username that MOVEit DMZ has never encountered before, MOVEit DMZ can create a new account on the DMZ system, based upon the username and template information you configure below.

Auto-create account on signon: ☒ Yes ☐ No

Auto-create account in Scheduler: ☐ Yes ☒ No

Sync existing user accounts in Scheduler: ☒ Yes ☐ No

Accounts authenticated by this source may be automatically marked as expired when the account either no longer exists on the LDAP server, or is disallowed by this source's Group Check Mask Rule.

Expire account when no longer authorized: ☐ Yes ☒ No

Templates consist of one or more template "variables", which are made up of fields from your LDAP server user entries, surrounded by square brackets ([]).

Microsoft Active Directory (AD) Configuration:

User Object Class: Object class of LDAP user records to search; can also take a complete LDAP search query

Example: (&(! (objectClass=computer))(objectClass=user))

Example: user

Username Field: Name of field containing username

Example: sAMAccountName

FullName Template: Template for building the user's display name

Example: [name]

Example: [lastName], [firstName] [middleName]

Email Template: Template for building the user's email address

Example: [sAMAccountName]@mycorp.com

Example: [mail]

Home Folder Template: Template for building the user's home folder path

Example: /Home/[sAMAccountName]

Notes Template: Template for building the user's notes field

Example: Automatically created based on LDAP user '[distinguishedName]' from corporate LDAP server. It may be possible to contact this user at telephone number '[telephoneNumber]'

Client Cert Field: Name of field containing client certificate

Example: userCertificate

User Object Class or LDAP Search String:

(&(! (objectClass=computer))(objectClass=user))

Username Field: sAMAccountName

FullName Template: [name]

Email Template: [mail]

☐ Ignore blank Email fields in LDAP source

Home Folder Template: /Home/[sAMAccountName]

Notes Template:

Client Cert Field:

[Test LDAP Search](#) (Requires JavaScript)

The following settings determine how new users authenticated by this authentication source will be created. The Default User Authentication Method determines whether the users should be authenticated by EXTERNAL AUTHENTICATION only, or also by MOVEit DMZ's internal user database, if the external authentication should fail. Administrators may also elect to use an existing user as a template for authenticated users by enabling the Create User As Clone Of feature, and selecting the appropriate template user.

Default User Authentication Method: EXTERNAL Only

☐ Create user as a clone of Helga Finlaysen (helga)

[Change LDAP User Settings](#)

Auto-Create Account Settings

As with the Authentication Only mode, the Auto-Create Account on Signon setting determines whether a new user will be automatically added to DMZ when they successfully authenticate. The Auto-Create Account in Scheduler setting determines whether users who exist on the LDAP server but not on DMZ will be automatically added as well.

Expire Account Setting

The Expire Account When No Longer Authorized setting allows users who were previously authorized by the LDAP server to be marked as expired if they are no longer allowed to sign on, either because they have been removed from the LDAP server, or no longer allowed by the Group Check Mask rule. Once a user has been expired, they will be deleted from the organization after seven days, unless the user becomes re-authorized on the LDAP server or an administrator manually changes the user's status.

User Object Class and Username Field Settings

The User Object Class and Username Field settings define the searches that DMZ will execute against the LDAP server both during user signons and during the nightly scheduled task. User Object Class indicates the value of the objectClass property that indicates an LDAP entry is a user. The Username Field indicates the name of the field that will contain the username of the user entry.

The User Object Class setting can also be used to perform more advanced LDAP queries. This can be useful in cases such as with Active Directory, where computers in the directory are also considered users. In order to only return true user accounts, a more advanced query is needed to get all objects with objectClass=user, but avoid those objects which also have objectClass=computer. This more advanced query can be put in the User Object Class setting, and the system will correctly interpret and execute it. For the above example, the User Object Class should be:

```
(&(!(objectClass=computer))(objectClass=user))
```

Fullname, Email, Home Folder, and Notes Templates

The Fullname, Email, Home Folder, and Notes template fields determine what values will be used for newly created users, and for synchronizing existing users. These template fields can use macros of any field in the LDAP user entry. The MOVEit DMZ specific macro [mi: userid] can be used in the Home Folder template to indicate the use of the MOVEit DMZ user ID for creating the user's home folder. Again, as with the Authentication Only mode, the Default Authentication Method setting determines whether newly created users will authenticate using both the external authentication sources and MOVEit DMZ's internal database, or just the external sources. Note that all four fields will be used when creating a user, but only the Fullname and Email fields will be used when synchronizing a user.

Note that with the Email template field, you can select *Ignore blank Email fields in LDAP source* to ensure that blank email addresses on the LDAP source will not be synchronized to MOVEit DMZ user settings. This will prevent any existing email entries in MOVEit DMZ from being overwritten with the blank entry from LDAP.

Client Certificate Field Setting

The Client Cert Field setting defines the LDAP field that contains client certificates in the user entry. If this setting is set to a non-blank value, DMZ will consider the LDAP server to be the authoritative client certificate repository, meaning any client certificates added manually through the web interface will be overwritten by whatever value is in the LDAP server. If client certificates are to be managed outside of the LDAP server, this field should be left blank.

If the value is not blank, client certificates found in the matching LDAP field will be added to DMZ's internal client certificate store so that they can be used for identification and authentication purposes. All listed certificates in the user's LDAP entry will be synchronized to DMZ's internal store.

Supported client certificate types are DER-encoded X.509 and Base64-encoded X.509 certificates. Other types will not be processed by MOVEit DMZ.

Note: Self-signed client certificates stored in DMZ's internal store will not be added to the Microsoft Trusted Root Store on the server during LDAP synchronization. This means that they will not be usable as an authentication method for MOVEit DMZ without manual intervention. For this reason, when using LDAP-stored client certificates with MOVEit DMZ, only use certificates that have been signed by a trusted CA certificate.

Test LDAP Search Option

The Test LDAP Search link can be used to test the user settings to ensure that they are correct for locating user accounts on the LDAP directory. Clicking the link will open the Advanced LDAP Search Test Results window, which will list the parameters of the test, the result of the test, and any diagnostic information collected during the test.

User Matching via Client Certificate Settings

These settings allow DMZ to more easily find a user's record in LDAP when provided only with a client certificate. They are only available if the Allow Username from Client Certificate setting is enabled on the Default HTTP Policy Settings page. See the ***Security Policies - Interface*** (on page 482) page for more details.

These settings provide a way for the system to more easily determine a user's LDAP identity from the information in their client certificate, if one is provided.

Client Certificate Value:

SAN Principal Name

Matching LDAP Field:

userPrincipalName

☒ Client certificate subject must match LDAP certificate

When the Allow Username from Client Certificate setting is enabled, users may choose to have MOVEit DMZ automatically detect their username based on the client certificate they provide. In addition to searching its own internal client certificate store, DMZ can also search LDAP external authentication sources, if any are available and have the Client Certificate Field setting configured. However, since client certificates are stored in LDAP as raw data values, they cannot be effectively searched for. To avoid having to do a potentially time-consuming search of the entire LDAP user list for the correct certificate, these settings allow administrators to match a value in the provided client certificate with a searchable field in LDAP.

The Client Certificate Value setting defines a value from a provided client certificate that will be searched for in LDAP in order to find the matching user entry. Available client certificate values are:

- Subject CN - The CN value in the certificate subject.
- Subject Email - The E value in the certificate subject.
- Subject Alternative Name (SAN) Extension - The value of the SAN extension, if one is present in the certificate. This X.509 V3 extension can have several parts included, but the main part is typically an email address.
- SAN Principal Name - The Principle Name value of the SAN extension, if one is present in the certificate. This value is typically used when authenticating a client certificate against an Active Directory environment, especially when using Smart Card based hardware client certificates, such as with the Department of Defense's Common Access Card (CAC) environment. Customers using such an environment should choose this option, and set the Matching LDAP Field value to `userPrincipalName`.

The Matching LDAP Field setting defines the LDAP field which the chosen client certificate value should match up against when searching for the user's LDAP entry.

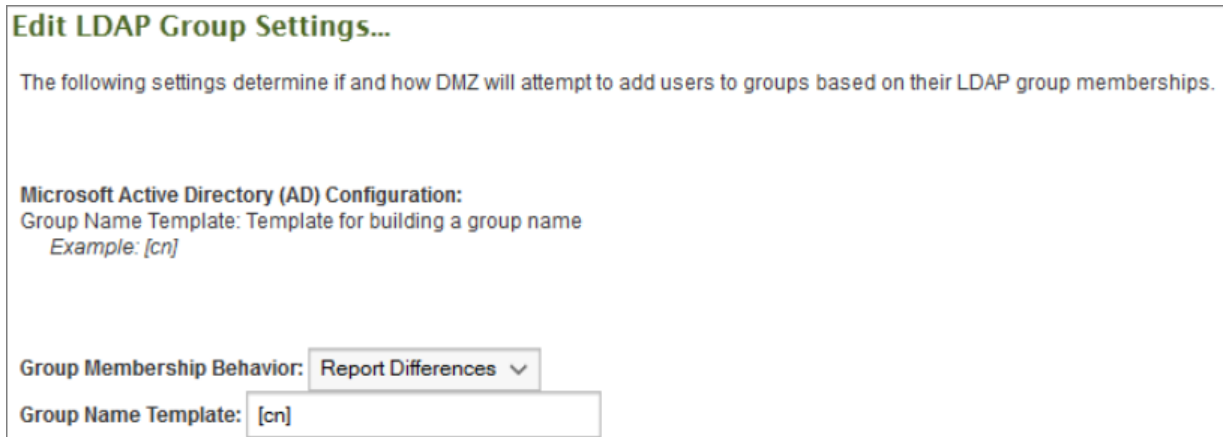
Create As Clone Settings

The Create User As Clone Of setting allows administrators to select an existing user as a template for users created by this authentication source. When this setting is enabled, the selected user will be cloned to create the new user account. If JavaScript is enabled on the browser and one or more template users exist in the organization, only template users will be shown in the dropdown menu by default. The **Show All Users** link will cause all users to be listed again. This feature is particularly useful when you want users created through the External Authentication features to have different allowed interfaces, authentication rules or permissions than users created through other interfaces.

If you plan on cloning users with preconfigured expiration policies (such as "expire after 30 days of inactivity"), you must use a "template user" (i.e. a user with a status of **template** rather than **active** or **inactive**). Cloning a template user allows MOVEit DMZ to carry an expiration policy from user to user, but template users are not themselves affected by expiration policies.

Edit LDAP Group Settings

The Edit LDAP Group Settings section determines how LDAP group memberships will be handled when authenticating, creating, and syncing users. LDAP group memberships can be mirrored on DMZ based on a set of masks and mask rules. Users can be allowed or denied from signing on to DMZ based on another set of group masks and mask rules.



Edit LDAP Group Settings...

The following settings determine if and how DMZ will attempt to add users to groups based on their LDAP group memberships.

Microsoft Active Directory (AD) Configuration:
Group Name Template: Template for building a group name
Example: [cn]

Group Membership Behavior: Report Differences ▼

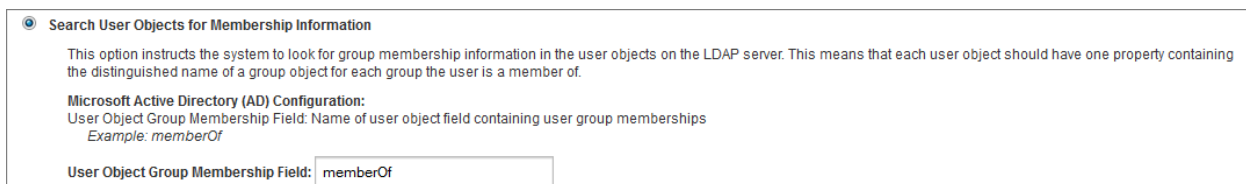
Group Name Template: [cn]

The Group Membership Behavior setting determines how group memberships will be dealt with. When set to **Ignore Differences**, LDAP group memberships will be ignored, except in the case of the Group Check Masks setting. When set to **Report Differences**, differences between DMZ group memberships and LDAP group memberships will be noted by the nightly scheduler as errors. When set to **Correct Differences**, differences between DMZ group memberships and LDAP group memberships will be corrected, if possible. DMZ groups will NOT be added automatically, only group memberships. Groups existing on the LDAP server but not on DMZ will be noted by the nightly scheduler as errors.

When an LDAP group is found, its object properties will be queried by DMZ, and retrieved. These properties can then be used as macros to determine the name of the group. One or more of these macros should be placed in the Group Name Template setting to allow DMZ to determine the name of the LDAP group to match against groups on the DMZ server.

Searching User Objects for Group Membership

When it comes to actually finding the LDAP groups a given user is a member of, there are two available methods. The first method is by searching the user's LDAP entry for properties that denote which groups the user is a member of. This method is the default and is used when the **Search User Objects for Membership Information** option is selected.



☒ **Search User Objects for Membership Information**

This option instructs the system to look for group membership information in the user objects on the LDAP server. This means that each user object should have one property containing the distinguished name of a group object for each group the user is a member of.

Microsoft Active Directory (AD) Configuration:
User Object Group Membership Field: Name of user object field containing user group memberships
Example: memberOf

User Object Group Membership Field: memberOf

The only setting available under this option is the User Object Group Membership Field. For each group the user is a member of, there should be one of these fields in the user's LDAP entry containing the distinguished name of the referenced group.

Searching Group Objects for Group Membership

The second method for determining a user's group memberships is by searching the group entries on the LDAP server looking for properties that denote that the current user is a member. If your LDAP server does not provide group membership information in its user entries, this is the option you should use if you want to synchronize group memberships between LDAP and MOVEit DMZ.

☒ **Search Group Objects for Membership Information**

This option instructs the system to look for group membership information in the group objects on the LDAP server. This means that each group object should have one property containing the distinguished name of a user object for each user that is a member of the group.

Microsoft Active Directory (AD) Configuration:
Group Object Class: Object class of group records to search; can also take a complete LDAP search query
Example: *group*
Example: *(objectClass=group)*
Group Object Path: Location of group objects
Example: *CN=Builtin,DC=main,DC=mycorp,DC=com*
Group Object Group Membership Field: Name of group object field containing user group memberships
Example: *member*

Group Object Class or LDAP Search String:

Group Object Path:

Group Object Group Membership Field:

There are three settings available under this option. The first is Group Object Class or LDAP Search String and is analogous to the User Object Class or LDAP Search String setting in the Edit LDAP User Settings section. This value should be set to the value of the objectClass property that indicates an LDAP entry is a group. If a more advanced query is necessary, this value can also be set to a complete LDAP query which should return group objects from the directory.

The second setting is Group Object Path. This defines the location in the LDAP directory where MOVEit DMZ should begin searching for group objects. This can be the same as the path provided in the Primary or Backup Server Path settings, or it can be different, in case those paths are set to user-specific locations.

Note: The Group Object Path value should not contain an LDAP host or URL. The host defined by the Primary or Backup Server Path setting will be used.

The third setting is Group Object Group Membership Field and is analogous to the User Object Group Membership Field setting under the Search User Objects for Membership Information option. For each user that is a member of an LDAP group, there should be one of these fields in the group's LDAP entry containing the distinguished name of the referenced user.

The Group Mask determines which groups DMZ should look at when checking LDAP group membership against DMZ group membership. The mask field should be a comma-delimited list of group names.

Group Mask:

☒ Include all groups except...

☐ Ignore all groups except...

The Group Check Mask determines which LDAP groups a user must or must not be a member of in order to be allowed to sign on to the system. The mask field should be a comma-delimited list of group names.

Group Check Mask:

☒ Allow all users regardless of group membership

☐ Deny users in groups except...

☐ Allow users in groups except...

[Change LDAP Group Settings](#)

Finally, the Group Mask settings determine which groups will be included when syncing LDAP and DMZ group memberships. The rule can be set to include groups except those matching one or more of the masks, or ignore groups except those matching one or more of the masks. The mask list can be one or more group name masks, separated by commas. Group name masks may contain the multiple-character wildcard *, and/or the single-character wildcard ?.

The Group Check Mask settings operate similarly to the Group Mask settings, but determine the group memberships used by the system to determine if a user should be allowed to sign on or be automatically created (or mentioned in the Scheduler error reports if the source is configured to not do auto-creation of users in the Scheduler). By default, this setting is set to allow all users regardless of group memberships. The rule can also be set to deny users except those in groups matching one or more of the masks, or to allow users except those in groups matching one or more of the masks. As with the Group Mask setting, the mask list can be one or more group name masks, separated by commas. Group name masks may contain the multiple-character wildcard *, and/or the single-character wildcard ?.

Active Directory "Lookup" Notes

The permission required to see properties of other users varies on each kind of LDAP server. On Active Directory server, the typical permissions required to see these properties are usually awarded to Domain Users. With this in mind, the user credentials you configure in the **Admin Login** fields should be at least a member of this group.

Active Directory Troubleshooting

While debugging authentication problems, the phrase (from the debug log)...

- **Error accessing primary LDAP server: A referral was returned from the server** usually means that the "path part" of the Primary Server Path (e.g. "LDAPS://main.mycorp.com/cn=Users,dc=main,dc=mycorp,dc=com") is not correct. The "host part" is probably correct.
- **Error accessing primary LDAP server: The server is not operational** usually indicates that the hostname or IP address listed in the Primary Server path is not correct, or that an LDAP server is not listening on that address. However, if this authentication source has been configured to use SSL (i.e., Primary Server Path begins ldaps://), this error could also mean that SSL was either not configured or not configured properly on the remote server.
- **AuthenticateByLDAP: Could not locate user 'freduser'** usually means one of two things. If this user is the ONLY user who cannot authenticate to the system, then it is likely that the Active Directory server really does not have a record for this user. However, if this message appears for ALL users, check the preceding line which begins with the phrase "SearchForUsers: filter=". In an Active Directory configuration, this line should look VERY similar to this phrase:

```
"SearchForUsers:  
filter='(&(objectClass=user)(samaccountname=freduser))'"
```

If there is any variation (except the expected username in place of `freduser`), double-check the value you configured for `Username` Field in the LDAP User section.

External Authentication - WS-Trust (Authentication Only)

The WS-Trust (Authentication Only) source lets you use an external Identity Provider (Microsoft Active Directory Federated Services (ADFS)), to authenticate users. Incoming usernames and passwords will be tried against the identity provider. The identity provider must support the WS-Trust protocol (see Requirements below).

The SAML 2.0 support provided by the Single Signon (See **Feature Focus - Single Signon** (on page 87)) allows users to authenticate through an external Identity Provider when using the MOVEit web interface. This model, which relies on the client to authenticate with the Identity Provider in order to create a SAML assertion to be "consumed" by MOVEit, is not available to non-HTTP interfaces. By also supporting the WS-Trust protocol, MOVEit can directly request a secure token in the form of a SAML 2.0 assertion document by including the user's provided username and password in the request. Assuming the same Identity Provider server supports both SAML and WS-Trust authentication, then users can use the same credentials to do both Single Signon through the web interface, and username/password authentication through FTP and SSH clients, or through Windows clients, such as the Ad Hoc Transfer Plug-in for Outlook and MOVEit Sync.

Requirements

To set up an external authentication source using WS-Trust, you need the following:

- An Identity Provider. MOVEit supports the following as the Identity Provider:
 - Microsoft Active Directory Federation Services (ADFS)
- The Identity Provider must support the WS-Trust version 1.3 protocol, and provide at least one username/password binding (a binding that accepts a UsernameToken, or HTTP basic or digest authentication).
- The Identity Provider must be on a host that MOVEit Server can connect to using HTTPS.
- The Security Token Service for communication between MOVEit and the WS-Trust server must be configured before you set up the WS-Trust source. The WS-Trust source requires an existing Identity Provider be configured in the MOVEit Single Signon settings page. The authentication source will be linked to that Identity Provider. If no Identity Provider is configured, you must add and configure one before the WS-Trust authentication source can be added.

Note: If you need to add an Identity Provider, see the Identity Provider section of the *User Authentication - Single Signon* (on page 422) topic.

Setting up the WS-Trust source

- 1 Check that you have met the requirements in the above section.
- 2 Add WS-Trust as an authentication source, as described in the *External Authentication - Overview* (on page 444) topic.
- 3 Configure this authentication method to use the Security Token Service.

Identity providers that support WS-Trust will provide a metadata file or URL that is used to configure the Security Token Service.

Click **Browse** to find and upload the metadata file for the provider; then click **Upload Metadata File**.

Or

Enter a URL for the providers's metadata, then click **Download Metadata File**.

Click **Add New Source** to add this authentication source.

The entry for the WS-Trust authentication source is created and added to list of sources on the Settings (Security) page.

- 4 To complete the setup, in the list of authentication sources, click **Edit** next to your WS-Trust source. The Edit Authentication Source page opens.
- 5 Make sure **Enabled** is set to **Yes**.
- 6 Make sure the Security Token Service endpoint is set to the appropriate location.
- 7 Edit user and group settings as appropriate.

These settings determine how the user information is added within MOVEit. By default, the authentication source is set to automatically create a user on signon. To change any of these settings, click **Edit Identity Provider Settings**.

Note: The WS-Trust authentication source shares its user and group settings with the linked Identity Provider.

The **Full Name Attribute**, and **Email Attribute** template settings determine what values will be used for the new user's full name, and email address fields if they are added to the MOVEit user account.

Auto Create User on Signon: By default, when a new user successfully signs on, an account will be created in MOVEit. If you want to disable it, click **False**.

Group membership behavior: This setting determines how group memberships will be dealt with. When set to **Ignore Differences**, identity provider group memberships will be ignored. When set to **Report Differences**, differences between MOVEit group memberships and identity provider group memberships will be reported in the log. When set to **Correct Differences**, differences between MOVEit group memberships and identity provider group memberships will be corrected, if possible. MOVEit groups will NOT be added automatically, only group memberships. Groups existing on the identity provider but not on the MOVEit server will be noted as errors.

Group membership attribute: Select from the list of object properties to set the name of the group, if a group exists on the identity provider.

8 Save any changes. You are now ready to use WS-Trust authentication.

Security Policies - User Settings

Folder Quotas

This section allows an administrator to edit the default user folder quota setting for the organization.

Edit Default User Folder Quotas...

User folder quotas apply to end users only, and encompass all file uploads a given user has made to the system (not including packages and attachments). Set the value to 0 to apply no quota.

Default User Folder Quota: ☒ KB ☐ MB

Change Default User Folder Quotas

Edit Folder Quota Warning Settings...

Folder quota warnings will be displayed to users when they get near their folder quota limit. The following settings define what "near" is. You may elect to warn users when usage is...

Folder Quota Warning Type:

Folder Quota Warning Value:

Change Folder Quota Warning Settings

User folder quotas may be added in kilobytes and megabytes and apply to all files a given user has uploaded to the system. Folder quota warning settings may also be edited here. Folder quota warning settings are shared with per-folder quotas.

Default Folder

This section allows an administrator to edit the default user chroot default folder setting for the organization.

Edit Default User Default Folder Settings...

When enabled, this setting causes FTPS and SFTP sessions to treat the user's default folder as the root of the folder tree.

☐ **Default Chroot Default Folder**

Change Default User Default Folder Settings

Users with this option enabled will see their default folder as their root folder when logging on from the FTPS and SFTP interfaces. The configured value will be applied to all new users, and an option will be given to apply the new setting to existing users as well.

Security Policies - Group

Default Permissions

The group policy permissions define the default settings for groups added to this organization. When changed, the new settings can also be applied to existing groups.

GroupAdmin Policy Settings

These settings define the default GroupAdmin settings for groups in this organization.

Edit GroupAdmin Policy Settings...

By default, GroupAdmins of groups may:

- ☐ Change the logo and announcement for their groups
- ☒ Add new users as group members and edit/delete existing group members
- ☐ List all users in the organization and add existing users as group members
- ☒ Change passwords of existing group members
- ☐ Enjoy following permissions on member home folders:
Read Write Delete List Notify Subs Admin
☐ ☐ ☐ ☐ ☐ ☐ ☒
- ☒ List and edit temporary users added by group members

Set a member's file quota to any value up to:

Set a member's ad hoc transfer quota to any value up to:

Set a member's per-package attachment quota to any value up to:

Change Default GroupAdmin Settings

Available policy settings include:

- Change the logo and announcement for this group: Determines whether GroupAdmins will have the ability to change the logo and announcement for their groups. If this option is enabled, GroupAdmins will be able to view the profile pages for their groups and will have access to the Edit Logo and Edit Announcement sections.
- Add new users as group members and edit/delete existing group members: Determines whether GroupAdmins will have the ability to add, delete and modify details about the end user members of their groups. If this option, or the Change Passwords of Existing Group Members option is enabled, GroupAdmins will be able to change the security status of end user group members as well.
- List all users in the organization and add existing users as group members: Determines whether GroupAdmins will be able to list all end users in the organization, and add those users to their groups, thereby gaining any administrative authority they are granted by the group over those users.
- Change passwords of existing group members: Determines whether GroupAdmins will have the ability to change passwords of the end user members of their groups. If this option, or the Edit/Delete Existing Group Members option is enabled, GroupAdmins will be able to change the security status of end user group members as well.
- Change permissions on member home folders: Determines whether GroupAdmins enjoy ADMIN permissions to the home folders of end user members of their groups.
- List and edit temporary users added by group members: Determines whether GroupAdmins will have administrative access to Limited Members of their groups. Temporary users created by group members are automatically assigned to their groups as Limited Members. This option should be enabled if you want GroupAdmins to be able to see and control who the group's full time end users are communicating with.
- Set a member's file quota to any value up to: Used to set a limit to how high GroupAdmins can set the user quotas for individual end user members of their groups. For example, if this value is set to 50 MB, a GroupAdmin may set an individual user quota to 1 MB or 25 MB but not 60 MB. A value of 0 KB or 0 MB indicates there is no restriction on the GroupAdmin's ability to set end user member file quotas in effect.
- Set a member's total package attachment quota to any value up to: Used to set a limit on how high Group Admins can set the user Package Quota setting for individual end user members of their groups. For example, if this value is set to 50 MB, a GroupAdmin may set an individual user quota to 10 MB or 20 MB but not 60 MB. A value of 0 KB or 0 MB indicates there is no restriction on the GroupAdmin's ability to set end user member package quotas in effect.
- Set a member's per package attachment quota to any value up to: Used to set a limit on how high Group Admins can set the user Per Package Quota setting for individual end user members of their groups. For example, if this value is set to 5 MB, a GroupAdmin may set an individual user maximum attachment size to 1 MB or 2 MB but not 6 MB. A value of 0 KB or 0 MB indicates there is no restriction on the GroupAdmin's ability to set end user member attachment quotas in effect.

Group Member Policy Settings

These settings define the default member settings for groups in this organization.

Edit Group Member Policy Settings...

By default, members of groups may:

- ☒ See limited members in their address book (if allowed to see individual group members)

[Change Default Member Settings](#)

See limited members in their address book: Determines whether Limited Members will show up in address books of end user group members who have groups in their address book with the Messages to Individual Members option enabled.

Security Policies - Remote Access

Default Rules

The remote access policy defines the list of IP addresses and/or hostnames from which users and administrators may access this organization.

Registered access settings may be applied to **users** or **administrators**. The **administrators** designation includes FileAdmins and Admins. The **users** designation includes Users and TempUsers. **WebPost** rules apply to anonymous users who submit webposts into the MOVEit DMZ system but never actually sign on.

Registered access for SysAdmins is configured in the Remote Access section of the **System Settings**. (For more information, see **Web Interface - Settings - Ad Hoc Transfer - Access - Unregistered Senders** (on page 505) > Unregistered Sender Remote Access Rules).

These settings may also be overridden by custom IP/hostname rules for particular users. (Some organizations will want to leave these default settings blank and **ONLY** allow specific IP access for each user.)

By default, administrators and users may only sign on from the local console. This is why there is a reminder on the home page of administrators to increase this access when the default values are set, and it is also why SysAdmins are given the chance to expand the range of allowed addresses during the creation of a new organization. Also by default, anonymous WebPost users may submit information to MOVEit DMZ, but may not create new WebPost folders.

Note: MOVEit DMZ does not support remote access from IPv6 addresses (clients). To avoid any connection problems, we recommend that you disable IPv6 addresses on the MOVEit DMZ server. To disable IPv6, in Windows, open the Local Area Connection Properties for the network interface card, and make sure the Internet Protocol Version 6 (TCP/IPv6) property is not selected.

In addition to the access rules for hosts, you can specify a list of trusted hosts for an organization. A host in the **Trusted Hosts** list will bypass the normal IP lockout and session IP consistency checks. In effect, when a user signs on to the organization from a trusted host, it works like signing on from the localhost. For more information, see the Trusted Hosts section of this document.

Administrator and FileAdmin Remote Access Rules

Rule	Hostname/IP	Comment
Allow	(All IPs)	
Allow	192.168.3.1	
Edit Access Rules		

User Remote Access Rules

Rule	Hostname/IP	Comment
Allow	(All IPs)	
Edit Access Rules		

Webpost Remote Access Rules

Rule	Hostname/IP	Comment
Allow (add folders)	192.168.3.162	
Allow (add folders)	(All IPs)	
Allow (add folders)	192.168.3.160	
Edit Access Rules		

The Remote Access rule list is made up of 3 sections:

- **Administrator and FileAdmin Remote Access Rules:** An access list which controls from which IP addresses or hostnames Administrators or FileAdmins may connect by default.
- **User Remote Access Rules:** An access list which controls from which IP addresses or hostnames end users may connect by default.
- **Webpost Remote Access Rules:** An access list which controls from which IP addresses or hostnames anonymous users may POST webposts from and/or ADD FOLDERS from. (New webpost folders can be automatically added if a new type of form begins submitting web information - see the WebPost help section for more information.)

Note: See also the **Unregistered Senders Remote Access Rules** (on page 505), located on the **Unregistered Senders** (on page 505) page.

Each section contains all current rules. At runtime, the rules will be processed in the top-to-bottom order displayed here.

There are several columns for each rule as follows:

- **Rule:** Whether the rule allows or denies access.
- **Hostname/IP:** The IP address or hostname of each rule.
- **Comment:** Any hint or notes the administrator wants to provide. Anything typed here is informational only and does not affect any other part of the rule.

In addition, an **Edit Access Rules** button for each section (below the last rule of the section) opens a separate page for each section, that is, one page each for Administrator and FileAdmin Remote Access Rules, User Remote Access Rules, and Webpost Remote Access Rules.

Separate Edit Access Rules Pages for Each Section

Clicking **Edit Access Rules** for any section of rules opens a separate page for that section. There are separate pages for Administrator and FileAdmin Remote Access Rules (shown below), User Remote Access Rules, and Webpost Remote Access Rules.

On each of these pages, administrators can move, edit, or delete a rule by using the buttons to the right of the rule.



Buttons and links appear for the various actions which may be performed on each rule.

- **Arrow buttons:** Move the rule up and down in the priority list - rules at the top of the list are processed first. (These buttons appear only when there are two or more rules.)
- **Edit:** Allows administrators to change details about the rule; opens the Edit Remote Access Rule page.
- **Delete:** Completely removes the rule from the access list.

In addition, the Add Remote Access Rule link (below the last rule) opens the Add Remote Access Rule page, where new rules can be added.

Add Remote Access Rule and Edit Remote Access Rule Pages

Add Remote Access Rule...
Enter a new remote access rule below and then click the Add Entry button. The Hostname/IP field can contain either a hostname or an IP address. Both types can contain wildcard characters, and IP addresses can also be in the form of a range. (e.g. 11.22.33.44, 11.22.33.*, 11.22.33.44-55, jsmith.mycompany.com, *.mycompany.com)

Rule	Hostname/IP	Priority
Allow ▾		Highest ▾
Comment (Optional) 		
Add Entry		

Note: The Add Remote Access Rule page (opened by the Add Remote Access Rule button) and the Edit Access Rule page (opened by the Edit button) are the same except that the Edit page is filled with existing values for the selected rule.

The fields here define a Hostname/IP address or range combination and whether it will be allowed or denied. The individual rule can be assigned a priority for applying it in combination with other access rules. For a new rule, fill out the fields to create a new remote access rule and then click the Add Entry button. Similarly, for an existing rule, change fields and then click the Update Entry button.

The fields and buttons on this page are:

- **Rule:** Values you can select are Allow or Deny.
- **Hostname/IP:** Text entry field for a hostname or an IP address. Both types can contain wildcard characters, and IP addresses can also be in the form of a range. Examples are jsmith.mycompany.com, *.mycompany.com, 11.22.33.44, 11.22.33.*, and 11.22.33.44-55.
- **Priority:** (Shown for the Add... page only, not Edit...) To specify initial placement in the list (whether at the top, bottom, or in middle). Values you can select are Highest, Middle, or Lowest.
- **Comment (Optional):** Text entry field.
- **Add Entry / Update Entry:** Click this button to close this page and add the new rule to - or update the existing rule on - the rules list.

Hostname/IP Masks

Hostname/IP entries can be individual hostnames, individual numeric IP addresses, or masks that allow matching against a range of hostnames or addresses. An asterisk (*) will match any value in a particular position. For example, 2* matches 23 or 213, *cat matches tomcat and bobcat and * matches all of the above.

A dash (-) will match numeric values which fall on or between the numbers on either side of the dash. For example, 2-4 matches 2, 3 and 4 but not 1 or 5.

Allow/Deny Decisions

When an incoming IP address or hostname is tested, rules are processed top-to-bottom. The first rule which applies to the incoming IP or hostname is the rule which actually allows or denies access.

By default, all IP addresses and hostnames are denied if they fall off the end of the list.

Specific IP addresses and hostnames (e.g. 192.168.3.4 or test.stdnet.com) should be at the top. Ranges of IP addresses and hostnames (e.g. 192.168.3.* or *.stdnet.com) should be in the middle. Catch-all entries (e.g. 192.*.*.* or *.edu) should be at the bottom.

Example

Given the following access list...

Allow/Deny	IP Address or Hostname
ALLOW	192.168.3.24
ALLOW	test.stdnet.com
ALLOW	192.168.4.*
ALLOW	*.bed.stdnet.com
DENY	192.168.5.1-64
ALLOW	192.168.5.*

...the following addresses will be allowed or denied access:

Incoming Address	Allowed	Reason
192.168.3.24	YES	Matches "ALLOW 192.168.3.24"
test.stdnet.com	YES	Matches "ALLOW test.stdnet.com"
192.168.4.21	YES	Matches "ALLOW 192.168.4.*"
feather.bed.stdnet.com	YES	Matches "ALLOW *.bed.stdnet.com"
192.168.5.21	NO	Matches "DENY 192.168.5.1-64"
192.168.5.121	YES	Matches "ALLOW 192.168.5.*"
192.168.6.34	NO	Does Not Match Any Entry

Console Connections

When a user signs onto the MOVEit DMZ server from a web browser running on the same machine as the MOVEit DMZ server itself, that user is said to be connected to the console if he or she connects to MOVEit DMZ using a URL which begins with `http://localhost...` or `http://127.0.0.1...` rather than the usual `http://MOVEitDMZ.nowhere.com...` URL.

These console connections are NOT subject to the remote access List. This exception prevents SysAdmins from locking themselves out with an empty Access List because they can always sign on from the same machine on which MOVEit DMZ runs. To prevent unauthorized access to MOVEit DMZ through the console, extra care should be taken to secure Windows users on MOVEit DMZ and the physical security of the server itself.

Trusted Hosts

This feature lets Org admins designate a host as a trusted host for their Organization, allowing the host the same privileges as local interfaces.

Under normal operations, clients that access MOVEit DMZ from any of the local interfaces will bypass the normal IP lockout and session IP consistency checks. This allows services like the MOVEit DMZ FTP server and the MOVEit DMZ SSH server to function properly, and present the client's IP address for display and logging purposes. A trusted host will also bypass these checks.



Hostname/IP	Comment
192.168.3.1	
192.168.3.162	

Edit Access Rules

This feature can be used in the following situations:

- To allow machine requests from a Trusted Host to supply an IP address as the effective IP address for machine transactions. (This is the <IPADDRESS> XML element in the MOVEit DMZ API). This feature is most often used when using MOVEit DMZ API within a separate web application to provide single-signon access to MOVEit DMZ. It allows the API session to be transferred to the client browser, and back again, and also allows API to present the client's IP address for display and logging purposes.
- To allow MOVEit to redirect to a Trusted Host after completing a non-wizard upload.
- To allow users to sign on from a Trusted Host regardless of other permissions and/or IP lockouts set for that host.

If someone is continually trying and failing to signon as an existing user, the originating IP address may be locked out. Trusted Hosts can be used to override the lockout behavior. The Trusted Hosts entries associated with the user's organization are consulted and if the client's IP address matches a trusted host, that IP address will not be locked out. If the failed attempts are being made as a user that doesn't exist, and no organization is specified, the Trusted Hosts entries for the default organization will be consulted.

- To allow users to change IP addresses within a session if the old or new IP address is trusted, regardless of the IP switching mask.

Note: Trusted Hosts will avoid many of the standard security safeguards built into MOVEit DMZ to prevent unauthorized access (though clients connecting through such hosts will not). NEVER ADD A HOST TO THIS LIST UNLESS YOU KNOW WHAT YOU ARE DOING! If you are uncertain as to whether a host should be added to this list, feel free to contact **Ipswitch MOVEit support** (<mailto:moveitsupport@ipswitch.com>) for assistance. Also, for security reasons, the All IPs mask of *.*.*.* will not be allowed as a Trusted Host entry.

To add an entry to the Trusted Hosts list:

- 1 Under Trusted Hosts, click **Edit Access Rules**.
- 2 Click **Add Remote Access Rule**.
- 3 Enter a hostname or IP address and optionally, a comment or description, then click **Add Entry**.

The **Hostname/IP** field can contain either a hostname or an IP address. Both types can contain wildcard characters, and IP addresses can also be in the form of a range. For example: 11.22.33.44, 11.22.33.*, 11.22.33.44-55, jsmith.mycompany.com, *.mycompany.com.

Note: Hostnames and IP addresses are not interchangeable. If myhost1 resolves to 192.168.1.200, and the list contains myhost1 but not 192.168.1.200, then users can access the host via URLs starting with https://myhost1 but not via URLs starting with https://192.168.1.200.

After you add the entry, it is shown in the list of allowed hosts.

- 4 You can return to the Trusted Hosts list and the entry will also be shown there.

To move a host entry:

Use the **Arrow** buttons to move the entry up and down in the priority list - entries at the top of the list are processed first. (These buttons appear only when there are two or more entries.)

To edit a host entry:

Locate the entry in the list of allowed hosts and click the **Edit** button and enter any changes.

To delete a host entry:

Locate the entry in the list of allowed hosts. Next to the entry, select **Delete**, then select **Yes** to confirm the deletion.

IP Lockouts

When an IP address is locked out, it is locked out across all organizations at a particular site. Any Admin may unlock an IP address, and IPs may be unlocked one at a time, or all at once with the **Unlock All IP Addresses** link. Once an IP address is unlocked it is unlocked for all organizations. Also, whenever an IP address is locked out, all SysAdmin users who have their notification property set to On+Admin will receive an email notification that the lockout has occurred. If there is only one non-system organization configured, Admin users in that org who have their notification property set to On+Admin will also receive email notifications.

Locked Out IP Addresses	
IP Address (Hostname)	Comment
192.168.197.160 (doc-marktwain.ftqa.com)	Locked out on 4/10/2014 4:35:24 PM using LoginName frank
Unlock All IP Addresses...	

Only SysAdmins may set IP Lockout Policy. (See the **IP Lockout Policy section** (on page 536) of the System Remote Access Policy page for more information). Starting in version 4.0, IP lockouts are enabled by default and set to lock out IP addresses after 15 bad attempts in any 5 minute period.

After you unlock an IP address, the user who triggered the IP lockout will still be locked and inactive. You can change the user's Account Status in the User Profile.

IP Switching

To prevent session hijacking, MOVEit DMZ normally does not allow the IP address used by a session to change over the course of that session. However, some firewalls and proxy servers use pools of IP addresses to assign to users who access the internet, and can sometimes assign different IP addresses to a user even within a single session. In order to allow these users full access to the server, the IP Switching feature allows administrators to set an allowable range within which a session IP address can change.



Edit IP Address Switching Mask...

The IP Address Switching Mask defines how much leeway the server gives to signed-on users to change their IP addresses during an active session. Normally MOVEit DMZ does not allow IP addresses to change at all during a session, as this can indicate a possible session hijacking. However, some firewalls and proxy servers use pools of IP addresses to assign to users who access the internet, and can sometimes assign different IP addresses to a user even within a single session.

IP Address Switching Mask: ▼

[Change IP Address Switching Mask](#)

By default, the IP Switching option is set to **None**, which corresponds to a subnet mask of 255.255.255.255, or /32. This prevents any sort of IP address switching. Other available values are:

- **Class C (255.255.255.0 or /24):** Allows the session IP address to vary within the Class C portion of the address. For example, if the original session IP address was 1.1.1.1, switching to 1.1.1.2 would be allowed, but switching to 1.1.2.2 would not.
- **Class B (255.255.0.0 or /16):** Allows the session IP address to vary within the Class B portion of the address. For example, if the original session IP address was 1.1.1.1, switching to 1.1.2.2 would be allowed, but switching to 1.2.2.2 would not.
- **Class A (255.0.0.0 or /8):** Allows the session IP address to vary within the Class A portion of the address. For example, if the original session IP address was 1.1.1.1, switching to 1.2.2.2 would be allowed, but switching to 2.2.2.2 would not.
- **All (0.0.0.0 or /0):** Allows all IP address switching.

Security Policies - Interface

These pages allows administrators to set the default policies - regarding HTTP, FTP, SSH, and Mobile interfaces - for all new users on the in the organization. Changes to the policies on these pages will be given the option of also being applied to all existing users in the organization. Policies set here can be changed per user in the **User Profile (User Authentication section)** (on page 286).

Note: For all of these interfaces, if you plan on using different interface policies for different groups of users, you may want to explore the various **create users as a clone of...** options available in MOVEit DMZ. For example, you may want all your users except those using External Authentication (EA) to present a certificate during the authentication process. To accomplish this, set the organization's default interface values to require client certs and set the EA source to clone a template user that does not require client cert authentication during new EA user creation.

HTTP

This page allows administrators to set the default HTTP interface policy for all new users in the organization. Changes to the policy on this page will be given the option of also being applied to all existing users in the organization. The policy options available are:

- **Allow HTTPS Access via Web Interface by Default:** Determines whether users will be allowed to access the system via web browsers.
- **Allow HTTPS Access via HTTP Clients by Default:** Determines whether users will be allowed to access the system via other HTTP clients, such as MOVEit Central, MOVEit DMZ API and the MOVEit Wizard.
- **SSL Client Cert Required by Default:** Determines whether users signing on to the HTTPS interface will be required to present a valid SSL client certificate in order to authenticate to the system.

Note: For SAML Single Signon users, the SSL Client Required option must be set to **No**.

- Password Also Required with SSL Client Cert by Default: Determines whether users who sign on to the HTTPS interface with a valid SSL client certificate will also be required to submit a valid password in order to authenticate to the system.
- Match Cert CN to Username/Full Name: When enabled, SSL client certificate that have a CN value that matches the username or full name of the incoming user AND is signed by a Certificate Authority trusted by the system will be considered valid and acceptable for authentication purposes.
- Allow Username from Client Certificate: When enabled, users will be given the option on the signon page to have MOVEit DMZ automatically determine their username from their client certificate and attempt to sign them on. DMZ will first search its internal certificate store for a matching certificate, then if possible it will search properly configured LDAP external authentication sources. If a matching certificate is found, the associated username is assumed and a signon is attempted. If a matching certificate is not found, or the user requires a password in addition to the client certificate, they will be returned to the signon page with a message indicating the need for further credentials.
- If a matching client certificate is found, and the user is successfully signed on with the associated username, a long-term cookie will be set which will allow DMZ to automatically forward them to the username autodetection routines in the future. Thus, the user will always log directly on to the system whenever they bring up the web site, as long as their client certificate is provided and is still valid.

FTP

This page allows administrators to set the default FTP interface policy for all new users in the organization. Changes to the policy on this page will be given the option of also being applied to all existing users in the organization. The policy options available are:

- Allow FTP/SSL Access by Default: Determines whether users will be allowed to access the system via secure FTP over SSL.
- Allow Insecure FTP Access by Default: Determines whether users will be allowed to access the system via insecure plain-text FTP. Requires Non-Secure FTP to be enabled and allowed for the IP addresses for each user. See the **FTP Configuration** (on page 577) doc page for more information.
- SSL Client Cert Required by Default: Determines whether users signing on to the FTP over SSL interface will be required to present a valid SSL client certificate in order to authenticate to the system.
- Password Also Required with SSL Client Cert by Default: Determines whether users who sign on to the FTP over SSL interface with a valid SSL client certificate will also be required to submit a valid password in order to authenticate to the system.
- Match Cert CN to Username/Full Name: When enabled, SSL client certificate that have a CN value that matches the username or full name of the incoming user AND is signed by a Certificate Authority trusted by the system will be considered valid and acceptable for authentication purposes.
- Holding Tank retention: Determines how long SSL client certificates and SSH client keys entered into the cert/key holding tank will be allowed to remain there. Certs or keys older than this number of days will be removed from the holding tank.

Management of trusted Certificate Authorities (CAs) and user holding tank certificates is also performed here. For more information on trusted CAs, see the ***System Configuration - SSL and SSH - SSL - Client Certs - Trusted CAs*** (on page 235) document page. For more information on the SSL client certificate holding tank, see the ***System Configuration - SSL and SSH - SSL - Client Certs - Holding Tank*** (on page 231) document page.

Client Certificates

All client certs are either "self-signed" or "CA-signed". The "CA-" indicates that a "Certificate Authority" has signed the client cert and vouches for the identity of the bearer. Furthermore, CAs are divided into "commercial CAs" that sell client cert issue and signing services to the general public (e.g., Thawte, GeoTrust, etc.) and "corporate CAs" that perform the same client cert functions for their own users.

MOVEit supports self-signed certs, commercial CA-signed certs and corporate CA-signed certs. A client cert may be delivered as a "*.pfx" file with a password or users may need to request it may need to request a cert from a CA.

Various browsers have different ways to install client certs. Internet Explorer (IE) uses the Windows Certificate Store; you can install and manage client certs through IE's "Certificate" dialog. Windows will also launch a client cert import wizard that will automatically install most client certs into IE if you just double-click "*.pfx" client cert file.

The Mozilla/Firefox line of browsers uses its own client cert store. To install client certs in these browsers you must use their "Certificate Manager".

Various browsers also have different ways to select client certs for authentication. The most common way is for the browser to simply ask you (via a pop-up dialog) about which client cert to use. When connecting to a MOVEit server, users may be prompted through their browsers to select a client cert after they fill in their username and password or before they view the sign on screen.

However, most browsers also have options to automatically present a client cert if only one is installed or not ask about picking a client cert if one was not presented. In these cases client cert authentication may be being used behind the scenes (in the "one cert, so don't ask" case) or not at all (in the "no certs installed, so don't ask" case).

Finally, the private key on a user's client cert may be password protected. If this is the case users may need to type in the password they created when they opted to protect this client cert or key store as well. (Usually, such prompting takes place once per session.)

SSH

This page allows administrators to set the default SSH interface policy for all new users in the organization. Changes to the policy on this page will be given the option of also being applied to all existing users in the organization. The policy options available are:

- **Allow SSH Access by Default:** Determines whether users will be allowed to access the system via SSH.
- **SSH Key Required by Default:** Determines whether users signing on to the SSH interface will be required to present a valid SSH client key in order to authenticate to the system.
- **Password also required with valid SSH Key by Default:** Determines whether users who sign on to the SSH interface with a valid SSH client key will also be required to submit a valid password in order to authenticate to the system.
- **Holding Tank retention:** Determines how long SSL client certificates and SSH client keys entered into the cert/key holding tank will be allowed to remain there. Certs or keys older than this number of days will be removed from the holding tank.

Management of user holding tank keys is also performed here. For more information on the SSH client key holding tank, see the **SSH Keys Holding Tank** (on page 259) document page.

Mobile

This page allows administrators to set the default Mobile interface policy for all new users in the organization. Changes to the policy on this page will be given the option of also being applied to all existing users in the organization. Policies set here can be changed per user in the **User Profile (User Authentication section)** (on page 286).sys

The policy options available are:

- **Allow access to the Mobile interface by default:** Determines whether users will be allowed to sign on to MOVEit by using the Mobile app or web.

Note: Ipswitch suggests that for security reasons you do not allow mobile access to admins, fileadmins or users that are used for bulk data transfers such as nightly FTPS/SFTP transfers.

- **Allow caching of credentials on mobile devices:** This determines whether mobile app users will be allowed to cache credentials on the device for quick sign-on using a PIN.
- **Required PIN length:** This specifies the minimum digits required for the PIN. Choose 4, 5, or 6 digits.

Note: The app always requires that users do not repeat or simply increment numbers when creating the PIN. For example, the app will not allow 1111 or 12345 as a PIN.

Security Policies - Folder

Permissions

This section controls default home folder permissions assigned to users.

Home Folder Permissions

When users sign on, the following permissions control their default permissions to their home folders. These default permissions can be added to or overridden by more specific permissions set on individual users' home folders.

User	Read	Write	Delete	List	Notify	Subs	Admin
(Home Folder Owner)	☒	☒	☒	☒	☒	☐	☐

The selected permissions will be implicitly given to a user for their first-level home folder. They will NOT be implicitly given to the user for any subfolders of their home folder.

Note: If all permissions are removed here, users will NOT be able to upload to, download from, or even see their home folder unless explicit permissions are added.

Quotas

This section allows the admin to edit the warning settings for folder quotas (actual folder quotas are determined on a per-folder basis). When a folder gets close to its file quota, a warning message may be displayed on that folder's file list page depending on the settings here. There are four settings available for quota warnings:

No Quota Warnings: No quota warnings are displayed.

...greater than given percentage of quota: When the amount of space used in the folder reaches the given percentage of the quota value, a warning is displayed. The given percentage is specified by the Quota Warning Value field.

...within given kilobytes of quota: When the amount of space used in the folder gets within the given number of kilobytes of the quota value, a warning is displayed. The given number of kilobytes is specified by the Quota Warning Value field.

...within given megabytes of quota: When the amount of space used in the folder gets within the given number of megabytes of the quota value, a warning is displayed. The given number of megabytes is specified by the Quota Warning Value field.

Copy/Move

This section allows the admin to edit the default Copy/Move settings for the organization. The one setting in this section determines the default value for the uploader information option provided when copying or moving a file in DMZ. The option allows the copying/moving user to insert their information as the uploader of the file, or leave the original uploader information.

Hint: Many more folder properties are configured through the **Folder Settings** links available from each folder.

Content Scanning - Anti-virus

System administrators enable Content Scanning at the system level. They may define various scanners but enable only one anti-virus (AV) and/or data loss prevention (DLP) scanner per system. Organization Administrators may disable a currently configured anti-virus scanner at the organization level. This page allows administrative users to enable or disable scanning for viruses for this organization.

For more information, refer to the topic ***Feature Focus - Content Scanning*** (on page 97).

Edit Anti-Virus Settings...

If an anti-virus scanner is configured for the system, these settings will control how it is used for this Organization.

Enable for this Organization:

☒ Enabled ☐ Disabled

Action on server error:

☒ Block Content ☐ Allow Content and Log

Change Anti-Virus Settings

Edit Anti-Virus Settings

- **Enable for this Organization:** Select *Yes* to enable virus scanning or *No* to disable virus scanning for the organization.
- **Action on Server Error:** Select *Block* to terminate transmission and return a violation if the ICAP connection times out or fails in some other way, or *Allow Content and Log* to allow transmission, but log a violation.

Important: When you configure scanning for both AV and DLP, MOVEit DMZ sends the data to both processes simultaneously. When the scanner reports a virus or a DLP policy violation that is configured in MOVEit to block the transmission, the transmission fails.

Content Scanning - Data Loss Prevention (DLP)

System administrators enable Content Scanning at the system level. They may define various scanners but enable only one anti-virus (AV) and/or data loss prevention (DLP) scanner per system. Organization Administrators may disable a currently configured DLP scanner at the organization level. This page allows administrative users to do the following:

- Enable or disable scanning for DLP policy violations for this organization
- Create sets of rules called rulesets that apply actions when data submitted to a DLP scanner violate specific DLP policies configured for the scanner

Note: User classes may not be assigned to user groups.

- Assign rulesets to user classes

Note: To assign rulesets to a user, you do so within the User Profile page for User Settings.

For more information about how to use these settings, refer to the topic ***Feature Focus - Content Scanning*** (on page 97).

Settings (Security)

Edit Data Loss Prevention (DLP) Settings...

If a DLP scanner is configured for the system, these settings will control how it is used for this Organization.

Enable for this Organization:

☒ Enabled ☐ Disabled

Action on server error:

☒ Block Content ☐ Allow Content and Log

Change DLP Settings

Edit User Class DLP Rulesets...

Assign DLP Rulesets to user classes, which will act as defaults for newly created users. You will also be prompted to apply changes to

Administrators:	Personal Data_Allow	▼	Change
File Admins:	Personal Data_Quarantine	▼	Change
Users:	Personal Data_Block	▼	Change
Temp/Guest Users:	Personal Data_Block	▼	Change

Configure DLP Rulesets...

You may add and/or edit your DLP Rulesets below.

Name

Personal Data_Quarantine
Personal Data_Block
Personal Data_Allow
CCN Policy Violation

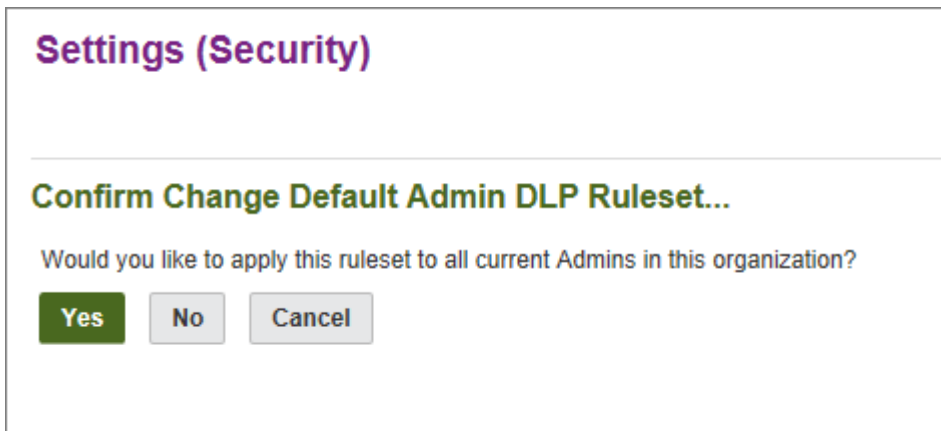
Edit Data Loss Prevention (DLP) Settings

- **Enable for this Organization:** Select *Yes* to enable DLP scanning or *No* to disable DLP scanning for the organization.
- **Action on Server Error:** Select *Block* to terminate transmission and return a violation if the ICAP connection times out or fails in some other way, or *Allow Content and Log* to allow transmission, but log a violation.

Edit User Class DLP Rulesets

After you have configured rulesets, you can select one to apply to a user class: *Administrators*, *File Admins*, *Users* or *Temp/Guest Users*.

- **Ruleset:** From the drop-down list select any previously defined ruleset. The default selection *-none-* does not filter the data for violations since it applies no rules. The selection is then applied to any new users configured for that class.
- **Change Ruleset:** Applies the ruleset to all currently configured users in that user class. Click *Yes* to the prompt to confirm.



Configure DLP Rulesets

In order to use DLP scanning, you must define rulesets and apply them to user classes or users.

- **Name:** Name of existing ruleset. The Edit button  allows you to change the ruleset. The Delete button  allows you to delete a defined ruleset.
- **Add DLP Ruleset:** Displays the Add DLP Ruleset page.

Add DLP Ruleset

The Add DLP Ruleset page allows you to define a ruleset.

Add DLP Ruleset...

DLP Rulesets determine how DMZ handles files that violate one or more DLP server policies. They can be applied at the user-class level, or at the user level.

Name:

Description:

Default Action:

- ☒ **Block** - Transfer will not be allowed.
- ☐ **Quarantine** - Upload will be allowed, but Download will not be allowed. Files will be tagged, and an audit log entry will be recorded indicating that the file violates one or more DLP policies. Files may be untagged later, at which point normal permissions will take effect.
- ☐ **Allow** - Transfer will be allowed, and files will be tagged. An audit log entry will be recorded indicating that the file violates one or more DLP policies.

- **Name:** Name of the ruleset.
- **Description:** Description for a Ruleset.
- **Default Action:** Action to invoke when one or more violations are found in the data by the DLP scanner, but none of the rules in the ruleset match the violations reported to MOVEit:
 - **Block:** Terminates transmission.
 - **Quarantine:** Upload will be allowed, but Download will not be allowed. Files will be tagged, and an audit log entry will be recorded indicating that the file violates one or more DLP policies. Files may be untagged later, at which point normal permissions will take effect.

- **Allow:** Transfer (upload and download) will be allowed, and files will be tagged. An audit log entry will be recorded indicating that the file violates one or more DLP policies.
- **Add Ruleset:** Displays the *Edit DLP Rules* section so you can specify one or more matches against DLP policies that will be applied.

Edit DLP Rules

The Edit DLP Rules section allows you to specify one or more matching criteria for policies that belong to this ruleset.

Edit DLP Rules

DLP Rules define the action MOVEit DMZ will take for a specific DLP policy or set of matching policies.

Policy Mask	Policy Action	Comment
No DLP Rules have been configured		

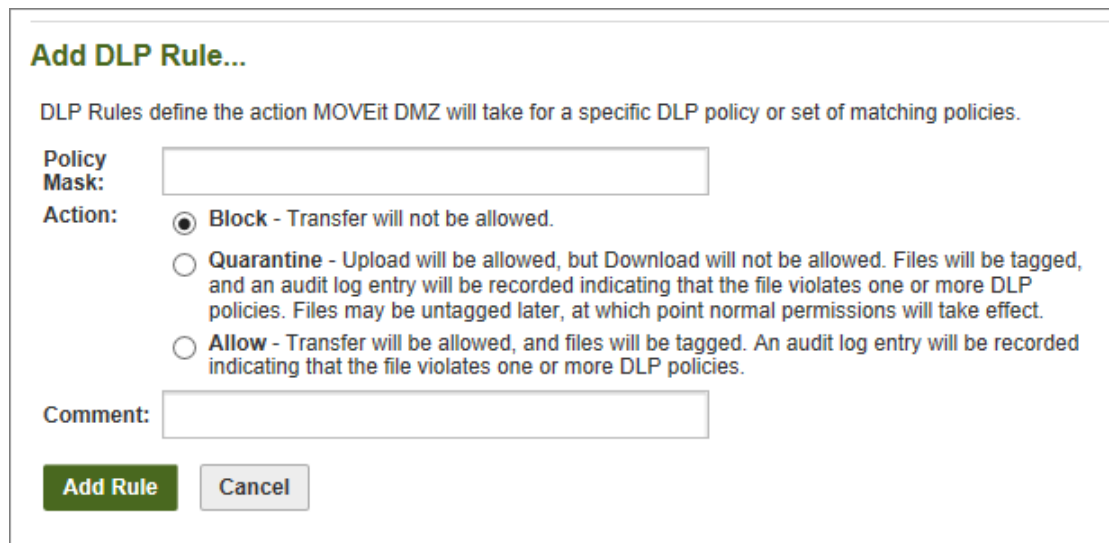
Add DLP Rule...

- **Policy Mask:** Values entered that MOVEit uses when it scans the information returned from the DLP scanner to determine if there was a policy violation.
- **Policy Action:** Action to take if there is a violation of the policy.
 - **Block:** Terminates transmission.
 - **Quarantine:** Upload will be allowed, but Download will not be allowed. Files will be tagged, and an audit log entry will be recorded indicating that the file violates one or more DLP policies. Files may be untagged later, at which point normal permissions will take effect.
 - **Allow:** Transfer (upload and download) will be allowed, and files will be tagged. An audit log entry will be recorded indicating that the file violates one or more DLP policies.

- **Comment:** Information pertinent to this particular policy mask.
- **Add DLP Rule:** Displays the Add DLP Rule page to enter a DLP rule.

Add/Edit DLP Rule

The Add/Edit DLP Rule page allows you to specify the mask and action for a DLP policy.



Add DLP Rule...

DLP Rules define the action MOVEit DMZ will take for a specific DLP policy or set of matching policies.

Policy Mask:

Action:

- ☒ **Block** - Transfer will not be allowed.
- ☐ **Quarantine** - Upload will be allowed, but Download will not be allowed. Files will be tagged, and an audit log entry will be recorded indicating that the file violates one or more DLP policies. Files may be untagged later, at which point normal permissions will take effect.
- ☐ **Allow** - Transfer will be allowed, and files will be tagged. An audit log entry will be recorded indicating that the file violates one or more DLP policies.

Comment:

Add Rule **Cancel**

- **Policy Mask:** Values entered that MOVEit uses when it scans the information returned from the DLP scanner to determine if there was a policy violation. Best practice is to use the asterisk wildcard on either side of a value so it matches a significant value within the response, for example *SSN*.

Important: This value must match a value in the response data returned by the DLP scanner. This is typically the name of the policy from the scanner. However, some DLP systems allow users to specify text to be returned, so the value might depend on how your DLP system is configured. For example, if you use *SSN* as the mask, and your scanner returns SSN as part of the data associated with that type of policy violation, MOVEit will apply the appropriate action for that violation.

- **Policy Action:** Action to take if there is a violation of the policy.
 - **Block:** Terminates transmission.
 - **Quarantine:** Upload will be allowed, but Download will not be allowed. Files will be tagged, and an audit log entry will be recorded indicating that the file violates one or more DLP policies. Files may be untagged later, at which point normal permissions will take effect.
 - **Allow:** Transfer (upload and download) will be allowed, and files will be tagged. An audit log entry will be recorded indicating that the file violates one or more DLP policies.
- **Comment:** Information pertinent to this particular policy mask.

Ad Hoc Transfer

Ad Hoc Transfer - Access - Registered Senders

This page allows an administrator to enable Ad Hoc Transfer for registered users. Ad Hoc Transfer provides the ability to send messages and files (via a package) to an individual user. This page is only visible when the Ad Hoc Transfer interface has been licensed and enabled.

Registered Senders

Which users may send packages?

☐ None - Ad Hoc Transfer is disabled
☒ All
☐ Members of groups that grant Ad Hoc Transfer access

Users allowed to send packages may always send packages to other users already listed in their address book. However, when users want to send packages to people who are not currently listed in their address books, the following settings control this behavior.

Which users may send packages to registered users not listed in their address books?

☐ None - Registered users can only send packages to users already listed in their address book
☒ All except temporary users
☐ Members of groups that grant this permission

Which users may send packages to recipients who are not currently registered users?

☐ None - Registered users can only send packages to other registered users
☒ All except temporary users
☐ Members of groups that grant this permission

Which users may send packages?

This first prompt's setting determines if no one, anyone, or just some registered users can send packages. The ability to send packages can be disabled or enabled for all members of an Organization, or it can be configured by the group setting.

- None - Ad Hoc Transfer is disabled: MOVEit DMZ will not allow registered users to send packages.

Note: If you select this option, no additional prompts are displayed on this page.

-
- All: MOVEit DMZ will allow registered users to send packages to registered users.
-

Note: If you select this option, additional prompts are displayed on this page.

- Members of groups that grant Ad Hoc Transfer access: MOVEit DMZ will allow registered users to send packages if they are a member of a group that grants this permission. (This group option leverages address book functionality as an organizational facility to provide finer control over permissions.)
-

Note: If you select this option, additional prompts are displayed on this page.

Note: If you want *unregistered* users to be able to initiate *sending* packages, you must select the second option for the first prompt. If you select the first or third options, the **Don't have an account?** prompt and Register and Send Files link will not be displayed on the Sign On page. Any settings on the **Ad Hoc Transfer - Access - Unregistered Senders** (on page 505) page will not be applicable. (A statement will be displayed on the top of that page to inform you that these settings will not be used because Ad Hoc Transfer is disabled. It will say: Ad Hoc Transfer is not enabled for all users. None of the settings on this page will take effect; to change this, go to the Registered Senders setting page.)

Note: The following second and third prompts and their settings are only visible when either the second or third option is selected, thereby enabling all or some users to send packages.

Which users may send packages to registered users not listed in their address books?

This prompt's setting determines who a registered user can send packages to, as controlled via the user's Address Book. You can set this option to configure whether a registered user can send packages to only those users in their Address Book, or to any registered user, or to users not known by MOVEit DMZ.

- None - Registered users can only send packages to users already listed in their address book: MOVEit DMZ will not allow registered users to send packages to recipients who are not already listed in their address book.
 - All except temporary users OR All including temporary users: MOVEit DMZ will allow registered users - either including or excluding temporary users as stated in the option - to send packages to existing registered and temporary users who are not already listed in their address book.
-

Note: This prompt's second setting option is tailored to either exclude or include Temporary Users (i.e., it states either **All except temporary users** or **All including temporary users**), based on the selection on the Ad Hoc Transfer - Access - Registered Senders page, in the prompt **Can temporary users send packages to additional registered users?**. (That prompt only shows if unregistered users are treated as temporary users and if unregistered users can send packages.) If the answer there is **No**, the option here will be **...except...**. If the answer there is **Yes**, the option here will be **... including...**

Note: If a user sends a package to an existing registered or temporary user, then no password notification is sent with the package, as the recipient can use their existing account to log on and retrieve the files.

Note: If you select this option, additional prompts are displayed on this page.

- Members of groups that grant this permission: MOVEit DMZ will allow registered users to send packages to users not currently in their address book if the senders are members of a group that grants this permission. (This group option leverages address book functionality as an organizational facility to provide finer control over permissions.)
-

Note: If you select this option, additional prompts are displayed on this page.

Which users may send packages to recipients who are not currently registered users?

This prompt's setting determines if registered users - *excluding* temporary users - can also send packages to users not known by MOVEit DMZ.

- None - Registered users can only send packages to other registered users: MOVEit DMZ will not allow registered users to send packages to recipients who are currently unregistered in MOVEit DMZ for the organization.
 - All except temporary users OR All including temporary users: MOVEit DMZ will allow all registered users (but not temporary users) to send packages to currently unregistered users.
-

Note: If a user sends a package to an currently unregistered user, then password notification is sent with the package, as the recipient does not have existing account to log on and retrieve the files.

- Members of groups that grant this permission: MOVEit DMZ will allow registered users to send packages to unregistered users if the senders are a member of a group that grants this permission. (The third group option leverages address book functionality as an organizational facility to provide finer control over permissions.)
-

Note: If you select this option, additional prompts are displayed on this page.

Note: If you allow all or some registered users to send packages to unregistered users, MOVEit DMZ will either create a temporary user or a guest user for each unregistered user. To set how the unregistered recipient is handled by MOVEit DMZ, see the settings in ***Ad Hoc Transfer - Access - Unregistered Recipients*** (on page 499).

Ad Hoc Transfer - Access - Unregistered Recipients

This page allows an administrator to configure, for the organization, the policy for sending packages to unregistered users.

Note: If you have not allowed users to send packages to unregistered recipients (in the last prompt of the Ad Hoc Transfer - Access - Registered Senders page), a statement will be displayed on the top of the page. The statement will inform you that these settings will not be used because no one can send to unregistered recipients.

Tip: However, even if have not allowed users to send packages to unregistered recipients, the first prompt under **Unregistered Recipients** *could* be used anyway, to determine how unregistered *senders* will be handled. This will occur if you allow unregistered users to self-register to send packages (in the first prompt of the Unregistered Senders page).

Unregistered Recipients

If permitted, how should access be granted to recipients or senders who are not currently registered users?

☒ Temporary Users - Create temporary user account for each unregistered user and protect each account with its own password.

☐ Package Passwords - Provide "guest" access for each unregistered user and protect each package with its own password.

Lookup email in LDAP sources and add matching external user instead of sending to an unregistered recipient for email addresses conforming to the following rule:

☐ Lookup for all except:

☒ Ignore for all except:

...these domains:

(separate multiple domains with commas; domain matching is not case sensitive; "abc.com" matches both "alice@abc.com" and "fred@xyz.abc.com")

If permitted, how should access be granted to recipients or senders who are not currently registered users?

Note: This setting determines how to handle *both* unregistered recipients *and* self-registering senders, if applicable.

This setting specifies whether unregistered users are to be treated as Temporary Users (with their registration expiring after several days) or Guest Users (just for the one-time sending of an individual package).

- **Temporary Users:** By default, MOVEit DMZ will create a temporary user for each unregistered recipient. See the Temporary User Password and Permitted Email Domains sections below to determine how the temporary user account is handled. You can also change these settings.
- **Package Passwords:** If you select this option, MOVEit DMZ will allow the unregistered recipient to access the package, but will not create a temporary user. See the Package Password and Permitted Email Domains sections below to determine how the guest user account is handled. You can also change these settings.

Lookup email in LDAP sources...

If the organization uses an **LDAP authentication method** (on page 444), you will also see this section under Unregistered Recipients. These settings enable MOVEit DMZ to check if the email address of an unregistered user matches an LDAP entry. In other words, it checks to see if an unregistered recipient has an LDAP account.

- **Ignore for all except:** By default, MOVEit DMZ will not do an LDAP lookup for unregistered recipients. You can add email domains to the ... these domains: text box, in which case MOVEit DMZ will do the LDAP lookup for email addresses that match a specified domain.
- **Lookup for all except:** Select this option to enable looking up emails in LDAP lookup+auth sources. When enabled, any potential unregistered recipients for packages (i.e. email address recipients that don't match any internal user) will be looked up in LDAP sources to see if there is a matching LDAP user that currently is not in the MOVEit DMZ system. If a match is found, MOVEit DMZ attempts to add that user to the system, and then updates the package recipient list to send the package to that new user, **INSTEAD** of creating a temporary user or sending to an unregistered recipient. You can add email domains to the ... these domains: text box, in which case MOVEit DMZ will not do the LDAP lookup for email addresses that match a specified domain.

Temporary User Password

Note: This section is displayed only if you select Temporary Users for the first prompt on this page.

Temporary users are an optional class of users that can be created by any registered user in an organization. To set up a new temporary user, a registered user needs only the email address of the temporary user. The default settings (shown below) allow the sender to add an email address when sending a package, and MOVEit DMZ then automatically creates the temporary user, generates a password, and sends it to the user. This means that when a user sends a package to an unregistered recipient, the recipient will receive two separate emails, the autogenerated message that contains the user password, and the package. All recipients of a package will be sent the same password, and they will be required to change their password on first sign-on.

Be aware that additional information can be added to the user profile at a later time.

Note: If you will have users that access Ad Hoc Transfer using the Outlook plugin, you must select the default option, which is: 'Do not ask the sender for a password, instead:' and 'Send an automatically generated password to each temporary user'

Temporary User Password

To set each temporary user's password:

- ☒ Do not ask the sender for a password, instead:
 - ☐ Send a time-limited "set password" link to each temporary user
 - ☒ Send an automatically generated password to each temporary user
- ☐ Ask the sender for a password for each user, then:
 - ☒ Send these passwords to each temporary user
 - ☐ Tell the sender to manually deliver each of these passwords
- ☐ Tell the sender which password was generated for each user and then tell the sender to manually deliver each of these passwords

To automatically deliver temporary user passwords and "set password" links:

- ☒ Send a separate credentials email message immediately after the temp user has been created.
- ☐ Send credentials in the same email message that contains the package notification and link

NOTE: This setting does not apply to senders using Ad hoc Plug-in 2.2 and higher, if the 'Package Notifications - Allow Ad hoc plug-in to send notifications directly' setting is set to Yes (in that case, credentials will always be sent separately)

Save

Cancel

Note: For Ad Hoc Plug-in for Outlook 2.2 and later, the setting for automatic delivery of the password does not apply if you have set the Content - Package Notifications setting for Send notifications directly to Yes. In this case, credentials will always be sent separately.

For creating a password, you can have MOVEit DMZ handle the communication with the temporary user by sending an autogenerated password, or sending a set password link, which allows the recipient to create their own password.

You can also assign responsibility for creating a password to the sender, and then auto-send the password, or let the sender deliver the passwords to the temporary users.

Finally, if you have selected to have MOVEit DMZ send passwords, you can choose whether to send the password to a recipient in a separate email, or to include the password in the package notification.

Note: While this delivery option will always apply for packages sent through the MOVEit web interface, the Ad Hoc Plug-in for Outlook will ignore this option when it is responsible for sending notifications to package recipients. This behavior is controlled in the Package Notifications settings page: when the plug-in is allowed to send the package notification itself, it will always send credentials separately, in a second email.

The credentials must be separate from the notification due to the way that the email thread is maintained in plug-in version 2.2 and later: if there are multiple recipients on the thread, the credentials cannot be sent in the same email thread as the package notification, as everyone on the thread would be able to see each other's password. Instead, the plug-in always sends the same package link to all recipients within an email thread, then individually sends each recipient credentials to access the package, in a second email.

Package Password

Note: This section is displayed only if you select **Package Password** for the first prompt on this page.

This section lets the administrator set options for using a package password. A package password is sent to a guest user who is the recipient of a package. The password is used for access to that package only. A guest user is different from a temporary user in that a MOVEit DMZ user profile is not created for the guest user. Note, however, that the security settings for Remote Access and IP Lockouts will apply to a guest user.

Package Password

To set each package's password:

- ☒ Do not ask the sender for a password, instead send an automatically generated password to each guest recipient
- ☐ Ask the sender for a password for each package, then:
 - ☒ Send that password to each guest recipient
 - ☐ Tell the sender to manually deliver that password
- ☐ Tell the sender which password was generated then tell the sender to manually deliver that password

To automatically deliver package passwords, use:

- ☒ A second email message dedicated to credentials.
- ☐ The same email message that contains the package notification and link

Save

Cancel

For creating a password, you can have MOVEit DMZ handle the communication with the guest user by sending an autogenerated password.

You can also assign responsibility for creating a password to the sender, and then auto-send the password, or let the sender deliver the passwords to the guest users.

Finally, if you have selected to have MOVEit DMZ send passwords, you can choose whether to send the password to a recipient in a separate email, or to include the password in the package notification.

Permitted Email Domains

This section allows administrators to limit the domains for the *unregistered* recipient email addresses. This helps prevent users from adding certain users as either temporary or guest should not be added as such. The domain list is a comma-delimited list of domains to match against. The rule settings determine whether matched domains will be allowed or denied. For example, a list of `yahoo.com`, `msn.com`, `gmail.com`, `ipswitch.com` will keep people from defining temporary users from some common free email domains and from Ipswitch domain.

Permitted Email Domains

Users may send packages to unregistered recipients as long as each recipient's email address conforms to the following rule:

☒ Allow all except:

☐ Deny all except:

...these domains:

(separate multiple domains with commas; domain matching is not case sensitive; "abc.com" matches both "alice@abc.com" and "fred@xyz.abc.com")

Upload/Download Wizard Access

Note: This section is displayed only if you select **Package Password** for the first prompt on this page.

This section allows administrators to enable or disable access to the Upload/Download Wizard by Guest users (whether recipient or sender).

By default, the option **Allow Guest users to take advantage of the Upload/Download Wizard** is selected.

Clear the checkbox and click **Save** to disable access to the Wizard for Guest users.

Upload/Download Wizard Access

By default, Guest users are allowed to use the Wizard to upload/download package attachments. If desired, access to the Wizard for Guest users can be disabled.

☒ Allow Guest users to take advantage of the Upload/Download Wizard

Save Cancel

Ad Hoc Transfer - Access - Unregistered Senders

This page allows an administrator to configure, for the organization, the policy for sending packages to unregistered users.

Unregistered Senders

Unregistered Senders

Ad Hoc Transfer is set to provide "guest" access for unregistered senders and recipients and to protect each package with its own password; to change this, go to the [Unregistered Recipients](#) setting page.

Can unregistered users send packages to registered users?

☒ No - only registered users can initiate

☐ Yes - Unregistered users may send to registered users

Save Cancel

A statement at or near the top of the section will state whether Ad Hoc Transfer is set to provide temporary or guest access for unregistered senders. This reflects your selection on the **Ad Hoc Transfer - Access - Unregistered Recipients** (on page 499) page, in the first prompt.

Note: If you have not allowed users to send packages (on the Ad Hoc Transfer - Access - Registered Senders page, in the first prompt, by selecting *either* the first *or third* option), a statement will be displayed on the top of the Unregistered Senders section to inform you that these settings will not be used because Ad Hoc Transfer is disabled. It will say: Ad Hoc Transfer is not enabled for all users. None of the settings on this page will take effect; to change this, go to the Registered Senders setting page. (To change this, go to the Ad Hoc Transfer - Access - Registered Senders page. Under the first prompt, select the second option.)

Can unregistered users send packages to registered users?

This prompt sets whether or not unregistered users are allowed to self-register to send.

- No - only registered users can initiate: MOVEit DMZ will not allow unregistered users to self register to send a package.

Note: If you select this option, no additional prompts are displayed on this page.

- Yes - Unregistered users may send to registered users: MOVEit DMZ will allow unregistered users to self register to send a package to registered users. (On the MOVEit DMZ Sign On page, users will see the Don't have an account? prompt and Register and Send Files link.)

Note: If you select this option, additional prompts are displayed on this page.

Note: The next prompts and their setting options (in the Unregistered Senders section of this page) are tailored to either Temporary Users or Guest Users, based on your selection on the *Ad Hoc Transfer - Access - Unregistered Recipients* (on page 499) page, in the first prompt.

... if they are enabled as Temporary Users

Note: The following prompts and options are shown if Temporary User is selected on the *Ad Hoc Transfer - Access - Unregistered Recipients* (on page 499) page, in the first prompt.

Can unregistered users send packages to registered users?

☐ No - only registered users can initiate

☒ Yes - Unregistered users may send to registered users

How do unregistered users self-register?

☐ Allow Unregistered Users to answer a Captcha question

reCAPTCHA public key:

reCAPTCHA private key:

☒ Send Guest Access code and an automatically generated password

Maximum Recipients:

Limit unregistered users to sending to no more than recipients.

How do recipient emails match against registered user accounts?

By default, for each recipient email address, packages will be sent to all user accounts that are configured with that email.

If a recipient email matches more than one user account, the following rules can be used to correctly identify the desired recipient user account(s).

☐ Only send package to the user whose Login Name matches the "Name" portion of the email, if such a user exists

☐ Only send package to user(s) that have the email configured as their primary email (i.e. the email occurring first in the user's list of emails)

Can unregistered users send packages to temporary users?

Note: This prompt is displayed only if Temporary User is selected on the **Ad Hoc Transfer - Access - Unregistered Recipients** (on page 499) page, in the first prompt.

- No - only to registered non-temporary users: MOVEit DMZ will not allow temporary users to send to other temporary users.
- Yes - Unregistered users may send to temporary users.: MOVEit DMZ will allow temporary users to send to other temporary users.

Can temporary users send packages to additional registered users?

Note: This prompt is displayed only if Temporary User is selected on the **Ad Hoc Transfer - Access - Unregistered Recipients** (on page 499), in the first prompt.

- No - Temporary users can only send to the users in their address book: After after the first package sent, for all subsequent sends, MOVEit DMZ will not allow temporary users to send to any registered non-temporary users that are not already in their address book.
- Yes - Temporary users may send to any registered users.: After after the first package sent, for all subsequent sends, MOVEit DMZ will allow temporary users to send to any registered non-temporary users that are not already in their address book.

How do unregistered users self-register?

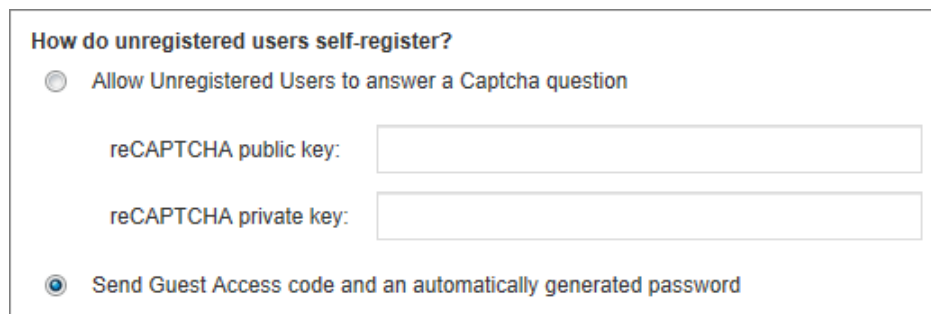
- Allow Unregistered Users to answer a Captcha question: When you use this setting, unregistered senders will experience the following when they click a link to self-register to send. The Register and Send page will provide a Captcha box for instant verification. The unregistered user will enter the email address of their intended recipient along with their own email address. Then, if the user successfully fills out the Captcha, they are signed into MOVEit DMZ.
- Instructions: To set this up, you need to enter a public key and a private key in the two fields provided.
- To get the keys, search the web for **recaptcha** follow the links to use the reCAPTCHA service on your site and to sign up, as applicable. The service is part of Google, so you need to create or use an existing Google account. Log in, enter a domain name and the page will display the Public Key and Private Key. Copy them and paste them into the two fields here.
- Send a time-limited **set password** link to each temporary user: The Register and Send page will enable the unregistered user to enter and submit the email address of their intended recipient along with their own email address. For verification, MOVEit DMZ sends the self-registering user an automated link by email. The link opens a MOVEit DMZ page without requiring a password. The linked to page allows the recipient to enter a username and request a password. MOVEit DMZ then sends the self-registering user a second email with another link that again logs them into a page without using a password, and then they can proceed from that point.

- Send an automatically generated password to each temporary user: The Register and Send page will enable the unregistered user to enter and submit the email address of their intended recipient along with their own email address. MOVEit DMZ sends the self-registering user an automatically generated password by email. The password and link allow the recipient log in and proceed from that point.

... if they are enabled as Guest Users

Note: The following prompt is shown with these two options if **Package Password** is selected on the **Ad Hoc Transfer - Access - Unregistered Recipients** (on page 499) page, in the first prompt.

How do unregistered users self-register?



The screenshot shows a configuration window titled "How do unregistered users self-register?". It contains two radio button options. The first option, "Allow Unregistered Users to answer a Captcha question", is currently unselected. Below it are two text input fields labeled "reCAPTCHA public key:" and "reCAPTCHA private key:". The second option, "Send Guest Access code and an automatically generated password", is selected with a blue radio button.

How do unregistered users self-register?

☐ Allow Unregistered Users to answer a Captcha question

reCAPTCHA public key:

reCAPTCHA private key:

☒ Send Guest Access code and an automatically generated password

- Allow Unregistered Users to answer a Captcha question: See the description and instructions above for the same prompt and setting for Temporary Users.
- Send Guest Access code and an automatically generated password: See the description above for the same prompt's last (third) setting for Temporary Users. (The options are worded slightly differently, but the description of the option for Temporary Users applies to this Guest User option as well.)

... if they are either Guest or Temporary Users

Note: The following prompt is always displayed.

Maximum Recipients

This setting allows administrators to limit the number of recipient email addresses that the self-registered sender can enter in their first or only package. This helps prevent newly self-registered users from sending to too many users.

Permitted Email Domains

This section allows administrators to limit the domains for the *registered recipient* email addresses. This helps prevent users from sending to certain registered users if they should be unable to. The domain list is a comma-delimited list of domains to match against. The rule settings determine whether matched domains will be allowed or denied.

Permitted Email Domains

Unregistered Users may register only if the submitted email address conforms to the following rule:

- ☒ Allow all except:
☐ Deny all except:

...domains that match:
(separate multiple domains with commas; domain matching is not case sensitive; "abc.com" matches both "alice@abc.com" and "fred@xyz.abc.com")

Unregistered Users may send packages to registered recipients as long as each recipient's email address conforms to the following rule:

- ☒ Allow all except:
☐ Deny all except:

...domains that match:
(separate multiple domains with commas; domain matching is not case sensitive; "abc.com" matches both "alice@abc.com" and "fred@xyz.abc.com")

Save

Cancel

Unregistered Sender Remote Access Rules

This section allows administrators to limit the Hostnames and IP addresses and ranges for *unregistered sender* remote access. This helps prevent or allow unregistered users access. The rule list is created and edited on a separate page accessed from the Edit Access Rules link. The existing access rules are listed on the Unregistered Senders page. At runtime, the rules will be processed in the top-to-bottom order displayed here.

Unregistered Sender Remote Access Rules

Rule	Hostname/IP	Comment
Allow	172.12.0.0	

Edit Access Rules

There are several columns for each rule as follows:

- Rule: Whether the rule allows or denies access.
- Hostname/IP: The IP address or hostname of each rule.
- Comment: Any hint or notes the administrator wants to provide. Anything typed here is informational only and does not affect any other part of the rule.

In addition, an **Edit Action Rules** link below the last rule opens a separate page for editing and adding access rules. Click this link to open the Unregistered Sender Remote Access Rules page.

Unregistered Sender Remote Access Rules Page

On this page, you can change details about the rules.



Buttons and links are provided for the various actions which may be performed on each rule.

- UP and DOWN arrow buttons: Move the rule up and down in the priority list - rules at the top of the list are processed first. (These buttons appear only when there are two or more rules.)
- Edit: Allows administrators to change details about the rule; opens the **Edit Remote Access Rule** (on page 472) page.
- Delete: Completely removes the rule from the access list.

In addition, the Add New Remote Access Rule link (below the last rule) opens the **Add Remote Access Rule** (on page 472) page, where new rules can be added.

Note: See the Web Interface - Settings - Security - Remote Access Policy subsection **Add Remote Access Rule and Edit Remote Access Rule Pages** (on page 472)

Ad Hoc Transfer - Content

Sending Packages

This section lets the administrator specify the **Note** portion of packages (the message body for packages composed in Outlook) should be handled. Should they be handled securely (sent by MOVEit only, and excluded from notification emails)? Or should they be included in the New Package Notification emails sent to recipients? After specifying the overall policy, specify whether users get a per-package option.

Sending Packages

Specify the handling of the "Note" portion of packages (the body of the message, if composed in Outlook). Should they be handled securely, sent by MOVEit only (the same way as the "attached" files)? Or should they be included in the New Package Notification emails sent to recipients?

The overall policy can be either absolute or just the default that senders can override on a per package basis.

The overall organization policy is to:

- ☒ Secure the Note - Exclude the Note from New Package Notification emails.
- ☐ Email the Note - Include the Note in New Package Notification emails.

Offer senders a per-package setting to change this?

- ☒ No - For each new package being created, just display a read-only setting or icon to indicate the policy in force (the overall policy you set above).
- ☐ Yes - Enable an editable per-package option that the sender can change; display the overall policy as the default.

Save

Cancel

What is the overall policy for handling package notes?

- Secure the Note: Exclude the package note from notification emails.
- Email the Note: Include the package note from notification emails.

Can users change note handling with a per-package **Secure the Note** setting?

- No - Do NOT enable a per-package Secure the Note option; the overall policy always applies.
- Yes - Enable a per-package Secure the Note option that the user can change; the overall policy will be the default.

Note: These policies apply to the Outlook plug-in (to the text typed into the body of the email used to create the package), to the MOVEit web UI, and to the MOVEit Mobile apps (iOS and Android), and the MOVEit Mobile Web.

Usage Considerations

Secure the Note is a package transfer-oriented approach to the message text composed by senders. An email notification is sent by the service, but it excludes the composed note.

In contrast, **Email the Note** is an email-oriented approach to the message text composed by senders.

Therefore, a consideration about **Secure the Note** is this: It is NOT well suited for users who want to use the package's note to inform the recipient that they are sending the securely attached files through MOVEit and to introduce the files. If they write such a note, it will NOT be visible in the *notification email* about the package.

On the other hand, Securing the note is well suited for entering confidential and sensitive information directly into the package's note.

How These Settings Affect the Outlook Plug-in

In Outlook, the note is the text the user enters in the email body when creating the package. If securing the note, that text is stripped out of the email that will be sent as a notification email to the recipients. The text will appear only in the package once it is accessed by the recipients.

Senders who look in their Outlook Sent folder will see only the notification email that was sent by email to the recipients. To see the text and the package sent, they can sign on to their MOVEit account (either in the Web UI or the Mobile App) and access their Sent (packages) mailbox.

How These Settings Affect the Subject

The Subject entered in Outlook will always be used in the New Package Notification. But for the MOVEit web UI and MOVEit Mobile, whether the Subject will be used in the New Package Notification depends initially on the Secure the Note setting used for the package note. If the package note is NOT secure, the Subject entered by the Sender will always be sent in the New Package Notification. If the note *is* secured, then the treatment of the Subject line depends on the Comment Field in **Web Interface - Settings - Appearance - Notification - Items Displayed** (on page 371).

Sending Files

This section lets the administrator set options that determine the type of content a user can send in a package, and limit the number of downloads of files sent in a package. These options apply to all users in the organization. Note that the options can also be set at the group level and at the user level, so that groups and individual users can have settings that differ from the organization setting.

The default settings allow all users to send files in a package, and allow any type of file to be sent. The default download limits are set to a maximum of 20 downloads per file, and all users are allowed to set a download limit (default is 10) for a particular package.

Sending Files

Which users may send files in their packages?

- ☐ None
- ☒ All
- ☐ Members of groups that grant this permission

Users may send files in their packages as long as each filename conforms to the following rule:

- ☒ Allow all files except:
- ☐ Deny all files except:

...those whose names match:

(separate multiple masks with commas; wildcard characters "*" and "?" are allowed; matching is not case sensitive)

Maximum download limit:

- ☐ No file may be downloaded from any package more than times

Which users can set specific download limits on their packages?

- ☐ All - use a default download limit of unless a default is set on the user's profile
- ☒ None - all packages will use the maximum download limit unless a more restrictive limit is set on the user's profile

Save

Cancel

The administrator can change the default settings for their organization. The settings are described below:

Which users may send files in their packages?

The ability to attach a file to a package can be allowed for all users, for members of groups who allow attached files, and for no users. By default, all users can attach files to a package. If 'None' is selected, packages can only contain a message (which makes Ad Hoc Transfer functionality equivalent to the 'Secure Messaging' functionality available in previous releases).

Users may send files in their packages as long as each filename conforms to the following rule

Allows the administrator to specify a list of filemasks to enforce on files attached to a package. Attached files that match at least one of the entries in the filemask ('those whose names match') list can be configured to be either allowed or denied.

Maximum download limit

The default setting for the maximum number of downloads is 20, which is set in 'No file may be downloaded from any package more than 20 times. This means that if a user sends a package to 5 recipients, each recipient could download a file from this package 4 times before the limit is reached. Your users' needs will vary, so you can also choose whether to enforce a strict download limit, allow users to set their own limits, or set the limit in a user's profile.

Which users can set specific download limits on their packages?

The default setting is set to allow all users to change the download limit, and uses a default of 10. The Administrator can strictly enforce a download limit by selecting 'None' for this option. If the Administrator has also set the option in a user's profile, the setting in the user's profile is used. This is a way to further restrict specific users who do not need the download limit specified in the default value.

Note: The Mobile apps and web do not offer senders the per package option. The default set here becomes an absolute value always used to limit downloads of packages sent from mobile. It can be overridden by the per user default setting, which will also be used as the absolute value always used to limit downloads from mobile. See **Attachment Download Limits** under **User Settings** in ***Web Interface - Users - Profile*** (on page 286).

When you save any changes, the configured setting is applied to all new users, and you have the option to also apply the new setting to existing users.

Package Quotas

This section lets the administrator configure options that determine the number of packages that a user can send in a specified time period ('Default User Quota'), and the total size of files in a single package ('Default Per Package Quota'). The default settings for both of these options are 'No quota', which means users can send an unlimited number for packages and the number of files in a package is unlimited.

Package Quotas

Default User Ad Hoc Transfer Quota:

☐ No quota

☒ Allow up to of packages to be sent every days (maximum value: 30 days)

Default Per-Package Quota:

☒ No quota

☐ Allow up to of files to be sent in each package

The administrator can change the default settings for their organization. Note that these options can also be set at the group level and at the user level, so that groups and individual users can have settings that differ from the organization setting. The settings are described below:

Default User Ad Hoc Transfer Quota

The Administrator can set the default value for both total size of packages sent, which includes all files attached, and the time period during which the quota applies. When you save any changes, the configured value will be applied to all new users, and an option will be given to apply the new setting to existing users as well.

Note: The Default User Ad Hoc Transfer Quota does not apply to guest users, but the Default Per-Package Quota does.

Default Per Package Quota

The Administrator can set the default value, which places a limit on the total file size of the attachments added to a single package. When you save any changes, the configured value will be applied to all new users, and an option will be given to apply the new setting to existing users as well.

Note: The Default Per-Package Quota applies to guest users.

Package Quota Warnings

This section lets the administrator configure options that determine when package quota warnings are sent to the sender of a package. The default setting warns the sender when they have used more than 80% of their quota, which is set in the Default User Quota field.

Package Notifications

These two sections (reached from the [Package Notifications](#) link) let the administrator configure options for:

- New package notifications sent to recipients
- Delivery notifications sent to the sender

New Package Notifications (Send on behalf of the sender)

For new package notifications to recipients, decide whether the **From:** field should show either the system's notification service or the sender's email address.

- Choose **No** to always show the system's notification service in the **From:** field. Any replies to packages will be addressed to the notification service's email address.
- Choose **Yes** for one of four choices of varying degrees of sending on behalf of user. In all **Yes** cases, any replies to these packages will always be addressed to the sender's email address.

New Package Notifications

For new package notifications to recipients, decide whether the "From:" field should show either the system's notification service or the sender's email address.

Send on behalf of the sender:

- ☒ No - always show the system's notification service in the "From:" field. Any replies to packages will be addressed to the notification service's email address.

- ☐ Yes

For each package notification, if the sender's email address meets the conditions, the sender's email address will be shown in the "From:" field. If not, the "From:" will show the notification service, but a "Reply-To:" value will be set to the sender's email address. Therefore, any replies to these packages will always be addressed to the sender's email address:

- ☐ Include

- ☐ Exclude

these domains:

(separate multiple domains with commas; domain matching is not case sensitive; "abc.com" matches both "alice@abc.com" and "fred@xyz.abc.com")

Allow Ad hoc Plug-in to send notifications directly:

For new package notifications to recipients, decide whether Ad hoc Plug-in version 2.2 and higher can send notifications directly to recipients through the email application. This setting does not apply to web interface users. Changes to this setting will take effect only after the plug-in's connector reconnects.

- ☐ No - MOVEit will always send package notifications on the sender's behalf
- ☒ Yes - Allow the plug-in to use the email application to directly send package notifications

Save

Cancel

The default **No** value sets the **From:** address of the new package notification as: *UserDisplayName* via *OrgDisplayName* Notification Service <email@domain.ext>.

The **Yes** option requires either **Include** or **Exclude**, each of which works with the optional **these domains** field. This results in essentially four choices, two of which are conditional depending on each sender's email address.

- To never show sender's email address, but set **Reply-To:** to the sender's email address: Choose **Include**, and leave **these domains** blank.
- To always show the sender's email address: Choose **Exclude**, and leave **these domains** blank.
- To only show the sender's email address if it is from certain domains: Choose **Include**, and specify one or more domains. If the sender's email address meets the conditions, the sender's email address will be shown in the **From:** field. If not, the **From:** will show the notification service, but a **Reply-To:** value will be set to the sender's email address.
- To generally show the sender's email address unless it is from certain domains: Choose **Exclude**, and specify one or more domains. If the sender's email address meets the conditions, the **From:** will show the notification service, but a **Reply-To:** value will be set to the sender's email address. If not, the sender's email address will be shown in the **From:** field.

For domain specifications, the following rules apply:

- Separate multiple domains with commas.
- Domain matching is not case sensitive. Unspecified sub-domains are matched by the domain, so that **example.com** matches **fred@sales.example.com** as well as **alice@example.com**.

Note: The conditional use of the sender's email address might be helpful if your MOVEit organization's SMTP server specifies domains that can pass through or domains that cannot. It could help with the handling of new package notifications sent on behalf of: a) unregistered recipients replying to the original sender, and b) newly self-registered senders. Use the domain specifications and settings so that, for emails from domains that will pass through, the sender's email address will be used in the **From:** field, but for those sender email domains that would bounce, the notification service is used instead (but the sender's email address is used as the **Reply-To:** value).

New Package Notifications (Allow Ad Hoc Plug-in to send notifications directly)

For the Ad Hoc Plug-in (Outlook) users, you can set this option as follows:

- **No**, to force MOVEit to send the package notifications. When you use this setting, the behavior will be the same as using plug-in version 2.1 or earlier. The plug-in will send the package to MOVEit, and MOVEit will handle sending notifications to each recipient individually, the same as using the MOVEit web interface to send the package.

- **Yes** (default), to allow the plug-in users running version 2.2 or later to send notifications and credentials directly to recipients. The package is still transmitted to the MOVEit server, which also determines the content of the notifications, but the plug-in will tell the email client (Outlook) to send the notification, instead of MOVEit. This option allows for MOVEit package attachments to be added to existing email threads, with potentially no interruption of the email conversation, so it is most useful when you will be using **Email the Note** (see Usage Considerations in this topic.)

Note: When this option is set to **Yes**, any temp user/package password credentials will always be sent separately from the notification. See the note in the **Unregistered Recipients - Temporary User Password** (on page 499) section.

Delivery Notifications

This section lets the administrator configure options that determine when delivery notifications are sent to the sender of a package. The default values 'Send immediately' and 'First read by each recipient' mean that the sender of a package will receive a delivery notification when a recipient first reads (or opens) the package notification.

Delivery Notifications

Delivery notifications are emails sent to the sender when packages are read, and/or attachments are downloaded. These notifications can be sent as soon as the package is read / an attachment is downloaded, or consolidated notifications can be sent at regular intervals.

Delivery interval:

☒ Send immediately

☐ Send every minutes

Send delivery notifications for:

☒ First read by each recipient

☐ First read and each file download

☐ Each file download

The administrator can change these options so that the sender does not receive a separate email notification for each event (first read and download). If the **Send every nn minutes** option is used, the sender will receive a delivery notification that batches the multiple events (for example, first read and download; or downloads by multiple recipients) into one notification sent according to the specified time interval. The administrator can also set the options so that the sender is notified only when a file is downloaded, or only on first read, or both.

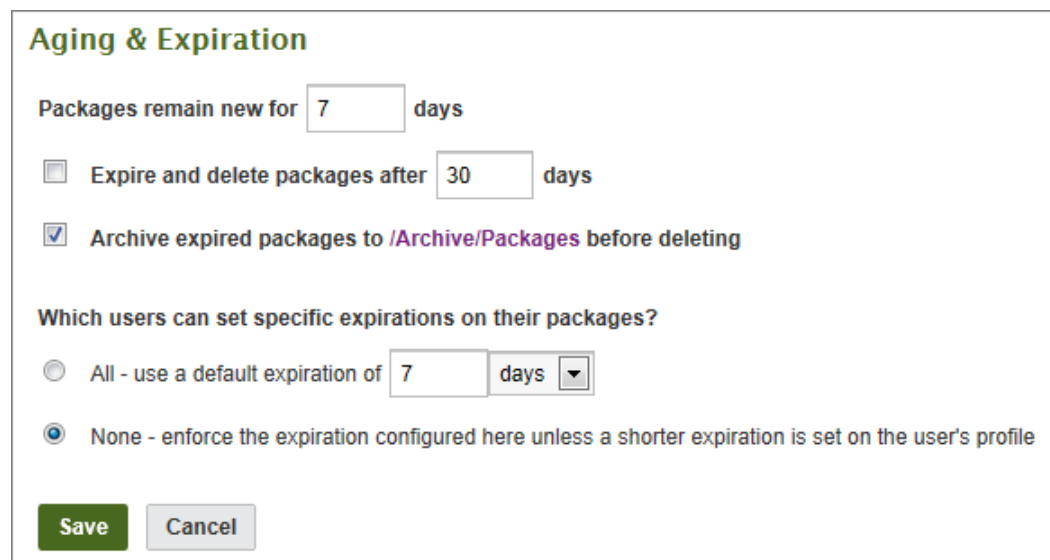
When you save any changes, the configured setting is applied to all new users, and you have the option to also apply the new setting to existing users.

Ad Hoc Transfer - Maintenance

Aging and Expiration

These settings provide aging and cleanup support for Ad Hoc Transfer and are similar to folder aging and cleanup. The administrator can set options that determine how long a package is considered new, how long a package is available to recipients, what happens to a package after it expires, and whether users can set these options themselves. These options apply to all users in the organization.

Note that the options can also be set at the group level and at the user level, so that groups and individual users can have settings that differ from the organization setting.



Aging & Expiration

Packages remain new for days

☐ Expire and delete packages after days

☒ Archive expired packages to **/Archive/Packages** before deleting

Which users can set specific expirations on their packages?

☐ All - use a default expiration of days

☒ None - enforce the expiration configured here unless a shorter expiration is set on the user's profile

The options are described below.

Packages remain new for *nn* days

By default, packages are considered new for 7 days, after which they are still available until expired.

Expire and delete packages after *nn* days

The Administrator can optionally select a maximum allowed package expiration time, which is 'Expire and delete packages after *nn* days' (default is 30 days). This keeps the package available for recipients for up through the specified number of days. The actual expiration could occur more frequently if users have been given the option to set specific expirations on their packages.

Archive expired packages to */directory/directory* before deleting

The option to archive before deleting is selected by default, but if not selected, packages are deleted upon expiration.

Which users can set specific expirations on their packages?

The administrator can also choose 'All' to let each user set the expiration on their packages; the administrator can change the default number of days for the user-set expiration.

Note: The Mobile apps and web do not offer senders the per package option. The default set here becomes an absolute value always used to expire packages sent from mobile. It can be overridden by each particular user's own default setting, which will also be used as the absolute value always used to expire packages from mobile. See **By default, packages will expire after** setting under **Package Expiration** in **Web Interface - Users - Profile** (on page 286).

Selecting **None** enforces the expiration configured in these organization-level options, unless a shorter expiration is set in the user's profile.

When the **Archive expired packages before deleting** setting is enabled, packages will be added to a nightly archive file before being deleted. The archive file is uploaded to the **Archive/Packages** folder as a zip file containing XML files for each secure message, as well as any attachments included with those messages.

To read the contents of a package archive, please consider using the command-line Archive Viewer utility.

Address Book Settings

The following options are set (by the administrator) in Ad Hoc Transfer, Access settings for Registered Senders, and determine who can send a package and to whom a package can be sent.

- Which users may send packages to registered users not listed in their address book? - When this option is set to allow a user to send packages, the user will still see the members of their address book when adding a new recipient, but the user will also be allowed to include any registered user in the organization as a package recipient by entering a username, real name, or email address into the search box.
- Which users may send packages to recipients who are not currently registered users? - When this option is set to allow a user to send packages, when the user sends a package to an unregistered recipient, MOVEit will check each recipient email address and see if it is already entered as an unregistered recipient in the user's address book. If it is not, the address will be added automatically. The user will be able to fill out the details of that entry at a later time. Users can also add an entry to their Address Book by clicking 'Manage your address book' which is available on the Home page and the Packages page.

Note: These same options can be configured so that the administrator controls the Address Book entries, and users can send packages only to a user found in their address book. In this way, the administrator can allow only registered users to send and receive packages.

In addition to the above options for registered user senders, the following options apply to unregistered user senders who become temporary users. These options are set (by the administrator) in Ad Hoc Transfer, Access settings for Unregistered Senders. (These options are only available if - on the Unregistered Recipients page - "Temporary Users" is selected instead of "Package Passwords" and if - on the Unregistered Senders page - unregistered users are allowed to send packages to registered users).

- Can unregistered users send packages to temporary users? - When this option is set to allow unregistered users to send to temporary users, the unregistered sender will - when adding a new recipient - be allowed to include any temporary user in the organization as a package recipient by entering a username, real name, or email address into the search box.
- Can temporary users send packages to additional registered users? - When this option is set to allow temporary users to send packages to additional registered users, the unregistered user will - when adding a new recipient - be allowed to include any registered user in the organization as a package recipient by entering a username, real name, or email address into the search box.

Miscellaneous

Miscellaneous - Aging

Audit Logs

Logs are retained online for a finite number of days before being purged and saved to the organization's Archive/Logs folder as an XML document. By default this value is 30 days. If this value is set to 0 days, online log entries are not purged.

Miscellaneous - Tamper Detection

MOVEit DMZ's audit log is a tamper-evident. No changes, deletions or additions can be made to the log without breaking the strict chain of cryptographic hashes locked to the specific content and order of log entries.

All chains must begin somewhere and the tamper-evident chain in MOVEit DMZ is no different. Starting hashes for MOVEit DMZ tamper-evident chains are retained in encrypted form in the registry. To further prevent against tampering, the hashes used are keyed hashes that require the input of the correct key to be matched and read.

To allow different organizations to maintain different archive periods on their own audit trails MOVEit DMZ maintains a single tamper-evident chain for each organization. When entries are archived, the starting hash of each organization is advanced to just before the oldest remaining record.

If MOVEit DMZ's TamperCheck scheduled task detects tampering, an email with related logs will be sent to the **Send Errors To** email address(es).

If tampering is encountered and detected, the starting hash of each organization is automatically advanced to the last known good position (i.e., now) after notifications are sent. However, MOVEit DMZ's **Reset** function provides an easy way to perform the same action at any time this.

View/Reset

Admins have access to a **View/Reset** link that takes them to a page that will allow them to advance their organization's starting hash to the present time.

Other Tamper-Evident Administration

SysAdmins have the power to reset the start hashes of all organizations. They also have the power to turn tamper-evident logs on and off (they are on by default). More information about this can be found in **Web Interface - Settings - System - TamperDetection** (on page 541).

Every night a scheduled tamper check process will go through all log entries and ensure that the chain of cryptographic hashes remains intact. If any problems are encountered, any administrator listed in the MOVEit DMZ Config utility's **Send Errors To** field will automatically be notified via email.

This check may also be initiated manually by administrators with access to MOVEit DMZ's console. (Start | Programs | MOVEit DMZ | MOVEit DMZ Log Tamper Check) Any TamperCheck that ends with the phrase **Completed with errors** should be considered a failed TamperCheck; the exact reason for the failure will be explained in the log. A web-based tamper-check is not available because checking the entire log of evidence for tampering often takes more time than the average web browser (or web browser user) is willing to wait.

System

System - Debug Logs

Configure & Download

If a technical problem is observed, this page gives SysAdmins the ability to change the debug levels of the core MOVEit DMZ application and the FTP and SSH services, and to retrieve debug logs from any of the MOVEit DMZ services (including FTP and SSH) remotely over a secure channel.

Configure Debugging Information...

A "rolling" debug log may be enabled to assist the developers of this site track down problems. This log SHOULD NOT be used for audit purposes, and SHOULD be set to a low level most of the time. Press the "Change Level" button to change the level of debugging information recorded in this file.

Core Application:

FTP Interface:

SSH Interface:

[Change Level](#)

Download Debug Logs...

Name	Size	Last Modification Time
 ArchiveLog.Log	767B	4/2/2014 1:00:15 AM
 ArchiveMessages.Log	158B	4/2/2014 1:00:24 AM
 ConsistencyCheck.Log	2KB	4/2/2014 1:00:27 AM
 CreateReports.Log	3KB	4/2/2014 1:00:43 AM
 DelayedNotifications.Err.OL1	0B	4/2/2014 6:55:11 AM
 DelayedNotifications.Err.OL2	0B	4/2/2014 6:50:11 AM
 DelayedNotifications.Err.OL3	0B	4/2/2014 6:45:11 AM

Debug Logs

The debug logs available on this page contain useful information for troubleshooting system problems. Often, when a problem with the system occurs, the debug logs will be the first thing MOVEit support will ask to see. In addition to being downloadable from this page, the debug logs can be accessed directly from the DMZ host server. They are located in the Logs subdirectory of the non-web directory for DMZ (by default, C:\MOVEitDMZ). For MOVEit DMZ web farm installations, this directory will be on the shared storage device.

An explanation of each debug log file follows:

- **DMZ_WEB.log** - This is the main debug log for the MOVEit DMZ application. It contains debug messages written out by the core application and the web interface.
- **DMZ_ISAPI.log** - This is the debug log for the MOVEit ISAPI file transfer module, which handles all web interface file transfers, including browsers, MOVEit Wizard, MOVEit Central, MOVEit EZ, and MOVEit DMZ API.
- **DMZ_FTP.log** - This is the debug log for the secure FTP interface. Events and errors in the DMZ FTP server will be found in this file.
- **DMZ_SSH.log** - This is the debug log for the FTP over SSH (SFTP) interface. Events and errors in the DMZ SSH server will be found in this file.
- **Other *.log Files** - The other *.log files listed are for the individual scheduler applications that run on a nightly basis. These will contain information about the most recent run of each application.
- ***.OLx Files** - The debug log files roll over when they reach a certain file size limit, which is configurable in the MOVEit DMZ Config program. A file that has reached this limit will be renamed to *.OL1 from *.log, and a new *.log file will be created. The existing *.OL1 file will be renamed to *.OL2, and so on through *.OL4. Hence, *.log is the current log, *.OL1 is the next oldest, and *.OL4 is the very oldest backup of a log file. If an error you are trying to find information about something that happened some time ago, you may need to look in the appropriate *.OLx file for it.

Note: For MOVEit DMZ web farm installations, the node number of the DMZ server will be part of the name of each of the DMZ_* debug files. For example, for web farm node 2, the main application debug log file would be named DMZ_WEB_02.log.

System - Auditing

Event Log

These options force MOVEit DMZ to write each audit log entry into a local Windows Event Log as well as the usual MOVEit DMZ audit database. Entries will either be created with a source of MOVEit DMZ Audit in the Windows Application Event Log or with a source of MOVEit_DMZ_Audit in the MOVEit Application Event Log. Audit log entries reporting successful actions will be entered as Information level events, while those reporting unsuccessful actions will be entered as Error level events.

Configure Event Log Settings...

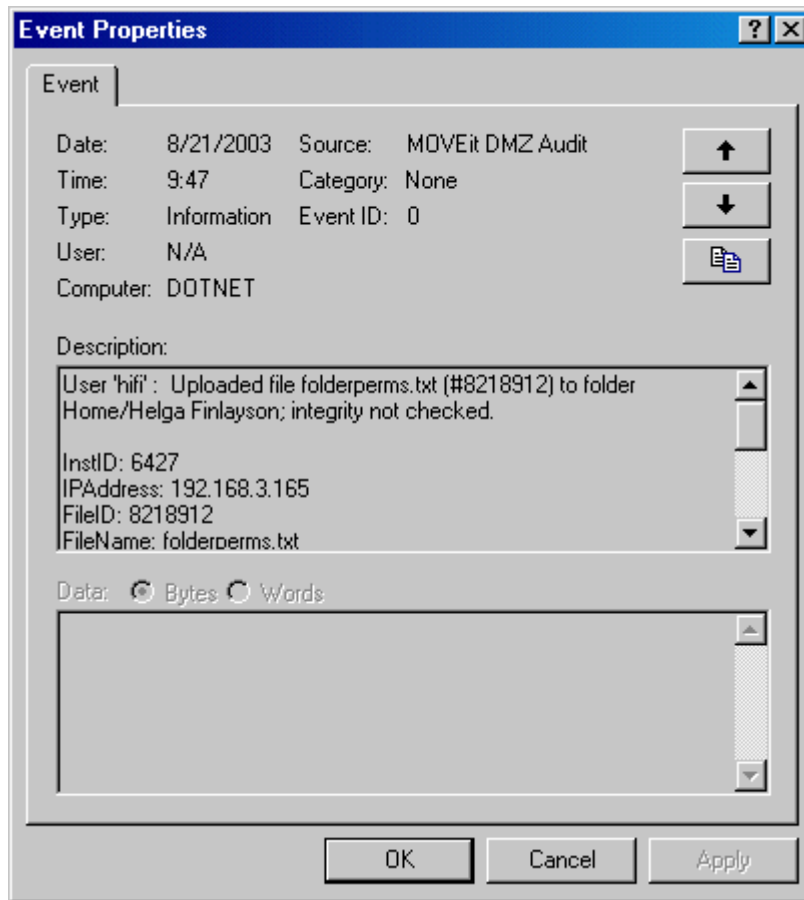
Set the Windows Event Logging setting below to Enabled to have MOVEit DMZ send its audit records to a Windows Event Log, in addition to its own audit log database. You can also choose which Windows log should receive the records.

Windows Event Logging: ☒ Enabled ☐ Disabled

Windows Event Log Name: ☐ Application ☒ MOVEit

[Change Setting](#)

An example of an entry written to the Windows Application Event Log is pictured below.



Although MOVEitDMZ has the ability to send audit entries directly to a remote Syslog server, there are also many utilities available which can send logs from local Event Logs to SysLog or SNMP management consoles. For more information about how to do this, see **SysLog and SNMP** (on page 737).

Syslog

These options force MOVEit DMZ to write each audit log entry to a remote Syslog server, as well as to the usual MOVEit DMZ audit database. SysLog is based on UDP (usually port 514) and is therefore a best efforts protocol in the sense that neither the client nor the server will know (or care) if SysLog messages are dropped by the network. Audit log entries reporting successful actions will be entered as Information level events, while those reporting unsuccessful actions will be entered as Error level events. A SysAdmin must configure a Syslog host in addition to enabling this setting. They can also optionally configure a Port to use for the connection (default = 514) and the Facility that audit messages will show up as on the Syslog management console (default = FTP).

Configure Syslog Settings...

Set the Syslog Logging setting below to Enabled to have MOVEit DMZ send its audit records to the specified Syslog host, in addition to its own audit log database. You can also optionally configure what Port and Facility the Syslog connection should use. [Click here](#) for more information about Syslog Logging in MOVEit DMZ.

Syslog Logging: ☒ Enabled ☐ Disabled

Syslog Host:

[Send Test Syslog Message](#)

Optional Settings:

The Syslog Port setting can be used to configure an alternate port for the Syslog connection. If left blank, the syslog port will revert to its default value. The Syslog Facility Setting can be used to define under what facility the MOVEit DMZ Syslog messages will show up on the remote Syslog host.

Syslog Port: Default Port = 514

Syslog Facility: Default Facility = FTP (11)

[Change Settings](#)

The Syslog Facility is used to help determine where from within the system the message originated. There are 24 different enumerated facilities to choose from:

Kernel (0)
User (1)
Mail (2)
System (3)
SecAuth1 (4)
Syslogd (5)
LinePrinter (6)
NetworkNews (7)
UUCP (8)
Clock1 (9)
SecAuth2 (10)
FTP (11)
NTP (12)
LogAudit (13)
LogAlert (14)
Clock2 (15)
Local0 (16)
Local1 (17)
Local2 (18)
Local3 (19)
Local4 (20)
Local5 (21)
Local6 (22)
Local7 (23)

The Send Test Syslog Message link can be used to test the current Syslog settings by sending a test message to specified host. Since the BSD Syslog implementation is based on UDP, the administrator will have to manually verify that the test message arrived at the remote Syslog management console.

Syslog Connect Test Results

Host=172.16.22.220

Port=514

Facility=11

A test message has been sent to the Syslog host '172.16.22.220'.
You should check this host to verify that the message has been received.
Be sure to save your Syslog settings if you have not done so already.

[Close Window](#)

If the test is successful, a message similar to below should show up in the Syslog management console on the remote Syslog server:

10/16/09 16:41:35

Info message from: 172.16.22.181

Hostname: MLA-PC

This is a test message sent by MOVEit DMZ using the following configuration: Host='172.16.22.220', Port='514', Facility='FTP (11)'

Error Display

When this option is enabled, end users will be shown a nicely formatted and branded error page in the rare event a system exception is generated by MOVEit DMZ. The page will contain details about the error and what was happening when the error occurred, as well as instructions to contact their tech support contact and inform them about the error. When this option is disabled, the user will simply be notified that an error occurred, and instructed to notify their tech support contact. (See the *Exception Handling* (on page 745) page in the Advanced Topics section for more information)

Failed Signons

Normally, MOVEit DMZ records every failed signon attempt that happens on the system to the audit log. On some busy systems however, large numbers of these records can make it difficult to search for other issues, and can slow down access to all audit log records. The options on this page help relieve this problem by allowing administrators to prevent certain types of signon failures from being recorded in the log.

Currently, the only available option is the Log Insecure FTP Failed Signons option. When set to No, this prevents audit log records from being written whenever someone attempts to access the DMZ FTP server in an insecure manner, if the DMZ FTP server is configured to not allow any insecure access. This option will NOT prevent audit log records from being written if the DMZ FTP server is configured to allow insecure access, but either the user's IP address or user account is prevented from using the insecure FTP interface.

System - User Authentication

SiteMinder

This section allows sysadmins to enable single-signon integration with CA's eTrust SiteMinder authentication product.

Enable SiteMinder Integration...

When set to Yes, the SiteMinder Integration option will cause the system to watch for HTTP headers specific to a SiteMinder Web Agent, indicating a user is authenticated and authorized to access this server. When these headers are present, normal user authentication procedures will be bypassed, and the user will be automatically logged on.

NOTE: When SiteMinder Integration is enabled, a shared secret string will be automatically generated and displayed here. This secret string must be added to the SiteMinder policy protecting this server as a static "WebAgent-HTTP-Header-Variable" response rule. The variable should have the name "HTTP_SM_MOVEITDMZ_SHAREDSECRET". The system will not accept SiteMinder authentication and authorization headers unless this header is present and contains the correct shared secret string.

Enable SiteMinder Integration: ☒ Yes ☐ No

SiteMinder Shared Secret: ks2unjpuhd9511e96bidauat968m739h

[Change SiteMinder Integration](#)

Enabling the option causes MOVEit DMZ to begin watching for the SiteMinder-specific HTTP headers that indicate a user has already been authenticated by a SiteMinder Policy Server acting through a SiteMinder Web Agent. When such headers are present, MOVEit DMZ will automatically log the user on, without having to prompt the user for authentication credentials again. This allows DMZ to achieve true single-signon integration when operating in a SiteMinder environment.

To add an additional measure of security to MOVEit DMZ's communication with SiteMinder, a special shared secret will be automatically generated whenever this setting is enabled. In order for DMZ to trust the HTTP headers injected into the request by the SiteMinder Web Agent, a special header with the name `HTTP_SM_MOVEITDMZ_SHAREDSECRET` must be included with a value of this shared secret. Such a header can be configured as part of a Response object in SiteMinder. See the *SiteMinder Integration* (on page 733) page in the Advanced Topics section for more information about configuring a Response object.

Unique Usernames

The sysadmin can set whether a username can be used in one MOVEit DMZ organization only, or whether it can be used in multiple organizations.

Unique Usernames

On this system, usernames are unique:

- ☒ **Across multiple organizations** - organizational sign on branding and site definitions are ignored during authentication, but two different organizations cannot have their own "jsmith" users.
- ☐ **Within individual organizations** - two different organizations can have their own "jsmith" users because organizational sign on branding and site definitions are used to tell the users apart during authentication.

[Change Setting](#)

- The default setting ('Across multiple organizations'), means that the username is not allowed to be used in any other organization on the system.
- The setting 'Within individual organizations' means that a username used by a user in one MOVEit DMZ organization is unique to that organization and thus can also be used in other organizations. Note that though the usernames can be used across organizations, user accounts cannot. The user will need a user account on each organization.

Note that if you are using MOVEit Central, or scripts, to access MOVEit DMZ, this setting can affect the ability of existing MOVEit Central accounts and scripts to authenticate to MOVEit DMZ.

When a username is used in multiple organizations, authenticating the username becomes a bit more complicated. Normally, the appropriate organization will be automatically determined by checking cookies or matching host names, but in some cases it may require users to provide an organization name. To authenticate, the organization must be identified. This can be done by:

- Setting up the hostname to match with the organization's base URL.
- Providing the Org ID in the query string.
- The user specifying which organization they want to log into (in the **username** field on the signon page). The necessary syntax is Org name, short name, or Org ID followed by a backslash (\) and then the username. For example, **testorg\fred** rather than just **fred**. This syntax should be communicated to all users who are members of multiple organizations because the username may become non-unique at any time (ie when the same username is added to another org).

System - Remote Access

SysAdmin Remote Access Rules

The remote access policy defines the list of IP addresses and/or hostnames from which system administrators may access this organization.

By default, SysAdmins may only sign on from the local console.

SysAdmin Remote Access Rules		
Rule	Hostname/IP	Comment
Allow	192.168.*.*	Allow from internal network
Edit Access Rules		

The Remote Access rule list is different for SysAdmins compared to other organizational Administrators. There is no section for end users and none for Webposts because these cannot be created in the System organization. The SysAdmin Remote Access Rules control from which IP addresses or SysAdmins may connect.

The process for setting up Remote Access Rules for SysAdmins is the same as that for organizational Administrators. You can find details and examples in the Remote Access Policy page.

Trusted Hosts

The Trusted Hosts permissions list for the Sysadmin organization can be set by Sysadmins only.

You can add a hostname or IP address here that will allow the sysadmin to login to MOVEit DMZ from a host that matches the hostname or IP address.

Trusted Hosts (for System organization only)

Hostname/IP	Comment
<i>There are no Trusted Hosts configured.</i>	
Edit Access Rules	

For most purposes, when trusted host access is needed, you will want to provide that access for a specific organization. The Trusted Hosts settings available to sysadmins now apply only to the System organization. A Trusted Host for an organization is defined by using the rules available in the ***Security Policies - Remote Access*** (on page 472) options.

Under normal operations, clients that access MOVEit DMZ from any of the local interfaces will bypass the normal IP lockout and session IP consistency checks. This allows services like the MOVEit DMZ FTP server and the MOVEit DMZ SSH server to function properly, and present the client's IP address for display and logging purposes. The Trusted Hosts permission list allows sysadmins to designate certain hosts as Trusted, allowing them the same privileges as local interfaces. This feature is most often used when using MOVEit DMZ API within a separate web application to provide single-signon access to MOVEit DMZ. It allows the API session to be transferred to the client browser, and back again, and also allows API to present the client's IP address for display and logging purposes.

Note: Hosts added to the Trusted Hosts permission list will avoid many of the standard security safeguards built into MOVEit DMZ to prevent unauthorized access (though clients connecting through such hosts will not). NEVER ADD A HOST TO THIS LIST UNLESS YOU KNOW WHAT YOU ARE DOING! If you are uncertain as to whether a host should be added to this list, feel free to contact Ipswitch MOVEit support for assistance. Also, for security reasons, the All IPs mask of *.*.*.* will not be allowed as a Trusted Host entry.

IP Lockout Policy

The IP Lockout settings allow SysAdmins to decide how many attempts in how short a time period are required to lock an IP address out. A lockout expiration option is also available which will automatically unlock locked out IP addresses after a configured time period.

Note: Under normal operations, clients that access MOVEit DMZ from any of the local interfaces will bypass the normal IP lockout and session IP consistency checks. This allows services like the MOVEit DMZ FTP server and the MOVEit DMZ SSH server to function properly, and present the client's IP address for display and logging purposes. The ***Security Policies - Remote Access*** (on page 472) options allow Org admins to allow access to certain hosts (trusted hosts), allowing them the same privileges as local interfaces.

Edit IP Lockout Policy...

Setting up an IP lockout policy will allow this site to lock out IP addresses from which several bad authentication attempts have been made. (This prevents someone from "brute forcing" a list of likely usernames and/or passwords into the system.) Press the "Change Lockout Policy" button to save changes to the IP lockout policy.

Enable IP Lockout: Yes: ☒ No: ☐

Lock out IPs after Tries in Minutes

Expire Lockouts After Minutes

Set to 0 to disable lockout expiration.

[Change Lockout Policy](#)

Starting in version 4.0, IP lockouts are enabled by default and set to lock out IP addresses after 15 bad attempts in any 5 minute period.

System - Notification

Default Return Address

Notifications are issued from MOVEit DMZ as if they were using this email address. Individual org-level Return Address settings will override this default. Some system-level messages to administrators will continue to come from this email address even if this setting is overridden at the organization level, however.

Hint: Set this value to a real email address if you would like to be notified of email notifications which cannot be delivered. (Delivery failure messages will be sent back to this return address.)

Base URL

This is the URL from which links in notification email messages are sent. This value should normally be something like <https://moveit.stdnet.com>. If you installed MOVEit DMZ into a subdirectory of your web site, this value should be something like <https://dotnet.corp.stdnet.com/midmz>. Values ending with `human.aspx` or `machine.aspx` will result in broken email notification links. A blank value will also result in broken email notification links.

System - Miscellaneous

Default Organization

SysAdmins can set a single organization as the default organization. This designation is of most use in branding the host. Without a default organization, someone arriving at the host (without specifying an OrgID) will see Org #0 branding. With a default organization, the same person will see the default organization's branding instead.

Wizard

SysAdmins can enable or disable the system-wide use of either the MOVEit Wizard Java or MOVEit Wizard Windows (ActiveX). When either of the Wizards have been disabled, users will no longer have access to that particular Wizard, even if they have previously installed and/or enabled a Wizard which has been disabled. Furthermore, there will be no mention of any disabled Wizards on the Account Options pages, the automatic Wizard installation pages, or any upload, download or attachment pages.

For the ActiveX Wizard, it is possible to specify the minimum acceptable version. Users who already installed a version of the Wizard with a version greater than or equal to the specified version will not be automatically prompted to download the most recent version. This can be a benefit to sites where the process of installing signed ActiveX controls requires intervention by an administrator. Users who wish to upgrade to the ActiveX Wizard anyway can do so via the Account Options page, assuming they have sufficient rights under Windows.

For more information about MOVEit Wizard, see the MOVEit Wizard section of the online manual.

Meta Refresh

This setting, when enabled, adds a meta refresh tag to the top of most DMZ pages. The refresh is set to refresh one minute after the IIS session expires, so it will effectively sign them out of the DMZ system. This adds to the security of a DMZ system, preventing a user from keeping possibly sensitive information displayed on their screen for long periods of time. When the user signs back in, they will be taken to the page they were viewing prior to the refresh.

Note: Secure Messaging composition pages are NOT affected by this setting, since secure messages may take a great deal of time to compose.

System - Tamper Detection

See *Web Interface - Settings - Miscellaneous - Tamper Detection* (on page 526) for a complete explanation of MOVEit DMZ Tamper Detection.

Reset All Orgs

This button found on the linked page resets the cryptographic start hashes of all organization's tamper-evident chains.

Configure

There is a system-wide on/off switch for MOVEit DMZ's tamper-evident features. The page available through this link flips this switch on and off.

System - Content Scanning

Overview

This section allows sysadmins to enable scanning of incoming files using a remote anti-virus server. MOVEit DMZ will submit incoming files to the anti-virus (AV) and/or Data Loss Prevention (DLP) server using the ICAP protocol. Files that are clean are then passed into the MOVEit DMZ filesystem.

Note: If you are using the AS2 Module to transfer files, be aware that content scanning does not apply to AS2 transfers. Use MOVEit Central to scan AS2 transfers for viruses.

For more information on the Content Scanning feature and associated logs and reporting, see the **Feature Focus - Content Scanning** (on page 97) topic.

Set Content Scanning

A name for the content scanner and the location (Server URL) for the content scanner are required settings. All of the Content Scanning settings apply to all MOVEit DMZ hosts on the system. The settings are described below:

Note: You can enable or disable Content Scanning for each organization in **Settings - Security Policies - Content Scanning**. You need to be signed on as an Organization administrator.

- **Scan uploads:** **Yes** means content scanning is enabled for the MOVEit DMZ system, for all organizations. **No** means content scanning is disabled for all organizations on the system.
- **Name:** This is a user-defined name for the content scanning activity, such as AV scan.
- **Server URL:** This is the address of the anti-virus (ICAP) server. This address requires the prefix `icap://` (for example: `icap://scansrv:1344`)
- **Server Type:** Use the default setting of **- Auto Detect -** or select the type of Anti-Virus server from the list of supported types.
- **Server allows "204" responses:** The default setting **Yes** will allow faster scanning, as the 204 response allows the server to return an updated header without body data.
- **Maximum file size to scan:** The default setting of 15 MB (recommended) means that uploaded files that exceed 15 MB in size will not be fully scanned. MOVEit DMZ does not exclude files larger than the size selected, it actually scans up to the size selected on all files. IF no problem is found in the partial scan, the file is allowed into the DMZ filesystem. If you do not want to have a maximum size for file scanning, enter 0 for this option.
- **Server connection timeout:** The default setting of 5 seconds means that if MOVEit DMZ cannot establish a connection with the scanning server within 5 seconds, a connection failure occurs. MOVEit DMZ will attempt to connect again until the maximum number of server connection tries is reached.

- **Server send timeout:** The default setting of 30 seconds means that if MOVEit DMZ cannot send to the anti-virus server within 30 seconds, a connection failure occurs. MOVEit DMZ will attempt to connect again until the maximum number of server connection tries is reached.
- **Server receive timeout:** The default setting of 30 seconds means that if the anti-virus server cannot receive from MOVEit DMZ within 30 seconds, a connection failure occurs. MOVEit DMZ will attempt to connect again until the maximum number of server connection tries is reached.
- **Server connection tries:** The default setting of 3 means that MOVEit DMZ will try up to 3 times to create the initial connection to the anti-virus server.
- **Change Content Scanning:** After making any entries or changes, click this button to apply the changes.
- **Test Content Scanning:** Tests the AV or DLP capability by sending a known fake infected file (EICAR.COM) to the ICAP server and ensuring that the file is marked as infected or ensuring that the DLP server was contacted successfully. (To avoid problems with other AV packages that may be running on the system, the EICAR is stored encrypted.) Before testing, be sure to save any changes to the settings by clicking the Change Content Scanning button.

The following screen shows an example of the configuration for a Sophos ICAP AV scanner.



Settings (System)

Configure Content Scanning Settings...

Configure an optional content scanner to have MOVEit DMZ send uploaded files to an ICAP server for inspection. Rejected files will be immediately discarded. This feature is most commonly used for virus scanning. [Click here](#) for more information about Content Scanning in MOVEit DMZ.

Scan uploads:	Yes: ☒ No: ☐
Name:	Sophos AV
Server URL:	icap://192.168.195.83:1344/avscan (e.g. icap://scansrv:1344/avscan)
Server Type:	Sophos Anti-Virus Dynamic Interface ▼
Server allows "204" responses: (Allows faster scanning)	Yes: ☒ No: ☐
Maximum file size to scan:	15 (MB)
Server connection timeout:	5 (seconds)
Server send timeout:	30 (seconds)
Server receive timeout:	30 (seconds)
Server connection tries:	3

(Be sure to save your changes first, then Test Content Scanning)

Logging

If a file was scanned, file detail pages will display the ICAP server information.

If a file fails the scan, the user who uploaded the file will see an error message at the top of the browser page.

Also, log file entries will report the user-configured name of the ICAP server used during the file upload. File records will also report the self-identification, version, and virus definition or DLP policy tag from the server.

Error code numbers (6100 - 6103) are used to report AV errors. This will help when filtering logs. If an upload fails due to content scanning, the corresponding log table records will contain the AV server name and, if possible, the name of the virus.

Error code numbers 0 and 6150 are used to report DLP policy violations, as follows:

- Error number 0 for violations that have been allowed or quarantined
- Error number 6150 for violations that have been blocked

Notifications

Notification macros for content scanning, if enabled, can report the scan results for both anti-virus (AV) and data loss prevention (DLP) scans.

AV and/or DLP information may be included in the following notifications:

- New File Upload Notification
- File Upload Confirmation
- New Package
- New Package Secure Attach
- New Temp User Package (with password)
- New Temp User Package (with password) Secure Attach
- New Temp User Package (with password link)
- New Temp User Package (with password link) Secure Attach
- New Guest Package
- New Guest Package Secure Attach
- File Non-Delivery Receipt
- File Upload List Notification
- File Upload List Confirmation
- File Not Downloaded List

- File Delivery Receipt
- Package Delivery Receipt
- Package Download Receipt
- Package Deleted By User
- Package User Was Deleted

The standard templates for these notifications do not include the content scanning results. You can add the macros that report the scan results by creating custom notification templates. Custom notifications are set in an organization via **Settings | Appearance | Notification | Custom**.

Reporting

You can add a Content Scanning report which shows blocked content scanning violations. An example of a violation is a file that failed an anti-virus (AV) check or violated a data loss protection (DLP) policy and was blocked. In this case, the report will show the name of the scanner, the file name, and the name of the virus (if known) or policy. If you are logged in as administrator for an organization, the report shows violations for your organization. If you are logged in as a system administrator, the report can show multiple organizations.

Organizations

Overview

Organizations describe discrete businesses; one per business. SysAdmins may work with Organizations by clicking the Orgs link on the left side of the screen.

Organizations

System Organization

Name	ID	Users	Folders	Files	
 (System)	0	1	7	2	

Licensed Organizations

Name	ID	Users	Folders	Files	
 Org 1	5209	5	12	4	  
 Org 2	1266	1	7	-	  

Add Organization

Sort by: Name - Org ID

The main list of Organizations has several columns:

- **Name:** The name of the organization. Used throughout the application.
- **ID:** The unique 4-digit ID of the organization. Rarely exposed except when used in WebPosts.
- **Users:** The current number of users (active and inactive) in this organization.
- **Folders:** The current number of folders in an Organization.
- **Files:** The current number of files stored in an Organization.

The following actions are also available:

- **Open:** Opens the **Organizational Profile** (shown below)
- **Delete:** Deletes this Organization (after confirmation)
- **Act as Admin:** Allows the SysAdmin to act as an Admin of the Organization. (SysAdmins cannot directly perform tasks such as selecting Organization colors or setting up IP access lists without first becoming Org Admins.)

Clicking the **Add New Organization** link opens the **Add a New Organization** process. This is a 4-step process which adds the new Organization, configures some basic remote access rules, adds a new administrator user in that Organization, and then signs the sysadmin out so they can sign on as the new administrator and begin adding users, folders, and files to the new Organization.

Organization names may contain the following characters (including capital letters):

abcdefghijklmnopqrstuvwxyz1234567890 . , ! \$? * # @ - _ = + () : ' ` ~ % ^ & [{] } ;

Definition of an Organization

There are two types of Organizations in MOVEit DMZ. First is the **(System)** Organization, which is used by SysAdmins to administer system-wide settings and create and maintain other Organizations. The System Organization should ONLY be used for these purposes, and not for adding users and transferring files. It is always present, cannot be deleted, and does not count against the number of organizations the system is licensed for. All other Organizations are called Licensed Organizations, or just Organizations for short. These are the Organizations under which most other MOVEit DMZ operations such as file transfer and secure messaging occur.

Any company, non-profit group or government agency is considered an Organization in the MOVEit DMZ world. Depending on which edition of MOVEit DMZ has been licensed, a single server may host a single Organization or multiple, independent Organizations, each with their own distinct data store, encryption scheme and security preferences.

Because MOVEit DMZ Organizations do not share information with each other, it can be somewhat confusing to determine when multiple Organizations are required. A simple rule of thumb is to create multiple Organizations when you want to pool resources with other, similar companies or resell MOVEit DMZ services. A few examples will probably make the distinction even clearer.

Example(s):

- Standard Bank Services purchases MOVEit DMZ to provide secure data transport and collection services to three member banks. None of the banks should be able to see the information any of the other banks has collected. Each of the three banks are MOVEit DMZ organizations.
- Standard Auto Manufacturer purchases MOVEit DMZ to exchange sensitive purchase orders, price sheets and other information with its suppliers. None of the suppliers should be able to see the information any of the other suppliers is exchanging with Standard Auto Manufacturer. Standard Auto Manufacturer is MOVEit DMZ's one and only organization; each of its suppliers will be users within the single organization.

Setup and Maintenance

Only SysAdmins have the power to add or delete Organizations. SysAdmins and Administrators both have the ability to configure Organizations, but some information (e.g., Name, Minimum SSL Strength, etc.) may only be configured by SysAdmins.

Profile

An Organization Profile displays details about a single organization and provides links to common administrative functions.

Organization Profile (Org 1)

General Information

Organization ID: 5209

Organization Name: Org 1

Short Name: Org1

Base URL: *Default value - <https://KEaston-08R2DOC.FTQA.com>*

Mobile URL: *Default value - <https://keaston-08r2doc.ftqa.com:8443/mobile/switch>*

Notes:

 [Change Information](#)

Security Information

Secure Connection Requirement: 128-bit [Change Req](#)

Administrator Package Access: Log viewing: Disabled Package/attachment viewing: Disabled [Change Settings](#)

Act as Admin and Edit: [Users](#), [Groups](#), [Folders](#), [Other Settings](#)

File/Folder and Ad Hoc UI: Both File/Folder and Ad Hoc [Change Setting](#)

Maximum User Count: 50 [Change Setting](#)

Prevent Changing Signon/Signoff Logging: Disabled [Change Setting](#)

General Information

This section displays the four-digit **Organization ID**, **Organization Name**, **Base URL**, and any **Notes** for this organization. The **Org Name**, **Base URL**, **Mobile URL**, and **Notes** can be changed by clicking the **Change Information** link. (This opens the Edit General Information screen.) The **Org ID** cannot be changed.

- **Organization ID:** The four-digit ID associated with this organization.
- **Organization Name:** The name of the organization. This name is displayed to all users in the organization whenever they signon, or receive notifications, or anything else related to the organization.
- **Short Name:** The Short Name is a shorter version of the organization name, used to quickly refer to that organization. It is not required, and is currently only used as an optional logon prefix to specify the organization to log on to (when the same username is used in multiple organizations).
- **Base URL:** The web address (URL) that clients use to access the organization. It is also used to generate links in the various notification emails that are sent out by the organization, such as for new files or new secure messages. If multiple organizations are in use, each with a different website and SSL server certificate, this URL specifies which website this organization is attached to. It should match the CN on the website's SSL server certificate. Otherwise, leave it blank in the Edit General Information screen to use the system-wide default value, which is automatically determined by the application.
- **Mobile URL:** The web address (URL) for the mobile app and mobile web. The system default is either 'http://BaseURL:8080/mobile/switch' or 'https://BaseURL:8443/mobile/switch' (depending on whether the BaseURL is http or https). Leave the value blank in the **Edit General Information** screen to use the default value.

Note: If MOVEit DMZ server installation was to a Virtual Directory, you must click **Change Information** and enter a Mobile URL that removes the name of the virtual directory from the *Base URL* portion of the Mobile URL. (The name of the virtual directory *will* be in the **Base URL** and will be the URL users use to connect to MOVEit DMZ and MOVEit Mobile). If you do not perform this step, Mobile App users will receive a 404 Not Found Error.

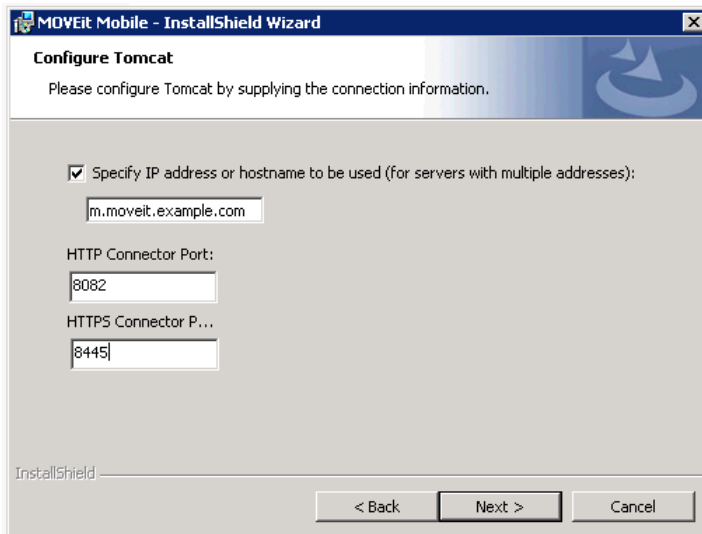
For example, assume the server is "example.com", the virtual directory is "**moveit**", and the URL users will use is "https://www.example.com/moveit". The default **Mobile URL** that will be provided will be "https://www.example.com:8443/moveit/mobile/switch". But you need to change this to "https://www.example.com:8443/mobile/switch".

Otherwise, only change this **Mobile URL** value to reflect changes made to the default Tomcat connection settings during mobile server installation (or if you installed MOVEit DMZ in a Virtual Directory).

The related mobile server installation step is shown below. Notice the specified hostname and changed port numbers in the example. These correspond to the BaseURL and port number portions of the Mobile URL. For example, based on the screen below, you would enter either of these in the Mobile URL:

http://m.moveit.example.com:8082/mobile/switch

https://m.moveit.example.com:8445/mobile/switch



- **Notes:** This field is visible only to SysAdmins, and can be used to keep any notes about the organization necessary.

Security Information

- **Secure Connection Requirement:** This defines the MINIMUM strength of the SSL connection over which MOVEit DMZ will permit communications. Normally set to 128-bit in any production environment.

Note: If this value is set on the **System** organization (#0), SysAdmins will have the option to apply the setting to ALL organizations.

- **Administrator Package Access:** There are two package access settings shown:
 - **Log Viewing:** Determines whether administrators can see audit log entries pertaining to packages (Ad Hoc Transfer). When enabled, package log entries will be viewable by administrators from the Logs page. When disabled, package log entries will only be viewable from the package itself.
 - **Package/attachment Viewing:** Optionally allow administrators only, or administrators and GroupAdmins to access user ad hoc packages and files. When enabled, administrators will be able to list user mailboxes, list the packages in those mailboxes, and then read the packages and download the attached files. Such views and downloads will not affect any view or download limits, but will be audited and viewable to the sender and recipients.
- **Change Setting:** opens the **Change Package Viewing Settings** (on page 556) page.

Note: If these values are set on the **System** organization (#0), they will be taken as the default to be applied to subsequently added organizations.

- **Act as Admin and Edit:** These link to specific organization pages - **Users, Groups, Folder, or Other Settings** - allow SysAdmins directly go to these specific organization pages and temporarily perform as Admins.
- **File/Folder and Ad Hoc-Only:** This displays which user interfaces are enabled (the File/Folder interface, the Ad Hoc Package interface, or both). The **Change Setting** link is enabled for organizations using a MOVEit DMZ with Ad Hoc license. The link opens the ***Change User Interface Settings*** (on page 553) page, which enables the SysAdmin to configure the user interface allowed for the particular organization.
- **Maximum User Count:** This displays the maximum total user count enabled for the organization. The **Change Setting** link opens the ***Change Maximum Users Count*** (on page 554) page, which enables the SysAdmin to configure maximum counts for Total Users, End Users, and Temporary Users for the particular organization.
- **Prevent Changing Signon/Signoff Logging:** This displays the setting for preventing logging of sign on and sign off events for the organization. Disabled means that the logging is not prevented. Enabled means that the logging is prevented. The **Change Setting** link opens the Prevent Changing Signon/Signoff Logging page, where you can change this setting.

Profile - Change User Interface Settings

The **Change User Interface Settings** page enables the SysAdmin to configure the user interface allowed for the particular organization. End users can be configured to see the File/Folder interface, the Ad Hoc Package interface, or both.

Change User Interface Settings...

This setting configures the user interface allowed for this Organization. End users will be allowed to see the File/Folder interface, the Ad Hoc Package interface, or both.

Show User Interface:

☐ File/Folder Interface Only
☐ Ad Hoc Package Interface Only
☒ Both File/Folder and Ad Hoc Interface

Change User Interface Settings

For this organization, select one of the choices:

- **File/Folder Interface Only:** Show the user interface for the shared access workspace (filesystem) capability.
- **Ad Hoc Package Interface Only:** Show the user interface for the email attachment-replacement capability.
- **Both File/Folder and Ad Hoc Interface:** Show both user interfaces.

Change User Interface Settings - After making a new selection, click this button to apply the change.

Return - Click this link to return to the **Organization Profile** page.

Profile - Change User Interface Settings

The Change Maximum User Count page enables the SysAdmin to optionally configure the maximum user counts for the particular organization.

Change Maximum User Count...

As System Administrator, you have the ability to limit the number of users that may be created in this Organization. Org Administrators will be notified on their home page when the number of users is within 10% of the configured maximum.

The system Maximum User Count is: Unlimited

☐ Maximum Total User Count for this Organization is Unlimited.

Maximum Total Users: Defines the total number of users that may be created in the Organization, including Admins of all types, End Users, and Temporary Users. Set to "0" for no organization level Maximum Total Users. May not exceed the "system Maximum User Count", which is the maximum number of users licensed.

Maximum Total Users:

Maximum End Users: Defines the total number of End Users that may be created in the Organization. Set to "0" for no organization level Maximum End Users. May not exceed the Maximum Total Users if that number is set to something other than 0. May not exceed the "system Maximum User Count", which is the maximum number of users licensed. Note: The sum of Maximum End Users and Maximum Temporary Users is allowed exceed the Total Maximum Users.

Maximum End Users:

Maximum Temp Users: Defines the total number of Temporary Users that may be created in the Organization. Set to "0" for no organization level Maximum Temp Users. May not exceed the Maximum Total Users if that number is set to something other than 0. Note: If the Maximum Total Users is set to 0, the Maximum Temp Users is allowed to exceed the "system Maximum User Count" (and will, in fact, not be capped by the system Maximum User Count).

Maximum Temp Users:

[Change Maximum User Counts](#)

As System Administrator, you have the ability of limit the number of users that may be created in this Organization. (Org Administrators will be notified on their home page when the number of users is within 10% of the configured maximum.)

The default for unlimited licenses is that the **system Maximum User Count** is **Unlimited** and the check box is selected for **Maximum Total User Count for this Organization is Unlimited**.

Clear the check box and three additional fields display:

- **Maximum Total Users:** Defines the total number of users that may be created in the Organization. (Includes Admins of all types, End Users, and Temporary Users.) Excludes deleted End Users. Excludes Guest Users. Setting to 0 means do not set an organization level Maximum Total Users. May not exceed the **system Maximum User Count**, which is the maximum number of users licensed.
- **Maximum End Users:** Defines the total number of End Users that may be created in the Organization. (Includes inactive End Users.) Excludes deleted End Users. Excludes Temporary Users, Guest Users, and Admins. Setting Maximum End Users to 0 means do not set an organization level Maximum End Users. May not exceed the Maximum Total Users if that number is set to something other than 0. May not exceed the **system Maximum User Count**, which is the maximum number of users licensed.

Note: The sum of Maximum End Users and Maximum Temporary Users *is allowed* exceed the Total Maximum Users.

- **Maximum Temp Users:** Defines the total number of Temporary Users that may be created in the Organization. (Includes inactive Temporary Users.) Excludes deleted Temporary Users. Excludes Guest Users, End Users, and Admins (all types). Setting Maximum Temp Users to 0 means do not set an organization level Maximum Temp Users. May not exceed the Maximum Total Users if that number is set to something other than 0.

Note: If the Maximum Total Users is set to 0, the Maximum Temp Users *is allowed* to exceed the "system Maximum User Count" (and will, in fact, not be capped by the system Maximum User Count).

Change Maximum User Counts - After entering new values, click this button to apply the changes.

Return - Click this link to return to the **Organization Profile** page.

Profile - Change Package Viewing Settings

The Change Package Viewing Settings page enables the SysAdmin to configure two package access settings for administrators of the particular organization: Log Viewing and Package/attachment Viewing.

Change Package Viewing Settings...

This setting, when enabled, allows audit log entries related to Ad Hoc Transfer to be shown in the main Logs page. This allows administrators to see all Ad Hoc Transfer related log entries in an organization.

Show Ad Hoc Transfer Entries in Log View: ☐ Disabled ☒ Enabled

This setting, when enabled, allows administrators to view the mailboxes and packages for users under their control, and download any attachments associated with those packages. This may be allowed for either administrators only, or administrators and GroupAdmins. Viewing a package or downloading an attachment will be audit logged and visible to the user, though no viewing or download limits will be affected.

Allow administrators to view user Ad Hoc Transfer packages and files:

Administrators and GroupAdmins may view user packages and files

Change Package View Settings

Show Ad Hoc Transfer Entries in Log View: Click Disabled or Enabled.

Allow administrators to view user Ad Hoc Transfer packages and files: Select one of the following three options for this setting:

- Disabled
- Administrators may view user packages and files, but GroupAdmins may not
- Administrators and GroupAdmins may view user packages and files

Change Package View Settings - After making new selections, click this button to apply the changes.

Return - Click this link to return to the Organization Profile page.

Schemes

Schemes - Overview

Schemes describe a set of colors and background images used by a particular organization. The scheme used by any particular organization is selected from the **Appearance** section of the **Settings** page.

A separate **Schemes** link and page is available only to SysAdmins, who can view, manage, and delete custom schemes.

All Color Schemes

Name	Type	Stylesheet	
MOVEit 2014	Stock	stylesheet_MOVEit_2014.css	
MOVEit Gray	Stock	stylesheet_MOVEit_Gray.css	

Select Which Color Schemes to View...

Pick a Type: [All Schemes](#) - [Stock Schemes](#) - [Custom Schemes](#)

The schemes list contains several columns:

- **Name:** The name of the scheme. Click on a name to display the **Scheme Profile** (on page 559) page for that scheme.

Note: ALL Admins in all organizations will be able to view these names, so do not use company-specific scheme names with custom schemes if you do not want your client organizations to know each other's identity. See [Upgrading from a Custom Scheme or a Supported Legacy Scheme](#) for a list of supported legacy schemes.

- **Type:**
 - **Stock:** Stock schemes are reinstalled with each new release; SysAdmins cannot add, delete or change them.
 - **Custom:** Custom schemes are managed completely by SysAdmins.

Note: A new install of MOVEit 8.1 comes with two schemes: MOVEit 2014 (default) and MOVEit Gray.

If you upgrade to MOVEit 8.1 while using a custom scheme or one of the supported legacy schemes, you will see the name of your custom/legacy scheme in this list also. See ***Upgrading to MOVEit 8.1 From a Custom Scheme or a Supported Legacy Scheme*** (<http://docs.ipswitch.com/MOVEit/DMZ8.1/Help/Admin/en/index.htm#28297.htm>) for a list of supported legacy schemes.

If you upgrade to MOVEit 8.1 while using one of the non-supported legacy schemes, your scheme will default to MOVEit 2014. See ***Upgrading to MOVEit 8.1 from a Non-Supported Legacy Scheme*** (<http://docs.ipswitch.com/MOVEit/DMZ8.1/Help/Admin/en/index.htm#28298.htm>) for a list of non-supported legacy schemes.

- **Stylesheet:** The name of the cascading stylesheet (*.css) associated with the scheme.
- **Available actions:**
 - **Open:** Opens the Scheme Profile (on page 559) (shown below)
 - **Delete:** Deletes a Schemes - Custom (on page 562) (after confirmation)
 - **Preview:** Opens a new window containing a preview of the selected scheme.

An Add Scheme link lets SysAdmins upload new schemes.

Scheme Profile

Scheme Profile displays details about a single scheme as well as the complete code used in the stylesheet.

Scheme Profile (Basic Tan)

Information

Name: Basic Tan
ID: 4169
Stylesheet: stylesheet_Custom_Basic_Tan.css

 [Edit Scheme Information](#)

Stylesheet Code

```
.sectiontitle
{
  FONT-WEIGHT: bold;
  FONT-SIZE: 12pt;
  COLOR: #000000;
  FONT-FAMILY: Tahoma, Arial, Lucida Sans Unicode, Verdana;
  BACKGROUND-COLOR: #CD9C9C
}
.userhead
{
  FONT-SIZE: 10pt;
  COLOR: #000000;
  FONT-FAMILY: Tahoma, Arial, Lucida Sans Unicode, Verdana;
  BACKGROUND-COLOR: #CD9C9C
}
.listrow1
{
  BACKGROUND-COLOR: #ffffff
}
```

Click **Edit Scheme Information** to change the name and the stylesheet of the scheme.

Note: The **Edit Scheme Information** link does not appear for stock schemes.

You can either click **Choose File** to select an existing css stylesheet, or edit the scheme's css code directly in the css window.

Edit Information

Name:

ID: 9738

Stylesheet: stylesheet_Custom_Teletracking.css

[Change Scheme Information](#)

Update Stylesheet

Select a new CSS file from your system:

No file chosen

[Update Stylesheet](#)

~ or ~

Update the stylesheet code directly:

```
.sectiontitle
{
    /* text-shadow: 1px 1px #ddd; */
    font-size: 1.8em;
    color: #00674E;
    display: block;
    /* border-top: 1px dotted #999; */
    margin-top: 10px;
    padding: 4px 0;
}

.sectiontitle_no_border
{
    border-top: 0px;
}

.userhead
{
    font-size: 1em;
    /* background: url(../images/userbar_bg.png) #be
```

[Update Stylesheet Code](#)

Schemes - Custom

SysAdmins are encouraged to create their own cascading stylesheets (*.css) and to upload them as custom schemes to be used by any organization on their system.

Creating a Custom Scheme

The following steps will quickly allow you to create and test a custom scheme.

- 1 Sign on with a SysAdmin account.
- 2 Click the **Schemes** link to list schemes and **Preview** the schemes.
- 3 Click the **Open This Scheme** button next to the scheme similar to the look you wish to achieve.
- 4 Create a new text file on your desktop and rename it **myscheme.css**.
- 5 Copy the **Stylesheet Code** from the **Scheme Profile** into your new stylesheet and save it.
- 6 Make changes to the stylesheet on the desktop and save. See **Recognized Styles** below for a list of css styles you can change to achieve the look you want.
- 7 From the **Scheme** list, press the **Add Scheme** link, browse to the stylesheet on the desktop, give it a name and upload it.
- 8 From the **Scheme** list, **Preview** your new scheme...and repeat from Step 6 as needed.

Recognized Styles

This section describes the css styles that you may edit to change the look of a scheme. If a style does not appear in your scheme's css, you may add it.

Style	Description
#maintable	ID of the main table that contains the content of each web page. This can be useful for putting a border around the content, or making it a different background color than the rest of the page, for example.
.sectiontitle	Sub-titles of content sections. Specify a font COLOR for this style.
.userhead	Color of the Search box background and the user bar at the top of the page that contains My Account and Sign Out. Specify a BACKGROUND-COLOR for this style.
	Note: Use #userbar to designate a separate color for the top user bar.

Style	Description
<code>a.userhead:link</code>	Color of the links in the user head section. Use of COLOR is required.
<code>a.userhead:visited</code>	Should be identical to <code>a.userhead:link</code> .
<code>a.userhead:active</code>	Should be identical to <code>a.userhead:link</code> .
<code>a.userhead:hover</code>	Should be identical to <code>a.userhead:link</code> .
<code>#userbar</code>	Color of the user bar at the top of the page that contains My Account and Sign Out.
<code>#userbar > td</code>	Color of the borders at the top and bottom of the user bar at the top of the page. Specify BORDER-TOP and BORDER-BOTTOM properties. Example: <code>{border-top:solid 1px #8CC63F; border-bottom:solid 1px #8CC63F}</code>
<code>.listrow1</code>	Odd rows in tables. Specify only a BACKGROUND-COLOR for this style.
<code>.listrow2</code>	Even rows in tables. Specify only a BACKGROUND-COLOR for this style.
<code>.texttiny</code>	Table headers, some table information. Should be similar to <code>.textsmall</code> .
<code>.textsmall</code>	Used for most standard text.
<code>.textnormal</code>	Despite its name, used by larger-than-normal text.
<code>.textbig</code>	Very large text. Should be similar to <code>.textnormal</code> .
<code>.userinput</code>	The font color and size used in user input boxes and drop-down lists. Should be similar to <code>.textsmall</code> .
<code>.userinputarea</code>	Text areas. Should be IDENTICAL to <code>.userinput</code> .
<code>.pageheadingimage</code>	Shows or hides legacy icons. See also Brand (on page 358).
<code>.bulletimage</code>	Shows or hides organization bullets. See also Brand (on page 358).
BODY	Document body. Use of at least BACKGROUND-COLOR is encouraged.
<code>a:link</code>	Color of links. Use of COLOR is required.
<code>a:visited</code>	Color of visited links. Specify a font COLOR.

Style	Description
<code>a:active, a: hover</code>	Color of links when your mouse hovers over them. Specify a font COLOR.
<code>#signonsubmitcontainer .button.signonbutton</code>	Color of the sign on button on the Sign On page. Specify a BACKGROUND-COLOR and font COLOR. You must also add <code>!important</code> to the code. Example: <code>#signonsubmitcontainer .button.signonbutton {background-color:red !important;}</code>
<code>#signonsubmitcontainer .button.signonbutton: hover</code>	Color of the sign on button on the Sign On page when your mouse hovers over it. Specify a BACKGROUND-COLOR and font COLOR. You must also add <code>!important</code> to the code. Example: <code>#signonsubmitcontainer .button.signonbutton: hover {background-color:blue !important;}</code>
<code>#signonauthcontainer</code>	Color of the sign on box. Specify a BACKGROUND-COLOR and BORDER.
<code>.signoncontainer a:link</code>	Style of links on sign on page. Specify a font COLOR and TEXT DECORATION.
<code>a.alert:link</code>	Color used by "HOT" links (i.e. locked out users). Use of COLOR is required. It is recommended that you keep this font COLOR red.
<code>a.alert:visited</code>	Should be identical to <code>a.alert:link</code> .
<code>a.alert:active</code>	Should be identical to <code>a.alert:link</code> .
<code>a.alert:hover</code>	Should be identical to <code>a.alert:link</code> .
<code>.button</code>	Standard button style. Specify a BACKGROUND-COLOR and font COLOR.
<code>.btnPrimary</code>	Color of primary buttons like Save, OK, Upload, Download, Send. Specify a BACKGROUND-COLOR and font COLOR.
<code>.btnSecondary</code>	Color of secondary buttons like Cancel, No, buttons that do not implement an immediate action, or buttons of tertiary importance. Specify a BACKGROUND-COLOR and font COLOR.
<code>.tab.selectedtab</code>	The color of the selected left navigation menu item. Specify a BACKGROUND-COLOR and a font COLOR.

Style	Description
<code>.tab a</code>	The color of the left navigation menu buttons. Specify a BACKGROUND-COLOR and a font COLOR.
<code>.tab a:hover</code> <code>.tab a:active</code>	The color of the left navigation menu buttons with mouse hover. Specify a BACKGROUND-COLOR and a font COLOR. <code>.tab a:hover</code> and <code>.tab a:active</code> usually have the same colors.

Upgrading from a Custom Scheme or a Supported Legacy Scheme

Below is a list of the supported legacy schemes in MOVEit 8.1:

Supported Legacy Schemes
MOVEit Gray
Basic Blue
Basic Green
Basic Tan
MOVEit
MOVEit 2005
Small Fonts Blue Grey
Small Fonts Blue Orange
Small Fonts Grey Teal
Small Fonts MOVEit 2005
Basic Blue Tan
Basic Brown
Basic Candy Red
Basic Red
Basic Teal
MOVEit 2003
Small Fonts Forest Tan

Supported Legacy Schemes
Small Fonts Maroon Grey
Small Fonts Maroon Maize
Small Fonts MOVEit 2003
Small Fonts Navy Grey
Small Fonts SNI Pro
Small Fonts White Navy
Windows XP Blue

If you upgrade to MOVEit 8.1 while using one of the supported legacy schemes above or while using a scheme you have already customized, you will still be able to use your existing scheme, but you will see the following changes:

- The Signon page has a new layout and color.
- The left navigation menu has a new look.
- Some text links have changed to buttons throughout the interface.

To alter these colors to match your existing scheme, see ***Schemes - Custom*** (on page 562).

To customize the left navigation menu colors in particular, follow these steps:

- 1 Determine your current DMZ color scheme via **Settings > Appearance/Brand > Color Scheme**.
- 2 Find the color scheme css file located at *MOVEit DMZ file directory\wwwroot\templates*. The default path is C:\MOVEitDMZ\wwwroot\templates.
- 3 Copy and paste the following css code at the end of your color scheme css file:

```
.tab a,
.tab span {
    font-weight:bold;
    color:#555555;
}
.tab a:link,
.tab a:visited {
    text-decoration:none;
}
.tab a:hover,
.tab a:active {
    text-decoration:none;
```

```
        background-color:#9A7B9C;
        color:white;
        border-top-color:transparent;
        border-bottom-color:transparent;
    }
    .tab.selectedtab a {
        background-color:#4D1F54;
        color:white;
        border-top-color:transparent;
        border-bottom-color:transparent;
    }

    #tab_home.selectedtab a,
    #tab_home a:hover,
    #tab_home a:active {
        background-image:url("../images/iconhome1-selected.png");
    }
    #tab_users.selectedtab a,
    #tab_users a:hover,
    #tab_users a:active {
        background-image:url("../images/iconuser1-selected.png");
    }
    #tab_groups.selectedtab a,
    #tab_groups a:hover,
    #tab_groups a:active {
        background-image:url("../images/icongroup1-selected.png");
    }
    #tab_folders.selectedtab a,
    #tab_folders a:hover,
    #tab_folders a:active {
        background-image:url("../images/iconfolder1-selected.png");
    }
    #tab_messaging.selectedtab a,
    #tab_messaging a:hover,
    #tab_messaging a:active {
```

```
        background-image:url("../images/iconpkg1-selected.png");
    }
    #tab_history.selectedtab a,
    #tab_history a:hover,
    #tab_history a:active {
        background-image:url("../images/iconlogs1-selected.png");
    }
    #tab_stats.selectedtab a,
    #tab_stats a:hover,
    #tab_stats a:active {
        background-image:url("../images/iconstats1-selected.png");
    }
    #tab_settings.selectedtab a,
    #tab_settings a:hover,
    #tab_settings a:active {
        background-image:url("../images/iconsettings1-selected.png");
    }
    #tab_orgs.selectedtab a,
    #tab_orgs a:hover,
    #tab_orgs a:active {
        background-image:url("../images/iconorg1-selected.png");
    }
    #tab_schemes.selectedtab a,
    #tab_schemes a:hover,
    #tab_schemes a:active {
        background-image:url("../images/iconscheme1-selected.png");
    }
}
```

- 4** Edit the following styles in the above added code so they match your desired color scheme:
- **.tab a:hover, .tab a:active:** The BACKGROUND-COLOR property is the color that displays when you hover your mouse over one of the left navigation menu items.
 - **.tab.selectedtab a:** The BACKGROUND-COLOR property is the color that displays when you select one of the left navigation menu items.

Select background colors that are of similar brightness for both of the above styles.

IMPORTANT: If the background colors you select are a light shade, you must also do the following:

-- Change the COLOR property for both styles from white to a dark color like black. (The COLOR property controls font color. If the BACKGROUND-COLOR is a light shade, the font COLOR will need to be dark to display clearly.)

-- Do not include any code that begins with `#tab_`. Either remove that code, or comment it out. (The `#tab_` code sets the icon colors in the left navigation menu to white upon hover or selection. If you select a light BACKGROUND-COLOR, you will want to keep the default dark icons.)

- 5 Return to MOVEit DMZ and click **Home**. The **Home** link in the left navigation bar will highlight with the color you specified.
-

Tip: If the highlights do not appear, clear your browser cache, restart the browser, and sign on to DMZ. If the highlights still do not appear, make sure you're using a browser that MOVEit DMZ supports.

Upgrading to MOVEit 8.1 from a Non-Supported Legacy Scheme

If you upgraded to MOVEit 8.1 while using one of the non-supported legacy schemes below, your scheme will switch automatically to the new MOVEit 2014 scheme.

Non-Supported Legacy Schemes
Emerald
Halloween
Harvest
Inverso
Leather
Mario Bros
Metal Light
Ocean
Olive Paper
Red Alert
Sci Fi Dark
Small Fonts Grey Red
Small Fonts Olive
Small Fonts Orange
Small Fonts Periwinkle
Small Fonts Red Periwinkle

Non-Supported Legacy Schemes
Small Fonts Rose
Small Fonts Sea Green
Small Fonts Steel
Small Fonts Steel Blue
Small Fonts Teal Violet
Small Fonts White Pink
Small Fonts Windows XP Blue
Standard Networks
Subtle Blue
Subtle Green
Subtle Orange
Subtle Purple
Subtle Red
Subtle Teal
Subtle Yellow
Valentine

Custom Background Images

Your custom scheme may require the use of custom background images. Because of the many different background image options possible, MOVEit DMZ does not provide an interface to directly upload these images into the system. (SysAdmins must instead copy these images into the proper directories on the filesystem by hand.) However, MOVEit DMZ DOES prefer that your custom background use a location and naming convention.

Save your custom background images in the `images\customscheme` directory. Name your images as `SCHEMENAME_STYLE.EXT`.

To access your custom image from a stylesheet, use the following *relative* syntax:

`BACKGROUND-IMAGE: url(../images/customscheme/SCHEMENAME_STYLE.EXT)`

Example:.

`BACKGROUND-IMAGE: url(../images/customscheme/acme_userhead.gif" )`

FTP Server

This section contains reference information describing the features of the MOVEit FTP server.

FTP - Overview

The MOVEit FTP server provides both FTP over SSL and insecure (regular) FTP services. SSL client certificate support is also available with the click of a checkbox. FTP access is provided to the same underlying folder and file structure made available through MOVEit's SSH and Web Interface as well.

Be aware that although "SSL" and "FTP over SSL" are Internet standard protocols (RFC 2228, etc.), Secure FTP is not implemented by all FTP clients. Since, for your protection, MOVEit FTP insists that all communications with the client be encrypted, not all FTP clients will work with MOVEit FTP by default. See **Client Support** (on page 793) for a current list of compatible clients. (Any client which supports AUTH SSL, AUTH TLS, EXPLICIT, IMPLICIT or RFC 2228 will generally work.)

Insecure FTP

To enable insecure (regular) FTP on your MOVEit FTP server, you must use the MOVEit DMZ Config utility to explicitly turn this feature on. The main disadvantage of insecure FTP is that usernames, passwords and sensitive data are passed in the clear in this mode.

To mitigate risk, it is usually recommended that insecure FTP be opened to internal hosts only. Where this is not an option, it is recommended that files at least be encrypted before they are sent, even though the username and password will still be transported unprotected across the Internet. (It is usually much less work to configure and deploy a secure command-line FTP client, such as MOVEit Freely, than it is to deploy a system relying on client-based encryption, however.)

Notable Features

MOVEit FTP runs as a standalone application (not part of IIS). Some of its notable features are listed below.

- Reads / writes directly to MOVEit's secure file storage. Unencrypted data is never written to disk.
- Uses secure communications via SSL encryption on both control and data ports.
- Supports all three forms of secure FTP: TLS-C, TLS-P and IMPLICIT.
- Uses MOVEit usernames and passwords. MOVEit IP restrictions are also supported.
- Uses MOVEit logging to record signons, signoffs, uploads and downloads.
- Runs as a Windows service named MOVEitDMZFTP. MOVEit FTP can also run as an ordinary desktop application; this capability is typically used for testing and troubleshooting.
- Uploads and downloads files, with compatible clients, using compression and integrity checking.
- Can be bound to a specific IP address.
- Supports Cleartext Cmd Channel (CCC), a finite number of FTP data ports and server-side NAT translation to help work around firewall and NAT issues.

Installation

MOVEit FTP is installed by the same setup program that installs MOVEit. The setup program offers the option to install MOVEit FTP as a service. The option is set by default.

Normally, you will install the program as a service. However, you can instead run the program manually by choosing the Start menu shortcut **RunMOVEit DMZ FTPmanually** after installation. In manual mode, MOVEit FTP displays a window containing two subwindows, one containing the status of the current connections and the other showing a scrolling list of messages.

MOVEit FTP's window is normally not displayed when it is running as a service. However, you can cause it to be displayed by changing the service to allow it to interact with the desktop. To do this on Windows 2003, choose Start / Settings / Control Panel / Administrative Tools / Services, and choose the MOVEit DMZ FTP service. Right-click and choose Properties. Choose the Log On tab. Choose *Allow service to interact with desktop*. You will have to stop and restart the service for this change to take effect.

Directory Structure

MOVEit FTP's directory structure is the same as that which is visible through the web interface, except for those users who have the "Chroot" option enabled for their default folder. Those users will only be able to see the files and folders in and below their default folder and will not be able to navigate to folders outside their default folder. See the *User Settings - Default Folder* section of the **Web Interface - Users - Profile** (on page 286) documentation page for more details.

The initial directory upon logon depends on the user type. End users and group admins will be placed in their default folder (usually their home folder), while administrators will be placed in the root folder.

User type	Initial directory
SysAdmin	/
Administrator	/
FileAdmin	/
GroupAdmin	The GroupAdmin's home directory or a designated default folder
User	The User's home directory or a designated default folder

TempUser N/A (*not allowed to sign on to FTP*)

A "dir" command shows only the folders to which the user is permitted access, so not all users will get the same results from a "dir".

Disabling the FTP Service

To disable the MOVEit FTP service you may use the Microsoft Services control panel to mark the MOVEit DMZ FTP service as disabled. The MOVEit DMZ "Check" utility (usually run after installations and upgrades) will automatically be aware if you have disabled the FTP service and will not try to check it in that situation.

FTP - Configuration

The MOVEit DMZ Config utility is used to configure the MOVEit FTP server. (Users, groups, folder settings and the like are generally maintained through the Web Interface or MOVEit API.) Run the configuration program by choosing the Start menu shortcut MOVEit DMZ Config. This program uses a tabbed dialog to group the settings by function.

MOVEit FTP will immediately apply configuration changes the next time a new connection is received.

Exception: If changes are made to the FTP explicit or implicit ports, the MOVEit FTP service must be restarted for these changes to take effect.

FTP Ports Tab

The screenshot shows the 'Configure MOVEit DMZ' dialog box with the 'FTP Ports' tab selected. The dialog has a title bar with a close button. Below the title bar is a tabbed interface with tabs for License, Status, Paths, Email, Settings, and Database. The 'Settings' tab is active, and within it, the 'FTP Ports' sub-tab is selected. The 'FTP Ports' section contains three main groups of settings: 'Control Ports', 'Data Ports', and 'Miscellaneous Settings'. In 'Control Ports', 'Explicit' is set to 21 (usually 21) and 'Implicit' is set to 990 (usually 990). 'Optional Ports that Require Client Certificates' has both 'Explicit' and 'Implicit' set to 0 (0 = none). In 'Data Ports', 'Active' is set to 20 (usually 20 or 989), 'Passive Range' is set from 3000 to 3100 (minimum range of 4), and the 'Enforce passive port range' checkbox is checked. In 'Miscellaneous Settings', 'Bind to IP Address' is set to 0.0.0.0 (0.0.0.0 = all available IP's), 'Connection Limit' is set to 32 (usually 32 - min 1 max 1000), and both 'Require passive transfers' and 'Allow CCC command' checkboxes are unchecked. At the bottom of the dialog are buttons for OK, Cancel, Apply, and Help.

License	Status	Paths	Email	Settings	Database
FTP Ports	FTP Certs	FTP IPs	SSL	SSH	SSH Ciphers

Control Ports

Explicit: (usually 21) Implicit: (usually 990)

Optional Ports that Require Client Certificates

Explicit: (0 = none) Implicit: (0 = none)

Data Ports

Active: (usually 20 or 989)

Passive Range: to (minimum range of 4)

☒ Enforce passive port range

Miscellaneous Settings

Bind to IP Address: (0.0.0.0 = all available IP's)

Connection Limit: (usually 32 - min 1 max 1000)

☐ Require passive transfers

☐ Allow CCC command

OK Cancel Apply Help

Control Ports

- **Explicit:** The default for the explicit FTP port is 21, the value used by most FTP servers. The explicit port requires the use of the AUTH command for TLS-C or TLS-P secure communication. Set to 0 to disable this port and type of FTP over SSL.
- **Implicit:** The default port for implicit secure FTP is 990. The implicit port is for FTP clients that negotiate a secure connection immediately at startup. Set to 0 to disable this port and type of FTP over SSL.
- **Client Certs Explicit:** The "client certs" explicit port is like the regular "explicit port" except it requires all connecting FTP clients to authenticate with an SSL client certificate. Set to 0 to disable this port and type of FTP over SSL.
- **Client Certs Implicit:** The "client certs" implicit port is like the regular "implicit port" except it requires all connecting FTP clients to authenticate with an SSL client certificate. Set to 0 to disable this port and type of FTP over SSL.

Data Ports

- **Active:** The active TCP port is the local TCP port from which active mode data connections to remote clients will be initiated. When not running in passive mode, FTP servers connect to clients to transfer data. Most FTP servers use a randomly-assigned local port number for this purpose. (The local port number is the TCP port number from which connections are made.) This works fine for many sites, but some sites have restrictive rules configured on their firewalls. MoveIT DMZ FTP allows you to tell the FTP server to always use the same port number on the initiating end of the connection. A typical value for this obscure setting is 20 for explicit FTP or 989 for implicit. You can only choose one of those two values, however. If you want the usual behavior of a randomly-assigned port number, use a setting of 0. If you are in doubt, just use the setting of 20.

Passive Range: This is a feature which helps sites which position a firewall between the MOVEit FTP computer and end users. (i.e., almost everyone) When running in passive mode, FTP dynamically creates ports on which it listens for data connections from the remote FTP clients. In order to accommodate this behavior, network administrators must allow incoming connections on these ports. The port numbers used for this purpose are normally greater than 1023, but otherwise cannot be predicted in advance. And because sessions are encrypted, there is no way for even a smart firewall to learn the port numbers on-the-fly. Hence, firewalls must normally be configured to allow outside users to connect to any port greater than 1023.

To address this, MOVEIT DMZ FTP provides an option to enforce the range of ports that it will choose when in passive mode. If you choose this option, you must select a range of ports on which FTP will listen for data connections; for instance, 2000-2200.

The advantage of this option is that it allows your network administrator to open up only a limited range of ports to which remote FTP clients can connect. This provides a modest increase in security on your site (when compared to opening up 64,000 or even just 4,000 ports!).

By default, the configured range is 3000-3100. Most sites will want to keep this range down to 4-100 consecutive ports. (The range used by most Windows client applications is 49152 - 65535).

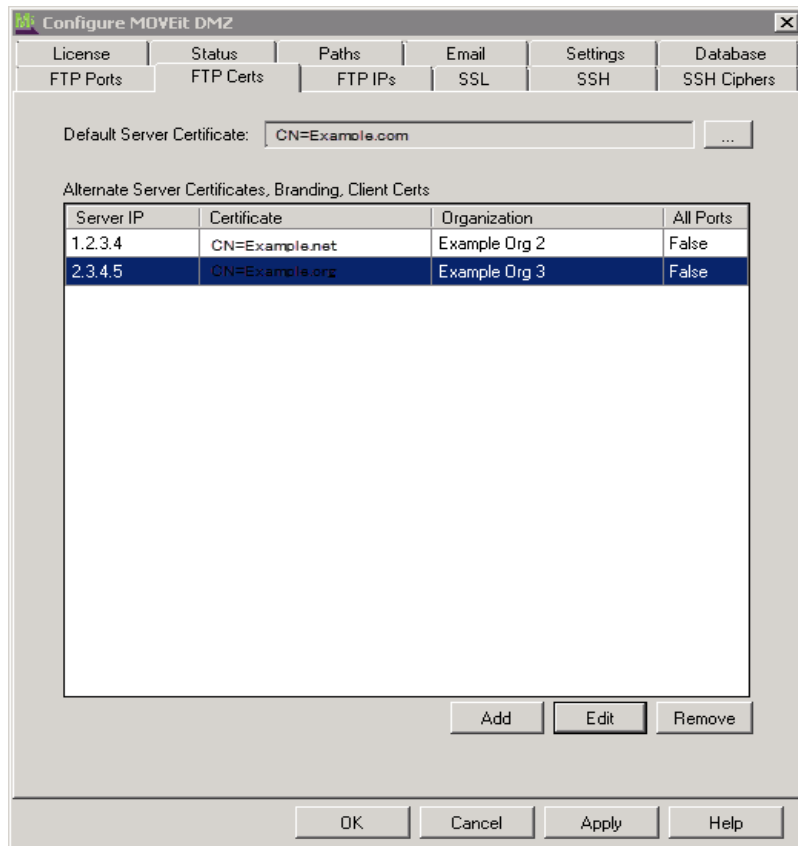
- **Enforce passive port range:** Check this to enforce the range configured above. (Otherwise, a port range of 49152 - 65535, set by the operating system, will apply.)

Miscellaneous Settings

- **Bind to IP Address:** Leave blank to bind to all available IP addresses (default). Enter a specific IP address to bind the FTP server (both explicit and implicit ports) to a specific IP address.
- **Connection Limit:** The maximum number of control connections the FTP server will listen to at any particular time. The default is 32. Be sure to set this number to a value larger than the number of FTP ports in your passive range.
- **Require passive transfers:** Check this to disallow active mode data connections. Most sites will want to check this option unless a significant number of their FTP clients use CCC and all firewalls involve know how to dynamically open FTP data ports.
- **Allow CCC command:** This option (disabled by default) allows the FTP over SSL interface to support the Cleartext Command Channel "CCC" command. This allows the FTP/SSL command channel to switch back from an encrypted channel to cleartext after a username and password have been safely sent and interpreted. CCC allows FTPS sessions to take advantage of firewalls that know how to handle NAT with non-secure FTP without opening fixed ports.

Warning: CCC carries the security risk of exposing file names, folder paths and other control information to anyone listening.

FTP Certs Tab



Default Server Certificate: The default certificate is the SSL server certificate used for transport encryption. This certificate must have already been created and installed on the system. Typically, you will use the same certificate that you have already installed on your MOVEit web server.

Certificates are normally purchased through a certification authority such as Thawte or Verisign. However, free software is available to allow you to create your own at no cost. For example, the Certificate Services component of Windows Server can be used to create certificates. Using certificates you created yourself is generally not recommended, because client programs consider them to be non-trusted, and raise warning dialogs.

Alternate Certificates, Branding, Client Certs: Alternate SSL server certificates may be assigned to each IP address of your MOVEit server. This is a way to have MOVEit FTP use a different certificate for connections through different networks.

Note: If you wish to run a secure "multi-homed FTP server", you may need to configure these options. You cannot use alternate server certificates if you decide to bind to a single IP address.

For example, if MOVEit is connected to the internet through one network interface card (NIC) and to a local intranet through another NIC, you can give an alternate certificate for use by connections through the second NIC.

The **Alternate Certificates, Branding, Client Certs** list displays the columns **Server IP** and **Certificate**, as the alternate certificate is paired with a specific local IP address or IP mask.

In addition, the list has these columns:

- **Organization** - Displays the organization name for each certificate.
- **All Ports** - Displays "True" if you are requiring client certs on all FTP command ports.

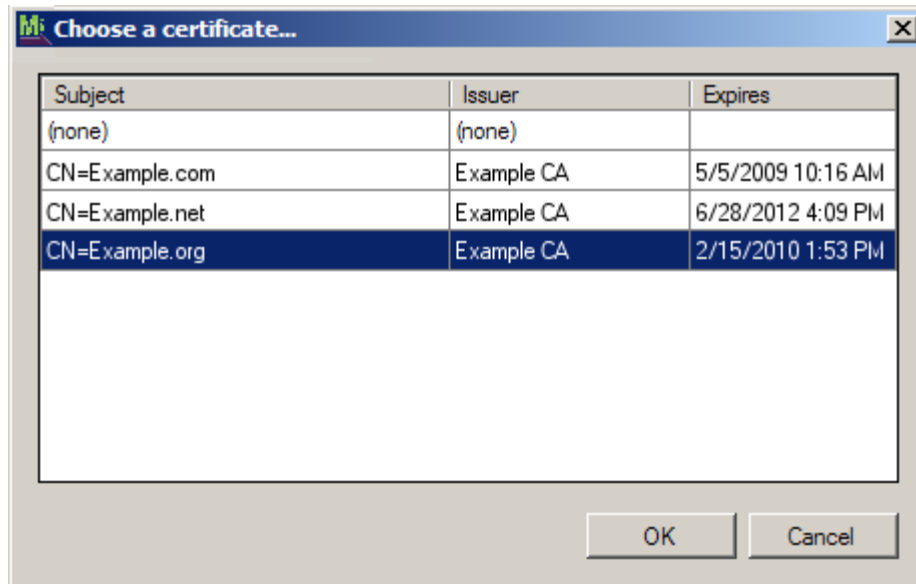
Click **Add** to open the **Add FTP Alternate Certificate** dialog.

In addition to linking particular certificates with particular IP addresses, you may also link a particular Organization to a particular IP address to present a different signon banner to FTP users rather than the default Org's banner.

You may also decide to enforce more stringent client certificate requirements, that is, require client certs on all FTP command ports for the particular alternate IP address (overriding the client certificate port settings of the default IP address binding, which is configured on the **FTP Ports** tab). If **Yes** is selected for this option in the dialog box, back in the **Alternate Certificates, Branding, Client Certs** list, the **All Ports** column will show "True" for that certificate entry.

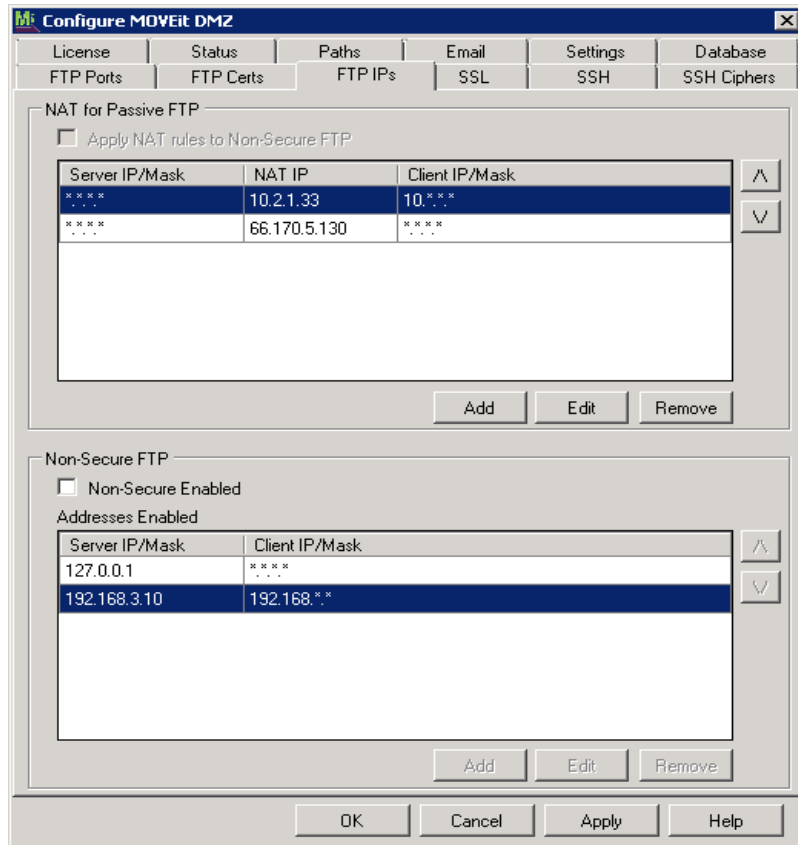
In the **Alternate Certificates, Branding, Client Certs** list, you can select a certificate and either click **Edit** (which opens the **Edit FTP Alternate Certificate** dialog) or **Remove**.

Server Certification Selection List



Clicking any of the "..." server certificate browse buttons will pop up a list of server certificates to select. Be sure to pick a certificate with an **Expires** date later than today. To select a certificate, double-click it, or select it and click the OK button.

FTP IPs Tab



NAT for Passive FTP

Whether to map IP addresses for Network Address Translation (NAT) is an advanced feature for sites that use a firewall to do "NAT'ing". It applies only to passive mode transfers. If you choose to use this feature, you should provide a list of NAT rules in most-specific-to-least-specific order with a "catch-all" at the bottom. Each NAT rule consists of an IP mask, and the external IP address to use for clients matching that mask. Each mask has the form "m.m.m.m", where each m is a decimal number like 208, or a * wildcard. Each external IP address is the usual dotted decimal number and should be the external IP address to which the firewall maps your FTP server.

The most common configuration resembles the following example. This provides an internal IP address (10.2.1.33) to clients connecting from internal clients (10.*.*), but provides an external IP address to all other (external) clients.

```
ServerIP=*. *.*.*, NatIP=10.2.1.33, ClientIPs=10.*.*.*
ServerIP=*. *.*.*, NatIP=66.170.5.130, ClientIPs=*. *.*.*.*
```

Another configuration involves "multihoming" where different hostnames have been mapped to different external IP addresses (66.170.5.130 and 66.170.5.131) which come in to two different internal IP addresses (10.2.1.33 and 10.2.1.34) on the same MOVEit DMZ machine. In this case we want to return the correct IP address for each external connection while still returning the correct address for internal clients.

```
ServerIP=10.2.1.34, NatIP=10.2.1.34, ClientIPs=10.*.*.*
ServerIP=*. *.*.*, NatIP=10.2.1.33, ClientIPs=10.*.*.*
ServerIP=10.2.1.34, NatIP=66.170.5.131, ClientIPs=*. *.*.*.*
ServerIP=*. *.*.*, NatIP=66.170.5.130, ClientIPs=*. *.*.*.*
```

If your NAT rules consist solely of the rule:

```
ServerIP=*. *.*.*, NatIP=208.33.33.33, ClientIPs=208.*.*.*
```

...then a client accessing any IP address your machine from 208.122.3.4 will be told to perform passive transfers to 208.33.33.33, even though the actual internal IP address of your FTP server may be something completely different, for example, 192.168.1.10. Clients accessing your FTP server from outside the 208.* domain will be given the actual address of your FTP server (192.168.1.10).

If you have more than one NAT rule, you can change the order of evaluation by using the up- and down-arrow buttons to the right side of the list.

Rules to handle localhost or 127.0.0.1 addresses are not necessary. Connections from these addresses will always be instructed to connect their data channels to the same address.

Non-Secure FTP

Whether to allow access from Non-Secure FTP clients. This feature lets you open the FTP server up to clients that do not use secure FTP (encrypted) transfers. This significantly reduces the security of MOVEit because data can potentially be "sniffed" on the network. But in some circumstances, such as inside a company's intranet, that level of security is not important. Or, in other cases, there is simply no other way to transfer securely from a certain client. In order to open FTP up to non-secure transfers, you need to not only check the enabling box, you also need to add the specific IP addresses or IP masks that are allowed to perform these non-secure transfers. Non-secure mode is enabled using pairs of IP addresses. Each pair consists of a local IP address (or mask) on the MOVEit server, (corresponding perhaps to a specific network interface), and an external IP address or mask corresponding to a network FTP client. As with the NAT list, you can move entries up and down within the list.

Before any of the configured IP addresses will be allowed to connect insecurely, the **Non-Secure FTP Enabled** checkbox **MUST** be checked (and confirmed).

This option **MUST** be enabled before any user-level "allow non-secure FTP" interface setting can be used.

Warning: Non-Secure FTP carries the security risk of exposing usernames, passwords, file data, file names, folder paths and other control information to anyone listening.

Diagnostic Logs

The MOVEit FTP server's diagnostic log settings can be changed on the Status tab of the configuration utility. For more information about this tab, see the ***Configuration Utility*** (on page 135) topic.

Paths Tab

The MOVEit FTP server communicates with MOVEit using the **Machine URL** configured on this tab. For more information about this tab, see the ***Configuration Utility*** (on page 135) topic.

Initial Banner Language

The initial security banner and notice will be provided in the default language of the default organization, or in English, if no default organization exists. (See the ***Miscellaneous*** (on page 540) system settings page for more information about default organizations.) To change the language of the initial security banner and notice, log on to default organization on the system as an org admin. Change the org's default language using the ***International*** (on page 414) settings page.

Selecting SSL Versions and SSL Encryption Methods (SSL Tab)

In the MOVEit DMZ Config utility, you can use the SSL Tab to *select the SSL versions and SSL encryption methods* (on page 175).

FTP - Glossary

FTP Protocol Terms

Active Transfer Mode - A method of establishing FTP data connections in which the server initiates a connection back to the client, typically from server TCP port 20 to a high numbered TCP port on the client. (The client chooses the high port on which it listens.)

Passive Transfer Mode - A method of establishing FTP data connections in which the client initiates a connection to the server, typically from a high numbered TCP port on the client to a high numbered TCP port on the server. (The server chooses the high port on which it listens.)

Data centers generally prefer the use of passive mode over active mode for two reasons:

- 1 Client site firewalls (and security people) typically have fewer complaints about passive mode because its all outbound traffic to them.
- 2 The risk of a server-resident "dial-out" trojan horse or other malicious client program is largely mitigated if the server never has to establish connections to the outside world.

FTP Over SSL Terms

Explicit Connection Mode - A method of establishing a secure FTPS control connection in which an unsecured channel is built up to use SSL after the client and server exchange a few parameter commands in the clear. There are two flavors of explicit mode: TLS-C and TLS-P. Both are supported by all MOVEit products. Typically run on TCP port 21.

Implicit Connection Mode - A method of establishing a secure FTPS control connection in which an SSL session is established immediately upon connection. (Similar to HTTPS's relationship to HTTP.) Typically run on TCP port 990.

Data centers generally prefer the use of implicit mode over explicit mode for three reasons:

- 1** Implicit mode connections will not be mangled by "FTP-aware" firewalls. (Explicit mode connections often fail with "handshake failed" messages when going through certain firewalls.)
- 2** Implicit mode offers no options to the client. (There are fewer options to mess up.)
- 3** Implicit mode connections begin life as secure connections, ensuring no username or passwords are ever accidentally "leaked" by shoddy clients or fumbling users before the channel can be secured.

Certificate Terms

CA - Abbreviation for Certificate Authority

Cert - Abbreviation for "Certificate" - See SSL Certificate

Certificate - See SSL Certificate

Certificate Authority - 1. A certificate used to sign (a.k.a. "issue") any other certificate. 2. A company or department which performs the operation of signing a certificate (e.g., Comodo, Thawte, etc.)

"Chain Up" - A phrase which indicates asks whether a particular certificate, the certificate's CA, the CA's CA, or any other member of the *chain* of CA signatures is signed by a particular CA. (e.g., "Does that client cert 'chain up' to Comodo?")

CN - Abbreviation for Common Name

Common Name - A text certificate attribute which frequently contains the username, full name, company name, hostname or email address of the person or computer a particular certificate was created for. (e.g., an SSL server cert might have a CN of "www.mycorp.com" and an SSL client cert might have a CN of "john.smith@mycorp.com")

Fingerprint - Usually, another name for "MD5 Hash", especially if SSH keys are involved. This term could also mean "SHA-1 Hash", especially if SSL certificates are involved. ("Fingerprint" tends to be more popular term in *nix environments. See also "Thumbprint")

Key - See "SSH Key"

MD5 Hash - A 128-bit checksum that is intended to uniquely represent an entire document or key. The MD5 algorithm is old; the FIPS-approved SHA-1 is preferred.

SHA-1 Hash - A 160-bit checksum that is intended to uniquely represent an entire document or key. The SHA-1 algorithm is approved by the *National Institute of Standards and Technology* (<http://csrc.nist.gov/cryptval/>).

SSH Key - A piece of data, a few kilobytes in size, that is used in setting up an SSH (Secure SHell) connection. An SSH key has two components, public and private, typically stored in separate files. The private component is secret; possession of this portion of the key is sometimes used as proof of identity, like a password. Any given SSH connection involves two SSH keypairs: one for the server, and one for the client.

SSL Certificate - A piece of data, a few kilobytes in size, which is assigned to a particular user or server and which is digitally signed by a trusted Certificate Authority. SSL certificates are used in establishing SSL (Secure Socket Layer) connections. Certificates issued to servers, such as web servers, are called server certificates. Certificates issued to individuals are called client certificates. Client and server certificates are used in different ways, and it is possible to use both during the establishment of an SSL connection.

Thumbprint - Usually, another name for "SHA-1 Hash", especially if SSL certificates are involved. This term could also mean "MD5 Hash", especially if SSH keys are involved. ("Thumbprint" tends to be more popular term in Windows environments. See also "Fingerprint".)

X.509 Certificate - Another name for SSL Certificate

FTP - Supported Commands

MOVEit DMZ FTP supports the following FTP commands:

Command	Comments
USER username	Indicates the MOVEit username to be checked in the MOVEit user database.
PASS password	Indicates the MOVEit password to be checked in the MOVEit user database.
AUTH type	Starts secure communication for the specified security type: TLS-C or TLS-P.
FEAT	Returns the feature set supported, specifically AUTH, PROT and PBSZ.
PROT type	Sets the data connection protection type. For TLS-C security, the PROT P command is required to enable security on the data channel.
PBSZ size	Sets the protection buffer size for encryption. Included for compatibility; the size is never checked.
CLNT name version	Sets the FTP client name and version for logging purposes.
LIST	Obtains a directory listing, with date, size, and filename in a format compatible with Microsoft's FTP server. Any command arguments beginning with "-" are ignored.
NLIST	Obtains a bare directory listing.
RETR fileID	Downloads a file, first checking that the current user has read access to the file. The fileID can be a complete file name, including an embedded fileID. MOVEit DMZ FTP will extract the fileID. When unique file names are enforced for a folder, the filename can be used in place of the ID.
STOR filename	Uploads a file. MOVEit will create a new fileID and return it in the 226 response.
APPE filename	Appends a file. This is only supported for resuming file transfers. MOVEit will create a new fileID, copy the old partial file and append new data, and return it in the 226 response.
CD ~	Changes current directory to the user's default (not home) directory.
CWD directory	Changes current directory. See below.

MKD directory	Creates a directory, if the user has permission to do so.
RMD directory	Deletes a directory, if the user has permission to do so.
DELE fileID	Deletes the file, if the user has permission to delete it.
RNFR fileID RNT0 filename	Changes the original file name associated with a file ID, if the user has permission to modify it.
REST skipcount	Sets the byte skip count for a subsequent RETR or STOR command. For RETR, MOVEit will skip the first "skipcount" number of bytes in the downloaded file. For STOR, MOVEit will copy the first "skipcount" number of bytes from the destination file to a new file then append the transmitted bytes.
SIZE filename	Reports the size in bytes of the named file, the same number returned in a directory list.
MODE type	Sets the mode in which data is to be transferred via the data connection, S for Stream Mode, and Z for Zip compression mode.
SYST	Reports the system type. The returned string indicates compatibility with the Microsoft Windows FTP server.
HELP	Displays a list of commands.
PORT	Initiates an active data connection. If configured to allow only passive connections, this is refused.
PASV	Initiates a passive connection. This is used by some FTP clients to accommodate firewalls that do not allow an FTP server to initiate TCP data connections.
QUIT	Quits the session.
CCC	If enabled, the Cleartext Command Channel command switches the command channel from encrypted to cleartext. See the " Allow CCC " <i>configuration option</i> (on page 577).
STAT	Returns brief information to properly authorized users about the FTP server including name, version and local time.

MOVEit DMZ FTP supports the following commands for the purposes of integrity checking:

Command	Comments

INTEGRITY type	Enables integrity checking on STOR and RETR. For type L, use "lump mode" data stream which compresses data on the fly and include a SHA1 hash of the file for integrity verification. For type H, "hash mode", the data stream is standard, and the client is responsible for checking the SHA1 hash for integrity verification. Type N turns integrity checking off.
XSHA1 filename	Returns the SHA1 hash of the file named, usually the most recently transferred file.
HASH OK/BAD	Notifies DMZ FTP, after a STOR or RETR, that the client has verified the file SHA1 hash and that it has matched (or not matched) the one passed in the data stream in lump mode, or returned by the XSHA1 command.

MOVEit DMZ FTP supports the following special command for changing a user's password:

Command	Comments
CHGPW <i>oldpass newpass newpass</i>	Sends a password change request to MOVEit DMZ for the logged on user. The old password is rechecked and the new passwords must match and meet strength requirements for the site.

MOVEit DMZ FTP supports the following commands in a nontraditional way:

Command	Comments
TYPE I or A	Implements the ascii and binary commands. Not supported; all transfers are binary. (In other words, MOVEit DMZ does not automatically add/strip carriage returns or perform other character manipulation.) If this is a concern, contact MOVEit Support (http://www.ipswitchft.com/company/contactsupport.aspx (http://www.ipswitchft.com/company/contactsupport.aspx)).

MOVEit DMZ FTP does not support the following commands:

Unsupported Commands: ACCT, SMNT, REIN, STOU, ALLO, ABOR, SITE

FTP - Recommended Configuration

Ipswitch recommends sites adhere to the following recommended configuration. This "passive, implicit" setup has been shown to be the most problem-free of any FTPS configuration at a number of large MOVEit sites.

- MOVEit DMZ FTP Server
 - Enable Require Passive Mode
 - Set Explicit Port to 21
 - Set Implicit Port to 990
 - Restrict Passive Ports on 3000 to 3003 (or some other range)
- IPSec Policy (FTP Rule Filters)
 - Allow TCP from AnyIP, AnyPort to MyIP, Port 21
 - Allow TCP from AnyIP, AnyPort to MyIP, Port 990
 - Allow TCP from AnyIP, AnyPort to MyIP, Port 3000
 - Allow TCP from AnyIP, AnyPort to MyIP, Port 3001
 - Allow TCP from AnyIP, AnyPort to MyIP, Port 3002
 - Allow TCP from AnyIP, AnyPort to MyIP, Port 3003
- Firewall Rules
 - Allow TCP from AnyIP, AnyPort to MOVEitDMZ, Port 21
 - Allow TCP from AnyIP, AnyPort to MOVEitDMZ, Port 990
 - Allow TCP from AnyIP, AnyPort to MOVEitDMZ, Port 3000
 - Allow TCP from AnyIP, AnyPort to MOVEitDMZ, Port 3001
 - Allow TCP from AnyIP, AnyPort to MOVEitDMZ, Port 3002
 - Allow TCP from AnyIP, AnyPort to MOVEitDMZ, Port 3003
- Client Configuration
 - Passive Transfer Mode (a.k.a. "Firewall Friendly")
 - Implicit Connection Mode

FTP - Troubleshooting

This document describes how to troubleshoot common FTP over SSL connectivity problems.

In addition to this document, see **System Configuration - Firewall** (on page 128) and **System Configuration - SSL and SSH - SSL - Client Certs - Troubleshooting** (on page 240) as needed for additional information and hints.

- General Procedures
- Most Common Problems
- How to Troubleshoot
- Common Symptoms and Resolutions
- Common Errors in Debug Log

General Procedures

There are four areas which are typically at the root of MOVEit DMZ FTP/SSL problems:

- MOVEit DMZ FTPS Server Configuration
- MOVEit DMZ IPSec Configuration
- Firewall Configuration
- Client Configuration

To diagnose FTPS problems, it is best to first try to duplicate the problem using a client (i.e. MOVEit Freely) installed on the MOVEit DMZ server itself. Doing so will eliminate both the "IPSec" policy and "the network". If no problems are observed when using a client locally, next try a client on the same segment (going through IPSec but not the firewall) and finally a client on an "external" segment (going through IPSec and the firewall).

CAUTION: Remember to uninstall any client used on the MOVEit DMZ host after you have completed troubleshooting to avoid unattended misuse.

Most Common Problems

The most common problems usually involve one of the following conditions:

- "FTP Aware" firewalls (e.g. Checkpoints) interfering in the FTPS explicit mode handshake.
- Improperly exported/imported certificates from existing servers.
- Missing firewall rules for implicit mode FTPS or data ports.
- Missing IPSec rules for implicit mode FTPS or data ports.

- Clients configured to use active mode, or to use implicit mode on the wrong port.
- Servers running without implicit mode enabled.
- Servers running behind a NAT device without any configured NAT masks.

This document covers diagnosing and correcting these problems and more.

How to Troubleshoot

Always begin your troubleshooting routine using a copy of MOVEit Freely temporarily installed on the same machine as MOVEit DMZ. This step avoids complicating your troubleshooting task by avoiding firewalls, routers and other network devices which may or may not be the culprit.

Throughout this section, the phrases "local client" and "remote client" are used to indicate an "FTPS client installed on the MOVEit DMZ server" and an "FTPS client installed on another desktop," respectively.

Also, remember that you may need to take different actions to different devices to get any changes to take effect. For example:

- You need to START and STOP the MOVEit DMZ FTP service after making changes through the MOVEit DMZ Configuration Utility.
- You need to "Un-Assign" and then "Assign" altered IPsec policies.
- You may need to refresh your firewall after making firewall changes.
- You will probably need to close and reopen connections after making client changes.

Common Symptoms and Resolutions

Local client times out when connecting to localhost in EXPLICIT mode.

- Check to see that the MOVEit DMZ FTP server is running correctly.
- Open the **Services** control panel and see if MOVEit DMZ FTP is Started
- Open the MOVEit DMZ Config application and make sure the **Explicit Port** is set to 21.
- Do a "netstat -a -n" from the command line and see that "Local Address=0.0.0.0:21" is in the "LISTENING" state.

Local client times out when connecting to localhost in IMPLICIT mode.

- Check to see that the MOVEit DMZ FTP server is running correctly.
- Open the **Services** control panel and see if MOVEit DMZ FTP is Started.
- Open the MOVEit DMZ Config application and make sure the **Implicit Port** is set to 990.
- Do a "netstat -a -n" from the command line and see that "Local Address=0.0.0.0:990" is in the "LISTENING" state.

Local client shows a "Handshake Failed" error while connecting.

- Double check your client configuration:
- You must access PORT 21 if using EXPLICIT mode.
- You must access PORT 990 if using IMPLICIT mode.
- If this certificate was exported from an existing secure server:
- Check the FTP server log file. If you have a "not loaded" message near the top, you are probably using a certificate which was imported without its private key.
- Perform the steps in the "Server Certificate Export/Import Instructions" as exactly as specified in the document.
- If you are replacing an existing certificate or have installed multiple certificates:
 - Check the FTP server log file. If you have an "expired" message near the top, you are probably using the wrong certificate for FTP. (Pick the newest/most applicable certificate.)
 - Open the MOVEit DMZ Config application and reselect your certificate. (FTP Certs Tab)
 - START/STOP the MOVEit DMZ FTP service.

Local client shows a "530 Error Accessing 'http://myhost/machine.aspx'" or other strange authentication error after connecting.

- Open the MOVEit DMZ Config application and make sure the following values are set as follows:
- Machine URL: http://localhost/machine.aspx
- Machine2 URL: http://localhost/machine.aspx
- START/STOP the MOVEit DMZ FTP service.
- If these values do not work, try these values instead:
 - Machine URL: https://(full hostname)/machine.aspx
 - Machine2 URL: https://(full hostname)/machine2.aspx
 - START/STOP the MOVEit DMZ FTP service.

- **HINT:** You can usually use the MOVEit DMZ Check utility to find/fix this kind of problem, as it will affect ALL users equally!

Remote Client times out when connecting to MOVEitDMZ in EXPLICIT mode.

- First check for the same "time out" problem using a Local Client.
- Make sure TCP port 21 is open from AnyIP, AnyPort to MyIP on your firewall(s).
- Make sure TCP port 21 is open from AnyIP, AnyPort to MOVEitDMZ on your firewall(s).

Remote Client times out when connecting to MOVEitDMZ in IMPLICIT mode.

- First check for the same "time out" problem using a Local Client.
- Make sure TCP port 990 is open from AnyIP, AnyPort to MyIP on your firewall(s).
- Make sure TCP port 990 is open from AnyIP, AnyPort to MOVEitDMZ on your firewall(s).

Remote Client shows a "Handshake Failed" error while connecting in EXPLICIT mode.

- First check for the same "handshake failed" problem using a Local Client.
- If this problem does not occur when using a Local Client but occurs reliably when using a Remote Client, there is likely an "FTP aware" firewall in between the Remote Client and MOVEit DMZ. "FTP aware" firewalls work well with insecure FTP but commonly mangle the SSL "bootstrap" process of explicit mode secure FTP
- Use implicit mode instead.

Remote Client shows a "Handshake Failed" error while connecting in IMPLICIT mode.

- First check for the same "handshake failed" problem using a Local Client.
- Double check your client configuration: you must access PORT 990, not port 21.

Username/password which works when used from Local Client does not work from Remote Client.

- Open the MOVEit DMZ web interface (sign on as an admin) and...
- Double-check that user's Remote Access settings. (You may be using Custom settings or Default settings to allow or prevent access from certain IP addresses.)
- Double-check that organization's Locked Out IP Address settings. (This IP address may have been locked out and may need to be reset.)

Remote Client gets "Passive Mode Required" error.

- Enable "Passive" mode or "Firewall Friendly" mode on your FTPS client configuration.

Remote Client gets "Bad Certificate" error.

- Configure your FTPS client to use the "normal" hostname of your MOVEitDMZ server (i.e. moveit.stdnet.com) rather than its IP address.
- Upgrade your server certificate to a "production" certificate, or...
- ...install this certificate (and perhaps its parent CA) on the client PC.

Remote Clients get "Non-Trusted Certificate" error.

- Configure your FTPS client to connect to the MOVEitDMZ server by HOSTNAME, not IP address.

Remote Client reports "Cannot Create Security Credentials" error while running under Windows 95 or 98.

- Old versions of Windows 95 and 98 may not have the SSL/TLS support required to run FTPS clients. Microsoft ships a program which contains the necessary upgrades with Windows 2000 called dsclient.exe. (This file is also available from Ipswitch.) This package needs to be installed on the remote client desktop - reboot required.

Remote Client cannot transfer files and/or list the contents of folders after signing on successfully.

- Discussion: File transfer and directory list operations make use of FTPS data connections. 95% of the time, problems related to file transfer and directory list operations are due to connectivity problems involving these data connections.
- Check the client logs to see if the server is returning a "Passive Mode Required" message and take the appropriate action, if required.
- Double-Check your MOVEit DMZ FTP Config:
 - Enable Require Passive Mode
 - Restrict Passive Ports on 3000 to 3003
- Double-Check your IPSec Policy (FTP Rule Filters)
 - Allow TCP from AnyIP, AnyPort to MyIP, Ports 3000-3003
- Double-Check your Firewall Rules
 - Allow TCP from AnyIP, AnyPort to MOVEitDMZ, Ports 3000-3003
- Double-Check your Client Configuration
 - Enable Passive Transfer Mode (a.k.a. "Firewall Friendly")
- Check the client logs and examine the contents of the "227 Entering Passive Mode (208,212,86,143,11,186)" message.
 - The FIRST FOUR numbers in the body of the message are the IP address to which the remote client is attempting to connect its data channels. (i.e. 208,212,86,143,... means that I am trying to connect to 208.212.86.143)
 - If this IP address is DIFFERENT from the IP address the client normally connects to (i.e. 10.1.1.2, we are probably encountering a NAT problem. See *FTP Server - Configuration* of this manual for information on how to configure a NAT mask in the MOVEit DMZ Config application. (Use of NAT masks will allow your FTP server to send the correct "227" IP addresses to machines inside and outside your NAT boundaries.)
 - The LAST TWO numbers in the body of the message indicate the TCP port to which the remote client is attempting to connect its data channels. (i.e. "...11,186") To convert these digits into a meaningful port number, multiply the first number by 256 and add the second number. (i.e. (11 x 256) + 186 = Port 3002)

- This port number should lie within the range of passive ports you configured on MOVEit DMZ FTP - if not, double check that the **Restrict** box has been checked next to this range in the MOVEit DMZ Config application.

Some remote clients, particularly command-line remote clients, correctly put the end user in his/her own home folder. However, other remote clients, particularly GUI remote clients, put the end user at the "root" folder instead.

- Discussion: MOVEit DMZ FTP usually puts end users in their home directories whenever they connect. Unfortunately, it's up to the client to respect that setting, and many Windows clients automatically try to "cd" to the root (\) upon connection, regardless of where the FTP Server directed the client to start.
- Configure GUI clients to respect your home directory, or...
- Use MOVEit DMZ's user-level "CHROOT" setting to lock users to their home or default folder.

Common Errors in Debug Log

The following errors from the MOVEit DMZ FTP debug log usually point to specific configuration problems.

- "530 Rejected--secure connection required" This indicates that an FTP client attempted to connect without using SSL when SSL was required.
- "Connection security error: Failed to receive secure data. - SSL negotiation failed: Security handshake failed. - A client certificate is required." This indicates that an FTP/SSL client attempted to connect without a client certificate when the FTP server was configured to require a client certificate.
- "Connection security error: Error 0x800b0109 (CERT_E_UNTRUSTEDROOT) returned by CertVerifyCertificateChainPolicy! - Connection security error: Error authenticating security credentials - SSL negotiation failed: Failed to verify the certificate trust." This indicates that an FTP/SSL client provided a client cert but the client cert did not chain up to a CA in the Microsoft Trusted Root Certificate Store.

Additional Help

For additional help, you may want to consult the Knowledge Base on our support site at

http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ
(http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ).

FTP - SSL Certificates

All client and server certificates used by MOVEit DMZ FTP must be X.509 certificates.

Server certificates (on page 182) let remote FTP clients confirm the identity of your FTP server and are an important part of SSL secure channel negotiation. A server certificate is always required by MOVEit DMZ FTP; in fact, MOVEit DMZ FTP will complain via email if it does not have at least one valid server certificate.

Client certificates (on page 222) help MOVEit DMZ confirm the identity of FTP clients. Client certificates are optional, but they must ALWAYS be provided when connecting to the optional **Client Certs Explicit Port** or the **Client Certs Implicit Port** on MOVEit DMZ, whether or not the certs are actually used during authentication (as per user-level authentication settings). As suggested by the configuration options, MOVEit DMZ supports client certificates on both its explicit and implicit ports, and over all three modes of FTP/SSL. (See **FTP - Configuration (Ports Tab)** (on page 577) for more information.)

An ever-expanding list of **compatible clients** (on page 793) and a **complete list of encryption options** (on page 175) is also included in this documentation.

Missing Certificates

MOVEit DMZ provides two "missing certificate" reminders to ensure at least one valid certificate has been installed. The first is the MOVEit DMZ Check utility which runs after each installation and upgrade and may also be run manually from the **Start | Programs | MOVEit DMZ** menu. This utility will report a connection error if the FTP server certificate is bad or missing. The second reminder is an email with certificate assignment instructions sent by the FTP server itself when the service is started. This email will be sent 14 days before a certificate expires, every day after a certificate expires and every day a certificate is not available.

Multiple Certificates

It is possible to assign multiple server certificates to the MOVEit DMZ FTP server as long as each different cert can be assigned to a different IP address. In other words, you need to expose multiple IP addresses on your MOVEit DMZ server if you want to support multiple certificates.

For technical details, please see **FTP Certs** in **FTP - Configuration** (on page 577).

FTP - Specific Clients - z/OS

This guide describes the overall process to use the Secure Sockets z/OS FTP client to securely connect to a MOVEit DMZ FTP Server.

Procedure

Step 1 - Check firewall issues using MOVEit Freely. Download and install MOVEit Freely from the **MOVEit Freely** (<http://www.ipswitchft.com/moveitfreely>) web site. Try connecting to a MOVEit DMZ host using this client. If you can connect successfully than there should not be any firewall issues.

**There is a known problem with FTP over SSL and Checkpoint firewalls. For more information, please see Checkpoint support article sk9930.*

Step 2 - Install Digital Certificates on the mainframe. There are two method for installing Digital Certificates into z/OS. First, using RACF you can use RACDCERT and a useful guide to use is <http://publibz.boulder.ibm.com/epubs/pdf/ichza441.pdf> (<http://publibz.boulder.ibm.com/epubs/pdf/ichza441.pdf>).

A second way to work with certificates (and usually a more fruitful way) is to use a utility called gskkyman which is a shell-based program. A useful guide can be found in Chapter 10 of Secure Sockets Programming. <http://publibfp.boulder.ibm.com/epubs/pdf/gska1a21.pdf> (<http://publibfp.boulder.ibm.com/epubs/pdf/gska1a21.pdf>)

- 1 Install any root certificates (e.g. Thawte) on the mainframe.
- 2 Install any intermediate certificates that might be use on the mainframe, this may be optional.
- 3 Install any server-certificates (e.g., mydmzhost.com) on the mainframe.

Step 3 - Change settings in FTP Client ParmS file. You can find an example of the parm file below.

- 1 Change the value of SECURE_CTRLCONN from CLEAR to PRIVATE.
- 2 Change the value of SECURE_DATACONN from CLEAR to PRIVATE.

```

*****
/
;
; Name of File:          SEZAINST(FTCDATA)
;
; Descriptive Name:      FTP.DATA (for FTP Client)
;
; SMP/E Distribution Name: EZAFTPAC
;
; Copyright:    Licensed Materials - Property of IBM
;
;              "Restricted Materials of IBM"
;
;              5694-A01
;
*****

```

```

;          (C) Copyright IBM Corp. 1977, 2002
;
;
;          US Government Users Restricted Rights -
;          Use, duplication or disclosure restricted by
;          GSA ADP Schedule Contract with IBM Corp.
;
;
;  Status:      CSV1R4
;
;
;
;  This FTP.DATA file is used to specify default file and disk
;  parameters used by the FTP client.
;
;
;  Note: For an example of an FTP.DATA file for the FTP server,
;  see the FTPSDATA example.
;
;
;  Syntax Rules for the FTP.DATA Configuration File:
;
;
;  (a) All characters to the right of and including a ; will be
;      treated as a comment.
;
;
;  (b) Blanks and <end-of-line> are used to delimit tokens.
;
;
;  (c) The format for each statement is:
;
;
;      parameter value
;
;
;
;

```

```
; The FTP.DATA options are grouped into the following groups in      *
; this sample FTP client FTP.DATA configuration data set:            *
;                                                                      *
; 1. Basic configuration options (timers, conditional options, etc.) *
; 2. Defaults for MVS data set creation                               *
; 3. Code page conversion options                                     *
; 4. DB2 (SQL) interface options                                     *
; 5. Security options                                               *
; 6. Debug (trace) options                                           *
;                                                                      *
; For options that have a pre-selected set of values, a (D) indicates *
; the default value for the option.                                   *
;                                                                      *
; Options that can be changed via LOCSITE subcommands are identified *
; with an (S).                                                       *
;                                                                      *
; *****
;
; -----
;
; 1. Basic FTP client configuration options -
; Timeout values, conversion options,
; and conditional processing options
;
; -----
```

ASATRANS FALSE ; (S) Conversion of ASA print

```
        ; control characters
        ; TRUE = Use C conversion
        ; FALSE = Do not convert (D)

AUTOMOUNT      TRUE      ; (S) Automatic mount of unmounted
                        ; DASD volumes
                        ; TRUE = Mount volumes (D)
                        ; FALSE = Do not mount volumes

AUTORECALL     TRUE      ; (S) Automatic recall of
                        ; migrated data sets
                        ; TRUE = Recall them (D)
                        ; FALSE = Do not recall them

AUTOTAPEMOUNT  TRUE      ; Automatic mount of unmounted
                        ; tape volumes
                        ; TRUE = Mount volumes (D)
                        ; FALSE = Do not mount volumes

BUFNO          5         ; (S) Specify number of access
                        ; method buffers
                        ; Valid range is from 1 through
                        ; 35 - default value is 5

CCONNTIME      30        ; Timeout value for successful
                        ; close of control connection.
                        ; Default value is 30 seconds.
```

; Valid range is 15 through 720.

CHKPTINT 0 ; (S) Specify the checkpoint interval
; in number of records.
; NB: checkpointing only works
; with datatype EBCDIC and block
; or compressed transfer mode.
; 0 = no checkpoints (D)

CONDDISP CATLG ; (S) Disposition of a new data set
; when transfer ends prematurely
; CATLG = Keep and catalog (D)
; DELETE = Delete data set

DATACTTIME 120 ; Timeout for send/receive data
; operations.
; Default value is 120 seconds.
; Valid range is 15 through 720.

DCONNTIME 120 ; Timeout value for successful
; close of data connection.
; Default value is 120 seconds.
; Valid range is 15 through 720.

DIRECTORYMODE FALSE ; (S) Specifies how to view the MVS
; data set structure:
; FALSE = All qualifiers below

```

;      (D)  LCWD are treated as
;           entries in the directory
; TRUE  = Qualifiers immediately
;           below the LCWD are
;           treated as entries in the
;           directory

;EXTENSIONS      UTF8      ; Enable RFC 2640 support.
EXTENSIONS AUTH_TLS      ; Default is disabled.
                        ; Control connection starts as
                        ; 7bit ASCII and switches to UTF-8
                        ; encoding when LANG command
                        ; processed successfully. CTRANS
                        ; and CTRLCONN are ignored.

FILETYPE      SEQ      ; (S) Client mode of operation
                        ; SEQ = transfer data sets or
                        ;      files (D)
                        ; SQL = submit queries to DB2

INACTTIME      300      ; The time in seconds to wait for
                        ; an expected response from the
                        ; server.
                        ; Default value is 300 seconds.
                        ; Valid range is 15 through 720.

ISPFSTATS      FALSE      ; TRUE = create/update PDS
```

		<pre>; statistics ; FALSE =does not create/update ; PDS statistics</pre>
MIGRATEVOL	MIGRAT	<pre>; (S) Migration volume VOLSER to ; identify migrated data sets ; under control of non-HSM ; storage management products. ; Default value is MIGRAT.</pre>
MYOPENTIME	60	<pre>; Connection timeout value in ; seconds. ; Default value is 60 seconds. ; Valid range is 15 through 720.</pre>
QUOTESOVERRIDE	TRUE	<pre>; (S) How to treat quotes at the ; beginning or surrounding file ; names. ; TRUE = Override current working ; directory (D) ; FALSE = Treat quotes as part of ; file name</pre>
RDW	FALSE	<pre>; (S) Specify whether Record ; Descriptor Words (RDWs) are ; discarded or retained. ; TRUE = Retain RDWs and transfer</pre>

```

;          as part of data
; FALSE = Discard RDWs when
;          transferring data (D)
;SOCKSCONFIGFILE /etc/socks.conf ; file path for SOCKS configuration
; file. The SOCKS configuration
; file specifies which FTP servers
; should be accessed via SOCKS

TRAILINGBLANKS  FALSE          ; (S) How to handle trailing blanks
; in fixed format data sets during
; text transfers.
; TRUE = Retain trailing blanks
;          (include in transfer)
; FALSE = Strip off trailing
;          blanks (D)

UMASK           027           ; (S) Octal UMASK to restrict setting
; of permission bits when creating
; new HFS files
; Default value is 027.

WRAPRECORD      FALSE        ; (S) Specify what to do if no new-line
; is encountered before reaching
; the MVS data set record length
; limit as defined by LRECL when
; transferring data to MVS.
; TRUE = Wrap data to new record
```

i

```
; There is no default
```

- ; There is no default

- ; There is no default

DIRECTORY	27	; (S) Number of directory blocks in
		; new PDS/PDSE data sets.
		; Default value is 27.
		; Range is from 1 to 16777215.

LRECL	256	; (S) New data set allocation LRECL. ; Default value is 256. ; Valid range 0 through 32760.
PRIMARY	1	; (S) New data set allocation ; primary space units according ; to the value of SPACETYPE. ; Default value is 1. ; Valid range 1 through 16777215.
RECFM	VB	; (S) New data set allocation ; record format. ; Default value is VB. ; Value may be specified as certain ; combinations of: ; A - ASA print control ; B - Blocked ; F - Fixed length records ; M - Machine print control ; S - Spanned (V) or Standard (F) ; U - Undefined record length ; V - Variable length records
RETPD		; (S) New data set retention ; period in days. ; Blank = no retention period (D)

; 0 = expire today
; Valid range 0 through 9999.
; NB: Note the difference between
; a blank value and a value
; of zero.

SECONDARY 1 ; (S) New data set allocation
; secondary space units according
; to the value of SPACETYPE.
; Default value is 1.
; Valid range 1 through 16777215.

SPACETYPE TRACK ; (S) New data set allocation
; space type.
; TRACK (D)
; BLOCK
; CYLINDER

UCOUNT ; (S) Sets the unit count for an
; allocation.
; If this option is not specified
; or is specified with a value of
; blank, the unit count attribute
; is not used on an allocation (D)
; Valid range is 1 through 59 or
; the character P for parallel
; mount requests

```

;UNITNAME      SYSDA          ; (S) New data set allocation unit
                                ; name.
                                ; There is no default.

```

```
VCOUNT      59          ; (S) Volume count for an
                        ; allocation.
                        ; Valid range is 1 through 255.
                        ; Default value is 59.
```

```
;VOLUME          WRKLB1,WRKLB2      ; (S) Volume serial number(s) to  
                                     ; use for allocating a data set.  
                                     ; Specify either a single VOLSER  
                                     ; or a list of VOLSERS  
                                     ; separated with commas
```

;

```
; 3. Text code page conversion options
```

;

```

; CCTRANS          dsn_qual          ; Control connection translate
;                                     ; table data set qualifier.
;                                     ; Used to search for
;      a) userid.dsn_qual.TCPXLBIN
;      b) hlq.dsn_qual.TCPXLBIN
; If CTRLCONN is specified, that

```

; value overrides CCTRANS.

;CTRLCONN 7BIT ; (S) ASCII code page for
 ; control connection.
 ; 7BIT is the default if CTRLCONN
 ; is not specified AND no TCPXLBIN
 ; translation table data set found.
 ; Can be specified as any iconv
 ; supported ASCII code page, such
 ; as IBM-850

;ENCODING SBCS ; (S) Specifies whether multi-byte or
 ; single-byte data conversion is
 ; to be performed on ASCII data
 ; transfers.
 ; MBCS = Use multi-byte
 ; SBCS = Use single-byte (D)
 ;

;MBDATACONN (IBM-1388,IBM-5488) ; (S) Specifies the conversion table
 ; names for the data connection
 ; when ENCODING has a value of
 ; MBCS. The names are the file
 ; system code page name and the
 ; network transfer code page name.

;SBDATACONN (IBM-1047,IBM-850) ; (S) file system/network transfer

```
; code pages for data connection.
; Either a fully-qualified MVS
; data set name or HFS file name
; built with the CONVXLAT utility -
;     HLQ.MY.TRANS.DATASET
;     /u/user1/my.trans.file
; Or a file system code page name
; followed by a network transfer
; code page name according to
; iconv supported code pages -
; for example
;     (IBM-1047,IBM-850)
; If the SYSFTSX DD-name is present
; it will override SBDATACONN.
; If neither SYSFTSX nor
; SBDATACONN are present, std.
; search order for a default
; translation table data set will
; be used.

;SBSUB      FALSE      ; Specifies whether untranslatable
; data bytes should be replaced
; with SBSUBCHAR when detected
; during SBCS data transfer.
; TRUE = Replace each
; untranslatable byte with
; SBSUBCHAR.
```


; for the data connection is used.

UCSSUB FALSE ; (S) Specify whether Unicode-to-EBCDIC
 ; conversion should use the EBCDIC
 ; substitution character or
 ; cause the data transfer to be
 ; terminated if a Unicode
 ; character cannot be converted to
 ; a character in the target
 ; EBCDIC code set
 ; TRUE = Use substitution char
 ; FALSE = Terminate transfer (D)

UCSTRUNC FALSE ; (S) Specify whether the transfer
 ; of Unicode data should be
 ; aborted if truncation
 ; occurs at the MVS host
 ; TRUE = Truncation allowed
 ; FALSE = Terminate transfer (D)

; -----

;

; 4. DB2 (SQL) interface options

;

; -----

DB2 DB2 ; (S) DB2 subsystem name

```

; The default name is DB2

DB2PLAN      EZAFTPMQ      ; DB2 plan name for FTP client
; The default name is EZAFTPMQ

SPREAD      FALSE      ; (S) SQL spreadsheet output format
; TRUE = Spreadsheet format
; FALSE = Not spreadsheet
;          format (D)

SQLCOL      NAMES      ; (S) SQL output headings
; NAMES = Use column names (D)
; LABELS = Use column labels
; ANY = Use label if defined,
;          else use name

; -----
;
; 5. Security options
;
; -----

SECURE_MECHANISM  TLS      ; Name of the security mechanism
; that the client uses when it
; sends an AUTH command to the
; server.
; GSSAPI = Kerberos support

```

; TLS = TLS

SECURE_FTP ALLOWED ; Authentication indicator

SECURE_LOGIN REQUIRED

; ALLOWED (D)

; REQUIRED

SECURE_CTRLCONN PRIVATE ; Minimum level of security for

; the control connection

; CLEAR (D)

; SAFE

; PRIVATE

SECURE_DATACONN PRIVATE ; Minimum level of security for

; the data connection

; NEVER

; CLEAR (D)

; SAFE

; PRIVATE

;SECURE_PBSZ 16384 ; Kerberos maximum size of the

; encoded data blocks

; Default value is 16384

; Valid range is 512 through 32768

; Name of a ciphersuite that can be passed to the partner during

; the TLS handshake. None, some, or all of the following may be

; specified. The number to the far right is the cipherspec id
; that corresponds to the ciphersuite's name.

CIPHERSUITE	SSL_NULL_MD5	; 01
CIPHERSUITE	SSL_NULL_SHA	; 02
CIPHERSUITE	SSL_RC4_MD5_EX	; 03
CIPHERSUITE	SSL_RC4_MD5	; 04
CIPHERSUITE	SSL_RC4_SHA	; 05
CIPHERSUITE	SSL_RC2_MD5_EX	; 06
CIPHERSUITE	SSL_DES_SHA	; 09
CIPHERSUITE	SSL_3DES_SHA	; 0A

KEYRING /SSLselfsigned/key.kdb

; It can be the name of an HFS
; file (name starts with /) or
; a resource name in the security
; product (e.g., RACF)

;TLSTIMEOUT 100 ; Maximum time limit between full
; TLS handshakes to protect data
; connections
; Default value is 100 seconds.
; Valid range is 0 through 86400

; -----

;

; 6. Debug (trace) options

;

; -----

```
;DEBUG      TIME      ;    time stamp client trace entries
;DEBUG      ALL       ;    activate all traces
;DEBUG      BAS       ;    active basic traces (marked with *)
;DEBUG      FLO       ;    function flow
;DEBUG      CMD       ; *  command trace
;DEBUG      PAR       ;    parser details
;DEBUG      INT       ; *  program initialization and termination
;DEBUG      ACC       ;    access control (logging in)
;DEBUG      SEC       ;    security processing
;DEBUG      UTL       ;    utility functions
;DEBUG      FSC(1)    ; *  file services
;DEBUG      SOC(1)    ; *  socket services
;DEBUG      SQL       ;    special SQL processing
```

FTP - Specific Clients - cURL

cURL is a one-shot command-line file transfer utility. It is free for any use and may be **downloaded here** (<http://curl.haxx.se/download.html>).

cURL may not be the easiest or prettiest client to use, but it is still a valuable utility because it runs on far more operating systems than any other secure file transfer client ever created (see *cURL Operating Systems* below).

MOVEit DMZ supports FTP/SSL and HTTPS uploads and downloads using cURL. cURL only supports explicit FTP over SSL at this time, so transfers will usually be initiated over port 21 and will be subject to the same firewall rules that other FTP/SSL transfers must adhere to.

FTP/SSL Downloads

Files may be downloaded directly from MOVEit DMZ (any version) with cURL if the full path to a particular file is known. The following example signs on to *i.stdnet.com* as *ftpboi* with password *a1s2d3* and downloads a file called *zerb.gif* from the */Home/ftpboi* folder.

```
curl -v -1 -o  
    "zerb.gif" --ftp-ssl --ftp-pasv -u ftpboi:a1s2d3 -Q "+CWD /Home/ftpboi"  
    "ftp://i.stdnet.com/zerb.gif"
```

Note the unusual path syntax. cURL cannot figure out FTP folder paths on its own so you must explicitly set the full path with the *-Q* argument. Also, the filename you wish to download must be in two places: the name of the output file (after the *-o*) and in the URL (at the end).

FTP/SSL Uploads

Files may be uploaded directly to MOVEit DMZ (any version) with cURL if the full path of the folder where a file is to be uploaded is known. The following example signs on to *i.stdnet.com* as *ftpboi* with password *a1s2d3* and uploads a file called *sdn.gif* into the */Home/ftpboi* folder.

```
curl -v -1 -T "sdn.gif" --ftp-ssl --ftp-pasv  
    -u ftpboi:a1s2d3 -Q "+CWD /Home/ftpboi"  
    "ftp://i.stdnet.com"
```

Note the unusual path syntax. cURL cannot figure out FTP folder paths on its own so you must explicitly set the full path with the *-Q* argument.

HTTPS Downloads

Files may be downloaded directly from MOVEit DMZ (version 3.2+) with cURL if the file IDs are known. The following example signs on to **i.stdnet.com** as a user named **httpboi** with password **a1s2d3** and downloads FileID #9102186 as **dwn.gif**. The second curl line will sign the related user off cleanly.

```
curl -k -1 -v -L -c cookie2.txt -o "dwn.gif"

    "https://i.stdnet.com/human.aspx?Username=httpboi&Password=a1s2d3&
    arg01=9102186&arg05=0/dwn.gif&arg12=downloaddirect&transaction=signon"

curl -k -v -b cookie2.txt "https://i.stdnet.com/human.aspx?transaction=signoff"
```

The filename you wish to download must be in two places: the name of the output file (after the -o) and in the URL (after the arg05 tag). Otherwise, the syntax is similar to that used during "direct file downloads" initiated by MOVEit DMZ API applications running on web portals.

HTTPS Uploads

Files may be uploaded into MOVEit DMZ if the destination folder IDs are known. For example, the following three-call snippet will upload a file called **hello1.gif** of size (in bytes) 87054 into a MOVEit DMZ folder with ID 318060437 on **i.stdnet.com** as a user named **httpboi** with password **a1s2d3**. The first curl line signs the related user on to MOVEit DMZ. The second curl line actually performs the transfer (remember to keep these lines together so they aren't interpreted as separate commands). Also, "--data-ascii" should be used in place of "--data-binary" for ascii files. The third curl line will sign the related user off cleanly.

```
curl -k -v -c cookie2.txt
"https://i.stdnet.com/human.aspx?transaction=signon&username=httpboi&password=
a1s2d3"

curl -b cookie2.txt -k -v --data-binary @hello1.gif      -H "Content-Type:
multipart/form-data"

    -H "X-siLock-AgentBrand: cURL" -H "X-siLock-AgentVersion: 4.32"

    -H "X-siLock-FolderID: 318060437" -H "X-siLock-OriginalFilename: hello1.gif"

    -H "X-siLock-FileSize: 87054"

"https://i.stdnet.com/moveitisapi/moveitisapi.dll?action=upload"
```

```
curl -k -v -b cookie2.txt "https://i.stdnet.com/human.aspx?transaction=signoff"
```

replace the example above with a POST-based example? something like the following? any curl users out there that can translate the above into a POST example?

```
curl -d "username=admin&password=admin&submit=Login" --dump-header headers https://hostname/resource
```

```
curl -L -b headers https://hostame/
```

```
curl --form "fileupload=@filename" https://hostname/resource
```

cURL Operating Systems

As of March 4, 2005, the operating systems on which

cURL is available as a native executable on a wide range of current and legacy operating systems. For more information, refer to the *cURL download site* (<http://curl.haxx.se/download.html>).

FTP - Interoperability - IIS FTP

Running IIS FTP and MOVEit DMZ on the Same Port Using Different IP Addresses

A handful of sites have requested the ability to run IIS FTP and MOVEit DMZ FTP on the same computer on the same port (usually 21). The only way that this configuration is possible is if the computer in question has multiple IP addresses. One reason people do this is to address a legacy situation which requires them to maintain an existing store of non-secure users on the same computer that MOVEit DMZ is installed. (So far, this has only happened when a third-party hosting service is involved.) Another reason people do this is to use IIS FTP as a way to access the log files, backup files and other data stored locally on a MOVEit DMZ server.

In this situation, MOVEit DMZ binds to the port on one IP address (usually the main IP address) and IIS FTP binds to the port on the other IP address. This is not how either FTP server behaves by default, however. Instead, both IIS FTP and MOVEit DMZ FTP like to bind particular ports to ALL IP addresses available on a system (i.e. "0.0.0.0") . There is a rather obscure setting in IIS to turn this behavior off under IIS FTP and there is an equally obscure setting in MOVEit DMZ FTP to convince our server to do likewise. The remainder of these instructions are concerned with the actual procedure required to set and test these values.

Changing IIS FTP to listen on only one IP address

Run the "Internet Services Manager" from the Start menu. For Windows Server 2008, use the "Internet Information Services (IIS) 6.0 Manager" shortcut. Open the Properties panel for your FTP site. On the "FTP Site" tab, change the IP Address from "(All Unassigned)" to one of the specific IP addresses on your machine. Apply/OK changes and then close the Internet Services Manager.

Changing MOVEit DMZ FTP to listen on only one IP address

- 1 Open the **MOVEit DMZ Config Utility** (on page 577) and go to the "FTP Ports" tab. Enter the IP address you wish to bind the MOVEit DMZ FTP server to in the "Bind to IP Address" field. Close the MOVEit DMZ Config Utility.
- 2 Restart the MOVEit DMZ FTP service.

FTP - Interoperability - Integrity Check How-To

In version 3.3 MOVEit DMZ opened up its FTP integrity check protocol to allow non-MOVEit FTP clients to begin to perform cryptographic integrity checks as well. (SmartFTP was the first non-MOVEit FTP client to take advantage of the open protocol.)

SHA-1 Cryptographic Integrity Check

Using integrity checks with MOVEit DMZ requires sending three short commands from the client to the server:

- INTEGRITY H - tells MOVEit DMZ that this client knows how to do integrity checking (pass this command once per session)
- XSHA1 [FileName] - asks MOVEit DMZ for the SHA-1 hash of a particular file (it is usually most efficient to ask for this information immediately after transferring that file)
- HASH OK/BAD - tells MOVEit DMZ that a locally calculated SHA-1 matches the XSHA1 hash was requested (only send this command after an XSHA1 command)

The local FTP client must be able to calculate SHA-1 hashes, of course. MD5 hashes MAY be allowed in the future, but only to support legacy FTP clients. CRC values will NEVER be allowed as they lack any cryptographic value and are thus almost useless in situations where non-repudiation is required.

Sample FTP Session

The following FTP session shows an FTP client session working with variations of the commands discussed above. A complete, successful integrity check has been highlighted in green.

```
ftp> QUOTE INTEGRITY H
200 Integrity mode selected
ftp> get HomePage.php
200 PORT command successful
150 RETR command started
226 Transfer complete. Integrity check pending.
ftp: 4890 bytes received in 0.70Seconds 6.79Kbytes/sec.
ftp> QUOTE XSHA1
500 XSHA1: parameters are incorrect
```

```
ftp> QUOTE XSHA1 HomePage.php
250 d6f63471acd1ab7dd647c86e6eea91d09f0fbb70
(at this point the FTP client calculates a SHA-1 hash
against the file it just downloaded and gets a
value of "d6f63471acd1ab7dd647c86e6eea91d09f0fbb70")
ftp> QUOTE HASH OK
200 Downloaded file has passed integrity check.
ftp> get HomePage.php
200 PORT command successful
150 RETR command started
226 Transfer complete. Integrity check pending.
ftp: 4890 bytes received in 0.64Seconds 7.45Kbytes/sec.
ftp> QUOTE XSHA1 HomePage.php
250 d6f63471acd1ab7dd647c86e6eea91d09f0fbb70
(at this point the FTP client calculates a SHA-1 hash
against the file it just downloaded and gets a
value of "c86e6eea91d09f0fbb70d6f63471acd1ab7dd647")
ftp> QUOTE HASH BAD
500 Downloaded file integrity check FAILED!
```

FTP - Certificates - Create Client Certificate

Use of SSL client certificates requires that individual users be issued certificates, typically one certificate per user. The process works like this:

- Someone (either the user or an administrator) creates a certificate request for the user.
- A Certifying Authority signs the request, thereby creating a client certificate.
- The client certificate is imported into the certificate database on the user's computer.

The first two steps can be done in a variety of ways. This document discusses how to perform these operations with **OpenSSL** (<http://www.openssl.org/>), a freeware command-line certificate manipulation program. You can obtain OpenSSL from *the OpenSSL binaries page*. (<http://www.openssl.org/related/binaries.html>)

Creating certificate requests

When using OpenSSL, there are two steps to creating a certificate signing request (CSR): creating the private RSA key, and creating the certificate request containing the user's name and other information.

First, create a key. User-entered input is shown in **bold**:

Example 1

```
C:\tmp>openssl genrsa -des3 -out clientcert.key 1024 Loading 'screen' into random state - done
```

Generating RSA private key, 1024 bit long modulus

```
.....+++++
```

```
.....+++++
```

```
e is 65537 (0x10001)
```

```
Enter pass phrase for clientcert.key: (the password is not echoed)
```

```
Verifying - Enter pass phrase for clientcert.key:
```

```
C:\tmp>
```

This example creates a 1024-bit key and stores it in clientcert.key. 1024 bits is a good level of security, but for even better security (but slower performance) you may choose a 2048-bit key.

Next, create the CSR:

Example 2

```
C:\tmp>openssl req -config \moveitdmz\util\openssl.conf -new -key clientcert.key -out clientcert.csr

Enter pass phrase for clientcert.key: (enter the password given above)

You are about to be asked to enter information that will be incorporated
into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [US]:US
State or Province Name (full name) [Some-State]:Wisconsin
Locality Name (eg, city) []:Madison
Organization Name (eg, company) [ACME Inc.]:Universal Exporters
Organizational Unit Name (eg, section) []:Accounting
Common Name (eg, fully qualified host name) []:Fred
Email Address []:fred@univ-exporters.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\tmp>
```

This example creates a certificate request for fred. The optional challenge password and company name are typically left blank. The file clientcert.csr is ready to be sent to the Certifying Authority who will sign the certificate.

Signing certificate requests

Once a certificate request has been created, it should be sent to a Certifying Authority for signing. A Certifying Authority can be:

- A commercial certificate firm such as *Thawte* (<http://www.thawte.com/>) or *Comodo* (<http://www.comodogroup.com/>), or
- A unit in your organization, such as the security group in your IT department, or
- Yourself (typically only in smaller companies)

If you want to make yourself a Certifying Authority so you will be able to sign CSRs yourself, you need a separate certificate. This type of certificate is issued to an administrator and is NOT needed by individual users. You can obtain such a certificate from various sources, including all three types listed above. If you work for a small organization, or are just testing, you may wish to create your own self-signed certificate. Self-signed certificates provide the same level of encryption as commercially-purchased types, but require a bit more effort before the server will "trust" them. Self-signed certificates are free and can have as long a lifetime as you want.

Creating your own self-signed certificate

To create a self-signed certificate so you can sign CSRs yourself:

Example 3

```
C:\tmp>openssl req -config \moveitdmz\util\openssl.conf -x509 -days 365 -newkey rsa:1024 -keyout MyCAcert.key
-out MyCAcert.cer
```

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

```
Generating a 1024 bit RSA private key
```

```
.....++++++
```

```
....++++++
```

```
writing new private key to 'MyCAcert.key'
```

```
Enter PEM pass phrase: (enter a new password that will be known only to the
administrator)
```

```
Verifying - Enter PEM pass phrase:
```

```
-----
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [US]:US

State or Province Name (full name) [Some-State]:Wisconsin

Locality Name (eg, city) []:Madison

Organization Name (eg, company) [ACME Inc.]:Universal Exporters

Organizational Unit Name (eg, section) []:IT Dept

Common Name (eg, fully qualified host name) []:UE IT Security

Email Address []:ueitsec@univ-exporters.com

C:\tmp>

This creates a 1024-bit certificate that expires in 365 days. In this example, the administrator creating the certificate is in the same organization as the client certificate applicant above, but in a different department. The key is written to MyCAcert.key and the public certificate to MyCAcert.cer. Be sure to keep the MyCAcert.key file and its password secure.

Signing certificate requests yourself

Once you have a signing key (either created yourself or obtained otherwise), you can sign CSRs:

Example 4

```
C:\tmp>openssl x509 -req -in clientcert.csr -days 1000 -CA MyCAcert.cer -CAkey MyCAcert.key -CAcreateserial -out clientcert.cer
```

Loading 'screen' into random state - done

Signature ok

```
subject=/C=US/ST=Wisconsin/L=Madison/O=Universal  
Exporters/OU=Accounting/CN=Fred/emailAddress=fred@univ-exporters.com
```

Getting CA Private Key

Enter pass phrase for MyCAcert.key: (enter the password of the CA cert)

```
C:\tmp>
```

This reads the user's certificate signing request and signs it, creating a client certificate in the file `clientcert.cer`. In this example, the certificate will be valid for 1000 days.

At this point, `clientcert.cer` is the public component of the client certificate, and `clientcert.key` is the private component. Some client software, most notably Microsoft Windows, requires that these files be converted to a different format before they can be used by the client. If you have access to the user's `clientcert.key` file (for example, if you performed the equivalent of Example 1 yourself), you can convert these two files into the single-file `.pfx` format required by Windows by using a command like:

Example 5

```
C:\tmp>openssl pkcs12 -export -in clientcert.cer -inkey clientcert.key -out  
clientcert.pfx
```

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

```
Enter pass phrase for clientcert.key: (enter the password created via "openssl  
genrsa" at the top)
```

```
Enter Export Password: (enter a new password. It can be the same as the openssl  
genrsa password)
```

```
Verifying - Enter Export Password:
```

```
C:\tmp>
```

The file `clientcert.pfx` now contains both the private and public components of the key. If the user created his or her own CSR and did not give you the `.key` file, the user will have to perform this `openssl pkcs12` command.

Importing client certificates on the user's computer

On the user's computer, the client certificate will have to be imported into the computer's certificate store. If the operating system is Microsoft Windows, the user should copy `clientcert.pfx` onto the computer and perform these steps:

- Double-click on the `.pfx` filename in Windows Explorer to run the Certificate Import Wizard
- On the Welcome page, choose Next
- On the File to Import page, choose Next (the filename will already be filled in)
- On the Password page:
 - Enter the export password you assigned above
 - Choose Mark the private key as exportable
 - Choose Next

- On the **Certificate Store** page, choose **Next** (Automatically will already be checked)
- On the **Completing** page, choose **Finish**
- At the **The import was successful** dialog, choose **OK**

The client certificate is now ready to be used. To double-check that the certificate has been installed, you may wish to examine the list of client certificates:

- Run Internet Explorer
- Choose **Tools | Internet Options...**
- Choose the **Content** tab
- Choose the **Certificates...** button
- On the **Personal** tab, you should see the newly-imported certificate
- For information on it, double-click the name of the certificate.

Installing the CA certificate on the server

If you created a self-signed CA certificate, you will need to install it on the server. This will enable the server to trust client certificates signed with this CA certificate. (If your CA certificate was issued by a major certificate vendor, this step is not necessary because the vendor's certificate is built into Windows.)

To run the Windows Certificate Wizard to import the CA certificate:

- Double-click on the **MyCAcert.cer** file to get the Certificate dialog
- Choose the **Install Certificate...** button
- On the **Welcome** page of the Certificate Wizard, choose **Next**
- On the **Certificate Store** page:
 - Choose **Place all certificates in the following store**
 - Choose **Browse...**
 - In the **Select Certificate Store** window:
 - Choose **Trusted Root Certification Authorities**
 - Choose **OK**
 - Choose **Next**
- On the **Completing** page, choose **Finish**
- In the **Security Warning** dialog, choose **Yes**
- In the **The import was successful** dialog, choose **OK**
- In the **Certificate** dialog, choose **OK**

SSH Server

This section contains reference information describing the features of the MOVEit SSH server.

SSH - Overview

The MOVEit DMZ SSH server provides both FTP over SSH and SCP2 services. SSH access is provided to the same underlying folder and file structure made available through MOVEit DMZ's SSH and Web Interface as well. SSH telnet access is NOT provided by this server.

Notable Features

MOVEit DMZ SSH runs as a standalone application (not part of IIS). Some of its notable features are listed below.

- Reads / writes directly to MOVEit DMZ's secure file storage. Unencrypted data is never written to disk.
- Uses secure communications via SSH encryption to encrypt usernames, passwords, directory listing, files and other data while in transit.
- Uses MOVEit usernames and passwords. MOVEit IP restrictions are also supported.
- Uses MOVEit logging to record signons, signoffs, uploads and downloads.
- Runs as a Windows service named MOVEitDMZSSH. MOVEit DMZ SSH can also run as an ordinary desktop application; this capability is typically used for testing and troubleshooting.
- Uploads and downloads files, with compatible clients, using compression to speed transfers.
- Uses SSH compression for faster transfers, when used with clients that implement compression (nearly all do).
- Can be bound to a specific IP address.

Typical SSH Environment

SSH is a secure transport protocol conceptually similar to SSL. Both protocols use public/private key cryptography to negotiate a shared key and symmetric encryption algorithm. This shared key is then used to encrypt succeeding data transfer. The main difference between the protocols is that SSL supports the concepts of "CA" and delegated trust, whereas SSH requires each endpoint to individually trust every other endpoint.

FTP over SSH is primarily associated with UNIX, whereas FTP over SSL is typically associated with Windows and mainframes.

SSL's ease of large-scale deployment is the reason why HTTP over SSL - HTTPS - is more popular than a (theoretical) "HTTP over SSH" protocol. SSH's ease of self-key-generation and configuration is the reason why telnet over SSH (typically also called just SSH) is more popular with router technicians and Unix server administrators than telnet over SSL. MOVEit DMZ takes advantage of both models by supporting both SSL and SSH.

For more information, see **SSH "Protocol Discussion"** (on page 647).

Installation

MOVEit DMZ SSH is installed automatically with MOVEit DMZ.

The setup program for MOVEit DMZ provides the option of installing MOVEit DMZ SSH as a service. Normally, you will install the program as a service. However, you can instead run the program manually by choosing the Start menu shortcut **RunMOVEit DMZ SSH manually** after installation. In manual mode, MOVEit DMZ SSH displays a window containing two subwindows, one containing the status of the current connections and the other showing a scrolling list of messages.

Note: In order to generate the server public key, MOVEit DMZ SSH server requires write access to the directory into which it is installed, typically Program Files\MOVEit. This is automatically granted when the program is running as a service under the local system account, which is the default. However, when you run the program manually under a non-administrative account, the program may not have write access to the directory.

MOVEit DMZ SSH's window is normally not displayed when it is running as a service. However, you can cause it to be displayed by changing the service to allow it to interact with the desktop. To do this on Windows 2003, choose Start / Settings / Control Panel / Administrative Tools / Services, and choose the MOVEit DMZ SSH service. Right-click and choose Properties. Choose the Log On tab. Choose *Allow service to interact with desktop*. You will have to stop and restart the service for this change to take effect.

Directory Structure

MOVEit DMZ SSH's directory structure is the same as that which is visible through the web interface, except for those users who have the "Chroot" option enabled for their default folder. Those users will only be able to see the files and folders in and below their default folder and will not be able to navigate to folders outside their default folder. See the User Settings - Default Folder section of the **Web Interface - Users - Profile** (on page 286) documentation page for more details.

The initial directory upon logon depends on the user type. End users and group admins will be placed in their default folder (usually their home folder), while administrators will be placed in the root folder.

User type	Initial directory

SysAdmin /

Administrator
r /

FileAdmin /

GroupAdmin The GroupAdmin's home directory or a designated default
 folder

User The User's home directory or a designated default folder

TempUser N/A (*not allowed to sign on to SSH*)

A "dir" command shows only the folders to which the user is permitted access, so not all users will get the same results from a "dir".

Disabling the SSH Service

To disable the MOVEit DMZ SSH service you may use the Microsoft Services control panel to mark the MOVEit DMZ SSH service as disabled. The MOVEit DMZ "Check" utility (usually run after installations and upgrades) will automatically be aware if you have disabled the SSH service and will not try to check it in that situation.

SSH - Configuration

The MOVEit DMZ Configuration program is used to configure the MOVEit DMZ SSH server. (Users, groups, folder settings and the like are generally maintained through the Web Interface or MOVEit DMZ API.) Run the configuration program by choosing the Start menu shortcut **MOVEit DMZ Config**. This program uses a tabbed dialog to group the settings by function.

MOVEit DMZ SSH will immediately apply configuration changes the next time a new connection is received.

Exception: If a change is made to the SSH port, the MOVEit DMZ SSH service must be restarted for this change to take effect.

SSH Tab

The screenshot shows the 'Configure MOVEit DMZ' dialog box with the 'SSH' tab selected. The 'SSH Configuration' section contains fields for 'Server Key' (b4:51:8a:9c:5d:7e:98:db:f0:88:08:52:31:b4:a0:1e), 'SSH Port' (22), and 'Bind to IP Address' (0.0.0.0). The 'Server Keys' section has a table with one entry: (default) with fingerprint b4:51:8a:9c:5d:7e:98:db:f0:88:08:52:31:b4:a0:1e. The 'Alternate Bindings' section has an empty table with columns for Server IP, Server Key, and Organization. Buttons for 'View', 'Add', 'Edit', 'Remove', 'Default', 'Add', 'Edit', 'Remove', 'OK', 'Cancel', 'Apply', and 'Help' are present.

License	Status	Paths	Email	Settings	Database
FTP Ports	FTP Certs	FTP IPs	SSL	SSH	SSH Ciphers

SSH Configuration

Server Key: b4:51:8a:9c:5d:7e:98:db:f0:88:08:52:31:b4:a0:1e View

SSH Port: 22 (default 22)

Bind to IP Address: 0.0.0.0
(0.0.0.0 = all available IP's)

Server Keys

Name	Fingerprint
(default)	b4:51:8a:9c:5d:7e:98:db:f0:88:08:52:31:b4:a0:1e

Add Edit Remove Default

Alternate Bindings

Server IP	Server Key	Organization

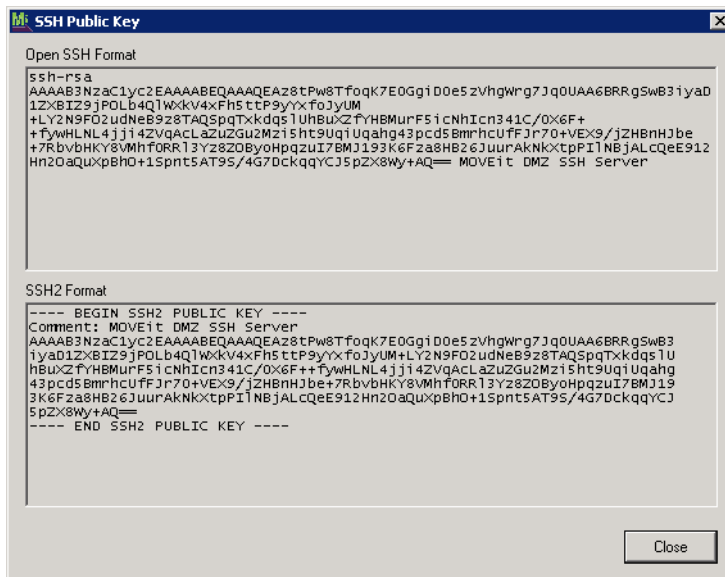
Add Edit Remove

OK Cancel Apply Help

SSH Configuration

- **Server Key:** The public key used for SSH sessions. This key is generated internally and the MD5 hash of the key displayed here for reference only. There is no mechanism to edit this value. Use the **View** button next to the MD5 field to view and/or **export the entire SSH public key** (on page 639).

To export MOVEit DMZ's SSH public key, click the **View** button on the **SSH** tab of the MOVEit DMZ Config utility. The dialog will show you the key in two different formats. Select all the text in the window displaying the format you wish to export, press **CTRL+C** to copy the text, then save it into a text file of your choice.

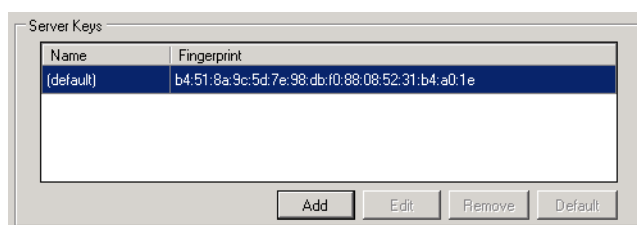


HINT: MOVEit DMZ's SSH server key never changes, so it's probably worth the extra time to export both formats of the same SSH server key while you're in the dialog. If you save these off (perhaps on an internal server) you may never need to come back to the **SSH** tab again.

- **SSH Port:** The TCP port on which to listen. The default is 22, the value used by nearly all SSH servers.
- **Bind to IP Address:** Leave blank to bind to all available IP addresses (default). Enter a specific IP address to bind the SSH server to a specific IP address.

Server Keys

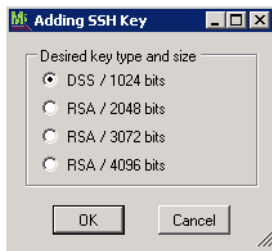
The **Server Keys** window shows the MD5 hash of the internally generated RSA 2048-bit server key. You may not edit or remove this default key.



If your MOVEit DMZ has multiple organizations, you may want to add a different server key for each organization. Doing so will make it easier to change only one organization's server key without affecting other organizations.

➤ **To add a new Server Key:**

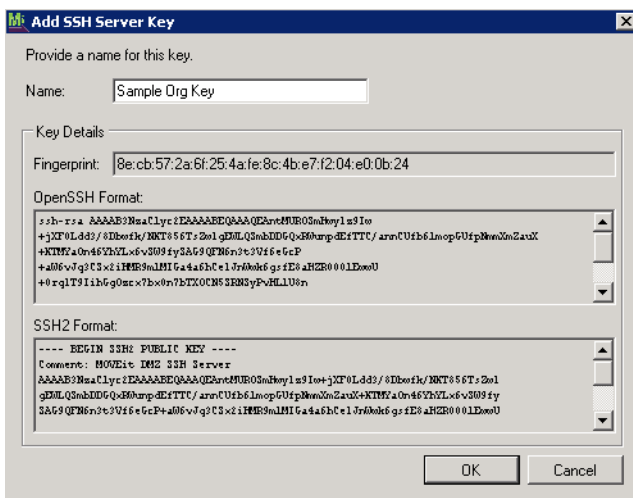
- 1 Click **Add** and then select the desired key type and size:



The DSS key type provides digital signatures but not key exchange or encryption. With DSS, signature generation is faster than signature verification.

The RSA key types provide digital signatures, key exchange, and encryption. With RSA, signature verification is faster than signature generation.

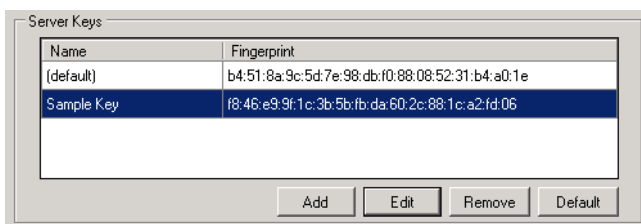
After you select a key type and size, the Add SSH Server Key window displays:



This window shows the key details, including Fingerprint, OpenSSH Format and SSH2 Format.

- 2 Enter a Name for the key and click OK.

The new key adds to the Server Keys window.

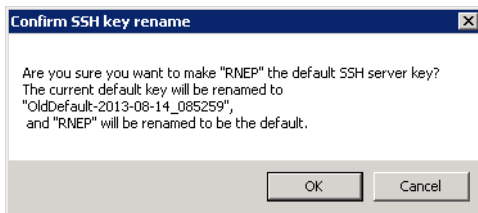


To edit a key's name, select the key and click **Edit**.

To remove a key, select the key and click **Remove**.

To make a key the default SSH server key, select the key and click **Default**. The current default key will be renamed to "OldDefault-year-month-day_XXXXXX" and the name of the key you have selected will be renamed "default."

- 3 When you see the Confirm SSH key rename message, click OK.



Alternate Bindings

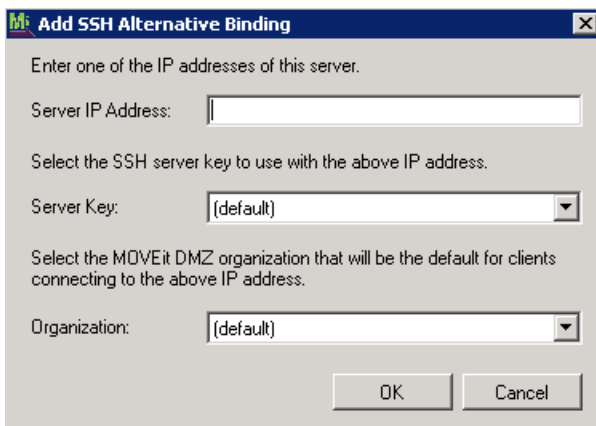
If your MOVEit DMZ has multiple organizations and it allows duplicate usernames across organizations, you can add an alternate binding to direct users to the IP address of their specific organization during signon by adding an alternate binding. You can also assign a unique server key to an organization so that any changes you make to that server key will affect only that organization.

Alternate Bindings lets you associate a Server IP, Server Key, and Organization.

➤ To add an alternate binding:

- 1 Under Alternate Bindings, click **Add**.

The Add SSH Alternative Binding dialog displays.

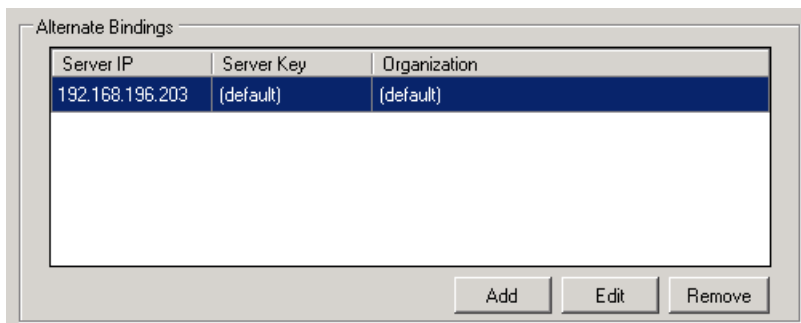


- 2 Enter the following:
 - **Server IP Address:** Enter a distinct IP address that does not already have an alternate binding (for example, 192.168.45.122). Do not select the default Bind to IP Address (0.0.0.0.).
 - **Server Key:** Select a server key from the drop-down list to bind to the Server IP address. Server keys appear here only if they have already been added to the **Server Keys** window.

- **Organization:** Select an organization from the drop-down list to bind to the Server IP address. In addition to your MOVEit DMZ organizations, you will see the following organizations in the drop-down list:
 - (default): Any organization can be assigned as the default. See **Web Interface - Settings - System - Miscellaneous** (on page 540) for information on how to assign a default organization.
 - (System): The System Organization is used by SysAdmins to administer system-wide settings and create and maintain other organizations. It is not likely that you will create an alternative binding for the System organization.

3 Click OK.

The new binding adds to the **Alternate Bindings** window.



To edit the Server IP, Server Key, and Organization of a binding, select the binding and click **Edit**.

To remove a binding, select the binding and click **Remove**.

Diagnostic Logs

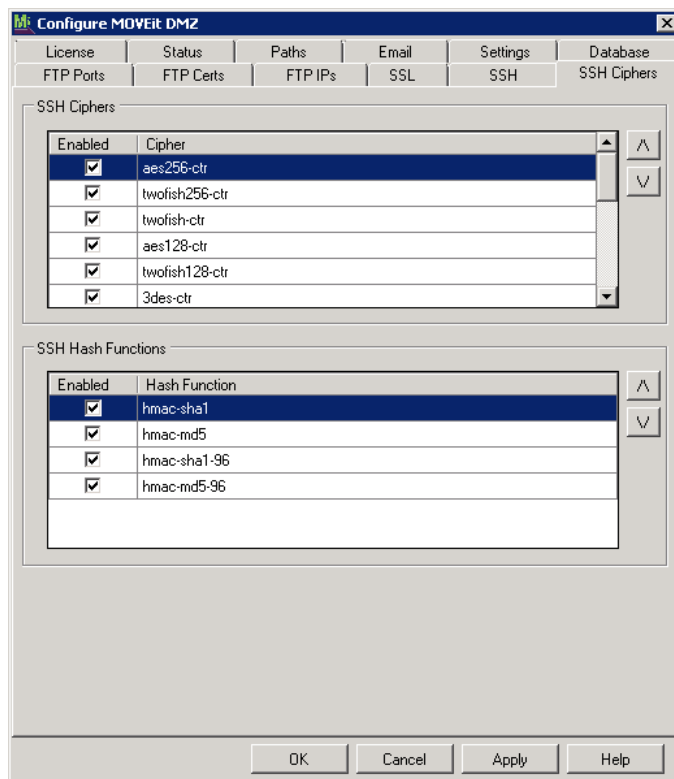
The MOVEit DMZ SSH server's diagnostic log settings can be changed on the Status tab of the configuration utility. See the *Configuration Utility* document for more information about this tab.

Paths Tab

The MOVEit DMZ SSH server communicates with MOVEit DMZ using the Machine URL configured on this tab. See the *Configuration Utility* document for more information about this tab.

SSH Ciphers Tab

The encryption and hashing algorithms that the MOVEit DMZ SSH server uses can be configured on the SSH Ciphers Tab. (The encryption and hashing algorithms used by the MOVEit DMZ SSL servers - **both HTTPS and FTPS** - are also configurable (on page 577).)



This tab lets you select the ciphers and hash functions used to secure the SSH connection.

For FIPS and PCI compliance, you may need to prevent the use of weak ciphers. For example, a PCI audit may flag the use of ciphers, such as MD5 and MD5-96. FIPS-approved cryptographic methods for SSH include (as of June 2013) 3des-cbc, aes128-cbc, aes192-cbc, and aes-256 ciphers with hmac-sha1 as the only approved hash function.

Note: Both the client's and the server's preferences are taken into consideration when choosing the actual cipher and hash function for a given session. There must be a common cipher and hash function on both sides or there will be an error.

Selecting SSH Ciphers

The SSH Ciphers section allows you to choose which ciphers are permissible, and their order of preference. By default, all ciphers are enabled.

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 weak ciphers or hashes, you should always put the stronger ones at the top of the list.

Selecting SSH Hash Functions

The SSH Hash Functions section allows you to choose which hash functions are permissible, and their order of preference. By default, all hash functions are enabled.

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.

Algorithms Used by SSH

Certain clients may want to know which algorithms the MOVEit DMZ server supports, so this section provides a complete list.

Many SSH clients can also obtain this information from MOVEit DMZ just by connecting because the SSH protocol requires the server to list which modes it supports. In other words, there is no security reason to keep this information private.

SSH Encryption Algorithms

MOVEit DMZ SSH server supports the following encryption algorithms.

- aes256-ctr
- twofish256-ctr
- twofish-ctr
- aes128-ctr
- twofish128-ctr
- 3des-ctr
- cast128-ctr
- aes256-cbc
- twofish256-cbc
- twofish-cbc
- aes128-cbc
- twofish128-cbc
- blowfish-cbc
- 3des-cbc (a.k.a. "triple-DES")
- arcfour
- cast128-cbc

SSH Hash Algorithms

MOVEit DMZ SSH server supports the following (keyed) hash algorithms.

- HMAC-MD5
- HMAC-SHA1
- HMAC-MD5-96
- HMAC-SHA1-96

SSH Compression Algorithms

MOVEit DMZ SSH server supports the following on-the-fly compression algorithms.

- none
- zlib (a.k.a. "gzip")

SSH - Protocol Discussion

This section introduces you to SSH and SSH/FTP by comparing and contrasting these protocols to FTP over SSL.

SSH/FTP is often referred to as "SFTP". Despite the unfortunate similarity in name, SFTP is a completely different protocol than FTP over SSL, which is commonly known as FTPS.

Standards

SSH is a proposed Internet standard documented in **RFC 4251** (<ftp://ftp.rfc-editor.org/in-notes/rfc4251.txt>) while SSH/FTP is a proposed Internet standard currently in "draft" (pre-RFC) status. SSL (the term popularly includes the more recent version of Secure Socket Layer known as TLS) is a proposed standard documented in **RFC 2246** (<ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt>), and FTP is an official Internet standard documented in **RFC 959** (<ftp://ftp.rfc-editor.org/in-notes/rfc959.txt>).

The overall SSH protocol comes in two major versions, SSH1 and SSH2. MOVEit DMZ SSH supports only the more common SSH2 protocol. Although the SSH2 protocol is fairly well-established, the SSH/FTP protocol is still undergoing significant revisions, some of which are incompatible with previous versions. This situation reflects the fact that the SSH/FTP protocol has not yet achieved "RFC" status.

The SSH file transfer protocol comes in versions 1, 2, 3, and 4. As of this writing, version 4 is brand new and has not been implemented by any known clients or servers. MOVEit DMZ SSH implements version 3 of the protocol.

Command Structure

SSH/FTP sessions consist of a series of command and response packets. The packets consist of structured binary information, including integer command codes and response codes. The commands correspond to file system I/O routines such as Open(), Read(), Write() and Close(). To download a file, for instance, the SSH/FTP client must open the file with an Open command followed by a number of Read commands and a Close command.

By contrast, FTP and FTP over SSL use ASCII commands delimited by CR LF. For example to download a file, the client would send a "PORT" or "PASV" command to set up the data connection, followed by a "RETR" command specifying the filename.

Port Number and Firewalls

SSH uses a single TCP port number - usually port 22 - for all types of connections. By contrast, SSL uses different port numbers for different applications. For instance, port 443 is typically used for HTTP over SSL, and port 990 is used for one version of FTP over SSL. Furthermore, FTP requires multiple port numbers during file transfers, as each individual file transfer creates a new connection on a new port.

The fact that port 22 is used for all SSH services makes it a bit difficult to have multiple SSH server products running on the same computer. But this is rarely an issue for systems running MOVEit DMZ. More importantly, the fact that port 22 is the only port required for SFTP - there are no separate data ports - makes SSH/FTP a more "firewall-friendly" protocol than FTP over SSL.

Encryption and Certificates

Both SSH and SSL use public key cryptography to exchange a session key, which is then used to encrypt the commands and data transmitted over the network. The security of the algorithms used by SSH is similar to those used by SSL, but SSH does NOT support the concept of a Certificate Authority (CA).

SSL requires a certificate, which is usually purchased from a Certifying Authority like **www.thawte.com** (**<http://www.thawte.com>**). A certificate vouches for the identity of the server. SSH uses a different approach, in which each server creates its own public key. There is no trusted authority to vouch for the identity of an SSH server. To make up for this, by convention, each SSH client remembers the public key of each server it has ever connected to. If, on a subsequent connection attempt, the server presents a different public key, the SSH client will warn the user that the SSH server may be a hostile server masquerading as the original server.

As a result of these differences, FTP over SSL (FTPS) servers can be more cumbersome to administer than SSH/FTP (SFTP) servers. But by virtue of the more sophisticated certificate scheme, FTPS servers are slightly more secure.

SSH - Server Keys - Overview

Users of SSH clients know to trust specific machines because their keys will match publicly available SSH fingerprints. As part of the instructions you give your clients, you **SHOULD** be distributing the fingerprint of your MOVEit DMZ SSH server so your clients can confirm the identity of your server. (Without this protection, anyone could spoof this or any other SSH server!)

The following OpenSSH session shows this mechanism in action. Specifically, OpenSSH asks the end user if they want to trust the remote server after displaying the MD5 hash of the remote server's SSH server key.

```
d:\>sftp sshftpuser@moveit.myorg.com
```

```
Connecting to moveit.myorg.com...
```

```
The authenticity of host 'moveit.myorg.com (33.44.55.66)' can't be established.
```

```
RSA key fingerprint is b4:51:8a:9c:5d:7e:98:db:f0:88:08:52:31:b4:a0:1e.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
sshftpuser@moveit.myorg.com's password:
```

MOVEit DMZ's SSH key is automatically generated the first time the server is started and an associated fingerprint is created at the same time. To view your MOVEit DMZ SSH key fingerprint log into a Windows console on your MOVEit DMZ server. Open Start -> All Programs -> MOVEit DMZ -> MOVEit DMZ Config and navigate to the SSH tab to view your MOVEit DMZ's SSH key MD5 hash.

Configure MOVEit DMZ

License	Status	Paths	Email	Settings	Database
FTP Ports	FTP Certs	FTP IPs	SSL	SSH	SSH Ciphers

SSH Configuration

Server Key:

SSH Port: (default 22)

Bind to IP Address:
(0.0.0.0 = all available IP's)

Server Keys

Name	Fingerprint
(default)	b4:51:8a:9c:5d:7e:98:db:f0:88:08:52:31:b4:a0:1e

Alternate Bindings

Server IP	Server Key	Organization

Server Key Backup

The MOVEit DMZ SSH server key is stored encrypted in the registry under the `SSHServer\PrivKey` registry entry. Any registry backup, including the registry backup performed by the **MOVEit DMZ Backup Utility** (on page 150), will back up this key.

Server Key Export

To export MOVEit DMZ's public SSH server key in either OpenSSH or SSH2 format, see the related instructions in **SSH - Configuration** (on page 639).

Requirements

MOVEit DMZ only supports FTP over SSH (or SFTP) and SCP2. SCP (SCP1) and all Terminal sessions will be denied access.

MOVEit DMZ SSH Server uses SSH Protocol 2 only. A client will not be able to connect to the MOVEit DMZ server using only Protocol 1. MOVEit DMZ SSH Server recommends using the following encryption ciphers: AES, 3DES, and Blowfish. (An ever-expanding list of **compatible clients** (on page 793) and a **complete list of encryption options** (on page 639) is also included in this documentation.)

Troubleshooting

If the SSH user is connecting to MOVEit with the correct username but the administrator does not see any SSH public key entries in the audit logs, it is likely that the end user has NOT yet generated a public/private key pair for SSH. End users can often use the `ssh-keygen -t rsa` command to generate these keys, but they should be advised to NOT enter a passphrase when prompted during the key generation; if a passphrase is entered it will be asked for during each subsequent attempt to connect and will spoil attempts to automate the process.

SSH - Specific Clients - OpenSSH Windows

Preparation

This guide assumes you have already installed a copy of OpenSSH for Windows.

If you have not already installed OpenSSH for Windows, be sure to **UNCHECK** the **Server** box on the **Choose Components** section during the installation of this client.

Instructions

- 1 Select or **CREATE** a directory where the OpenSSH `known_hosts` and key files will be located (`\Program Files\OpenSSH\bin\ssh` is a good choice). We will refer to this directory as `SSHDIR` throughout this guide. When referenced in a command, be sure to substitute in your value.
- 2 Open a command-prompt, navigate to the `\Program Files\OpenSSH\bin` directory, and execute the following command:

```
sftp -oUserKnownHostsFile=SSHDIR\known_hosts user@host
```

This will come back with a warning that the host is not known. Enter **yes** to the question. This will add the host's key to the `known_hosts` file. Then, simply press **CONTROL+C** to leave the application.

Example:

```
C:\Program Files\OpenSSH\bin>sftp
-oUserKnownHostsFile=C:\Progra~1\OpenSSH\bin\ssh\known_hosts
sshkeyboy@dotnet.corp.stdnet.com
Connecting to dotnet.corp.stdnet.com...
The authenticity of host 'dotnet.corp.stdnet.com (192.168.3.15)' can't
be established.
RSA key fingerprint is
ce:08:6f:28:87:b6:50:f4:84:e5:37:c2:68:89:33:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'dotnet.corp.stdnet.com,192.168.3.15' (DSA)
to the list of known hosts.
sshkeyboy@dotnet.corp.stdnet.com's password:
(CONTROL+C)
C:\Program Files\OpenSSH\bin>
```

- 3 Execute the following command:
`ssh-keygen -t rsa`

When asked to enter a file to save the key in, use this value:

SSHDIR\id_rsa

When asked for a password, simply hit enter (and again when asked to confirm). This will create an RSA key which will be used to authenticate to the server. The ssh-keygen program should give the key files their correct permissions automatically.

Example:

```
C:\Program Files\OpenSSH\bin>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (P7 $"/.ssh/id_rsa):
c:\progra~1\OpenSSH\bin\ssh\id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
c:\progra~1\OpenSSH\bin\ssh\id_rsa.
Your public key has been saved in
c:\progra~1\OpenSSH\bin\ssh\id_rsa.pub.
The key fingerprint is:
44:a8:8c:88:3f:3f:91:8a:16:07:e4:c6:4a:6e:b8:df xxxx@jglshuttle
C:\Program Files\OpenSSH\bin>
```

4 Execute the following command:

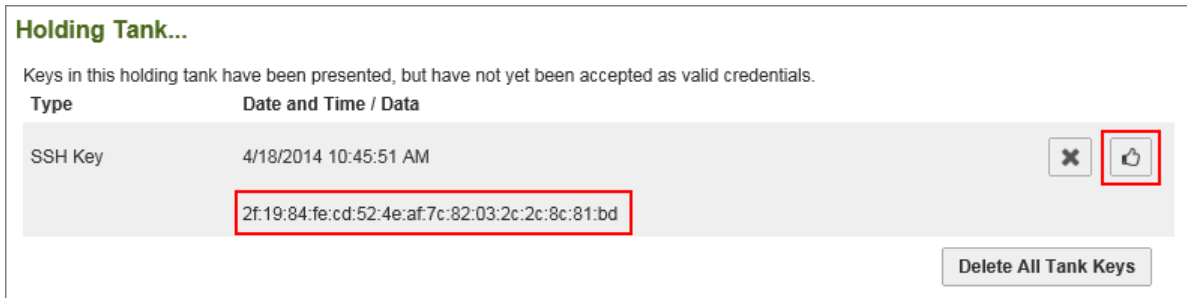
```
sftp -oUserKnownHostsFile=SSHDIR\known_hosts
-oIdentityFile=SSHDIR\id_rsa user@host
```

This will come back asking for the user's password. Simply Control-C out of the program at this point.

Example:

```
C:\Program Files\OpenSSH\bin>sftp
-oUserKnownHostsFile=c:\progra~1\OpenSSH\bin\ssh\known_hosts
-oIdentityFile=c:\progra~1\OpenSSH\bin\ssh\id_rsa
sshkeyboy@dotnet.corp.stdnet.com
Connecting to dotnet.corp.stdnet.com...
sshkeyboy@dotnet.corp.stdnet.com's password:
(CONTROL+C)
C:\Program Files\OpenSSH\bin>
```

- 5 The new key's fingerprint should now be logged on the DMZ host. Log on through the web interface as an administrator, click up the user's profile, go into the user's SSH policy, and ACCEPT the SSH key from the client key holding tank. (The key fingerprint is circled in RED in the image below.)



Open the user's profile and under User Authentication > SSH Policy > Current SSH Keys, add this fingerprint. A properly configured user will have a profile similar to the following:

User Profile (kristina)

General Information

Username: kristina
Full Name: kristina
User ID: kristina23t5a3u1
Permission: Administrator
Notifications: via HTML-Format Email (user@ipswitch.com) + Administrative Alerts
Language: English
Created: 2/26/2014 12:43:53 PM by Default SysAdmin

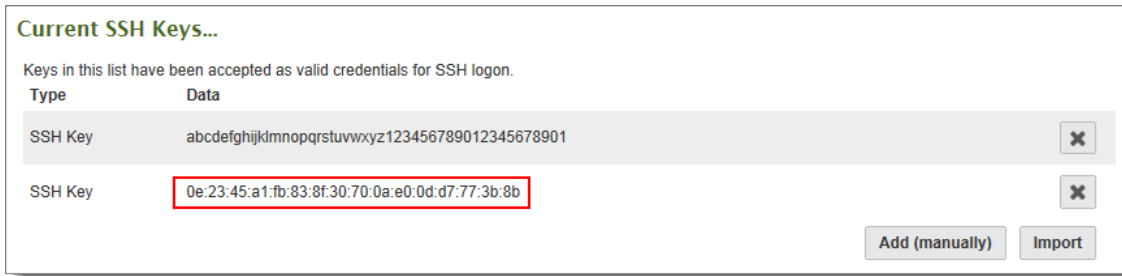
 [Change Information](#)
 [View Home Folder \(/Home/kristina\)](#)
 [View Folder Access List](#)
 [View User Logs](#)

User Authentication

Last Signon: 4/1/2014 7:31:22 AM
Account Status: Active - [Change Status](#)
Expiration Policy: No Policy Set - [Change Policy](#)
Authentication Source: MOVEit Only
Password: - [Change Password](#)

Credentials Required for Access: *(in addition to Username)*

HTTP Server:	Web Interface: Password Only with SSL	HTTP Policy
	HTTP Clients: Password Only with SSL	
FTP Server:	Secure (SSL): Password Only with SSL	FTP Policy
	Insecure: Not Allowed	
SSH Server:	SSH Client Key OR Password	SSH Policy
Mobile Interface:	Password, no caching allowed	Mobile Policy



- 6** You should now be able to automatically connect to the DMZ host via SFTP using the following command:

```
sftp -oUserKnownHostsFile=SSHDIR\known_hosts
-oIdentityFile=SSHDIR\id_rsa user@host
```

Example:

```
C:\Program Files\OpenSSH\bin>sftp
-oUserKnownHostsFile=c:\progra~1\OpenSSH\bin\ssh\known_hosts
-oIdentityFile=c:\progra~1\OpenSSH\bin\ssh\id_rsa
sshkeyboy@dotnet.corp.stdnet.com
Connecting to dotnet.corp.stdnet.com...
sftp> pwd
Remote working directory: /Home/SSH Key Boy
sftp> cd ..
sftp> cd ..
sftp> dir
Distribution
Home
WebPost
sftp>
```

- 7** To use SFTP in an automated setting, use the `-b` command-line option to supply SFTP with a list of commands to be issued.

Example:

```
C:\>type sftp_commands.txt
cd /Home/Steve
put certreq.txt
dir
quit
```

```
C:\>c:\progra~1\openssh\bin\sftp
-oUserKnownHostsFile=c:\progra~1\openssh\bin\ssh\known_hosts
-oIdentityFile=c:\progra~1\openssh\bin\ssh\id_rsa -b
sftp_commands.txt steve@dotnet.corp.stdnet.com
Connecting to dotnet.corp.stdnet.com...
sftp> cd /Home/Steve
sftp> put certreq.txt
Uploading certreq.txt to /Home/Steve/certreq.txt
sftp> dir
DecSet_6858908.exe
MIFreelyInst_9971297.exe
brain_1731860.wav
certreq_1140952.txt
decryptedFile_5848271.dat
dmz_backups_2157003.html
webpost_bundle_4594384.xml
sftp> quit
```

SSH - Specific Clients - OpenSSH Unix

Generating SSH Keys

At the shell prompt type the following:

```
ssh-keygen -t rsa
```

This will start the generation of a RSA SSH key to use with MOVEit DMZ. Hit enter to accept the default location of the key. Also, hit enter to leave the passphrase blank. The dialog will look similar to the dialog below:

```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key (/home/sms/.ssh/id_rsa):
```

```
Enter passphrase (empty for no passphrase):
```

```
Enter same passphrase again: Your identification has been saved in  
/home/someuser/.ssh/id_rsa.
```

```
Your public key has been saved in /home/someuser/.ssh/id_rsa.pub.
```

```
The key fingerprint is:
```

```
xx:2d:28:59:90:xx:20:69:xx:45:ec:77:2a:de:a5:xx sms@somehost
```

You will need the fingerprint information for the login credentials into MOVEit DMZ. The fingerprint looks like: xx:2d:28:59:90:xx:20:69:xx:45:ec:77:2a:de:a5:xx

ssh-keygen will create a public and private key pair for use in authentication. The private key is stored in ~/.ssh/identity (or ~/.ssh/id_rsa), whereas the public key is stored in ~/.ssh/identity.pub. In most SSH setups, the public key must be placed in a ~/.ssh/authorized_keys file on a remote machine, but MOVEit DMZ stores fingerprints of these public keys in its user record instead. (See the *Keys* section for more information.) Having a valid public/private key pair will allow connections to the SSH interface of MOVEit DMZ based upon RSA authentication instead of passwords.

If a file called ~/.ssh/known_hosts exists and the end user has opted to trust the public key of a MOVEit DMZ server, this file should contain the hostname and/or IP address of the MOVEit DMZ server as well as its public key. Although it is possible to edit this file by hand, it is instead recommended that end users permit their SSH clients to make the necessary changes to this file instead.

OpenSSH Field Tips

The following observations and workarounds have been observed and deduced by technical support staff working with the OpenSSH client in the field.

- Some older (2001?) versions of OpenSSH do not support the -b batch file command. However, these versions do seem to support the "sftp user@host < batchfile.txt" input pipe syntax instead.
- Some versions of OpenSSH also seem to be locked and do not permit the use of the -oIdentityFile command. (In other words, they can only use the current user's default identity file.) In this case, a local *nix user who username matches the MOVEit DMZ username must be used in order to get SSH client key authentication to work.

Web Farms

This section describes how to configure MOVEit DMZ to run multiple nodes in a tiered architecture, commonly called a Web Farm.

Web Farms - Overview

MOVEit DMZ supports running in a tiered architecture, commonly called a web farm. In this architecture, the application nodes are generally separated from the support nodes, such as database and filesystem servers, and any number of application nodes can be present in the farm. Additional nodes can be easily added if necessary, and if any one application node fails, the others continue to run, providing resilient access to the application. A load balancer provides access to the application nodes, and directs requests to each node, skipping any nodes that are not operational.

Components

A MOVEit DMZ web farm requires the following components:

- One or more MOVEit DMZ servers to act as application nodes.
- A database server or cluster, accessible from the application nodes (Microsoft SQL Server 2008 or 2012 is recommended as the database application).
- A fileserver or cluster, accessible from the application nodes using Microsoft File Sharing.
- A network load balancer to provide a single access point for external connections to access the application nodes.

Application Nodes

Each application node is a server containing a licensed copy of the MOVEit DMZ software. Each node is automatically assigned a node number when it is added to the farm, starting with node 1 when the farm is created. The nodes run independently of each other, having only minimal contact through node status and auditing records in the database that are constantly updated while each node is active. However, each node accesses the same database and filesystem as all the others.

Database Server

The database server should be a separate server from the application nodes and, in the most secure architectures, on a separate network from the application nodes with access controlled by a firewall. For increased reliability, a database cluster may be used, as long as the cluster is available to the application nodes via a single IP address.

Fileserver

As with the database server, the fileserver should be a separate server from the application nodes and, in the most secure architectures, on a separate firewalled network from the application nodes. For smaller farms, the fileserver and database server may be the same system, though for maximum performance and reliability, they should be separate. Again, as with the database server, using a fileserver cluster increases reliability of the farm, as long as the cluster is available to the application nodes via a single IP address.

Load Balancer

The load balancer provides a single access point for external connections to access the application nodes. It should be capable of monitoring the health and connectivity of the application nodes, so that when one fails, it is removed from the load balancer's list of servers to forward connections to. It should also be capable of continuing to forward subsequent connections from a client to the same application node, once a session has been established. This is especially important when using non-HTTP services such as FTP and SFTP.

MOVEit DMZ web farms can be used with hardware load balancers from companies like Cisco and F5, or the Windows Network Load Balancing service from Microsoft.

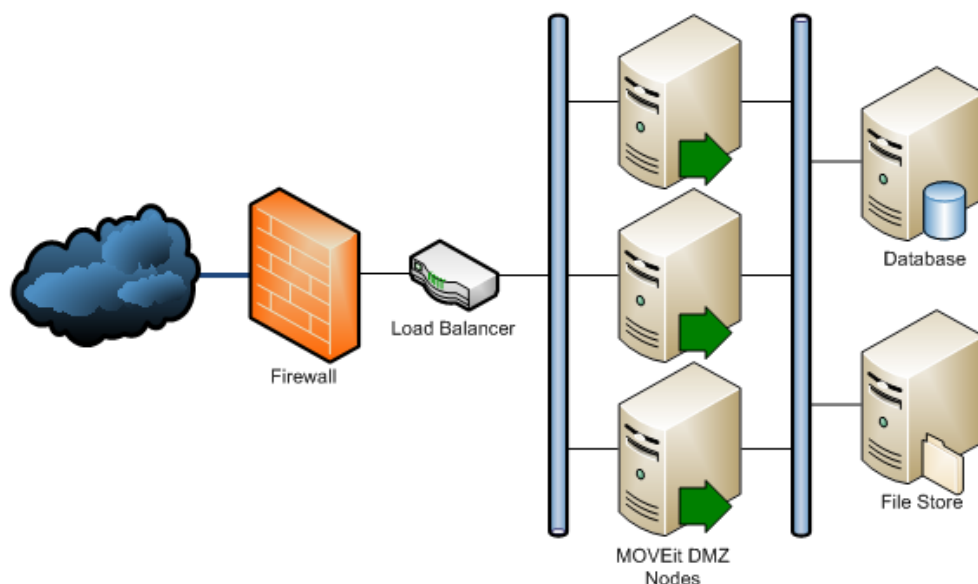
Webfarms - Architecture

A MOVEit DMZ webfarm uses a tiered architecture, separating the database and file store segments from the MOVEit DMZ application servers. In this way, MOVEit DMZ application servers can be added to the farm at will, providing increased ability to handle web requests. Additionally, the database and file store servers can be upgraded independently to handle increased load, or even clustered to provide even more performance and reliability.

Below are examples of possible MOVEit DMZ webfarm architectures. Each architecture has shared features, such as a load balancer to distribute requests to the MOVEit DMZ nodes, and a separate internal network for connecting the MOVEit DMZ nodes to the database and file store servers. Differences include whether a firewall is used to protect the database and file store servers from the MOVEit DMZ nodes, and whether the database and file store servers are clustered.

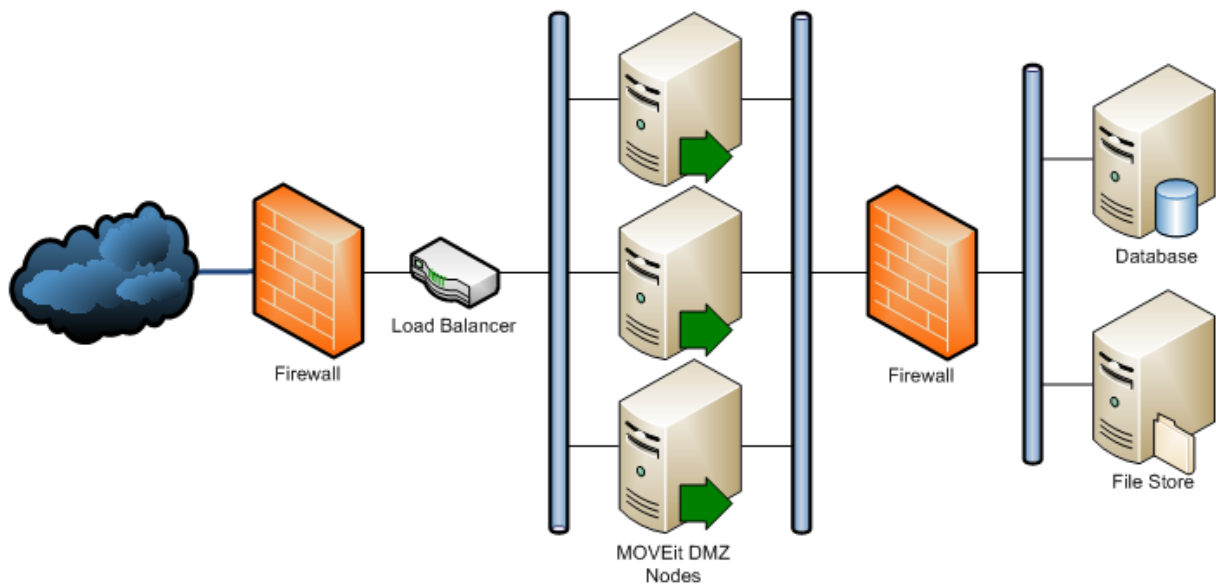
Simple Tiered Webfarm

This is an example of a simple tiered MOVEit DMZ webfarm. A load balancer distributes requests to the individual MOVEit DMZ nodes, each of which connects via a separate internal network to the database and file store servers.



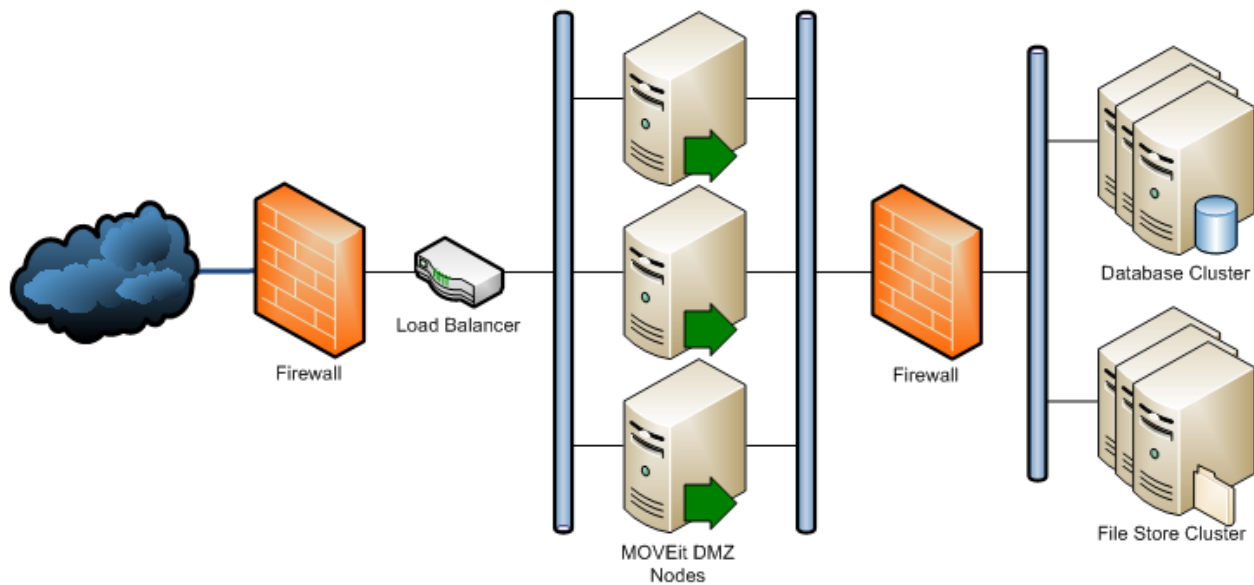
Secure Tiered Webfarm

In this example, a firewall separates the database and file store servers from the MOVEit DMZ nodes. As the most internet-facing servers in the farm, the MOVEit DMZ nodes are the most susceptible to being attacked and compromised. The firewall helps guard against further penetration into the more vital internal servers, in the unlikely event one of the MOVEit DMZ nodes is compromised.



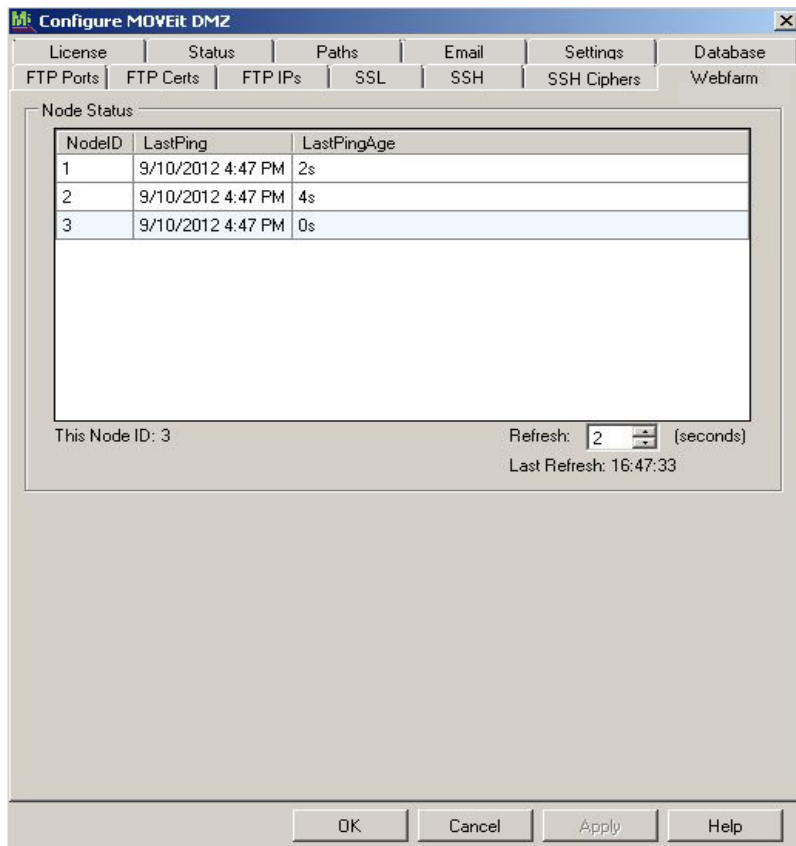
Secure Clustered Tiered Webfarm

In this example, the database and file store servers are clustered, providing increased reliability and performance. The clusters appear as a single server to the MOVEit DMZ nodes, but are able to tolerate hardware failures that would normally cause the entire webfarm to fail in an unclustered farm.



Web Farms - Webfarm Tab

The MOVEit DMZ Config program will display the **Webfarm** tab when it detects that the current MOVEit DMZ server is a member of a web farm. On this tab can be found the current status of the application nodes in the farm, including the node ID, the last time each node updated its status, and the amount of time that has passed since that last status update.



Nodes are generally displayed in a normal font, indicating that the node has updated its status within the last 60 seconds. This is a good indication that the node is healthy and active. If the node has not updated in over 60 seconds, the entry will be listed in italics, indicating something may be wrong with the node. If the node has not updated in over 60 minutes, the entry will be listed in red italics, indicating that something is almost certainly wrong with the node.

The current node ID is listed below the node status list, and the current node's entry in the node status list will have a light blue background. Finally, a refresh option is available to change how frequently the config program checks the status of the nodes, and the time of the most recent refresh is displayed.

Web Farms - Technical Discussion

MOVEit DMZ web farm support relies upon several capabilities that provide support for a tiered architecture, as well as synchronization of important shared information across the web farm application nodes.

Remote Database Support

MOVEit DMZ has always been able to use remote databases, but this ability is rarely used. With the addition of support for Microsoft SQL Server in MOVEit DMZ version 6.0, the ability to access a remote database became even more important, as few customers would consider using a locally resident installation of SQL Server to provide database services for MOVEit DMZ, as is the default for MySQL installations. As a result, MOVEit DMZ's support for remote databases has been improved to make configuring DMZ to use a remote database much easier than before. Simply open the Database tab on the *Configuration Utility* (on page 135) to view and edit database access settings.

Remote Filesystem Support

In version 6.0, MOVEit DMZ gained the ability to store only its encrypted file store on a remote server, leaving the rest of the files local on the DMZ server. Additionally, its access to the remote files store is gained by mounting the remote share internally using a provided username and password, making configuration of DMZ to use a remote file store much easier than before. Simply open the Paths tab on the *Configuration Utility* (on page 135) to view and edit file store location and authentication settings.

High Availability Service

The MOVEit DMZ High Availability Service (MOVEitDMZHA) is responsible for updating an application node's status information while it is active, and for keeping the application nodes' settings, shared files (such as logo images and CSS stylesheets), and SSL certificates synchronized. Additionally, it is responsible for shutting down the MOVEit DMZ services if it detects a loss in connectivity to either the database or the file store. While installed during a normal MOVEit DMZ installation, the service is only configured and started when a node is added to a web farm.

If Windows Network Load Balancing is used as the load balancer for the web farm, the High Availability service will stop the NLB service on its associated application node when a loss in connectivity is detected, and will restart the NLB service when the connectivity problem is resolved. This prevents connections from being routed to a node that is currently not active.

Error Notification

If the High Availability service detects a connectivity issue, in addition to shutting down the MOVEit DMZ services, it will send an email notification to the currently configured "Send Errors To" email address for the system. The message includes information about which server is encountering the error, what error was detected, and what steps the High Availability service has taken as a result of the error. If the error conditions change, additional messages will be sent to keep administrators updated about the state of the ongoing errors on the node. Finally, if connectivity is re-established, in addition to restarting the MOVEit DMZ services, an email notification will be sent informing administrators of this fact.

Web Farms - Installation - Prerequisites

Before creating a MOVEit DMZ web farm, you must have the following:

- Two or more MOVEit DMZ application servers which will house the application nodes of the web farm.
- A database server that is remote from the application nodes. You need to use Microsoft SQL Server as the database application.
- A fileserver (NAS) that is remote from the application nodes. For smaller installations, this may be combined with the database server, but for best performance they should be separate.
- A network load balancer deployed between the application nodes and the clients who will be accessing the MOVEit DMZ application (typically the internet).
- MOVEit DMZ installation software, and the MOVEit DMZ Web Farm Conversion Assistant utility.
- A MOVEit DMZ license that authorizes the use of the number of application nodes to be used.

Web Farms - Installation - Pre-Installation Steps

The following steps should be performed before creating a web farm:

- 1** Make sure each node and the NAS have Windows networking access to each other.
Normally, this means making sure that TCP port 445 is open between all machines if a firewall or router is used in between any of the MOVEit DMZ nodes or the MOVEit DMZ nodes and the NAS.
- 2** Create a shared directory and a user with full access to it on the NAS.
This NAS account must be granted FULL access to the shared folder. The NAS account you create or select MUST be a member of the Local Administrators group on the MOVEit DMZ server. For more information about configuring the NAS, see the **Remote Filesystem** (on page 790) doc page.
- 3** Copy MOVEit DMZ database to the database server if necessary.

If the MOVEit DMZ database is not already present on the web farm database server, it must be copied there before creating a web farm. If you are electing to migrate to a remote SQL Server database from a local MySQL database in addition to creating a web farm, perform that migration at this time. Please see our ***knowledge base article***

(http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ) on converting MOVEit DMZ to SQL Server for more information.

Web Farms - Installation - Installation Steps

The following steps should be performed to create a MOVEit DMZ web farm:

Install MOVEit DMZ on node 1 if necessary

If an existing MOVEit DMZ server is not being used, install MOVEit DMZ on one of the nodes now. This will be node 1 of the web farm, and the web farm will take its initial settings from this node.

If the MOVEit DMZ database has not been migrated to the web farm database server, do this now. Note that you cannot use localhost as the database for a web farm. Use the MOVEit DMZ SQL Server Conversion Assistant to help migrate a local MySQL database to a remote SQL Server database server.

Please see the *knowledge base article*

(http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ) on converting MOVEit DMZ to SQL Server for more information.

Finally, before continuing with the web farm installation process, perform a full backup of the first MOVEit DMZ server to assist with recovery if necessary later.

Install MOVEit DMZ on remaining application nodes

Install MOVEit DMZ on the remaining application nodes at this time. Order does not matter. If a MOVEitDMZ_Install.INI file is available from a previous DMZ install, copy it to the root of the C: drive before running the installation program to use those settings. Otherwise, try to use the same settings during the install process as were used on the first DMZ server.

Run MOVEit DMZ Web Farm Conversion Assistant on node 1

- 1 Select "Create new webfarm" to have the utility create a new web farm based on this MOVEit DMZ server. Click Next to continue.
- 2 Enter (or confirm) database settings. The utility will attempt to populate the fields with the current database settings of the DMZ server. Most of the time these will be correct, and you can continue by clicking Next. (You need to use a Microsoft SQL Server database).

- 3 Enter files share settings. Enter the full UNC path to the web farm files share, as well as the user and password that will be used to access it. If the MOVEit DMZ files directory content has not already been copied to the web farm files share, click the provided checkbox to have the utility copy the files itself. Click Next to continue.
- 4 Click the Save web farm settings file checkbox and enter a path for the settings file. This will allow subsequently added web farm nodes to be installed very easily, and helps prevent mistyping settings during configuration that could cause problems. You may choose not to do this step, but it is highly recommended. Click Next to continue.
- 5 Confirm the displayed settings, or fix any displayed problems. Once all settings are confirmed, click Next to begin the web farm creation process.

At this point, the conversion assistant will:

- Stop the MOVEit DMZ services
- Create and initialize the web farm settings
- Copy the MOVEit DMZ server's registry settings, custom logo, color scheme, and template files, and SSL certificates to the auditing mechanism
- Copy the files directory contents to the files share if necessary
- Configure the MOVEit DMZ High Availability server for web farm operation
- Restart the MOVEit DMZ services

If any errors occurred, see the log file indicated on the final page of the utility for details.

If you elected to save the web farm settings to a file, copy the resulting file to the other nodes that will be added, and to a safe location internally for storage.

Run MOVEit DMZ Web Farm Conversion Assistant on remaining application nodes

- 1 Select "Add to existing webfarm" to have the utility add the node to the web farm created above. If the previously saved settings file is available, select "Load settings from INI file" and enter the location of the file. Click Next to continue.
- 2 Enter database and files share settings, if necessary. This step will be skipped if a valid settings file was loaded in the previous step.
- 3 Confirm the displayed settings, or fix any displayed problems. Once all settings are confirmed, click Next to begin adding the node to the existing web farm.

At this point, the conversion assistant will:

- Stop the MOVEit DMZ services
- Configure the server to use the existing web farm settings
- Load the registry settings, custom logo, color scheme, and template files, and SSL certificates stored during the web farm creation
- Configure the MOVEit DMZ High Availability server for web farm operation
- Restart the MOVEit DMZ services

If any errors occurred, see the log file indicated on the final page of the utility for details.

Update the MOVEit DMZ App Pools in IIS

You must update the App Pools that MOVEit DMZ uses ("moveitdmz ISAPI Pool" and "moveitdmz Pool") to run as the same user that MOVEit DMZ uses to connect to the external file storage location (NAS). This user should also be a member of the Local Administrators group on the MOVEit DMZ Server.

The reason for this is that, if the connection to the external file store fails, Windows will attempt to reconnect using the credentials of the App Pool. Therefore, if the App Pool user does not have permission to access the NAS, MOVEit DMZ will not be able to access the file system.

Test each application node

The best way to test each node is to run the MOVEit DMZ Check utility on each node. Remember that all nodes will now be using the user accounts from the first node.

Web Farms - Software Upgrade

This procedure describes how to upgrade a MOVEit DMZ web farm from one version of the software to another. (All nodes in the system must be upgraded at once; different nodes cannot run different versions of MOVEit DMZ.)

- 1** Using the MOVEit DMZ Configuration Utility, stop the services on each of the MOVEit DMZ web farm nodes. All the services must be down to prevent interlock problems when updating software. (Shut down services on Node 1 LAST to prevent an accidental failover!) Also, after stopping all services, be sure to close the "DMZ Config" program on all nodes before installing any software; if this program is not closed, your installations may require you to reboot the server.

- 2 Run the standard MOVEit DMZ software update program on the lowest node number (presumably, node 1). Answer Yes to "Do you want to perform the database upgrade?" Do NOT run the InstallChecker after updating the software; wait until all the nodes are updated. If you do run the InstallChecker, it may work normally for node 1, but will definitely fail on other nodes.
- 3 Using the MOVEit DMZ Configuration Utility, stop the services on web farm node 1.
- 4 Run the standard MOVEit DMZ software update program on the remainder of the nodes. Answer No to "Do you want to perform the database upgrade?" Do NOT run the InstallChecker after updating the software; wait until all the nodes are updated. If you do run the InstallChecker, expect to see a "Database down" error and know that none of file transfer tests will work.
- 5 After you have finished updating all web farm nodes with the latest version of both MOVEit DMZ, go back to web farm node 1 and use the MOVEit DMZ Configuration Utility to start the services. Then go to the remaining web farm nodes, and use the MOVEit DMZ Configuration Utility to start the services.
- 6 After these services are running, it is now safe to run the MOVEit InstallChecker on any node; normal results are to be expected on any node which runs the InstallChecker.

Upgrade operations are written to the "C:\MOVEitDMZWebfarm_Install.log" file.

Windows Updates

There are two ways to apply non-MOVEit software upgrades, such as Windows patches, to a MOVEit DMZ web farm. Choosing which procedure to follow depends on how much downtime you are willing to accept, as well as how many patches and updates need to be applied.

Procedure 1

This procedure should be used if there are is only a small number of updates to apply, and all can be applied with only a single reboot. It minimizes the amount of downtime the web farm will encounter, but also limits the number and complexity of the updates that can be applied.

- 1 Run DMZCheck on a node to get a baseline status of the web farm setup.
- 2 Leave all nodes running. Apply updates to the node(s) and reboot. Reboot each node, if required.
- 3 Once all nodes have been updated, use the DMZ Config program to check that the web farm setup is back up.
- 4 Run DMZCheck on the same node and compare the result to the baseline status.

Procedure 2

This procedure should be used if there are a large number of updates to apply, or if most updates require a reboot before applying other updates (for example, one of the updates is a service pack). This procedure requires more downtime, as the web farm will need to be completely unavailable between the time the procedure is started, and it is complete. However, it allows much more flexibility in the numbers and types of updates that can be applied.

- 1** Run DMZCheck on a node to get a baseline status of the web farm setup.
- 2** Stop the HA services on all nodes by running the MOVEit DMZ Config program, switching to the High Availability tab, clicking the Advanced button, and then clicking the Stop button for the HA Service entry in the Services section. Answer Yes when asked to stop the other services as well.
- 3** Using the Windows Services manager, set the Startup Type for the HA services to Disabled on all nodes. This will prevent the services from attempting to start after reboots.
- 4** Apply all updates to all servers. The HA services will stay down during multiple reboots.
- 5** Once all nodes have been updated and have booted, set the Startup Type for the HA services on the master node to Automatic, and start both services.
- 6** Once all nodes have been updated, use the DMZ Config program to check that the web farm setup is back up.
- 7** Run DMZCheck on the same node and compare the result to the baseline status.

Advanced Topics

This section contains advanced information on technical aspects of MOVEit.

AS2 and AS3

In most situations MOVEit Central version 4 or greater is required to perform AS2 or AS3 file transfers. (MOVEit Central also supports AS1.) However, MOVEit DMZ version 4 or greater is also required to act as an AS2 server in these situations, and MOVEit DMZ (any version) a good choice for an AS3 server as well.

For a complete discussion of AS1, AS2 and AS3 and the specific ways the MOVEit family supports these protocols, please see the MOVEit Central documentation.

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 URL and File Specifics

MOVEit DMZ receives AS2 messages and asynchronous AS2 MDNs through 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.

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.

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 of 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 still be used to quickly 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.

User Forms

The documents referenced below are templates to be used by operations staff when designing their own access request forms and instructions to end users. All documents are in Rich Text Format (RTF) format, so they can be used directly in any word processor such as Microsoft Word, StarOffice, PerfectOffice or even Windows WordPad.

You may need to add corporate logos, licensing language, legalese and other sections to complete your documents, but these templates are intended to highlight the information most administrators/operators and end users need to exchange when setting up a new client to perform file transfer with MOVEit DMZ.

Access Request Form

Access Request Form

(http://docs.ipswitch.com/MOVEit/DMZUserForms/MOVEitDMZ_AdvancedTopics_UserForms_AccessRequest.rtf) - Asks the user for basic information like preferred client, expected IP address and other information. (It is unlikely that any organization will provide as many choices as are available on this form, but that is what the delete key is for.)

Instructions by Protocol

Instructions for FTP over SSL Clients

(http://docs.ipswitch.com/MOVEit/DMZUserForms/MOVEitDMZ_AdvancedTopics_UserForms_FTP_Client_Intro.rtf) - Template to tell the user what client(s) to use to connect, which IP address/username/password and other information to use and additional information about the expected behavior of the transfer.

Instructions for FTP over SSH Clients

(http://docs.ipswitch.com/MOVEit/DMZUserForms/MOVEitDMZ_AdvancedTopics_UserForms_SSH_Client_Intro.rtf) - Similar to previous, but for FTP over SSH.

Instructions for HTTPS Clients - Similar to previous, but for HTTPS.

Database - Schema

A partial MOVEit DMZ database schema is listed below. This schema will be helpful if you are writing your own custom reports against MOVEit DMZ log records.

```
log (  
    ID bigint(20) NOT NULL auto_increment,  
    LogTime datetime default NULL,  
    Action varchar(16) default NULL,  
    InstID int(11) NOT NULL default '0',  
    Username varchar(128) default NULL,  
    TargetID varchar(128) NOT NULL default '',  
    TargetName varchar(128) NOT NULL default '',  
    FolderID int(11) NOT NULL default '0',  
    FileID varchar(12) default NULL,  
    IPAddress varchar(16) default NULL,  
    Error int(11) NOT NULL default '0',  
    Parm1 varchar(4096) default NULL,  
    Parm2 varchar(4096) default NULL,  
    Parm3 varchar(4096) default NULL,  
    Parm4 varchar(4096) default NULL,  
    Message text,  
    AgentBrand varchar(1024) default NULL,  
    AgentVersion varchar(16) default NULL,  
    XferSize double default '0',  
    Duration double NOT NULL default '0',  
    FileName varchar(1024) default NULL,  
    FolderPath varchar(4096) default NULL,
```



```

ResilNode tinyint(4) NOT NULL default '0',
Cert text,
Hash varchar(40) default NULL,
VirtualFolderID int(11) NOT NULL default '0',
VirtualFolderPath varchar(4096) default NULL
)

```

HINT: To see a quick list of different actions and error codes in YOUR log, either run this query from a database query tool:

```
SELECT Action,Error,Count(*) FROM log GROUP BY Action,Error;
```

...or run a custom report with these values:

Fields: Action,Error,Count()*

Tables: log

Group By: Action,Error

Sample output:

<i>Action</i>	<i>Error</i>	<i>Count(*)</i>
<i>sec_signoff</i>	<i>0</i>	<i>317</i>
<i>sec_signon</i>	<i>0</i>	<i>582</i>
<i>sec_signon</i>	<i>2025</i>	<i>72</i>

```

activesessions (
    Username varchar(128) NOT NULL default '',
    RealName varchar(64) default NULL,
    InstID int(11) NOT NULL default '0',
    IPAddress varchar(16) default NULL,
    LastTouch datetime default NULL,

```

```
SessionID varchar(32) default NULL,  
DMZInterface int(11) NOT NULL default '0',  
ResilNode int(11) NOT NULL default '0'  
)
```

```
files (  
    ID varchar(12) NOT NULL default '',  
    InstID int(11) NOT NULL default '0',  
    FolderID int(11) NOT NULL default '0',  
    FileSize double NOT NULL default '0',  
    OriginalFileTypeID int(11) NOT NULL default '0',  
    UploadStamp datetime default NULL,  
    UploadUsername varchar(128) NOT NULL default '',  
    UploadComment text,  
    UploadIP text,  
    UploadAgentBrand varchar(24) default NULL,  
    UploadAgentVersion varchar(8) default NULL,  
    DownloadCount int(11) NOT NULL default '0',  
    MaxDownloads int(11) NOT NULL default '1',  
    OriginalFilename text,  
    Deleted int(11) NOT NULL default '0',  
    Thumbnail int(11) NOT NULL default '0',  
    UploadIntegrity int(11) NOT NULL default '0',  
    ParentID varchar(12) NOT NULL default '0',  
    Recipients text,  
    Name text,
```

```
DeliveryRcpt int(11) NOT NULL default '0',
Attachments text,
ReadStatus int(11) NOT NULL default '0'
)
```

folders (

```
ID int(11) NOT NULL default '0',
InstID int(11) NOT NULL default '0',
Name text,
Owner varchar(128) NOT NULL default '',
Description text,
ResponsePath text,
SystemType int(11) NOT NULL default '0',
FolderType int(11) NOT NULL default '0',
FileType int(11) NOT NULL default '0',
CleanType int(11) NOT NULL default '0',
CleanTime int(11) NOT NULL default '30',
SenderReminderType int(11) NOT NULL default '0',
SenderReminderTime int(11) NOT NULL default '60',
SenderReminderLastDoneStamp datetime default NULL,
RecipientReminderType int(11) NOT NULL default '3',
RecipientReminderTime int(11) NOT NULL default '15',
RecipientReminderLastDoneStamp datetime default NULL,
Deleted int(11) NOT NULL default '0',
ResponseType int(11) NOT NULL default '1',
ResponseText text,
```

```
ResponseTime int(11) NOT NULL default '10',
NewTime int(11) NOT NULL default '7',
HideHistory int(11) NOT NULL default '1',
Thumbnails int(11) NOT NULL default '0',
ParentID int(11) NOT NULL default '0',
ParentInheritRights int(11) NOT NULL default '1',
PostUploadNotificationType int(11) NOT NULL default '0',
EnforceUniqueFilenames int(11) NOT NULL default '0',
FolderPath text,
Quota double NOT NULL default '0',
CreateStamp datetime default NULL,
AllowFileOverwrite int(11) NOT NULL default '0',
FileMasks text,
FileMaskRule int(11) NOT NULL default '0',
SubfolderCleanTime int(11) NOT NULL default '0',
ResponseSubject varchar(255) NOT NULL default '',
LastChangeStamp datetime default NULL,
NoDownloadNotificationType int(11) NOT NULL default '0',
NoDownloadNotificationTime int(11) NOT NULL default '30'
)
```

```
folderuser (
  ID int(11) NOT NULL auto_increment,
  Username varchar(128) default NULL,
  GroupID int(11) NOT NULL default '0',
  FolderID int(11) NOT NULL default '0',
```

```
Relationship int(11) NOT NULL default '0',  
InstID int(11) NOT NULL default '0',  
OverrideFlag int(11) NOT NULL default '0'  
)
```

```
groups (  
  ID int(11) NOT NULL auto_increment,  
  InstID int(11) NOT NULL default '0',  
  Name varchar(128) default NULL,  
  Description text,  
  MaxMemberQuota double NOT NULL default '0',  
  CanCreateTempUsers int(11) NOT NULL default '0',  
  AdminFolderAccess int(11) NOT NULL default '0',  
  DisplayProfile int(11) NOT NULL default '-1',  
  AllowAttachments int(11) NOT NULL default '0',  
  MaxMaxAttchSize double NOT NULL default '0',  
  AdminTempUserAccess int(11) NOT NULL default '1',  
  TempUsersInAddrBookExpansion int(11) NOT NULL default '0',  
  AdminMemberAccess int(11) NOT NULL default '1',  
  AdminMembershipAccess int(11) NOT NULL default '0',  
  AdminMemberPasswordAccess int(11) NOT NULL default '1',  
)
```

```
groupuser (  
  ID int(11) NOT NULL auto_increment,  
  InstID int(11) NOT NULL default '0',
```

```
    GroupID int(11) NOT NULL default '0',  
    Username varchar(128) default NULL,  
    Relationship int(11) NOT NULL default '0'  
)
```

```
msgposts (  
    ID int(11) NOT NULL auto_increment,  
    InstID int(11) NOT NULL default '0',  
    FileID varchar(12) NOT NULL default '0',  
    FileTypeID int(11) NOT NULL default '0',  
    FileSize double NOT NULL default '0',  
    UploadStamp datetime default NULL,  
    UploadUsername varchar(128) NOT NULL default ''  
)
```

```
newfiles (  
    FileID varchar(12) NOT NULL default '0',  
    FolderID int(11) NOT NULL default '0',  
    Username varchar(128) NOT NULL default '',  
    InstID int(11) NOT NULL default '0'  
)
```

NOTE: The users table schema has changed recently to include the LoginName field. Custom reports, or other processes using the users table and listing out usernames should now use LoginName instead of Username.

```
users (  

```

```
Username varchar(128) NOT NULL default '',
LoginName varchar(128) NOT NULL default '',
InstID int(11) NOT NULL default '0',
RealName varchar(128) default NULL,
Password varchar(32) default NULL,
Email text,
Notes text,
LastLoginStamp datetime default NULL,
PasswordChangeStamp datetime default NULL,
Permission int(11) NOT NULL default '0',
Deleted int(11) NOT NULL default '0',
Status varchar(16) NOT NULL default 'active',
StatusNote text,
PassHistory text,
UseCustomHostPermits int(11) NOT NULL default '0',
MustChangePassword int(11) NOT NULL default '0',
ExemptFromPasswordAging int(11) NOT NULL default '0',
ReceivesNotification int(11) NOT NULL default '1',
CreateStamp datetime default NULL,
ExpireStamp datetime default NULL,
AuthMethod int(11) NOT NULL default '0',
LastChangeStamp datetime default NULL,
Quota double NOT NULL default '0',
DefaultFolder int(11) NOT NULL default '0',
TempPassword varchar(80) NOT NULL default '',
UserListLength int(11) NOT NULL default '10',
CanCreateTempUsers int(11) NOT NULL default '2',
```

```
FileListLength int(11) NOT NULL default '100',
MessagingSignature varchar(255) default '',
CreateUsername varchar(128) default '',
DenyMultiSignons int(11) NOT NULL default '0',
AllowAttachments int(11) NOT NULL default '2',
MaxAttchSize double NOT NULL default '0',
LangUser varchar(12) NOT NULL default 'en',
EmailFormat int(11) NOT NULL default '1',
AuthSourceID int(11) NOT NULL default '0',
FTPCertRequired int(11) NOT NULL default '0',
FTPCertPlusPW int(11) NOT NULL default '1',
SSHCertRequired int(11) NOT NULL default '0',
SSHCertPlusPW int(11) NOT NULL default '0',
AllowedInterfaces int(11) NOT NULL default '31',
ExpirationPolicy int(11) NOT NULL default '0',
DefaultMsgDelivRcpt int(11) NOT NULL default '0',
ChrootDefaultFolder int(11) NOT NULL default '0',
)
```

```
certinfo (
```

```
    ID int(11) NOT NULL default '0',
    Username varchar(128) default NULL,
    InstID int(11) NOT NULL default '0',
    CertType int(11) NOT NULL default '0',
    DataType int(11) NOT NULL default '0',
    Timestamp datetime default NULL,
```


CertData text

)

sysstats - see also **Scheduled Tasks - SysStat** (on page 754) - (

ID bigint(20) NOT NULL auto_increment,
StatTime datetime default NULL,
FilesDriveRootPath varchar(128) NOT NULL default '',
FilesDriveSpaceFree double NOT NULL default '0',
FilesDriveSpaceUsed double NOT NULL default '0',
FilesSpaceUsed double NOT NULL default '0',
DBDriveRootPath varchar(128) NOT NULL default '',
DBDriveSpaceFree double NOT NULL default '0',
DBDriveSpaceUsed double NOT NULL default '0',
DBSpaceUsed double NOT NULL default '0',
LogsDriveRootPath varchar(128) NOT NULL default '',
LogsDriveSpaceFree double NOT NULL default '0',
LogsDriveSpaceUsed double NOT NULL default '0',
LogsSpaceUsed double NOT NULL default '0',
FilesTotalDB int(10) NOT NULL default '0',
FileSizeTotalDB double NOT NULL default '0',
CPUUsagePercentTotal tinyint(3) NOT NULL default '0',
CPUUsagePercentDMZ tinyint(3) NOT NULL default '0',
CPUUsagePercentISAPI tinyint(3) NOT NULL default '0',
CPUUsagePercentIIS tinyint(3) NOT NULL default '0',
CPUUsagePercentDB tinyint(3) NOT NULL default '0',
CPUUsagePercentDMZFTP tinyint(3) NOT NULL default '0',

CPUUsagePercentDMZSSH tinyint(3) NOT NULL default '0',
CPUUsagePercentSched tinyint(3) NOT NULL default '0',
CPUUsagePercentCentral tinyint(3) NOT NULL default '0',
CPUUsagePercentResil tinyint(3) NOT NULL default '0',
MemUsedTotal double NOT NULL default '0',
MemFreeTotal double NOT NULL default '0',
MemUsedDMZ double NOT NULL default '0',
MemUsedISAPI double NOT NULL default '0',
MemUsedIIS double NOT NULL default '0',
MemUsedDB double NOT NULL default '0',
MemUsedDMZFTP double NOT NULL default '0',
MemUsedDMZSSH double NOT NULL default '0',
MemUsedSched double NOT NULL default '0',
MemUsedCentral double NOT NULL default '0',
MemUsedResil double NOT NULL default '0',
VMSizeDMZ double NOT NULL default '0',
VMSizeISAPI double NOT NULL default '0',
VMSizeIIS double NOT NULL default '0',
VMSizeDB double NOT NULL default '0',
VMSizeDMZFTP double NOT NULL default '0',
VMSizeDMZSSH double NOT NULL default '0',
VMSizeSched double NOT NULL default '0',
VMSizeCentral double NOT NULL default '0',
VMSizeResil double NOT NULL default '0',
HandlesTotal int(10) NOT NULL default '0',
HandlesDMZ int(10) NOT NULL default '0',
HandlesISAPI int(10) NOT NULL default '0',

```
HandlesIIS int(10) NOT NULL default '0',
HandlesDB int(10) NOT NULL default '0',
HandlesDMZFTP int(10) NOT NULL default '0',
HandlesDMZSSH int(10) NOT NULL default '0',
HandlesSched int(10) NOT NULL default '0',
HandlesCentral int(10) NOT NULL default '0',
HandlesResil int(10) NOT NULL default '0',
ProcessesTotal int(10) NOT NULL default '0',
ThreadsTotal int(10) NOT NULL default '0',
ThreadsDMZ int(10) NOT NULL default '0',
ThreadsISAPI int(10) NOT NULL default '0',
ThreadsIIS int(10) NOT NULL default '0',
ThreadsDB int(10) NOT NULL default '0',
ThreadsDMZFTP int(10) NOT NULL default '0',
ThreadsDMZSSH int(10) NOT NULL default '0',
ThreadsSched int(10) NOT NULL default '0',
ThreadsCentral int(10) NOT NULL default '0',
ThreadsResil int(10) NOT NULL default '0',
SessionsTotal int(10) NOT NULL default '0',
SessionsActive int(10) NOT NULL default '0',
ResilNode tinyint(3) NOT NULL default '0'
)
```

Note: In the above listing, ResilNode is the web farm node for the application doing the DB insert.

Note: In the above listing, the following were for recording information about programs used in the now-deprecated Resiliency service: CPUUsagePercentResil, MemUsedResil, VMSizeResil, HandlesResil, and ThreadsResil.

To see a full database schema, if you have selected MySQL as your database engine, issue this command with the appropriate credentials from the appropriate path using the Windows command line.

```
D:\MySQL\Bin>mysqldump --user=root --password=mypass -d moveitdmz >  
d:\temp\dbdump.txt
```

Database - Troubleshooting

MOVEit DMZ uses a database server to store information about everything from organization settings, to user account information, to folder and file information. Normally, this database operates silently, behind the scenes of MOVEit DMZ, and requires no active maintenance on the part of the administrator to operate.

Rarely, however, one or more database tables can become corrupted and will cause part of the MOVEit DMZ application to stop functioning. 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. (See also *Alternate Backup Suggestions* below.) 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 DMZ debug log. MOVEit DMZ accesses the database server several times during a typical session, and when serious database problems occur, they are always logged to the debug log. For more information about debug logs, see the **Debug Logs** (on page 527) manual page. Here are some examples of table corruption errors that would be found in the debug log:

```
[TCX][MyODBC]Can't open file: 'folderperms.MYD'. (errno: 145)
```

```
[TCX][MyODBC]Got error 134 from table handler
```

The problems that can be encountered with databases are sometimes specific to the brand of database engine in use. Most of the suggestions here apply when MySQL is being used as the database engine.

Automatic Repair - MySQL

Recent versions of MOVEit DMZ have enabled a MySQL 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 DMZ 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
./moveitdmz/folderperms
```

```
041122 1:14:00 read_const: Got error 134 when reading table
./moveitdmz/folderperms
```

```
041122 1:41:46 Warning: Checking table: './moveitdmz/folderperms'
```

041122 1:41:46 Warning: Recovering table: './moveitdmz/folderperms'

Manual Repair - MySQL

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 any MOVEit DMZ services during the manual repair process. (For the purposes of this discussion MOVEit DMZ services include FTP, SSH, IIS, Windows Scheduler, MySQL and SysStat.) 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 DMZ system and log in to the MySQL server using the root account created during the DMZ 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 moveitdmz
```

Once logged in, execute the CHECK TABLE command against the table you believe has been corrupted, like so:

```
CHECK TABLE folderperms;
```

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 folderperms;
```

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 for assistance.

Alternate Backup Suggestions

Many backup programs (Veritas, for example) often corrupt open database or configuration files; this behavior is somewhat platform-specific. To avoid these problems, try one or both of these field-tested suggestions:

- Use a scheduled batch file to **COPY** the database files to a stage location. Tell the backup to ignore the actual database files and backup the (closed) stage files instead. To perform the backup copy, please consider using the (tested and documented) mysql_backup.bat available from the MOVEit / DMZ / Extras folder on the MOVEit DMZ support server.
- Use the **MOVEit DMZ Backup utility** (on page 150) to make a full copy of the database. Tell the backup to ignore the actual database files and backup the (closed) MOVEit DMZ backup file instead.

Additional Help

For additional help, you may want to consult the Knowledge Base on our support site at

http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ

(http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ).

Database - Remote Access

Secure, Remote Read-Only Access Using MOVEit DMZ API

The easiest and most secure way to pull information out of the MOVEit DMZ configuration and audit database remotely is to use MOVEit DMZ API's "ReportRunCustom()" method and custom queries. This method requires users to authenticate with MOVEit DMZ credentials, protects data in transit with SSL and is firewall friendly because it uses HTTPS on port 443.

For example, to get a list of at most 5 users whose full names start with A in XML format, you could use the following VB code with MOVEit DMZ API.

```
Dim boolOK as Boolean = false

Dim fields as String = "Username,RealName,Email,Notes"

Dim tables as String = "users"

Dim criteria as String = "RealName LIKE 'A%'"

Dim groupings as String = ""

Dim order as String = "RealName"

Dim limit as String = "5"

Dim OutputFormat as String = "XML"

Dim LocalPath as String = "d:\reports\newest_5_A_users.xml"

boolOK = ReportRunCustom( fields, tables, criteria, groupings, order, limit,
OutputFormat, LocalPath )

IF boolOK then...
```

See **Web Interface - Reports - Custom Reports** (on page 341) and the MOVEit DMZ API documentation for more information. (You do not need to pre-configure custom reports on MOVEit DMZ to use them from MOVEit DMZ API, but the DMZ Custom Reports documentation contains a complete explanation of how each of the fields used in the API function call are used.)

If you desire read/write access to the database that cannot be achieved through MOVEit DMZ API, you may want to use a more complex solution that involves direct access to the database.

Establishing Secure, Remote Access to MOVEit DMZ's database

➤ *If Your Database Engine is MySQL*

To securely access the underlying MySQL database MOVEit DMZ uses to store its configuration and audit logs through a an ODBC connection, you must set up a user in the MySQL database and set up a secure channel using stunnel.

Remote access to the MOVEit DMZ database may also require the 3.51 version of the MySQL ODBC driver (MyODBC), available at no charge from MySQL (and installed by default with MOVEit DMZ and MOVEit Central). However, several other MySQL database drivers, including several non-ODBC drivers for .NET, have been tested as well.

These instructions will set up a secure MySQL port listening on TCP port 33062. Modify the necessary stunnel configuration file to change this value.

A complete set of instructions to do remote reporting using this tool (including stunnel CLIENT instructions) can be found in the MOVEit Central manual.

Set Up Read-Only Database User on MOVEit DMZ

In most cases you will want to set up a read-only user to access the MOVEit DMZ database. While certain tweaks of the database are allowed, unless you really know what you are doing it would be easy to wreck your configuration and/or run afoul of MOVEit DMZ's tamper-evident check feature. (This is essentially the same reason why other software vendors who store configurations in custom flat-file formats instead discourage people from hacking in with their favorite hex editors; yes, it's possible, but watch out!)

- 1 Open a command prompt on MOVEit DMZ.
- 2 CD into the Bin subfolder of your MySQL root folder. (e.g., D:\MySQL\Bin)
- 3 Run this command (using the appropriate root password):

```
D:\mysql\bin>mysql --user=root --password=31r00t0
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 19660
Server version: 5.0.44-classic-nt MySQL Enterprise Server - Classic
(Commercial)
```

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

- 4 Once at the `mysql>` command prompt, issue the following commands (substitute `micentral` and `m1c3ntra1` with the username and password you would like to use when connecting from your remote clients):

```
mysql> GRANT SELECT,CREATE TEMPORARY TABLES ON moveitdmz.* TO
'micentral'@'localhost' IDENTIFIED BY 'm1c3ntra1';
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> exit
Bye
```

- 5 Finally, test the permissions you just set up with the following commands (substitute appropriate credentials where necessary):

```
D:\mysql\bin>mysql --user=micentral --password=m1c3ntra1 moveitdmz
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 19660
Server version: 5.0.44-classic-nt MySQL Enterprise Server - Classic
(Commercial)
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql> select count(*) from users;
```

```
+-----+
| count(*) |
+-----+
|      42 |
+-----+
```

```
1 row in set (0.08 sec)
```

```
mysql> insert into log set ID=1;
ERROR 1044: Access denied for user: 'micentral@localhost' to database
'moveitdmz'
mysql> exit
Bye
```

Set Up STunnel Server on MOVEit DMZ

- 1 Open a command prompt on MOVEit DMZ.
- 2 CD into the Util subfolder of your MOVEit DMZ root folder. (e.g., D:\MOVEitDMZ\Util)
- 3 Run this command (and look for the following output):

```
D:\moveitdmz\Util>stunnel_makecert
D:\moveitdmz\Util>openssl genrsa -out stunnel_key.pem 2048
Loading 'screen' into random state - done
```

Generating RSA private key, 2048 bit long modulus

.....+++

....+++

e is 65537 (0x10001)

```
D:\moveit dmz\Util>openssl req -config stunnel_makecert_parms.txt -new
-x509 -key stunnel_key.pem -out stunnel_mysqlserver.pem -days
```

- 4 Run this command (there is no need to change the configuration on this server):

```
D:\moveitdmz\util>stunnel stunnel_mysqlserver.conf
```

- 5 If this command fails, you will see an error dialog box which says something like **Stunnel server is down due to an error...** and then a larger dialog box which contains details about the error. Whether or not this command succeeds, you will see a small STunnel icon (stunnel_icon.gif (904 bytes)) in your tray.
- 6 If all is well, you are ready to move to the next section. If there were problems, right-click on the STunnel icon and select **Exit**.

Set Up STunnel As a Service

After testing your new connection, run the following commands to install stunnel as a service (so it starts automatically).

- 1 Exit the stunnel application on both MOVEit DMZ and MOVEit Central.
- 2 On MOVEit DMZ, execute the following command to install the service (watch for **Created service** pop-up):

```
D:\moveitdmz\util>stunnel -install stunnel_mysqlserver.conf
```
- 3 On MOVEit DMZ, execute the following command to start the service:

```
D:\moveitdmz\util>net start stunnel
```

➤ *If Your Database Engine is Microsoft SQL Server*

If you have selected SQL Server as your database engine, you can securely access the data using standard Microsoft drivers, such as ADO and ADO.NET. To cause all communications between your program and Microsoft SQL Server to be encrypted, simply include the following in your connection string:

```
TrustServerCertificate=yes; Encrypt=yes;
```

Package - Archives

Once a package has been archived, it is no longer available to users on the system. However, administrators are free to download the archive file and extract it, giving them access to all the packages transferred through the organization within the archived time period. The archive file format is straightforward; administrators can easily write their own programs to split apart the archive and display the contents, or use the Package Archive Viewer provided by Ipswitch.

Archive Format

The archive file is merely a zip file containing all the package and attachment files for the archived period. Each file is named with the ID of that file from the system with no extension. The files are not encrypted, so they can be opened and read easily once extracted from the archive file.

The individual package files contain all the necessary information about each package in a simple XML format. An example archived package file is presented below:

```
<msgarchive>

<msg>

  <head>

    <address>

      <from>

        <type>user</type>

        <username>jsmith</username>

        <realname>John Smith</realname>

      </from>

      <to>

        <type>user</type>

        <username>helga</username>

        <realname>Helga Finlayson</realname>

      </to>

    </address>
```

```
<timestamp>6/10/2004 4:58:58 PM</timestamp>

<attachment>

  <id>3665038</id>

  <originalfilename>picture.jpg</originalfilename>

  <size>56621</size>

  <integrity>1</integrity>

</attachment>

<subject>Example Package</subject>

</head>

<body>

  <![CDATA[

    John,

    Here is a test message for you.

    --Helga

  ]]>

</body>

</msg>

<readstatus>10</readstatus>

<history>

</history>

</msgarchive>
```

The first section of the archived package file is the package itself, contained in the `msg` tags. The `head` section contains information about the sender, the recipients, the timestamp, the attachments, and the subject of the package. The `body` section contains the message itself inside CDATA tags, complete with any HTML formatting contained in the original package.

Next will be meta-information about the package from the system at the time it was archived. The `readstatus` element will contain the read status of the package when it was archived. The possible codes are 0 if no recipients have read the package, 5 if some recipients have read the package, and 10 if all recipients have read the package. Finally, any history items regarding the package will be provided in the `history` section.

Package Archive Viewer

To allow easy access to package archives, Ipswitch makes available a simple command-line application which parses the entries in an archive and generates HTML representations of the packages for easy viewing. This application can be found on the Ipswitch MOVEit DMZ file server, located at <http://www.myipswitch.com> (<http://www.myipswitch.com>). Look in the `\MOVEit\MOVEit DMZ\Extras` folder for the file named `MsgArchiveViewer.zip`. The program requires the Microsoft .NET Framework to run. To install, simply unzip the file into a directory, such as `C:\MsgArchiveViewer`.

The program operates on the unextracted individual package and attachment files, so the zipped archive files from the desired time period need to be downloaded from MOVEit DMZ and extracted into a directory, such as `C:\MsgArchiveViewer\Archives`. Next, choose an output directory, such as `C:\MsgArchiveViewer\Output`, where the program will write the message HTML files, the attachment files, and the package index file. Finally, execute the program with the `--inputpath` and `--outputpath` arguments set defining the location of the extracted archive files and the location of the output folder respectively:

```
msgarchiveviewer --inputpath=c:\msgarchiveviewer\archives  
--outputpath=c:\msgarchiveviewer\output
```

Paths with spaces in them can be used by surrounding the entire argument with quotes, like so:

```
msgarchiveviewer "--inputpath=c:\msg archives\input" "--outputpath=c:\msg  
archives\output"
```

If you want more information about what the program is doing, add the `--debug` option.

Once the program is done running, look in the output directory for a file named `index.html`. This is the package index file written by the program, and contains a complete list of the packages found in the input directory. Clicking on a package will show you the individual package itself. Sender, recipient, timestamp, and subject information are all included at the top of the package, and a list of attachments is included at the bottom. Clicking on an attachment link will direct you to the attachment file itself.

Packages - Spell-Check Dictionaries

Overview

MOVEit DMZ uses the **GNU Aspell** (<http://aspell.sourceforge.net/>) program as a back-end for its spell-checking services for packages. This program uses a flexible dictionary mechanism to determine whether words are misspelled or not, and is easily expandable. As an example, MOVEit DMZ comes with two custom-made additional dictionary files, including a 60,000-term medical dictionary, which are configured to be used by the Aspell back-end by default.

Creating custom dictionaries for use by Aspell is relatively easy to do. All that is required is creating a text file containing your word list, compiling that text file into an Aspell dictionary file, and finally telling Aspell to use that dictionary file.

Creating dictionary files and configuring Aspell to use them requires access to the Aspell program and data files, which are stored in the **Aspell** subdirectory of your MOVEit DMZ non-web directory (by default, D:\MOVEitDMZ) on your server.

Creating a Word List File

A custom dictionary starts with a text file containing a list of words. Each word should be on a separate line and the last line should be left blank. The wordlist file can be named anything and stored anywhere, however it is recommended you follow the examples included, which store the file as a **.wordlist** file in the **bin** subdirectory of the **Aspell** directory (e.g., D:\MOVEitDMZ\Aspell\bin\custom.wordlist). In the case of the examples, the wordlist files are called **medical.wordlist** and **sni.wordlist**.

Creating a Dictionary File

Once you have a custom wordlist file, the next step is to create a compiled dictionary file based on that wordlist file. To manually compile a dictionary file from your wordlist file, open a command-prompt and CD to the **bin** subdirectory of the **Aspell** directory. Then, execute the following command:

```
aspell --lang=en create master en-custom.rws < custom.wordlist
```

...being sure to use the correct name of your wordlist file as the final argument. Again, the dictionary file created by this process can be called anything, but for ease of maintenance, it is recommended you use a format similar to the examples - this means starting the filename with the language of your dictionary (typically **en** for English), followed by a dash and the name of your wordlist file, and ending with the extension of **.rws**.

If you plan on periodically making changes to your custom dictionary, it would be best to create a batch file to run the above compilation command. See the `build_en-medical.bat` and `build_en-sni.bat` examples.

Configuring Aspell to Use Your Dictionary

Once the dictionary file has been created, the final step is to configure Aspell to use that dictionary file when spell-checking input. Aspell stores its dictionary files in the `dict` subdirectory of the `Aspell` directory, so copy your `.rws` dictionary file there to begin.

To allow Aspell to use multiple dictionaries at once, it utilizes `.multi` files, which tell Aspell which dictionary files to use for which language. Each `.multi` file contains a list of commands, one on each line, which tell Aspell how to put together a complete list of words for spellchecking. The most used `.multi` files are the files `en.multi` and `en_US.multi`. Open these two files up in a text editor, and you will see that they are fairly similar (`en.multi` includes the `en_GB-only.rws` dictionary, which contains a British-English wordlist). You should also see commands to load the two included example dictionaries, `en-medical.rws` and `en-sni.rws`. To load your custom dictionary, add a similar `add` command with your dictionary file as the argument to both `.multi` files. Aspell should immediately begin using your custom dictionary when spell-checking input.

Service Integration - Anti-virus

The use of anti-virus products on both desktop and server computers tends to be an important part of a corporate information security policy. Since a MOVEit DMZ server is typically placed in a network segment that is exposed to the Internet, the use of a well-maintained anti-virus product on the server is generally recommended. However, there are a few points to keep in mind when setting up an anti-virus product on a server running MOVEit DMZ. This section is intended to provide MOVEit DMZ operators with information and recommended configurations regarding the use of anti-virus products on a MOVEit DMZ server.

Note: See *Feature Focus - Content Scanning - Anti-virus* (on page 97).

Uses and Limitations of Anti-virus

Since MOVEit DMZ is a secure file transfer and storage system, there are two main reasons why an operator would want to run anti-virus on the host server:

- 1 Protect the server itself from viruses that could reduce performance, compromise security, or even disable the system entirely.

- 2** Inspect the files being transferred through the system to ensure virus-infected files are not allowed into or out of the internal network.

Protecting the host server from virus infection is certainly important in making sure that the system runs reliably, and we recommend the installation and use of a suitable anti-virus program to do so. Inspecting the files being stored on and transferred through the MOVEit DMZ application, however, is not possible due to the security model of the application.

Anti-virus and the MOVEit Security Model

One of MOVEit DMZ's hallmark features is that it encrypts files before writing them out to disk. As a result, the unencrypted file data is never available on disk, and therefore never available to disk-checking anti-virus programs. For maximum security, most files are not even stored in memory in their entirety, but are instead read and written in smaller chunks. This makes most files unavailable to memory-checking anti-virus programs as well.

In addition to the fact that an anti-virus program should never be able to identify an actual virus in a MOVEit-DMZ-encrypted file, the nature of file encryption makes false positives a possibility as well. It is possible that the process of encrypting a file can generate inside that file a sequence of bytes that anti-virus programs may read as a virus signature. Therefore, it is recommended that anti-virus programs be configured to ignore the MOVEit DMZ encrypted file store entirely.

In order to verify that files transferred through a MOVEit DMZ server are virus-free, the best place to install anti-virus software is on an internal MOVEit Central or other platform where the complete, unencrypted files are placed for further processing. In fact, virus detection, quarantining, and/or cleaning actions performed by most realtime anti-virus packages will be logged in MOVEit Central's transaction log.

Recommendations

When installing and configuring an anti-virus program on a MOVEit DMZ server, there are a few points which should be kept in mind:

- Most MOVEit DMZ servers are placed in an isolated network segment, often called a DMZ (DeMilitarized Zone). Such servers tend to be independent from the rest of the network, and are usually not added as members of a Domain or Active Directory tree. For the same reasons, centrally-managed anti-virus programs tend to have a harder time accessing and maintaining installed instances on DMZ servers. Therefore, anti-virus programs are usually installed in independent or stand-alone mode on DMZ servers, and thus will require independent configuration, virus updating, and event checking.

-
- To avoid possible false positive virus matches, and to prevent an anti-virus program from quarantining or even deleting files from the MOVEit DMZ store, the anti-virus program should be configured to ignore the DMZ store location. Encrypted files are stored in the **Files** subdirectory of the MOVEit DMZ **non-web** directory (typically D:\MOVEitDMZ). Therefore, for a typical installation, the anti-virus program should be configured to ignore D:\MOVEitDMZ\Files.
 - It is also a good idea to configure the anti-virus program to ignore MOVEit DMZ's database files, since they could possibly contain binary data that might be interpreted as a virus signature (several fields in the database are stored encrypted). If your database is MySQL, data files are typically stored in the **Data** subdirectory of the MySQL installation directory (typically D:\MySQL). Therefore, for a typical installation, the anti-virus program should be configured to ignore D:\MySQL\Data. If your database is Microsoft SQL Server, the files are typically stored in a directory like: C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data.

Service Integration - CAC Integration

Overview

When enabled for external authentication, MOVEit DMZ can integrate into a Common Access Card (CAC) environment to allow users to access MOVEit DMZ without having to provide a username and password. The hardware certificate provided by the user's CAC Smart Card can be used to both identify and authenticate the user. This page details how to configure MOVEit DMZ to function properly in a CAC environment.

CAC Environments

CAC environments, particularly those used by the U.S. Department of Defense (DOD), typically use Smart Cards containing hardware-based SSL client certificates as identification and authentication mechanisms. User information is stored in a directory, typically Microsoft Active Directory. When a user inserts their Smart Card into a reader at a workstation and enters the proper PIN code, the hardware certificate is used to identify which user is logging on and authenticate them.

MOVEit DMZ can use the same hardware client certificate to determine the identity of the user who is trying to access the site, and match the certificate against the copy contained in the user's Active Directory account to verify the user's identity.

Configuring MOVEit DMZ for CAC Support

Integrating MOVEit DMZ with a CAC environment involves several steps. First, the CAC CA certificate must be trusted as a valid signing certificate on both the MOVEit DMZ server and in MOVEit DMZ itself. Next, a DMZ external authentication source must be configured for the directory, to allow user information and authentication to be controlled by that directory. Next, the Allow Username from Client Certificate option must be enabled in the org-level HTTP policy settings page. This allows MOVEit DMZ to identify an incoming user based solely on their provided client certificate. Finally, the external authentication source must be configured to read a value from the provided client certificate and match it against a value in the user directory. This allows DMZ to identify the user's information in the directory.

Ensure CA Certificate is Trusted

The CA certificate that user client certificates are signed with must be trusted by the Windows server that MOVEit DMZ is running on by chaining up to a certificate in the Microsoft Trusted Root Certificate Store. Users will not be allowed to access the MOVEit DMZ application unless the CA certificate that signed it is trusted.

The CA certificate must also be marked as a trusted CA in the MOVEit DMZ application itself. If the CA certificate is not trusted by MOVEit DMZ, users will not be allowed to sign on with their client certificates. See **System Configuration - SSL and SSH - SSL - Client Certs - Trusted CAs** (on page 235) for more information about trusting a CA certificate in MOVEit DMZ.

Configuring External Authentication Source

Initial configuration of the external authentication source will be similar to setting up any other LDAP source. CAC integration requires an LDAP Lookup+Authentication source as many different user properties are queried from the LDAP server. See **Security Policies - External Authentication - LDAP Lookup** (on page 454) for more information about configuring such a source.

In addition to the normal parameters, CAC integration requires the proper configuration of the Client Cert Field value. This is the name of the field in the LDAP directory which contains the client certificate data for the user. For Active Directory servers, this value is called `userCertificate`. Without this value, MOVEit DMZ will be unable to match the user's client certificate against their certificate in the directory, and will thus be unable to authenticate the user.

Configuring Username from Client Certificate Option

The Allow Username from Client Certificate option can be found on the **Settings - Security Policies - Interface - HTTP** page in the MOVEit DMZ web interface. This option allows DMZ to identify the user from their client certificate. See **Security Policies - Interface** (on page 482) for more information about this setting.

Normally, DMZ will be able to determine the user's identity by looking in its locally cached certificate store. If this is unsuccessful, such as if the user is new to the system, or their client certificate has recently been changed, DMZ will go out to the directory server configured in the external authentication source to look for a matching user record. This is where the following settings take effect.

Configuring User Matching via Client Certificate

When MOVEit DMZ needs to determine the user's identity from the directory server, the **Client Certificate Value** and **Matching LDAP Field** settings allow it to more easily search for the user's directory entry based on information in the provided client certificate. These options become available in the external authentication source once the org-level **Allow Username from Client Certificate** option is enabled. See **Security Policies - External Authentication - LDAP Lookup** (on page 454) for more information about these settings.

For CAC environments, typically the **Principal Name** value in the certificate's **Subject Alternative Name (SAN)** extension is used as the identifier when matching the certificate to a user entry in the directory server. For Active Directory servers, this value is matched to the `userPrincipalName` field.

User Interaction

Once CAC integration is configured, users will be able to access MOVEit DMZ without providing a username or password, as long as their hardware client certificate is available. First-time access to the DMZ site will still result in the signon page being displayed. However, with the **Allow Username from Client Certificate** option enabled, a link will be provided prompting the user to click if they have a client certificate and would like to automatically sign on. If this process is successful, a long-term cookie will be set on the user's browser which will instruct DMZ to automatically forward the user to the client certificate identification process in the future, so they shouldn't need to see the signon page again from that point on, unless their cookie gets removed or they access the site from a different computer.

NOTE: MOVEit DMZ can be configured to require passwords with client certificates when authenticating users. If this option is enabled at the organization level, or on a user-by-user basis, users may not be able to access the DMZ site without providing a username and password. Users who require passwords with client certificates will be returned to the signon page if they attempt an automatic signon with a message indicating that further credentials are required.

CAC Authentication Process

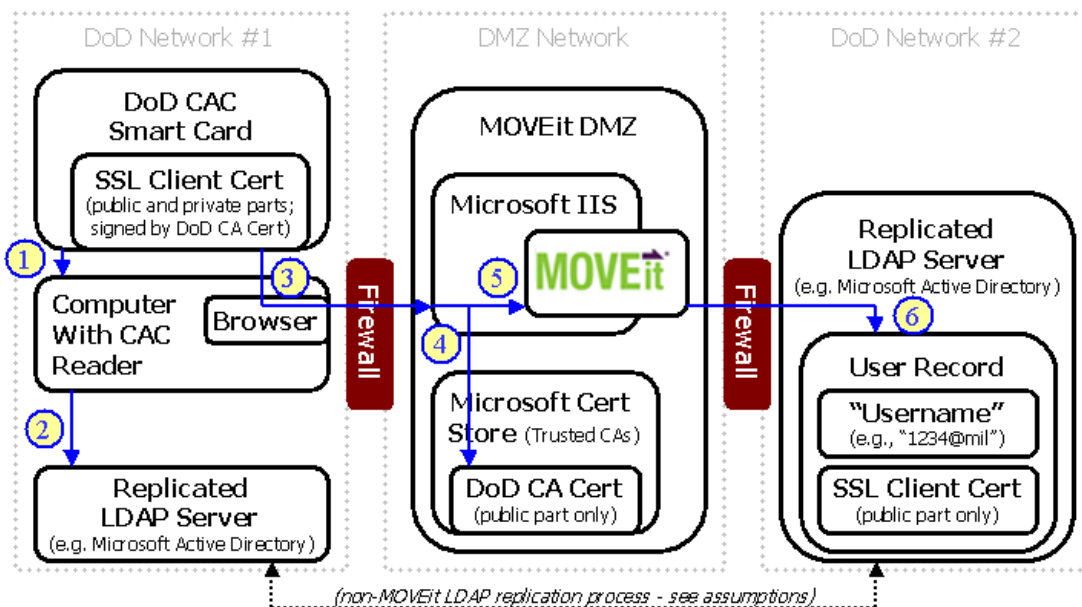
MOVEit DMZ CAC authentication assumes that either:

- The necessary user records are automatically replicated between LDAP servers on DoD Network #1 and DoD Network #2. (MOVEit products play no part in this replication.)
- or
- DoD Network #1 and DoD Network #2 are really the same network.

How browser-based CAC authentication works with MOVEit DMZ:

- 1** DoD user presents their CAC on a computer with a CAC reader and enters a PIN or other credentials.
- 2** If CAC authentication succeeds, the computer looks up necessary account information from its domain controller (e.g., Microsoft Active Directory server) and allows the DoD user to access the computer system.
- 3** When the DoD user opens a web browser session from this computer, the DoD CA-signed SSL client certificate stored on the CAC will be used to authenticate to any web servers that require client certificate authentication. This certificate (and its private key) will also be used to encrypt SSL communications in these cases.

- 4 When the DoD user opens a web browser session from this computer to a MOVEit DMZ system, the related SSL connection will terminate in Microsoft IIS server. Microsoft IIS will only permit this SSL connection if the public part of the DoD CA certificate that signed the CAC client cert is installed in the Trusted CA section of the Microsoft Certificate Store on the MOVEit DMZ server.
- 5 If IIS permits the SSL connection, the MOVEit DMZ software will display a sign on page, offer a link for CAC authentication or automatically authenticate the DoD user.
- 6 If CAC authentication is chosen or used (i.e., no separate username is provided on the MOVEit DMZ sign on page), MOVEit DMZ will look up a valid user on its back end LDAP server using attributes of the CAC client certificate. If a matching user record is found and the public SSL client certificate stored in the LDAP record matches the CAC client certificate, the DoD user will be allowed on to the MOVEit DMZ system.



Service Integration - Local Mail Relay

Overview

You should consider using Windows Server's IIS SMTP server as a local mail relay on your MOVEit DMZ system if any of the following conditions apply.

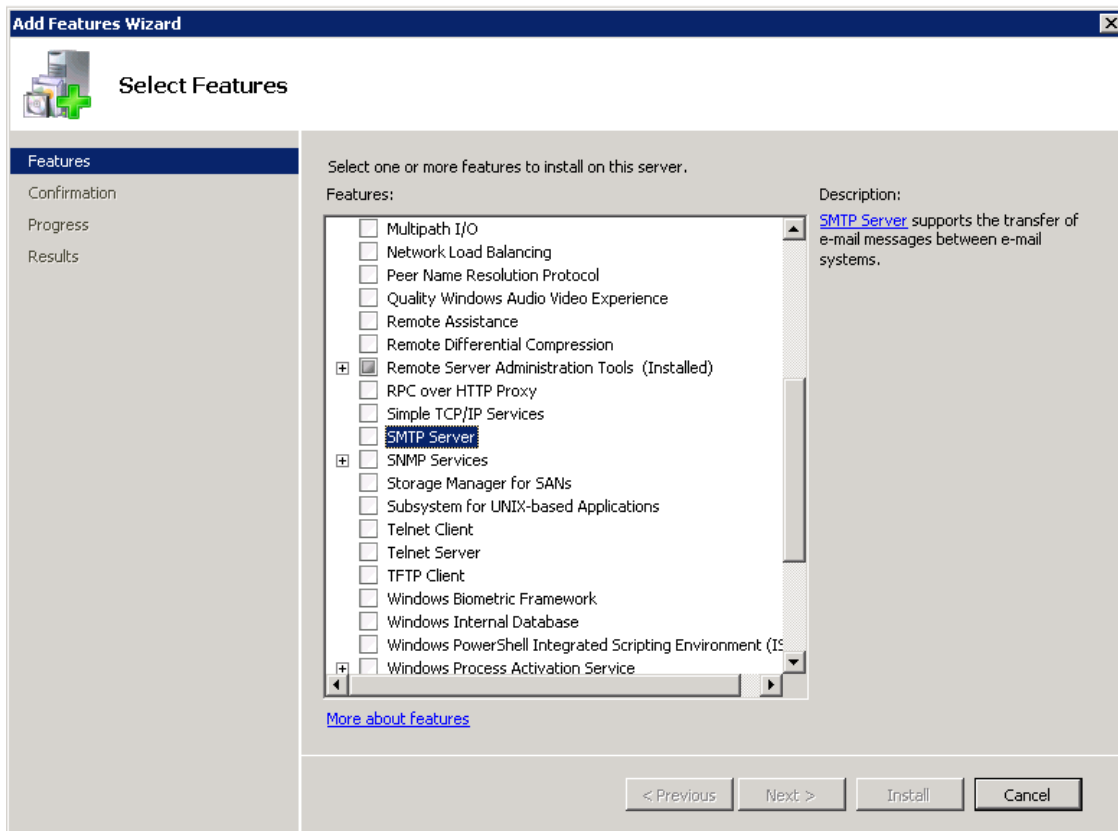
- Uploads are taking much longer than expected
- You have a slow or busy mail server
- You may be sending 20 or more email notifications out for a single upload
- Your mail server requires an advanced method of authentication for relaying mail
- Your MOVEit DMZ server has more than 100 users (this is generally the reason we recommend sites of any size set their email server to `localhost`)

MOVEit DMZ sends out new file notifications and upload confirmations immediately after saving the related file to disk. While this approach affords near real time response, it also forces MOVEit DMZ to wait for each message to be sent before another can be attempted. When MOVEit DMZ is dealing with busy mail servers or a lot of recipients, the upload process will spend more time sending email than saving files. To keep MOVEit DMZ from having to wait up to 10 seconds for each message to be sent, we can instead spool these messages to the local SMTP server, which will then spool these mail messages out to real email servers when they are better able to accept the traffic.

If a local mail relay server is configured, DMZ can use this to queue up outgoing mail instead of going directly to the main mail server. This frees DMZ up to move on to other tasks, and can provide a noticeable improvement in responsiveness for most file transfer operations.

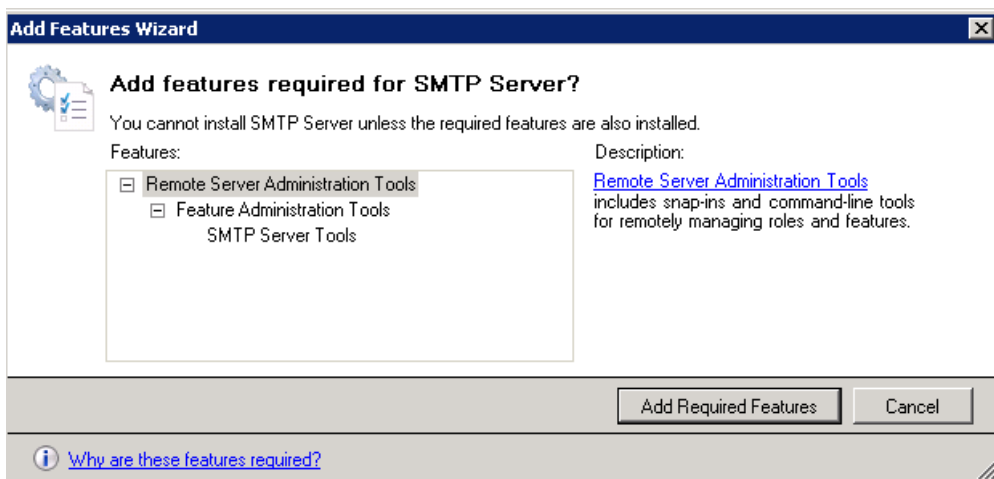
Instructions

- 1 Ensure that you have the SMTP Server component installed in your local IIS server. Using the **Server Manager** from **Administrative Tools**, select **Features > Add Features** and select **SMTP Server**.

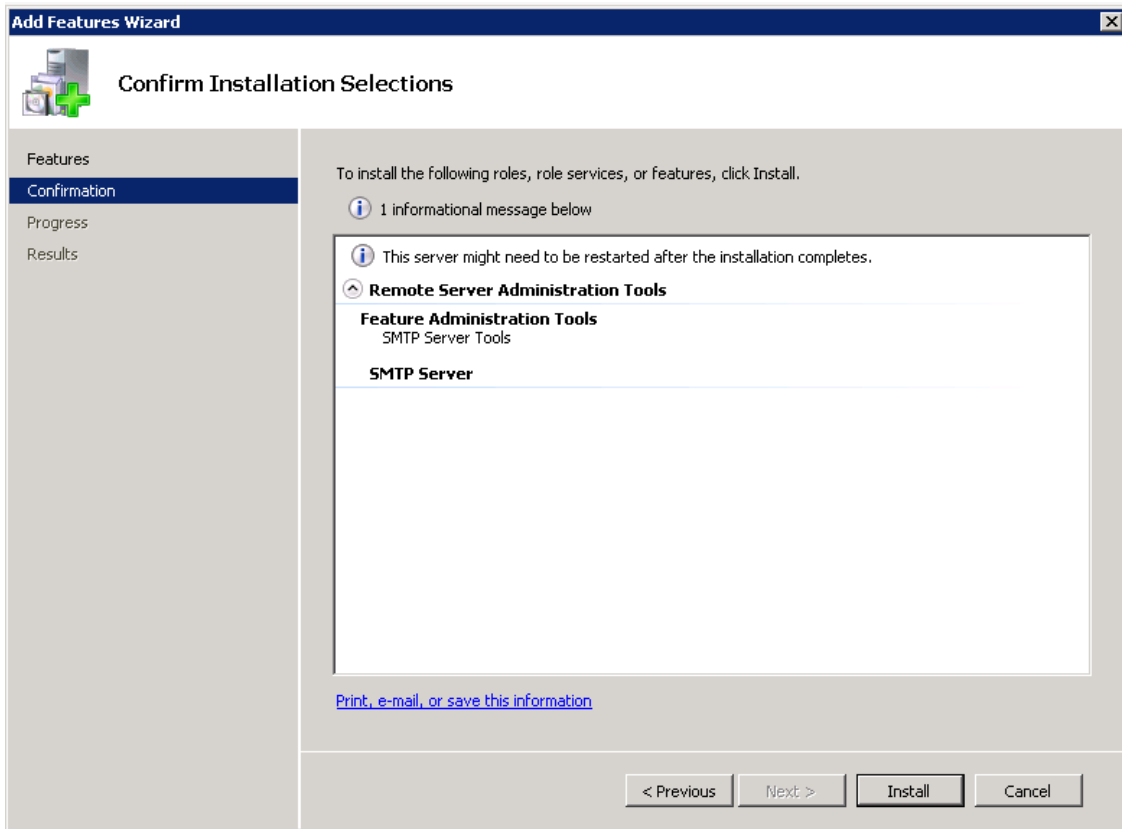


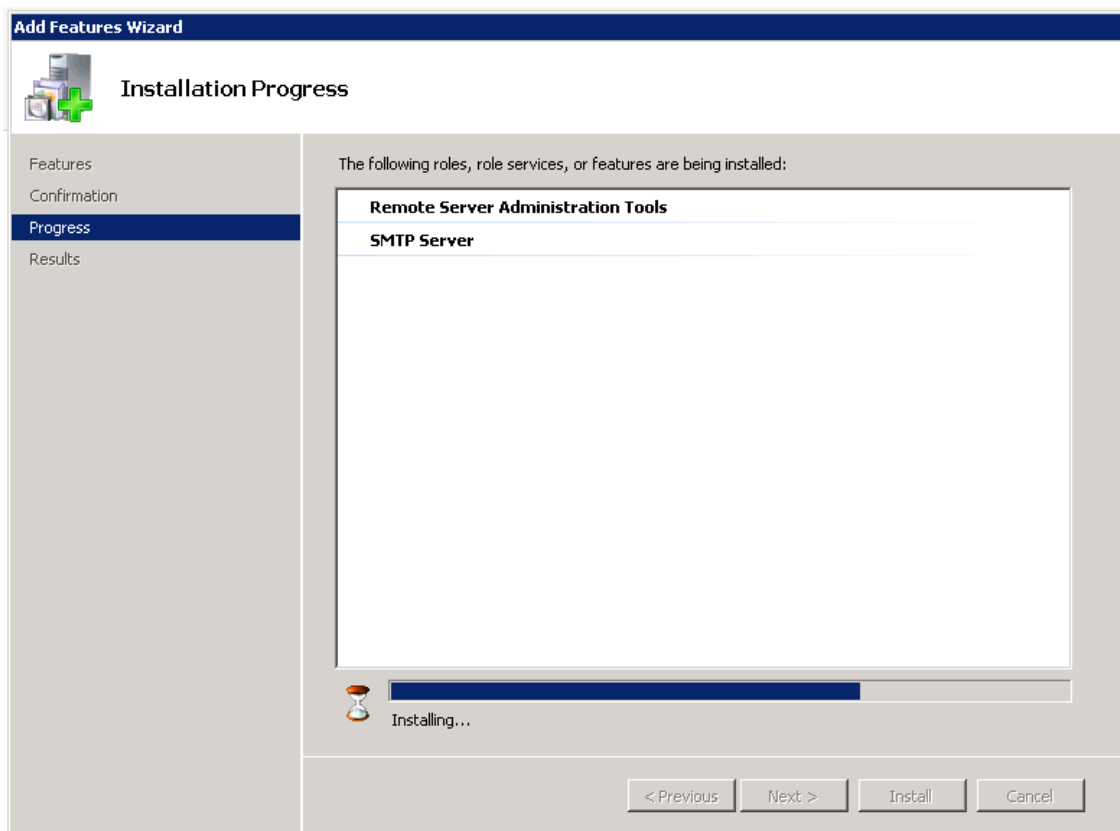
Note: If SMTP Server is already installed, you will see it already selected, grayed out, with (Installed) after it.

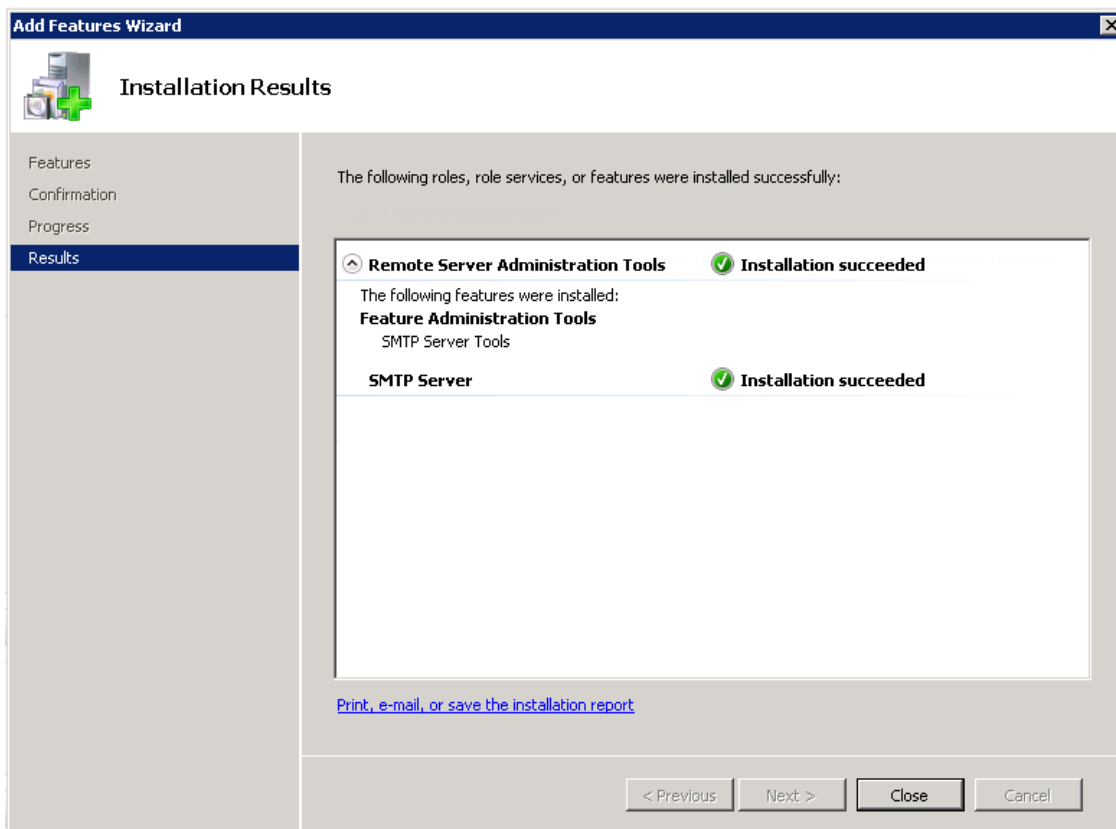
The Add Features Wizard displays.



- 2 Click Add Required Role Services and then click Next > Install.

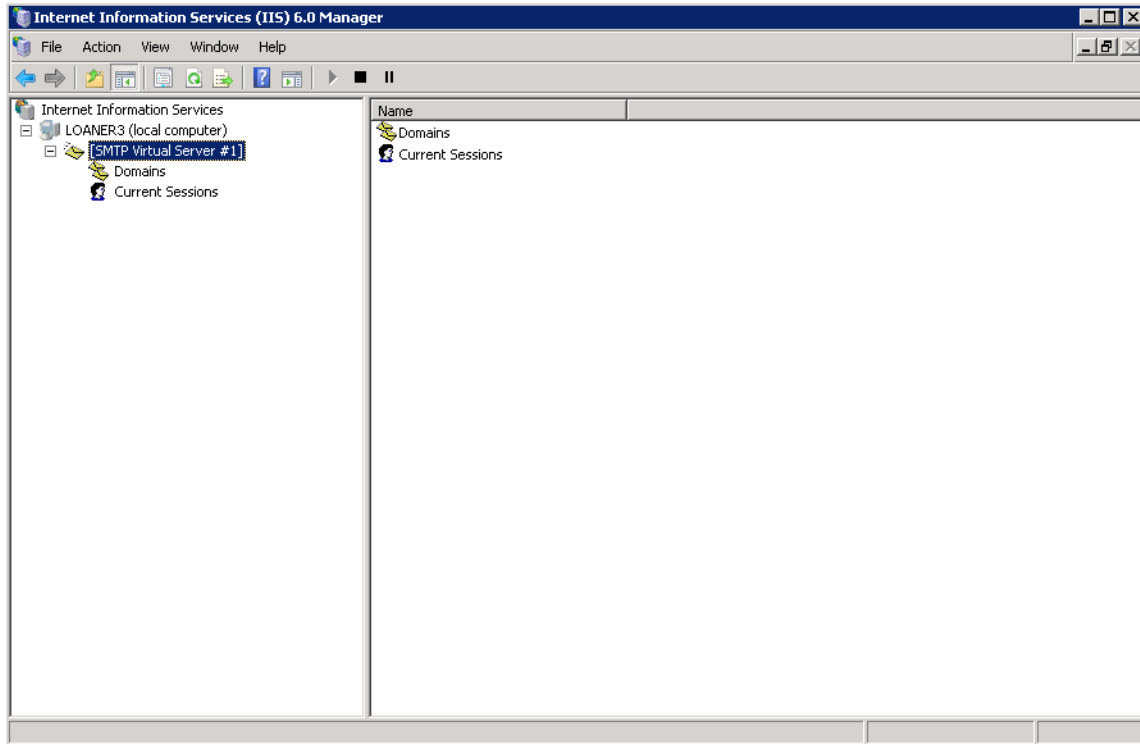






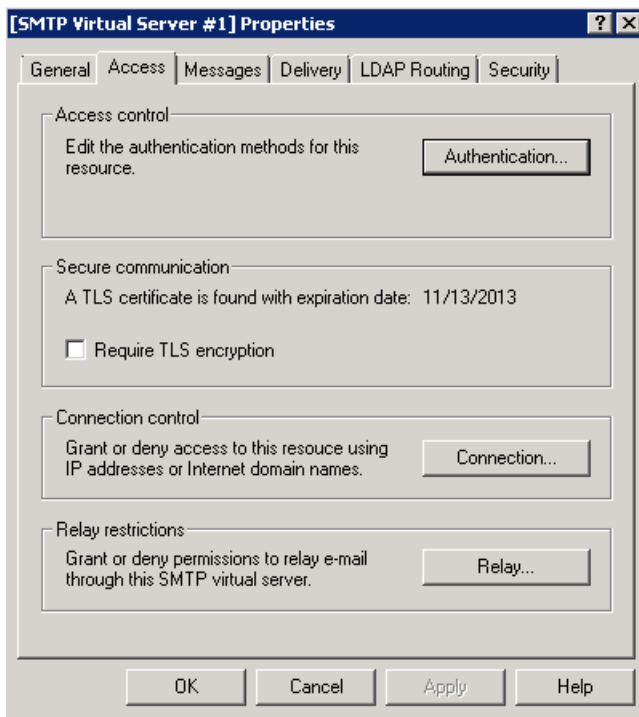
- 3 After installation completes, click **Close**.
- 4 Click **Start** and in the Search Programs and Files box type IIS.

- 5 Select Internet Information Services (IIS) 6.0 Manager. You should see a [SMTP Virtual Server #1] node in your IIS administration window under the local machine.

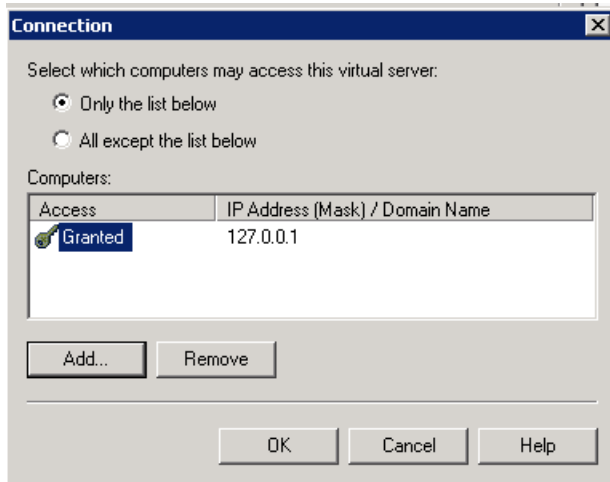


- 6 Right-click [SMTP Virtual Server #1] and click Properties.

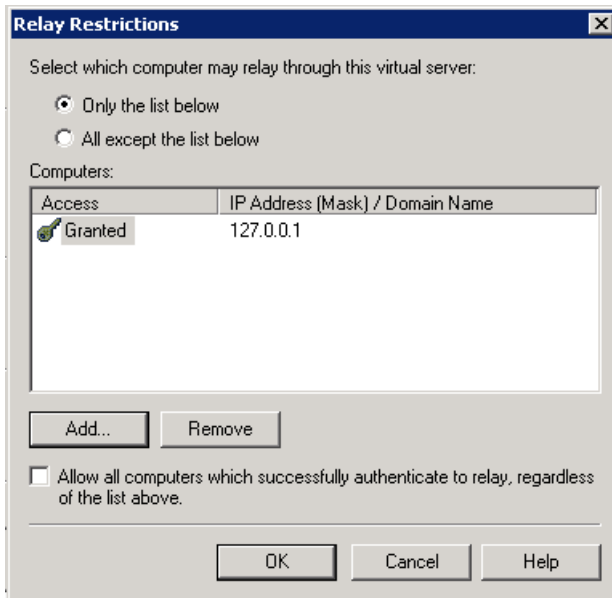
- 7 In the Properties window, select the **Access** tab.



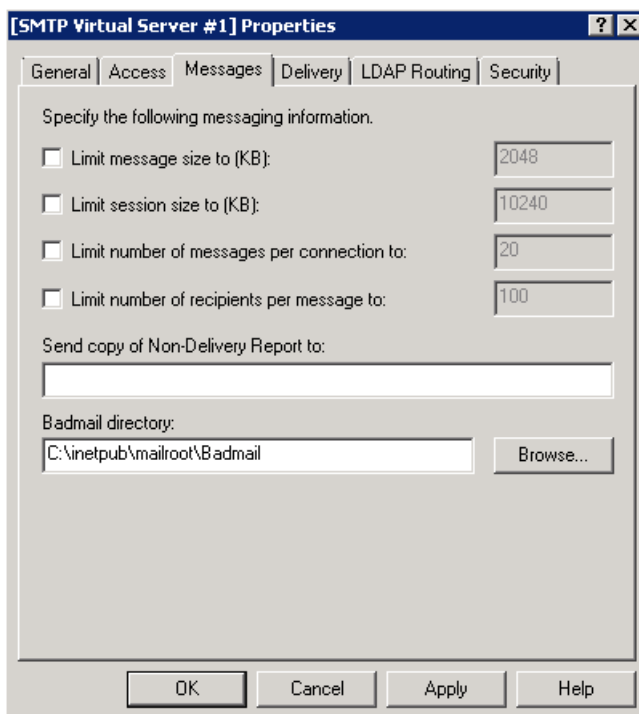
- 8 In the **Access** tab, click **Connection**. Restrict access to the SMTP server by selecting the **Only The List Below** option and adding the localhost IP address 127.0.0.1 to the access list. Click **OK** to exit the window.



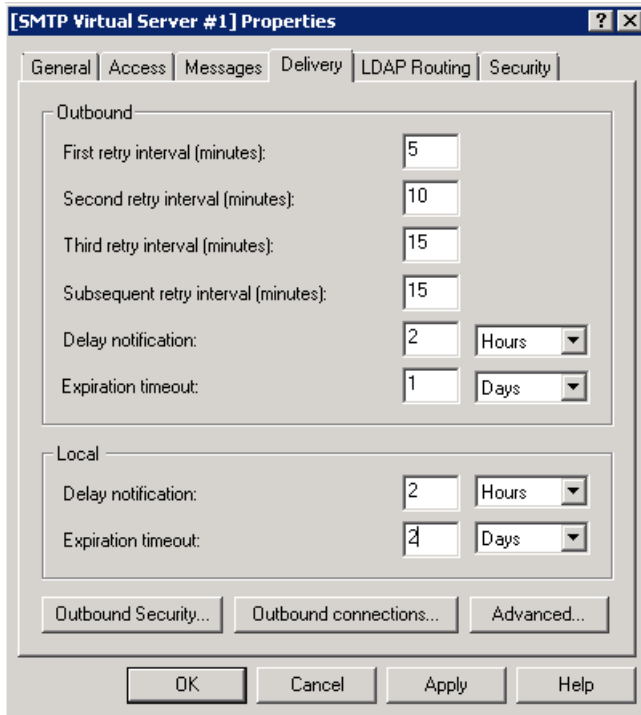
- 9 In the **Access** tab, click **Relay**. Restrict relay access to the SMTP server by selecting the **Only The List Below** option and adding the localhost IP address 127.0.0.1 to the access list. Make sure the **Successful Authentication Relay** option is turned off at the bottom of this window. Click **OK** to exit the window.



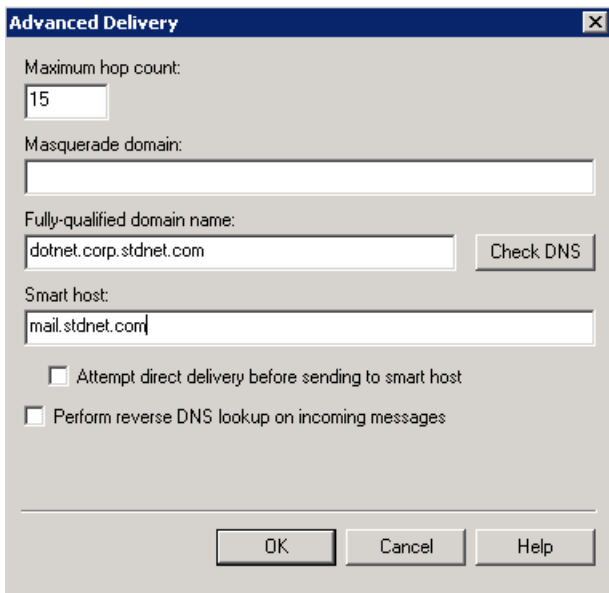
- 10 In the **Properties** window, switch to the **Messages** tab. In the **Messages** tab, turn off all the message limits.



- 11** 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.



- 12** In the **Delivery** tab, click **Advanced**. Set the **Fully Qualified Domain Name** setting to the name of your MOVEit DMZ server. Set the **Smart Host** setting to the name of your main SMTP server.



- 13** 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.

- 14** The final step is configuring your DMZ server to use the new local SMTP service. Open the MOVEit DMZ Config program (Start -> Programs -> MOVEit DMZ) and switch to the **Email** tab. Enter **localhost** as the **Server** name. Click OK to exit the Config program. The change should happen immediately; no restart is required.

The screenshot shows the 'Configure MOVEit DMZ' dialog box with the 'Email' tab selected. The dialog has a title bar with a close button. Below the title bar is a tabbed interface with the following tabs: FTP Ports, FTP Certs, FTP IPs, SSL, SSH, SSH Ciphers, License, Status, Paths, Email (selected), Settings, and Database. The 'SMTP Configuration' section contains a 'Server' text box with 'localhost' entered, a placeholder '(e.g. mail.example.com)', and a 'Timeout' spinner box set to '30' with the label '(Seconds)'. The 'Key Email Addresses' section contains a 'Default From:' text box with 'notify@standardnetworks.com' entered, a placeholder '(e.g. notify@example.com)', and a 'Send Errors To:' text box with 'support@standardnetworks.com' entered, a placeholder '(e.g. admin@example.com)', and a large empty text area below it. At the bottom are four buttons: OK, Cancel, Apply, and Help.

FTP Ports	FTP Certs	FTP IPs	SSL	SSH	SSH Ciphers
License	Status	Paths	Email	Settings	Database

SMTP Configuration

Server:
(e.g. mail.example.com)

Timeout: (Seconds)

Key Email Addresses

Default From:
(e.g. notify@example.com)

Send Errors To:
(e.g. admin@example.com)

OK Cancel Apply Help

Tuning

You will probably want to tinker with the **outgoing connection limit** (default is 1000) if one of your goals is to keep MOVEit DMZ 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 DMZ server configured to use it.

Troubleshooting

An easy way to troubleshoot your mail relay loop is to run the **reporterrors.exe** executable found in your **MOVEitDMZ\Scheduler** folder from the command line. This utility will either send a very short message to the error email address configured in your MOVEit DMZ Config program or report a connection problem regarding the email server.

Problem: Cannot connect to local mail relay.

Solution 1: Open the **Services** from **Start | Programs | 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 | Programs | 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 the **reporterrors.exe** utility 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 test 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 **MAIL SERVER** field in your MOVEit DMZ 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]**)

You can also use the **MOVEit DMZ Check** utility to test mail relay loops. In version 4.0 it acquired the ability to test email relay against an email address you type in while the program is running, so it may be the better tool to use if you suspect trouble with particular email addresses.

Service Integration - RADIUS/ODBC Authentication

To authenticate against usernames and passwords stored in a remote database table, MOVEit DMZ can use the MOVEit RADIUS/ODBC Authentication service. This service accepts RADIUS requests from MOVEit DMZ and then looks up the attempted username and password from a local ODBC source.

Almost any database can be supported with this mechanism, as the service uses an arbitrary ODBC connection string and generic SQL queries. (MySQL and SQL Server examples are provided.)

Recommended Platform

The most secure way to run this service is to install it on the same machine as the database server; in this case all usernames and passwords are protected with the encrypted RADIUS channel. A less secure way is to install this service on a different internal machine; in this case the username and password is encrypted between MOVEit DMZ and the box running the MOVEit RADIUS/ODBC Authentication service, but is probably not encrypted between the MOVEit RADIUS/ODBC server and the database server. The least secure way is to install this service on the MOVEit DMZ system itself; in this case the username and password are sent in the clear between the MOVEit DMZ and an internal database server.

Installation

To install the MOVEit RADIUS/ODBC Authentication service, you need to download and install two packages:

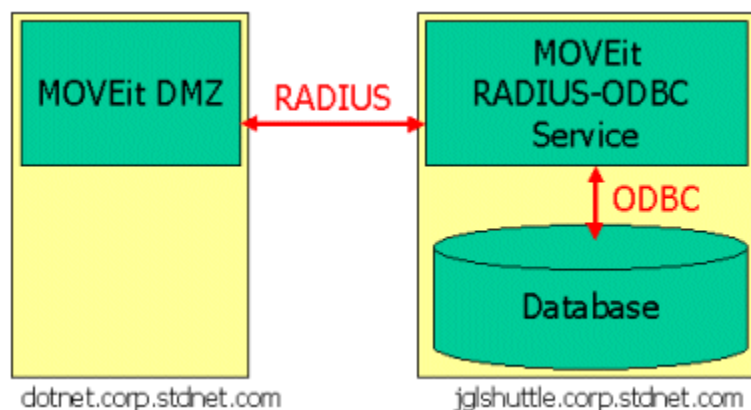
- Microsoft .NET Framework version 1.1 (or higher)
- MOVEit RADIUS-ODBC Authentication (available in the / MOVEit / DMZ / Extras folder on the MOVEit support site, <http://www.myipswitch.com> (<http://www.myipswitch.com>))

The MOVEit RADIUS-ODBC Authentication SERVER will install as a Microsoft Service, so you can start and stop it with the Services control panel or a `net stop/start moveitradius` command from the command prompt. Unlike some other MOVEit services, MOVEit RADIUS-ODBC service itself has no user interface. Serious errors encountered by the service are logged in the Application event log under MOVEitRADIUS.

There is also a GUI configuration CLIENT installed with the MOVEit RADIUS-ODBC Authentication package. This client can be started from the START menu via Programs | MOVEit DMZ | Configure MOVEit RADIUS.

Configuration

For the purposes of illustration, assume a system called `dotnet.corp.stdnet.com` is running MOVEit DMZ. A second system called `jglshuttle.corp.stdnet.com` hosts both the username/password database service and the MOVEit ODBC-RADIUS Authentication service.



The usernames and passwords are stored in a (MySQL) database called `radiustest` in a table called `userlookup`.

```
mysql> select * from userlookup;
+----+-----+-----+-----+
| ID | UName | EIPass | Description |
+----+-----+-----+-----+
| 1  | rad001 | pass001 | New Radius User |
| 2  | rad002 | pass002 | New Radius User |
| 3  | rad003 | pass003 | New Radius User |
+----+-----+-----+-----+
3 rows in set (0.03 sec)
```

On MOVEit DMZ, an administrator sets up a remote RADIUS authentication source to point to `jglshuttle.corp.stdnet.com` and enters the shared secret.

RADIUSODBC04.gif" width="532" height="229" alt="RADIUSODBC04.gif (10704 bytes)"/>

Finally, to configure the MOVEit RADIUS-ODBC service, an administrator opens the Configure MOVEit Radius utility and enters the following values:

Configure MOVEit Radius

RADIUS protocol

UDP Port:

Shared Secret:

Again:

Database

ODBC connection string

Connection:

Set for DB:

Host:

Username:

Password:

Database:

Table:

Username field:

Password field:

The values on this dialog are used in the following way by the MOVEit RADIUS-ODBC service

- **UDP Port:** The UDP port on which the service will listen for connections. Default is 1645.
- **Shared Secret (and Again):** A phrase used to encrypt the RADIUS connection. This value **MUST** match the shared secret value configured on MOVEit DMZ.
- **(ODBC) Connection:** The ODBC Connection String used to connect and authenticate to the database. The exact value of this string will vary from database vendor to database vendor. To quickly fill in the proper values for MySQL or SQL Server databases, click the appropriate **Set for DB** button immediately below this field. A very good list of connection strings for other database vendors can be found at <http://www.connectionstrings.com> (<http://www.connectionstrings.com/>).
- **(Database) Host:** The IP address or hostname of the username/password database service.
- **(Database) Username:** The username used to CONNECT to the username/password database.
- **(Database) Password:** The password used to CONNECT to the username/password database.
- **(Database) Database:** The NAME of the username/password database.
- **(Database) Table:** The name of the TABLE in the username/password database.
- **(Database) Username Field:** The name of the field in the table which contains cleartext usernames.
- **(Database) Password Field:** The name of the field in the table which contains cleartext passwords.

Make sure to fill in ALL values, otherwise the MOVEit RADIUS-ODBC service will likely NOT work.

All values set using this configuration dialog are saved to the HKLM\SOFTWARE\Standard Networks\MOVEitRadius registry entry. The values of the **Shared Secret** and the **Database Password** are encrypted here, and can only be set through this dialog. To use new settings, the MOVEit RADIUS service must be restarted.

Testing

One way to test the operation of the configured MOVEit RADIUS-ODBC service is to simply try signing on with registered users from a properly configured MOVEit DMZ session. RADIUS messages and errors will appear in the MOVEit DMZ debug log when the debug level is set to **DEBUG ALL**.

MOVEit RADIUS Test Client

An alternate way to test the operation of this (or any) RADIUS service is to download and run the MOVEitRADIUSTestClient (available in the Distribution \ MOVEit \ DMZ \ Extras folder on the MOVEit support site, https://www.ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ (http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ)).

WARNING: Do NOT install the MOVEit RADIUS Test Client on your MOVEit DMZ machine. The interaction of some underlying libraries used by both the test client and MOVEit DMZ could cause MOVEit DMZ to NOT authenticate RADIUS users.

Installation

Like MOVEit DMZ itself, the RADIUS test client requires the use of the .NET Framework. Install the framework before proceeding. Installation of the RADIUS test client simply involves extracting the contents of a ZIP file into a single folder on your test machine. (MOVEit Wizard can, of course, unzip this file if another ZIP utility is not available.) Make sure to install the test client on the machine you intend to test from. Running the client from a remote file server may cause permissions problems which could keep the client from running correctly. If you see the error **The .Net framework did not grant the permission.....**, this is most likely the cause.

Operation

The MOVEit RADIUS test client is a graphical utility named **MOVEitExtAuthTest.exe**. Run it by double-clicking on the file. Then, fill in the appropriate information for the RADIUS server you wish to test, and click the **Authenticate** button.

Diagnosing RADIUS

The following screenshots show the MOVEit RADIUS test client in action as it encounters one successful signon and three different common problems.

Connected OK, Authenticated OK:

The screenshot shows a window titled "MOVEit External Authentication" with a "RADIUS" tab selected. The window is divided into three main sections: "Server", "User", and "Debug".

Server Section:

- Radius Server Host:
- Port:
- Shared Secret:

User Section:

- Username:
- Password:
- Buttons: and

Debug Section:

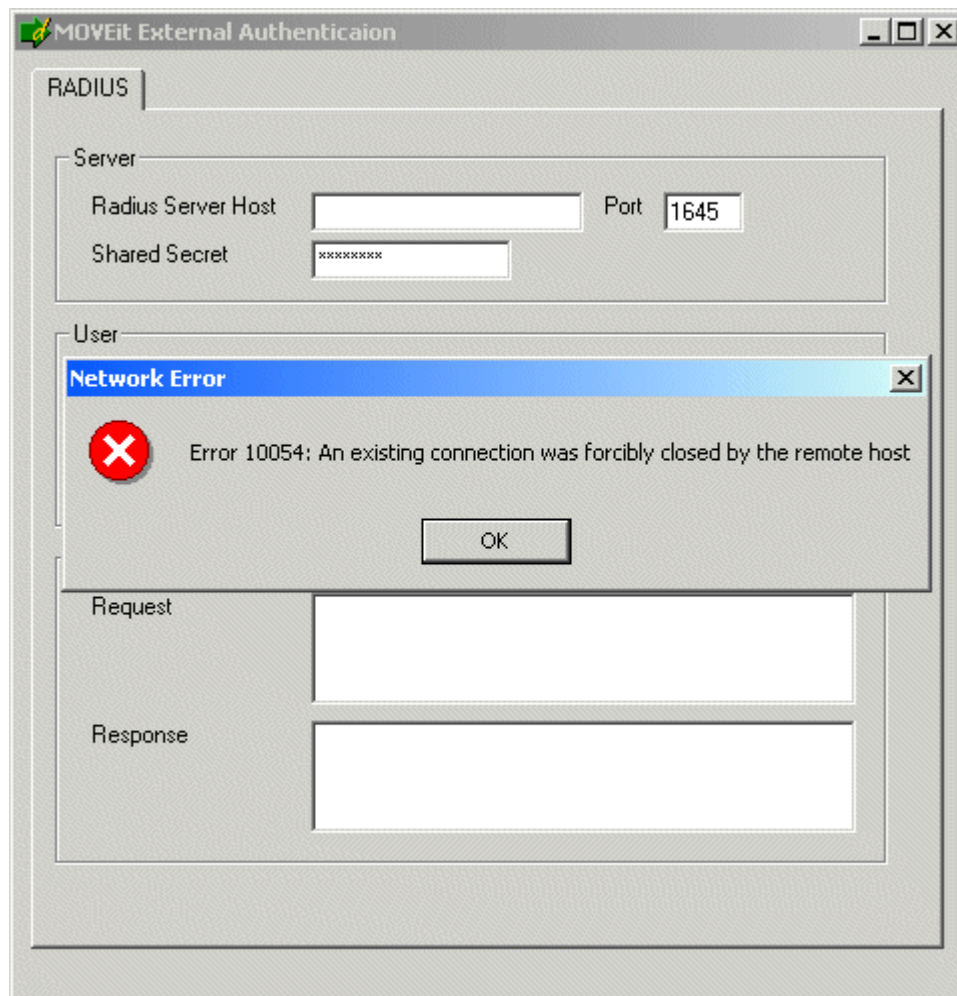
- Request: Code 01 id 04 Authen eab5124730d934710957d7259ce98020 Attr 0: Type 01 726164303031 Attr 1: Type 02
- Response: Code 03 id 04 Authen cf9ccfa4bf9c3a4a65b4d439847442af

Connected OK, Bad Username or Password:

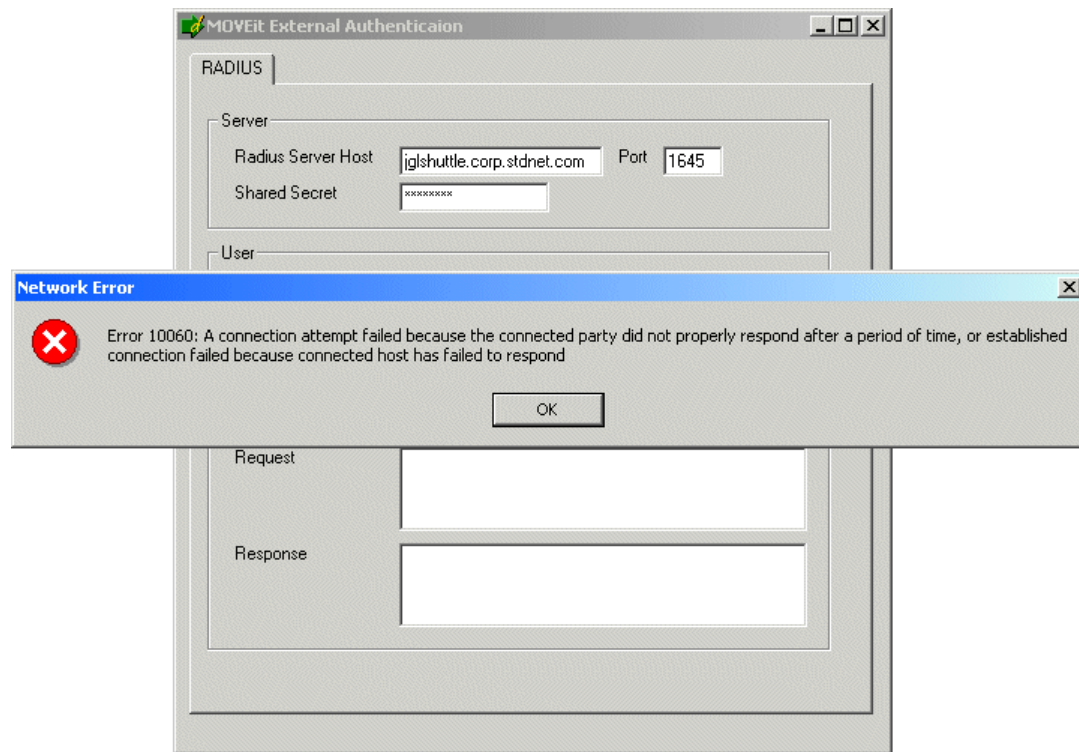
The screenshot shows the 'MOVEit External Authentication' window with the 'RADIUS' tab selected. The 'Server' section contains 'Radius Server Host' (iglsuttle.corp.stdnet.com), 'Port' (1645), and 'Shared Secret' (masked). The 'User' section shows 'Username' (pass001) and 'Password' (masked). An 'Authenticate' button is highlighted, and the status is 'Not authenticated'. The 'Debug' section shows a 'Request' and a 'Response' with their respective hex codes and attributes.

Section	Field	Value
Server	Radius Server Host	iglsuttle.corp.stdnet.com
	Port	1645
	Shared Secret	XXXXXXXXXX
User	Username	pass001
	Password	XXXXXXXXXX
	Action/Status	Authenticate (button) / Not authenticated
Debug	Request	Code 01 id 04 Authen eab5124730d934710957d7259ce98020 Attr 0: Type 01 726164303031 Attr 1: Type 02
	Response	Code 03 id 04 Authen cf9ccfa4bf9c3a4a65b4d439847442af

Failed to Connect - Invalid Host:



Failed to Connect - RADIUS Service Not Listening (Wrong Server?):

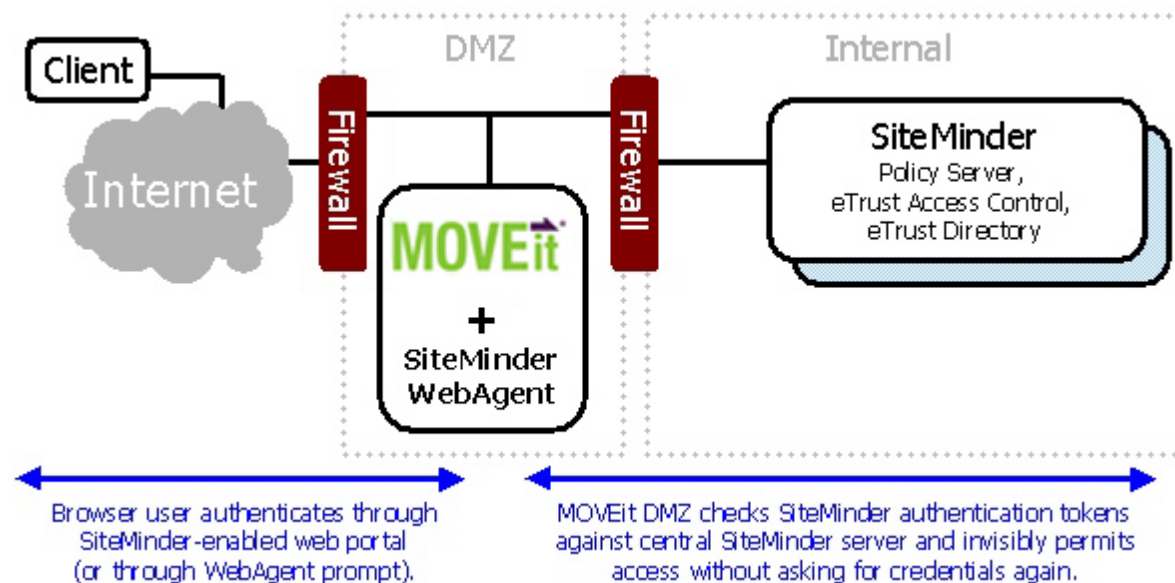


Service Integration - SiteMinder Integration

Overview

When enabled for external authentication, MOVEit DMZ can interface with CA's eTrust SiteMinder product to enable single-signon to a DMZ server operating in a SiteMinder environment. This allows users to log on to DMZ without having to enter their credentials, as long as they are already authenticated to the SiteMinder environment. This page details how to configure both MOVEit DMZ and SiteMinder to allow DMZ to function properly in a SiteMinder-integrated environment. For more details about configuring the SiteMinder Policy Server and Web Agents, see the documentation for these products.

Note: The SiteMinder integration feature, and these instructions, were developed for SiteMinder version 6.0 SP5.



Installing the SiteMinder Web Agent

Follow the steps indicated by the SiteMinder Web Agent installation guide. Enter valid administrative credentials for accessing the SiteMinder Policy Server. Enter a **Trusted Host Name** and a valid **Host Configuration Object** name (must already be defined on the Policy Server). Enter the IP address of the **Policy Server**. When prompted to select a **Virtual Site** to be configured, choose the web site that MOVEit DMZ was installed to. Finally, Enter a valid **Agent Configuration Object** name (must already be defined on the Policy Server) and choose to enable the **Web Agent**.

Configuring MOVEit DMZ for SiteMinder

Configuring MOVEit DMZ to integrate with SiteMinder simply involves enabling the SiteMinder Integration option through the web interface. This option may be found by signing on to MOVEit DMZ as a SysAdmin, and then finding the SiteMinder settings page under **Settings | System | User Authentication**. For details about the setting, see **System - User Authentication** (on page 534).

After enabling this setting, be sure to note the SiteMinder **Shared Secret** value. SiteMinder will need to be configured to return this value to MOVEit DMZ as part of a Response object before DMZ will begin trusting the SiteMinder HTTP headers injected into an authenticated and authorized request by the Web Agent.

Configuring SiteMinder for MOVEit DMZ

Because MOVEit DMZ requires several allowances to be made in SiteMinder, it is generally wise to create a separate Agent Conf Object and a separate Realm or Sub-Realm in the SiteMinder Policy Server to protect the DMZ server. This allows the following necessary changes to be made without affecting other protected servers.

Ignore Localhost Requests

Several of MOVEit DMZ's file transfer mechanisms involve making requests from the local server back to itself. To allow these to function correctly, the SiteMinder Web Agent needs to be configured to ignore requests to the local computer. Depending on how your server is configured, this is done in one of two ways.

If MOVEit DMZ is the only running website on the server, then this is done by adding the server's computer name to the IgnoreHost parameter on the Agent Conf Object being used by the Web Agent on the server. Note that the computer name should be used here, not localhost as one might assume. SiteMinder resolves localhost to the computer name before checking the IgnoreHost value, so adding localhost will not exempt local connections.

If there are other websites on the server (more specifically, if the MOVEit DMZ website is not configured to bind to **All Unassigned** IP addresses), then an alias to the MOVEit DMZ website must be added to the IgnoreHost parameter. If an alias for the MOVEit DMZ website already exists, enter that value in the IgnoreHost parameter on the Agent Conf Object. Otherwise, create one by either adding it to a DNS directory that is accessible by the DMZ server, or by adding it to the **hosts** file in C:\WINDOWS\SYSTEM32\drivers\etc.

Once the alias has been set up and SiteMinder has been configured to ignore it, change the Machine URL setting in the MOVEit DMZ Config program's **Paths** tab to use the alias, so that machine connections will be ignored by SiteMinder.

Note: If this latter method is used, be aware that the MOVEit DMZ Checker program will not work unless it is configured to test the alias URL. You can change the test settings for **Checker** by clicking **Options | Configure....**

Ignore MOVEitISAPI Requests

Neither the ActiveX nor the Java-based MOVEit Wizard clients are able to access and submit the SiteMinder identification cookies necessary to operate against a SiteMinder-protected website. Therefore, the MOVEitISAPI module which they both use for file transfer operations needs to be exempted from protection by SiteMinder in order for browser-based file transfers with the MOVEit Wizard clients to work properly. Since such file transfers cannot be done without an established MOVEit DMZ session anyway, this should not pose a security risk to the server.

To exempt the MOVEitISAPI module from SiteMinder protection, a Sub-Realm needs to be created under the Realm that protects the MOVEit DMZ server. This sub-realm should have a resource filter of **moveitisapi/moveitisapi.dll** and should be marked as **Unprotected**.

Add a Response Object

In order for MOVEit DMZ to trust the HTTP headers provided by the SiteMinder Web Agent, a special static header needs to be included that contains the shared secret value automatically generated by DMZ when its SiteMinder Integration setting is enabled. This header can be added by creating a new Response object under the policy Domain that protects the MOVEit DMZ server. The new Response object must include a static WebAgent-HTTP-Header-Variable attribute with a variable name of `SM_MOVEITDMZ_SHAREDSECRET` (so that the full HTTP header name ends up being `HTTP_SM_MOVEITDMZ_SHAREDSECRET`), and a variable value equal to the DMZ shared secret string. Once the Response object has been created, it will need to be added as a Response to the Rule which covers the MOVEit DMZ server in the appropriate domain Policy object.

Providing Alternate Credentials

When configured to use an installed and working SiteMinder Web Agent, MOVEit DMZ will no longer prompt users for credentials when they arrive at MOVEit DMZ's web browser interface. The username of the logged-in SiteMinder user will be used as the username for the MOVEit DMZ account as well.

As such, there is no direct way to log on to MOVEit DMZ with a different username than the one being used to authenticate to SiteMinder. If this becomes necessary (such as for logging in as an administrator user with a different username), log on to DMZ as usual (using SiteMinder), then apply the following query string to the URL in the web browser:

```
?transaction=signoff&arg12=signon
```

These query string parameters instruct DMZ to log off the current user account, and return the signon screen to the browser. From the signon screen, a different username and password can be entered. DMZ will use the provided username and password to authenticate the user instead of the current SiteMinder information.

Service Integration - SysLog and SNMP

Beginning in version 7.0, MOVEitDMZ has the ability to directly log events to SysLog management consoles. For more information on how to set this up, please visit **Web Interface - Settings - System - Auditing** (on page 529). In order to send audit log events to SysLog or SNMP management consoles in previous versions of MOVEitDMZ, Audit entries must first be logged to the Windows Event Log, whereby a third-party utility could be used to forward these events along to a SysLog or SNMP server. This guide briefly describes several easy-to-obtain utilities which will send MOVEit DMZ entries from the Windows Event Log to a SysLog Server 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

A mature (10+ year old) commercial client called **Event Reporter** (<http://www.eventreporter.com/en>) is available to perform filtering on event logs before sending them to a SysLog. This client was available online for \$49 on February 18, 2005.

Snare

A freeware client called **Snare** (<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** (<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. This client was available online for \$45 on February 18, 2005.

winlogd

A freeware utility called **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** (<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. This client was available online for \$45 on February 18, 2005.

Service Integration - Time Synchronization

The NTP time services (RFC 1305) are a useful way to synchronize server clocks to a known good value.

Ipswitch recommends (and uses) a Windows utility called w32tm.exe (Windows32Time) as an NTP client application on MOVEit DMZ servers. Detailed information about this client can be found by looking for w32tm documentation on Microsoft's site, but most time client configuration involves only one parameter (which server to use) and only one action (how to force a time synchronization now).

Time services are built Windows Server. Use the procedure below, from a command prompt, to configure them.

Assign a New Time Server to W32Time

Execute the following command (where ntp.yourisp.net has been replaced with the hostname of a reliable time server such as pool.ntp.org):

```
C:\>net time /setsntp:ntp.yourisp.net
```

Force W32Time to Sync Time Now

Execute the following command:

```
C:\>w32tm /resync /nowait Sending resync command to local computer... The command completed successfully.
```

Virtual Servers and Time Services

When running time clients on virtual servers (such as products from VMware or Microsoft's VirtualPC), it has been observed that the clock of the host operating system will usually be regarded as more authoritative than data from time clients running on the virtual servers. For example, if the host operating system says it is now 3:25 and a remote time server said it is 3:27, someone on the virtual OS console may see the time jump to 3:27 and then back to 3:25 in short order.

To minimize strange interactions like this, care should be taken to keep the host operating system's time up to date and to avoid the use of time clients on virtual servers.

Available Time Servers

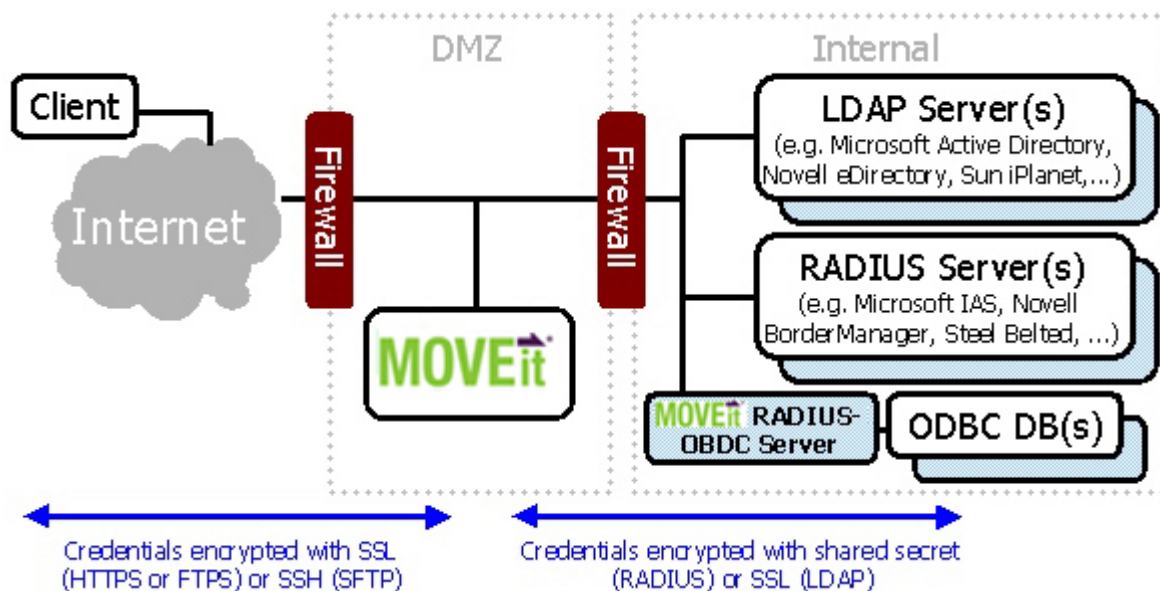
A list of time servers available to the public is maintained at <http://support.ntp.org/bin/view/Servers/NTPPoolServers> (<http://support.ntp.org/bin/view/Servers/NTPPoolServers>).

Service Integration - Web Integration

Integration of MOVEit DMZ with other existing web applications can be achieved using several of DMZ's available features. To offer seamless transitions between an existing web application and MOVEit DMZ, external authentication, single signon, and logo and color scheme customization all need to be combined. For MOVEit DMZ API based web applications that need to transfer users to the MOVEit DMZ server without requiring another signon, the session transfer capability can also be used.

External Authentication

To keep the user from having to remember multiple login accounts, and to ease maintenance of account databases, use MOVEit DMZ's external authentication feature to tie DMZ into your existing user authentication facility. MOVEit DMZ supports authenticating against both RADIUS and LDAP servers, along with its own internal user database. If you are using a SAML Identity Provider for authentication, MOVEit DMZ can be configured to use the Identity Provider. See the External Authentication section of the *User Policy Settings* (on page 419) page for more information.



Single Signon

To allow an existing web application to transfer a logged in user seamlessly to MOVEit DMZ, DMZ accepts username and password information via HTML form fields. Optimally, the existing web application should provide a secure page with a button the user can click to transfer to the DMZ application. See the *Simple Single Signon Support* section of the **URL Crafting** (on page 783) page for more information.

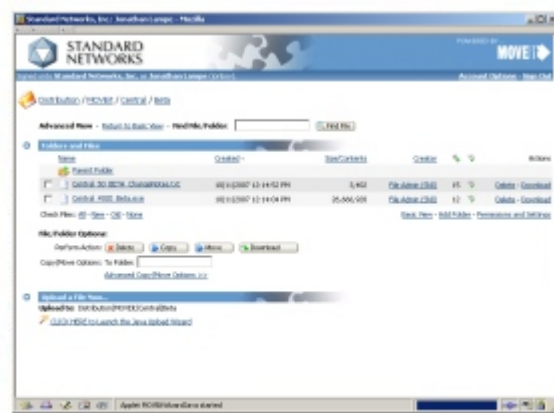
MOVEit DMZ also provide support for SAML Single Signon via a third-party Identity Provider. For more information, see **User Authentication - Security Policies- Single Signon** (on page 422).

Custom Logos and Color Schemes

To keep users from believing that they've left the confines of a corporation's existing web application, MOVEit DMZ's custom logo and color scheme features can be used to make MOVEit DMZ appear as similar to the existing web application as necessary. Use the custom logo and bullet features to add corporate logos and bullet images to a DMZ organization. Use the custom HTML header feature to add more advanced header code to a DMZ organization, such as flash logos or javascript menus. Select one of the many stock color schemes included with MOVEit DMZ to closely match the existing web application, or add a custom color scheme to match it exactly. See **Brand Settings** (on page 358) for more information about each of these features. Information about creating custom color schemes can be found in **Custom Schemes** (on page 562).



Main Web Site



Branded MOVEit DMZ

Session Transfer

Some customers use MOVEit DMZ API to provide some MOVEit information and services inside their own web applications. Instead of logging on directly to MOVEit DMZ, visitors to these sites instead log on to the web application, which uses an internal copy of MOVEit DMZ API to do its own logon to MOVEit. This way, companies can provide information from their MOVEit DMZ server to visitors without having them leave the company website. However, for more advanced features, such as the MOVEit Wizard, it may become necessary to have the user move to the MOVEit server itself. Normally, the existing session that the MOVEit DMZ API object has with MOVEit cannot be transferred across servers, meaning the user would have to sign on again to access MOVEit directly.

To avoid this problem, MOVEit provides a mechanism for transferring an existing client session from the API-enabled server to the MOVEit server. First, the host that the MOVEit DMZ API application resides on must be marked as Trusted (see the **Trusted Hosts section** (on page 536) of the System Remote Access Policy page for more information). Next, the API application must send the user to a special ASPX page provided by MOVEit DMZ, called `apilink.aspx`, and provide the current session ID using an HTML form. This page takes the session ID argument and sets the appropriate cookie information on the client's browser, then forwards the client on to MOVEit DMZ. The following example shows a URL and session id sent via the HTTP POST method.

Note: Previous versions of MOVEit DMZ suggested using the HTTP GET method to send the session id. Security best practices call for using the POST method instead of the GET method. If your web integration uses HTTP GET, and you want to continue to use the GET method, you need to set the following registry entry to allow the continued use of this method.

Set the MOVEit DMZ registry value `AllowInsecureQueryStrings` to "1" to allow GET requests for sensitive transactions, and allow GET requests to include session IDs in `apilink.aspx`. For more information, see the **Registry Settings** (on page 764) section in the Technical Reference topic.

The original GET example suggested this:

```
https://moveit.yourcompany.com/apilink.aspx?sessionid?=<sessionID>
```

You can use a POST example like the following:

```
<BODY onload="document.forms[0].submit();">

<FORM action="https://moveit.yourcompany.com/apilink.aspx" method="POST">

  <INPUT type="hidden" name="sessionid" value="{Session ID}"/>

  <NOSCRIPT>

    <P>Press this button to continue:</P>
```

```

<INPUT type="submit" value="Continue"/>

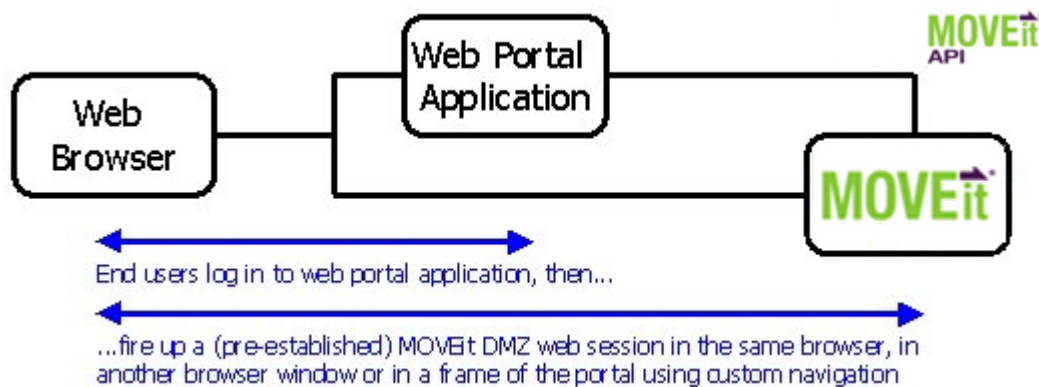
</NOSCRIPT>

</FORM>

</BODY>

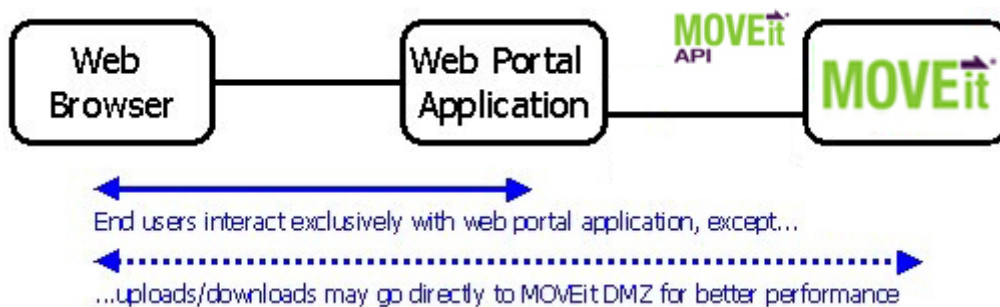
```

The session ID can be accessed from the MOVEit DMZ API object. See the MOVEit DMZ API documentation for more information.



Direct Upload/Download

MOVEit DMZ supports direct, secure uploads and downloads initiated by other web applications.



Using MOVEit DMZ in this manner allows customers to use MOVEit DMZ for secure storage of all their portal's sensitive files. It also allows customers to take advantage of MOVEit DMZ's buffered transfers; otherwise handling of large files is an issue with many portal applications because they attempt to work with files on disk or all at once in memory. Typically, MOVEit DMZ API is used to initiate a secure upload and download by performing a session transfer at the same time. Complete documentation about this procedure (and a sample application) is available in the MOVEit DMZ API Windows documentation set.

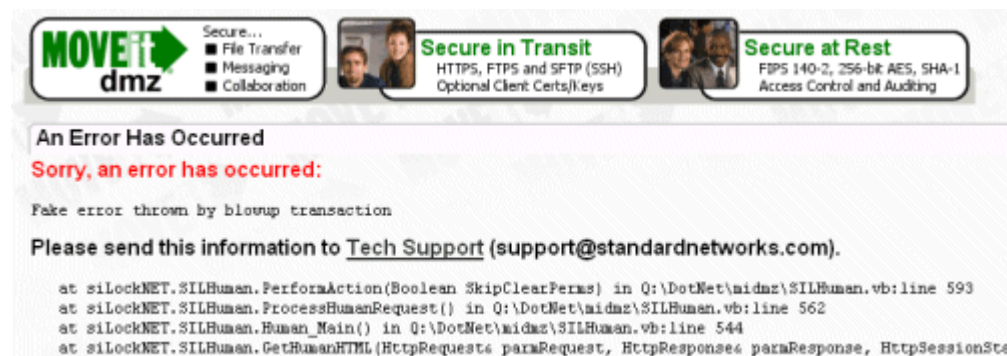
See also *Direct Download* in **Advanced Topics - URL Crafting** (on page 783).

System Internals - Exception Handling

In the rare event of an internal error occurring during the normal operation of a MOVEit DMZ server, DMZ will contain such an error, and display a friendly message to the end user who was unlucky enough to encounter it. The message contains the description of the error, and the call stack of the application at the time of the error, as well as instructions to report the error to the appropriate technical support person or group, whose contact information is also displayed.

Some company audits may require a demonstration of this error handling capability. For this reason, a special transaction which causes a harmless exception to be thrown inside DMZ is available. To execute this transaction, add the `csrftoken` and the phrase `transaction=blowup` to your URL query string, as shown in the example. For example, if your MOVEit DMZ server is located at `https://moveit.mycompany.com/`, you would first signon to your DMZ server, and then load the following URL into your browser:

`https://moveit.mycompany.com/human.aspx?csrftoken=e815606238a4c8abc83e1977d60a8e40d391c27f&transaction=blowup`



To suppress the appearance of the specific internal error displayed on this page from end users, disable the Show System Error Messages system setting. SysAdmins can change this setting by clicking on the [link](#) on the Settings page.

System Internals - MOVEit DMZ Error Codes

MOVEit DMZ will sometimes list a four-digit error code in an audit log entry and will always return an error code in response to API requests. The following list may provide more insight into codes encountered in these situations, but the error description (if any) will usually provide a more specific explanation.

ERROR_NONE = 0

ERROR_INTERNAL = 100

ERROR_OTHER = 200

ERROR_INVALID_USERNAME = 2010

ERROR_NOPERM = 2020

ERROR_INVALID_CREDENTIALS = 2025

ERROR_DATABASE_UPDATE = 2040

ERROR_DATABASE_OPEN = 2042

ERROR_DATABASE_CONN = 2044

ERROR_DATABASE_READ = 2046

ERROR_INVALIDUSER = 2050

ERROR_INVALID_FOLDERID = 2056

ERROR_INVALID_FILEID = 2058

ERROR_INVALID_FILETYPE = 2060

ERROR_INVALID_PARENTID = 2068

ERROR_INVALID_PARENTINHERITRIGHTS = 2069

ERROR_INVALID_FOLDERTYPE = 2070

ERROR_INVALID_FOLDERNOTETYPE = 2071

ERROR_INVALID_INSTID = 2072

ERROR_INVALID_USERPERM = 2074

ERROR_INVALID_FOLDERNOTETIME = 2075

ERROR_INVALID_EMAILADDRESS = 2076

ERROR_NO_EMAILADDRESS = 2077

ERROR_INVALID_FOLDERSYSTEMTYPE = 2080

ERROR_INVALID_FOLDERCLEANTIME = 2085

ERROR_INVALID_FOLDERCLEANTYPE = 2086

ERROR_INVALID_FOLDERNEWTIME = 2088

ERROR_DUPLICATE_FOLDERNAME = 2090

ERROR_DUPLICATE_FILENAME = 2092

ERROR_INVALID_FOLDERNAME = 2100

ERROR_INVALID_FILENAME = 2102

ERROR_FILE_IS_DELETED = 2104

ERROR_FILESYSTEM_FOLDERCREATE = 2210

ERROR_FILESYSTEM_FOLDERDELETE = 2220

ERROR_FILESYSTEM_FILECREATE = 2230

ERROR_FILESYSTEM_FILECOPY = 2234

ERROR_FILESYSTEM_FILEMOVE = 2236

ERROR_FILESYSTEM_FILEDELETE = 2240

ERROR_FILESYSTEM_FILEOPEN = 2244

ERROR_FILESYSTEM_IN_USE = 2250

ERROR_FILESYSTEM_NOT_FOUND = 2251

ERROR_INVALID_XMLREQUEST = 2310

ERROR_INVALID_TRANSACTION = 2320

ERROR_INVALID_PASSWORD = 2410

ERROR_INVALID_LANGUAGE = 2411

ERROR_INVALID_USERREALNAME = 2412

ERROR_INVALID_CLIENT_CERT = 2414

ERROR_NO_CLIENT_CERT = 2415

ERROR_CLIENT_CERT_REQUIRED = 2416

ERROR_INTERFACE_NOT_ALLOWED = 2417

ERROR_INVALID_SSHKEY = 2420

ERROR_UPLOAD_INVALIDPARMS = 2430

ERROR_INVALID_INSTFORMRESP = 2500

ERROR_INVALID_AUTHSOURCE = 2505

ERROR_INVALID_INSTHISTTIME = 2510

ERROR_INVALID_HOSTPERMIT = 2520

ERROR_INVALID_HPPRIORITY = 2522

ERROR_INVALID_HPPERMITID = 2524

ERROR_INVALID_HPHOST = 2526

ERROR_INVALID_HPRULE = 2528

ERROR_INVALID_HOST = 2540

ERROR_INVALID_COMMENT = 2670

ERROR_DUPLICATE_FOLDERUSER = 2674

ERROR_INVALID_FOLDERUSER = 2678

ERROR_INVALID_PASSPHRASE = 2680

ERROR_DUPLICATE_INSTNAME = 2684

ERROR_REGISTRY_KEYCREATE = 2688

ERROR_INVALID_INSTNAME = 2692

ERROR_REGISTRY_KEYDESTROY = 2696

ERROR_REGISTRY_KEYCHANGE = 2698

ERROR_UPLOAD_FILECREATE = 2700

ERROR_UPLOAD_MISC = 2710

ERROR_CANT_ACCESS_SERVER = 2800

ERROR_SERVER_APP = 2801

ERROR_INVALID_PARAMETER = 2850

ERROR_SETTINGS_OUT_OF_DATE = 2860

ERROR_ILLEGAL_TRANSLATION = 2904

ERROR_FAILED_TRANSLATION = 2908

ERROR_BROWSER_FILEPUSH = 2954

ERROR_INVALID_FILEBUNDLETYPE = 2958

ERROR_BUNDLE_EMPTYFILES = 2964

ERROR_INVALID_DEBUGLEVEL = 2968

ERROR_INVALID_URL = 2972

ERROR_MULTI_SIGNON_PROHIBITED = 2974

ERROR_ILLEGAL_USERATHOST = 2976

ERROR_UNAUTHORIZED_USER = 2978

ERROR_UPLOAD_EMPTYFILE = 2980

ERROR_QUOTA_EXCEEDED = 2982

ERROR_INVALID_FOLDERACCESS = 2984

ERROR_INVALID_NOTE = 2988

ERROR_INVALID_GROUPNAME = 3108

ERROR_DUPLICATE_GROUPNAME = 3112

ERROR_INVALID_GROUPID = 3116

ERROR_EXPIRED_SESSION = 3200

ERROR_FAILED_WEB_REQUEST = 3201

ERROR_PROXY_NOT_AUTHORIZED = 3202

ERROR_ENCRYPTION = 3300

ERROR_LICENSING = 3400

ERROR_EMAIL = 3500

ERROR_DOWNLOAD = 3600

ERROR_HASH_CHECK_FAILED = 3601

ERROR_DELETE_FILE = 3610

ERROR_SCRIPT = 3700

ERROR_UPLOAD = 3800

ERROR_LICENSE = 3900

ERROR_LANGUAGE_IN_USE = 3950

ERROR_TAMPERED = 3960

ERROR_AUDITING_DISABLED = 3961

ERROR_TAMPER_RESET = 3962

ERROR_ALREADY_RUNNING = 4000

ERROR_ALREADY_CHECKED_OUT = 4010

ERROR_NOT_CHECKED_OUT = 4011

ERROR_CANNOT_CHECK_IN = 4015

ERROR_DOES_NOT_EXIST = 4020

ERROR_STOPPED_BY_USER = 4030

ERROR_PROXY_PROBLEMS = 4040

ERROR_SSL_WEAK = 4100

ERROR_NO_THUMBNAIL = 4200

ERROR_INVALID_AUTHMETHOD = 4300

ERROR_INVALID_RADIUS_SETTINGS = 4301

ERROR_CREATE_RADIUS_USER_FAIL = 4302

ERROR_AUTHED_OFF_BACKUP_RADIUS = 4303

ERROR_INVALID_LDAP_SETTINGS = 4311

ERROR_CREATE_LDAP_USER_FAIL = 4312

ERROR_AUTHED_OFF_BACKUP_LDAP = 4313

ERROR_DISALLOWED_BY_DEFAULT_EXPIRATION_POLICY = 4350

ERROR_DISALLOWED_BY_PARENT_EXPIRATION_POLICY = 4351

ERROR_BAD_MESSAGE = 4400

ERROR_AS2_MDN_TIMEOUT = 4500

ERROR_IGNORE_FILE = 5000

ERROR_MISSING_PARAM = 5100 ' Used by Central

System Internals - NTFS Permissions

This guide contains Ipswitch recommendations for NTFS permissions on Windows folders on a MOVEit DMZ system.

To make the configuration of permissions easier, you should create a new **MOVEit System** group to hold all the users under which the MOVEit DMZ application runs. This group should contain the following users. After creating this group and applying permissions as described below, you will usually need to reboot your machine before these permissions take effect, as some of these users only sign on during a reboot.

User/Group	Description
System	Built-in LocalSystem account (used by MOVEit's scheduled tasks)
IUSR_...	Built-in anonymous web access account (used by online application)
IWAM_...	Built-in anonymous web access account (used by online application)
ASPNET	Built-in ASP.NET account (used by online application)
NETWORK SERVICE	(Windows 2003 Only!) Built-in group for network services (used by online application)

The following table shows which permissions to assign to the **MOVEit System** group as well as the **Administrators** group. (Administrators need access to install/update the application.) It is recommended that you first install MOVEit DMZ at least once before applying these permissions. (MOVEit DMZ will set up the directory structure.) Read permissions are assigned by default; they actually include **list** and **execute** permissions.

Windows Folder	Administrators	MOVEit System
(isapiroot)	Full	Read/Execute/List
(mysqlroot)	Full	Full
(nonwebroot)	Full	Read/Execute/List
(nonwebroot)\certs	Full	<i>Full</i>
(nonwebroot)\com	(Inherit)	
(nonwebroot)\files	Full	Full

(nonwebroot)\installscripts	Full	(None)
(nonwebroot)\logs	Full	Full
(nonwebroot)\messagefiles	<i>(Inherit)</i>	
(nonwebroot)\scheduler	Full	Full
(nonwebroot)\util	Full	(None)
(program files)\moveit	Full	Read/Execute/List
(webroot)	Full	Read/Execute/List
(webroot)\bin	<i>(Inherit)</i>	
(webroot)\COM	<i>(Inherit)</i>	
(webroot)\doc	<i>(Inherit)</i>	
(webroot)\images	<i>(Inherit)</i>	
(webroot)\images\bullets	<i>(Inherit)</i>	
(webroot)\images\customscheme	<i>(Inherit)</i>	
(webroot)\images\instlogos	Full	Full
(webroot)\templates	Full	Full

If even tighter NTFS control is desired, the following changes are recommended:

- If you are using MySQL as your database engine, run MySQL under a different usercode. (By default, this is SYSTEM.) Remove permissions to the (mysqlroot) folder from MOVEit System and give them instead to the specific MySQL user.
- Adopt a policy where all appearance changes must be done by hand (rather than through the MOVEit DMZ interface). This change would allow you to propagate the security settings of (webroot)\images to all its subfolders.
- Change the usercode under which MOVEit DMZ's scheduled tasks run. (By default, this is SYSTEM.) Update the MOVEit System group with this information.
- Limit access to the (nonwebroot)\scheduler folder to only that user under which MOVEit DMZ's scheduled tasks run.

System Internals - Scheduled Tasks

Overview

MOVEit DMZ includes several applications which run periodically on the server, collectively called the **Scheduled Tasks**. These applications take care of maintaining a MOVEit DMZ system, and executing time-based actions such as delayed notifications and password expirations. The applications are run by two tasks in the **Windows Scheduled Tasks** list, which are added automatically during the MOVEit DMZ installation.

There are two groups of Scheduled Tasks, with some applications being in both groups. The first group is the **DayTime** group, which, by default, runs every 5 minutes of every day between 2AM and 12AM. Applications in this group are those which need to run throughout the day, such as for issuing delayed notifications, and cleaning up cached entries in the database. The **Windows Scheduled Tasks** entry that runs this group is called **MOVEitDayTimeTask**.

The second group is the **Nightly** group, which, by default, runs every night at 1AM. Applications in this group are mostly responsible for checking the consistency of the MOVEit DMZ system, archiving logs and secure messages, and expiring data. The **Windows Scheduled Tasks** entry that runs this group is called **MOVEitNightlyTask**.

In version 3.4 a batch file called **RunOneTask** was also introduced to allow administrators to selectively run individual tasks. More information about this utility can be found below.

Below is a list of the applications in each group.

DayTime Tasks

DeleteParmFiles

- Cleans up stale parameter files needed for communication between the MOVEit DMZ application and the MOVEitISAPI file transfer module.

EmailNotify

- Sends delayed notifications to both senders and recipients.

TableCleanup

- Deletes stale sessions and folder permissions granted to various sessions.

- Reenables users and IP addresses locked out for signon violations.

Nightly Tasks

ArchiveLog

- Archives and then deletes audit log entries from the database once they are older than the configured retention period. Stores the archives in the `/Archive/Logs` folder on the MOVEit DMZ filesystem. This task also resets tamper-evident hash chains to reflect the new start of each organization's audit logs after logs are archived/deleted.

ArchiveMessages

- Archives (optional) and then deletes package messages and attachments once they are older than the configured retention period. Stores the archives in the `/Archive/Packages` folder on the MOVEit DMZ filesystem.

ConsistencyCheck

- Makes sure records in various database tables are consistent. For example, it may check that a file, the folder that contains the file, and the user who uploaded the file all belong to the same organization.
- Makes sure database records match file system data and vice versa. In this check, each file and folder record in the database is matched up with a file and folder on the Windows file system.

If the ConsistencyCheck task finds errors, it will send a notification to the configured administrative e-mail address recommending that a DBFixup be performed to reconcile the errors. Run DBFixup from on the MOVEit DMZ console through the **Start | Programs | MOVEit DMZ** menu and it will step you through several prompts. You will need the password of the MySQL user that is used by MOVEit DMZ to access the database. This is a password that is set up at installation. For each database error, the DBFixup will either delete the offending table entry or modify it to make it consistent. For file system errors, DBFixup will delete un-matched files and folders.

Note: If MOVEit DMZ is running in a web farm environment, DBFixup can be run on any node, but only by a user who has access to the shared filesystem on the NAS backend. If DBFixup is not run by a user with the appropriate access, an error message will be displayed noting the requirement.

Note: DBFixup should be run as administrator.

In some cases, especially if there is a heavy overnight load while the consistency checker is running, it is possible to report false positives. The checker may find files that were in the process of being created, deleted, or moved at the exact time the checker ran. These errors will usually disappear the next day that the ConsistencyCheck task runs. If there is any doubt about a reported inconsistency, there is no harm in just waiting another day. The information in the notification email can also be used to research a file or folder ID through the Web interface.

CreateReports

- Executes any scheduled reports that should be run and saves the report contents to their configured locations.

DeleteParmFiles

See above.

DeletePendingUsers

- Removes deleted users from the database once they are no longer referenced by other elements.
- Expires temporary users and issues warnings about pending temporary user expirations.

EmailNotify

See above.

GarbageCollection

- Deletes old files from folders with the file cleanup option enabled.
- Marks new files as not new once they are older than the folder's configured NewTime setting.
- Deletes partial files older than 12 hours.
- Deletes old and empty subfolders from folders with the subfolder cleanup option enabled.
- Marks new secure messages as not new once they are older than the organization's configured NewTime setting.
- Deletes old, unassigned SSH keys and SSL certs from the holding tank.

PasswordAgeUsers

- Suspends users whose passwords are older than the configured password aging settings.
- Sends warning notifications to users whose passwords are within the configured password age warning settings.
- Sends notifications to interested administrators and GroupAdmins about password expirations and password warning notifications.

SyncLDAP

- Synchronizes the properties of advanced-LDAP-authenticated users on the MOVEit DMZ server with the associated user records on the LDAP server.

- Optionally adds user records for users that are found by the LDAP authentication source but do not exist yet on MOVEit DMZ.

SysCheck

- Checks on the first day of every month to see if any of the system debug levels are at or above the **Some Debug** level. If so, sends an email message to the **Send Errors To** email address(es), noting that high debug levels can impact performance.
- Checks the remaining space available on each local system drive. If any drive has less than a configurable number of megabytes remaining, sends an email message to the **Send Errors To** email address(es), noting which drives are low on space.

By default, the minimum drive space remaining value is **1024MB (1GB)**. This value can be changed through the MOVEit DMZ Config utility.

- Checks every few minutes that the machine and ISAPI URLs are still valid. The main reason that these URLs suddenly become invalid is that someone makes a security change to the IIS server and neglects to run the MOVEit DMZ Check utility to see whether their change is fatal or not. If either of these URLs time out, return a bad message or otherwise appear unhealthy, SysCheck sends an email message to the **Send Errors To** email address(es) with some suggestions to resolve the problem.
- If Content Scanning (Anti-virus and/or Data Loss Prevention) is enabled, checks every few minutes that the scan engine is available. If the scan engine is not available, sends an email message to the **Send Errors To** email address and warns that the MOVEit DMZ server will not be able to transfer files until this situation is addressed. When the scan engine becomes available again, sends an email that states that scanning is now working.

TamperCheck

- Goes through all log entries (by organization) and ensures that each organization's chain of cryptographic hashes remains intact. If any tampering is detected, a notification with an explanation and logs are sent to the **Send Errors To** email address(es).

A MOVEit DMZ Log Tamper Check link that manually starts TamperCheck (and displays running results in a command-line window) is available from the Start menu under the MOVEit DMZ program group. Any TamperCheck that ends with the phrase **Completed with errors** should be considered a failed TamperCheck; the exact reason for the failure will be explained in the log and in the notification email messages.

Logging and Error Handling

Each one of these applications writes its own log file to the common MOVEit Logs folder. (Typically, this is something like D:\moveitdmz\logs). Each run of generates a new log (subsequent runs do not append to an existing log), so old logs are automatically grandfathered so that up to 5 old copies of each scheduled application's log file are available.

Each scheduler application also writes out a log file specifically for errors that it encounters. These files will end in a .err extension, and will also be automatically grandfathered, just as the normal log files are. When no errors occur, the error log file will be empty. Otherwise, the specifics of the error encountered will be written out in the file. Also, if an error does occur, an email message will be sent to the **Send Errors To** email address configured for the system informing the recipient which host the error occurred on and which application encountered the error. The contents of the error log file will be included in the body of the email, and the appropriate normal log file for the application will also be attached to the email.

Manually Running a Single Task (RunOneTask)

The daily and nightly sets of scheduled tasks may be run manually as a set at any time through the Windows Scheduled Task interface. However, to run individual tasks within a set, you must use a batch file utility called RunOneTask, also located in your Scheduler directory.

```
D:\MOVEitDMZ\Scheduler>runonetask
```

```
Usage: RunOneTask NonWebDir moveitDSN TaskToRun
```

If you have installed MOVEit DMZ into a folder whose name uses spaces, you should use the 8.3 version of any foldernames provided to ensure RunOneTask is run properly. For example, if I have installed MOVEit DMZ into the D:\m i\mi dmz folder (instead of the usual D:\moveitdmz\midmz) then my RunOneTask command should resemble the following example.

```
D:\m i\mi dmz\Scheduler>runonetask d:\mi09f8~1\midmz~1 moveitdmz syscheck
```

```
NonWebDir=d:\mi09f8~1\midmz~1 SchedLogDir=d:\mi09f8~1\midmz~1\logs
```

```
BEGIN One Task Run of syscheck
```

```
    1 file(s) moved.
```

```
    1 file(s) moved.
```

```
END One Task Run of syscheck
```

MOVEit SysStat Service

In addition to the two groups of Scheduled Tasks, there is one more application which, while not directly scheduled, does run periodically. This is the SysStat service, which is responsible for periodically recording several performance statistics in a table in the MOVEit DMZ database. These values can be used to get a good overall picture of the health of the server.

By default, the SysStat service wakes up every 323 seconds (roughly five minutes) and records samples of the various performance statistics that it keeps track of. The default 323 second sleep period is chosen to make sure the service remains offset from the more even 5 minute schedule of the daytime scheduled tasks. Every 72 cycles, the service also does a complete check of disk utilization for each of the various MOVEit DMZ components. This operation is performed only periodically because the disk utilization values typically change far more slowly than other system performance statistics, and because the disk check takes longer to accomplish and requires more system resources than the sampling of the other statistics. Also for this reason, the SysStat service will not do a full disk utilization check on the first run after it starts up. Instead, the first disk check will be performed at a random future run, and then periodically after that.

The above configuration values are customizable, as is the length of time which the service keeps statistics in the database for (the default is 30 days). The values can be changed on the Miscellaneous tab of the **MOVEit DMZ Configuration Utility** (on page 135).

The SysStat service stores its statistics samples in the **sysstats** table in the MOVEit DMZ database. The fields available in the table are listed below, along with descriptions of their contents. Fields prefixed below with an asterisk indicate those fields which are only populated every 72 cycles by default. During off-cycles, these fields are set to 0.

- ID - Simple auto-incrementing ID number for each entry
- StatTime - Date/Time stamp indicating when the samples in the entry were recorded
- ResilNode - If the system is in a web farm DMZ cluster, this will contain the node number the samples in the entry were recorded on.
- FilesDriveRootPath - Root drive path of the MOVEit DMZ encrypted file store.
- FilesDriveSpaceFree - Number of bytes available on the drive containing the MOVEit DMZ encrypted file store.
- FilesDriveSpaceUsed - Number of bytes used on the drive containing the MOVEit DMZ encrypted file store.
- *FilesSpaceUsed - Number of bytes used by solely the MOVEit DMZ encrypted file store.
- DBDriveRootPath - Root drive path of the MOVEit DMZ MySQL database.
- DBDriveSpaceFree - Number of bytes available on the drive containing the MOVEit DMZ MySQL database.
- DBDriveSpaceUsed - Number of bytes used on the drive containing the MOVEit DMZ MySQL database.
- *DBSpaceUsed - Number of bytes used by solely the MOVEit DMZ MySQL database.
- LogsDriveRootPath - Root drive path of the MOVEit DMZ debug log store.
- LogsDriveSpaceFree - Number of bytes available on the drive containing the MOVEit DMZ debug log store.
- LogsDriveSpaceUsed - Number of bytes used on the drive containing the MOVEit DMZ debug log store.
- *LogsSpaceUsed - Number of bytes used by solely the MOVEit DMZ debug log store.
- FilesTotalDB - Number of files on the MOVEit DMZ system according to the database records.
- FilesSizeTotalDB - Total bytecount of files on the MOVEit DMZ system according to the database records.
- CPUUsagePercentTotal - Total percentage of CPU usage by all running processes.
- CPUUsagePercentDMZ - Percentage of CPU usage by the MOVEit DMZ web application (aspnet_wp).
- CPUUsagePercentISAPI - Percentage of CPU usage by the MOVEit ISAPI module. As an ISAPI module, MOVEit ISAPI is run under the DLLHOST.EXE application. The SysStats service automatically determines which running DLLHOST process is responsible for the MOVEit ISAPI module, and determines the CPU usage percentage of that process.
- CPUUsagePercentIIS - Percentage of CPU usage by the IIS webserver (inetinfo).
- CPUUsagePercentDB - Percentage of CPU usage by the MySQL database server (mysqld-nt).
- CPUUsagePercentDMZFTP - Percentage of CPU usage by the MOVEit DMZ FTP server (MIFTPSrv).

- CPUUsagePercentDMZSSH - Percentage of CPU usage by the MOVEit DMZ SSH server (MIDMZSSHSrv).
- CPUUsagePercentSched - Percentage of CPU usage by the various MOVEit DMZ scheduler applications (GarbageCollecti, EmailNotify, ArchiveLog, DeletePendingUs, PasswordAgeUser, ArchiveMessages, ConsistencyChec, DeleteParmFiles, SyncLDAP).
- CPUUsagePercentCentral - Percentage of CPU usage by the MOVEit Central application, if running (MICentral).
- MemUsedTotal - Total bytecount of memory used by all running processes.
- MemFreeTotal - Bytecount of available memory.
- MemUsedDMZ - Bytecount of memory used by the MOVEit DMZ web application.
- MemUsedISAPI - Bytecount of memory used by the MOVEit ISAPI module.
- MemUsedIIS - Bytecount of memory used by the IIS webserver.
- MemUsedDB - Bytecount of memory used by the MySQL database server.
- MemUsedDMZFTP - Bytecount of memory used by the MOVEit DMZ FTP server.
- MemUsedDMZSSH - Bytecount of memory used by the MOVEit DMZ SSH server.
- MemUsedSched - Bytecount of memory used by the various MOVEit DMZ scheduler applications.
- MemUsedCentral - Bytecount of memory used by the MOVEit Central application, if installed.
- VMSizeDMZ - Bytecount of virtual memory used by the MOVEit DMZ web application.
- VMSizeISAPI - Bytecount of virtual memory used by the MOVEit ISAPI module.
- VMSizeIIS - Bytecount of virtual memory used by the IIS webserver.
- VMSizeDB - Bytecount of virtual memory used by the MySQL database server.
- VMSizeDMZFTP - Bytecount of virtual memory used by the MOVEit DMZ FTP server.
- VMSizeDMZSSH - Bytecount of virtual memory used by the MOVEit DMZ SSH server.
- VMSizeSched - Bytecount of virtual memory used by the various MOVEit DMZ scheduler applications.
- VMSizeCentral - Bytecount of virtual memory used by the MOVEit Central application, if installed.
- HandlesTotal - Total count of handles open by all running processes.
- HandlesDMZ - Count of handles open by the MOVEit DMZ web application.
- HandlesISAPI - Count of handles open by the MOVEit ISAPI module.
- HandlesIIS - Count of handles open by the IIS webserver.
- HandlesDB - Count of handles open by the MySQL database server.
- HandlesDMZFTP - Count of handles open by the MOVEit DMZ FTP server.
- HandlesDMZSSH - Count of handles open by the MOVEit DMZ SSH server.
- HandlesSched - Count of handles open by the various MOVEit DMZ scheduler applications.
- HandlesCentral - Count of handles open by the MOVEit Central application, if installed.
- ProcessesTotal - Total count of running processes.
- ThreadsTotal - Total count of running threads by all running processes.

- **ThreadsDMZ** - Count of running threads owned by the MOVEit DMZ web application.
- **ThreadsISAPI** - Count of running threads owned by the MOVEit ISAPI module.
- **ThreadsIIS** - Count of running threads owned by the IIS webserver.
- **ThreadsDB** - Count of running threads owned by the MySQL database server.
- **ThreadsDMZFTP** - Count of running threads owned by the MOVEit DMZ FTP server.
- **ThreadsDMZSSH** - Count of running threads owned by the MOVEit DMZ SSH server.
- **ThreadsSched** - Count of running threads owned by the various MOVEit DMZ scheduler applications.
- **ThreadsCentral** - Count of running threads owned by the MOVEit Central application, if installed.
- **SessionsTotal** - Total ASP.NET sessions registered with MOVEit DMZ.
- **SessionsActive** - Total active (touched within last 5 minutes) ASP.NET sessions registered with MOVEit DMZ.

If serious errors occur during a statistics gathering cycle, SysStat will report them by sending an email message to the **Send Errors To** email address configured on the system, as well as by logging the errors in the **Windows Application Event Log**. In most cases, SysStat will record the information it was able to gather and continue its work. If SysStat is unable to gather information on a particular field, it will typically record a value of 0 or -1 for that field. The value -1 indicates an unknown error occurred. The value 0 is used in the case of a known error occurring (most often a process that SysStat is gathering information on is not running). Note that a value of 0 for a field does NOT always imply that an error occurred (CPUUsagePercent is often 0 for processes that are running but not doing anything).

A value of -1 is also recorded in certain database- and filesystem-related fields when the database and/or filesystem is remote. This is usually the case when MOVEit DMZ is in a webfarm configuration. Additionally, database performance statistics will only be recorded for a local MySQL database; local and remote SQL Server databases will not be queried for performance statistics.

MOVEit DMZ Helper Service

The MOVEit DMZ Helper service performs a number of utility functions for other MOVEit DMZ services.

- **CA and Client Certificate Management** - The web interface services (IIS, etc.) do not run with sufficient privileges to directly alter the Microsoft Certificate Store. The MOVEit DMZ Helper service allows the web interface to indirectly create, import and delete certificates from the store.

System Internals - Technical Reference

This technical document describes the file structure, registry entries and other details of the MOVEit DMZ system. Generally this information is only important for administrators (i.e., SysAdmins) who set up and troubleshoot MOVEit DMZ systems.

Note: Location names like [Web Files] are used only as a notation in this document; they do not refer to literal directory names or registry key names on a MOVEit system.

File System

[Non-Web Files]

By default, the [Non-Web Files] directory is D:\MOVEitDMZ. This value is configurable during installation and may be changed by advanced administrators using the MOVEit DMZ Config program.

- **\Aspell** - Contains the GNU Aspell spell-checking utility used by MOVEit DMZ's secure messaging spell-checking mechanism
 - **\bin** - Contains the Aspell executable and associated libraries as well as the source text files for the custom word lists included with MOVEit DMZ and the batch files used to compile them
 - **\data** - Data files used by Aspell
 - **\dict** - Compiled dictionary files, alias files, and .multi dictionary loading command files used by Aspell
- **\Certs** - Used to communicate certificates between the MOVEit DMZ web application (which does not have permission to directly alter the Microsoft Certificate Store) and the MOVEit DMZ Helper service (which can and does). In standalone systems, a single C000 subfolder will be found here
- **\COM** - Holds several COM object library files
- **\Files** - Root filesystem of DMZ. This is where DMZ's files are actually stored
 - **\Files\{OrgID}** - Root filesystem of a single Organization
 - **\Files\{OrgID}\{FolderID}** - Contains encrypted files belonging to a specific folder
- **\InstallScripts** - Various scripts used by the MOVEit DMZ install packages
- **\Logs** - Debug log files generated by MOVEit DMZ applications
- **\MessageFiles** - International message files for use by VB and C programs
- **\Scheduler** - Various scripts used by the MOVEit DMZ scheduler
- **\Util** - Various utilities for use by administrators and MOVEit DMZ install packages
 - **\Codecs** - Codec libraries used by the 7-Zip application
 - **\Formats** - Format libraries used by the 7-Zip application

- `passdict.txt` - A cleartext, text file containing a list of dictionary words which are not allowed to be part of any password used in Organizations with a password complexity of Sturdy or higher. Each word or phrase is on its own line; entries are case-insensitive

[Web Files]

The [Web Files] directory is configurable during installation and may be changed by advanced administrators using the MOVEit DMZ Config program.

- `\bin` - Holds MOVEit DMZ library files
- `\COM` - Store of web-browser ActiveX controls
 - `MOVEitUploadWizardxxx.ocx` - MOVEitWizard high speed upload control
- `\images` - Images used to display MOVEit DMZ web interface
 - `\bullets` - Stock bullets used when customizing organization appearance
 - `\customscheme` - Custom background images used in custom schemes (style sheets)
 - `\en` - English versions of text-based button images
 - `\xx` - Versions of text-based button images for language code xx
 - `\InstLogos` - Organization-specific logos and buttons
- `\java` - Store of web-browser Java applets
 - `MOVEitWizard.jar` - MOVEit Wizard Java applet store
- `\templates` - XSL templates, CSS stylesheets and Javascript used to format information for web interface display
 - `\en` - English versions of the internationalized XSL templates
 - `\xx` - Versions of the internationalized XSL templates for language code xx

- **AS2Rec2.ashx** - Used to receive AS2 transmissions (file messages and MDNs) and store them in the MOVEit DMZ filesystem
- **apilink.aspx** - This file does not actually exist in the web files directory. Instead, it is a trigger which is looked for by the MOVEit DMZ application to indicate that an instance of MOVEit DMZ API wishes to transfer its existing session to a user's browser.
- **ColorSchemePreview.aspx** - Used by Administrators to preview alternate color schemes.
- **DMZTest.aspx** - A very simple ASP.NET test application which simply prints the current date. Useful for making sure the .NET framework is installed correctly.
- **DownloadFile.aspx** - Used by all web users to retrieve files from MOVEit DMZ.
- **DownloadReport.aspx** - Used by administrators to download reports directly from MOVEit DMZ.
- **favicon.ico** - Icon file displayed by most browsers in the URL bar, tabbed browsers and lists of favorites.
- **Human.aspx** - The web interface.
- **Machine.aspx** - Used by various MOVEit clients and modules to communicate with MOVEit DMZ.
- **Machine2.aspx** - Used internally by various MOVEit components to manage high speed file transfers.
- **palette.htm** - Static HTML page used to display a color palette for composing secure messages.
- **SpellCheck.aspx** - Used to perform secure messaging spelling checks.
- **SysStat.aspx** - Early display of system statistics. Not currently used.
- **TestSettings.aspx** - Used by MOVEit DMZ to test various settings, such as External Authentication sources.
- **ThinPoll.aspx** - Provides quick idea of whether or not a particular user has new files. Not currently used.
- **ViewFile.aspx** - Used by MOVEit DMZ to display thumbnails and full size images stored in the encrypted file store.
- **ViewGraph.aspx** - Used by MOVEit DMZ to generate graph images for the Quick Statistics page.
- **WebPost.aspx** - Used by web form submitters to send data into MOVEitDMZ.
- **web.config** - .NET configuration file for the MOVEitDMZ application.

[ISAPI Files]

The [ISAPI Files] directory is configurable during installation and may be changed by advanced administrators using the MOVEit DMZ Config program.

- **MOVEitISAPI.dll** - The MOVEitDMZ ISAPI filter used to handle high speed web transfers.
- **MOVEitFilt.dll** - The MOVEitDMZ ISAPI filter used to get around bugs in various browsers that do not recognize certain suggested filename headers. This filter handles file downloads so that browsers display correct filenames when prompting to save.

[Database Files] (only if MySQL is the database engine)

If you are using MySQL as your database engine, the [Database Files] directory is configurable during installation and may be changed by advanced administrators using the MOVEit DMZ Config program. If the location of the MySQL data files is changed, this change will also need to be reflected in the MY.INI file. By default, it is D:\MySQL.

- **Bin** - Location of MySQL server and client executables, as well as supporting libraries.
- **Data** - Location of database data file folders and MySQL error file.
 - **moveitdmz** - Location of MOVEit DMZ database files. Note that this directory may not be named moveitdmz. This folder's name will be that of the MOVEit DMZ database given during installation. The default is moveitdmz.
 - **mysql** - Location of MySQL database files, which contain database user information as well as access lists.

- **Share** - Contains language support files for MySQL database server.
- **[HOSTNAME].err** - A running log file containing any significant events that have happened to the database server. Will include error information, such as located and repaired table corruption messages, as well as non-error information, such as startup and shutdown times.
- **%WINDIR%\MY.INI** - This file does not reside in the [Database Files] directory, but instead can be found in the main Windows directory (usually C:\WINDOWS). This file contains paths and options for the MySQL server, most importantly the path to the data files. If the [Database Files] directory is changed, this file should also be changed.

Registry Entries

MOVEit DMZ uses the following base key in the registry:

For 64-bit systems: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Standard Networks\siLock

For 32-bit systems: HKEY_LOCAL_MACHINE\SOFTWARE\Standard Networks\siLock

[Root Key]

- **AllowInsecureQueryStrings** - Security best practices call for using the POST method instead of the GET method. If your web integration uses HTTP GET, and you want to continue to use the GET method, you need to set this registry entry to allow the continued use of this method. Set to "1" to allow GET requests for sensitive transactions, and allow GET requests to include session IDs in apilink.aspx.
- **CacheFlushIntervalMB** - The interval in MB for how frequently to flush the Windows file cache buffer to disk during file uploads (Default = 0). If CacheFlushIntervalMB doesn't exist or is 0, the cache buffer is flushed at the end of the upload, which is the standard behavior. For large file uploads, this can potentially cause client timeouts while waiting for the entire cache buffer to be flushed, especially if the target file system isn't local. Configure this setting to have MOVEit DMZ periodically flush the Windows file cache buffer in order to avoid doing one large cache flush at the end of the upload.
- **DBEngine** - The database engine being used by MOVEit DMZ. Either MySQL or SQL Server. If the value is not present, MySQL is assumed.
- **DSN** - The ODBC Data Source Name of the MOVEit DMZ database. (By default: moveitdmz)
- **EmailAddrAutomation** - The email address from which MOVEit DMZ's automatically generated email messages will appear to originate.
- **EmailAddrForErrors** - The email address to which significant MOVEit DMZ errors will be sent.
- **EmailRelayChoice** - Used by the MOVEit DMZ Check utility to store which type of email relay check should be performed.
- **EmailRelayCustomEmailAddr** - Used by the MOVEit DMZ Check utility to store the email address to be used if using an email relay check that goes to an alternate address.

- **EmailServer** - The SMTP server through which email messages will be sent.
- **EmailServerConnectionTimeout** - The number of seconds MOVEit DMZ will wait before timing out when it cannot connect to the configured SMTP server (Default = 30). This key will not be created by the program itself, and is only used to override the internal default value of the program.
- **FilesBaseDir** - The real location of root filesystem of DMZ, usually [Non-Web Files]\Files.
- **FilesBaseDirPassword** - An encrypted copy of the password used to access a remote filesystem, if one is being used as FilesBaseDir.
- **FilesBaseDirUsername** - The username used to access a remote filesystem, if one is being used as FilesBaseDir.
- **ForceFileSystemAS2MDN** - Typically, using the file system to manage synchronous AS2 MDNs is only necessary when MOVEit DMZ is part of a WebFarm system. Enabling this option will force MOVEit DMZ to ALWAYS use the file system for managing synchronous AS2 MDNs. This may be desirable in certain situations, for instance when a standalone MOVEit DMZ installation uses advanced IIS related configurations. (0=no, 1=yes)
- **ForceMachine2** - Whether MOVEitISAPI should always use the traditional machine2.aspx approach to accessing the database. You may wish to set this obscure option if you are having difficulty with the optimizations in MOVEitISAPI that bypass machine2 in favor of direct database access. (0=no [the default], 1=yes)
- **IPLockoutEnable** - Whether or not IP Lockout is enabled. (0=no, 1=yes)
- **IPLockoutExpireTime** - How many minutes IPs will be locked out before they are automatically reenabled.
- **IPLockoutNumber** - How many login failures must occur in X minutes to lock out a single IP. (Default = 15)
- **IPLockoutTime** - In how much time X login failures must occur to lock out a single IP. (Default = 5)
- **ISAPIDir** - The real location of [ISAPI Files].
- **LangSiteDefault** - Default language to use for the system.
- **LangsSiteAllowed** - A comma-delimited list of language codes available to the organizations on the system. Set by the system administrator.
- **LicenseKey** - The MOVEit DMZ license key
- **LogAuditEventSource** - Which Windows Event Log entries are written to and with what name. (MOVEit_DMZ_Audit = MOVEit Event Log; MOVEit DMZ Audit or missing = Application Event Log)
- **LogAuditSyslogFacility** - Which facility to be used when logging audit entries to a remote Syslog server. (Default = FTP)
- **LogAuditSyslogHost** - The host name or IP address of the remote Syslog server to send audit entries to.
- **LogAuditSyslogPort** - Which port to be used when logging audit entries to a remote Syslog server. (Default = 514)
- **LogAuditToEventLog** - Whether or not audit log entries are also sent to the Windows Event Log. (0=no, 1=yes)

- **LogAuditToSyslog** - Whether or not audit log entries are also sent to a remote Syslog server. (0=no, 1=yes)
- **LongTermCookieDuration** - A duration code determining how long the long term cookies will be set to last. Format is a number and a duration letter (s = seconds, n = minutes, h = hours, d = days, m = months, y = years). For example, 15n would indicate 15 minutes, 6m would indicate 6 months, and 2y would indicate 2 years. (Default = 2y)
- **MaxSessionTimeoutMinutes** - The number of minutes the session timeout will be extended to for HTTP and HTTPS file transfers (Default = 120)
- **MetaRefreshEnabled** - Whether or not pages will include a meta refresh tag to force a refresh after the session has timed out. (0=no, 1=yes)
- **MinWizVersion** - Minimum version of ActiveX Wizard this server supports.
- **MultipleWebsites** - Retired option used by MOVEit DMZ 3.2-3.4.1 to determine whether or not multiple websites point to the same copy of MOVEit DMZ. (0=no, 1=yes) In versions 3.4.2+ of MOVEit DMZ, this option should always be set to 0 for best performance. (Multiple web sites are handled automatically through different IIS session handling.)
- **MySQLDir** - The location of the MySQL database installation (Default = c:\mysql). Used only if MySQL is being used as the database engine.
- **MySQLMoveitPW** - An encrypted copy of the DMZ MySQL user password. Used only if MySQL is being used as the database engine.
- **MySQLRootPW** - An encrypted copy of the root MySQL password. Used only if MySQL is being used as the database engine.
- **NonWebBaseDir** - The real location of [Non-Web Files].
- **NoWiz** - Bit field indicating the enabled/disabled status of the various MOVEit Wizard objects. When the first bit is enabled ($\text{NoWiz} \& 1 > 0$) the ActiveX wizard will not be loaded. When the second bit is enabled ($\text{NoWiz} \& 2 > 0$) the Java wizard will not be loaded.
- **NoXSLObjectCache** - An optional key which when set to 1 will cause MOVEit DMZ to not use its internal XSL template cache. In this case, each template will be loaded from disk every time it is used. This is useful for development environments where templates are being modified frequently, but should not be present on production systems.
- **ShowSystemErrorMessages** - Whether or not system error messages will be shown to users who run across them. (0=no, 1=yes)
- **SSLCipherSuites** - A list of all ciphers suites available system-wide for use with SSL (including both HTTPS and FTPS), in order of preference, with the enabled/disabled status of each. Note: This list is maintained only for convenience and replication purposes. The actual settings are controlled via Windows API functions. Thus, changing this setting directly in the registry will NOT change the system's SSL settings.

- **SSLVersions** - A list of the SSL and TLS versions enabled for use by all SCHANNEL-based servers on this system. Note: This list is maintained only for convenience and replication purposes. The actual settings are controlled via registry keys in HKLM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols. Thus, changing this setting directly in the registry will NOT change the system's SSL version settings.
- **SuppressHashing** - Whether to suppress adding a tampercheck hash to each log record. (0=no, 1=yes). By default, this value is not present; it defaults to 0. Setting this value to 1 increases performance, at the cost of security. If hashing is suppressed, tampering of the database will not be detected.
- **SysCheckMinDiskSpaceMB** - The minimum number of megabytes the local drives on the server must have before the SysCheck application will begin sending notifications to the system errors email address (Default = 1024 (1GB)). This key will not be created by the program itself, and is only used to override the internal default value of the program.
- **SysStatsOldDays** - The number of days worth of data the system statistics service should keep in the database (Default = 30). This key will not be created by the program itself, and is only used to override the internal default value of the program.
- **SysStatsSkipByteCountEvery** - The number of cycles the system statistics service will skip between per-file folder size checks. These checks take time, so they are not executed every cycle (Default = 72). This key will not be created by the program itself, and is only used to override the internal default value of the program.
- **SysStatsSleepTime** - The number of seconds the system statistics service will sleep between cycles (Default = 323). This key will not be created by the program itself, and is only used to override the internal default value of the program.
- **Update** - An incrementing counter used to determine when registry changes have been made and need to be propagated.
- **URLHuman** - The URL users SHOULD use to access this site. This value is to compose [click here](https://moveit.myhost.com) links back to the MOVEit DMZ web interface. (Generally should be similar to <https://moveit.myhost.com>.)
- **URLMachine** - The URL of machine.aspx. (Should be identical to URLMachine2, but missing the 2.)
- **URLMachine2** - The URL of machine2.aspx. (Should be identical to URLMachine, plus the 2.)
- **WebBaseDir** - The real location of [Web Files].
- **WebNum** - The IIS Website number of the DMZ website.
- **\Farm**
 - **Appnode** - Indicates the unique identifier (1, 2, 3, etc) of the current node.
- **\I18N**
 - **\DMZB**
 - **IDFile** - Path to the VB message ID file
 - **MsgFilePrefix** - Full path prefix for VB message files
 - **\DMZC**

- IDFile - Path to the C message ID file
 - MsgFilePrefix - Full path prefix for C message files
- \Institutions
 - \[OrgID]
 - Key - The AES-encrypted Organizational passphrase
- MySQL - This key contains database access settings for the MySQL database. These values are only used when MySQL is the database engine being used by MOVEit DMZ.
 - Database - Name of the MySQL database.
 - OptionA - Primary MySQL database connection string.
 - OptionB - First backup MySQL database connection string.
 - OptionC - Second backup MySQL database connection string.
 - OptionN - Non-pooled MySQL database connection string.
 - Password - Encrypted copy of the password used to access the MySQL database.
 - RetryConnectCount - Number of times to retry failed database connections (default 1).
 - RetryConnectSleep - Number of milliseconds to wait between retry attempts (default 750).
 - Server - Hostname or IP address of the MySQL database.
 - User - Username used to access the MySQL database.
- \SNICOMLog
 - AlwaysFlush - When set to 1, every debug message will be written to disk as soon as it comes in. This can slow down the debug log writing process, but can be helpful when you want to see the latest debug entries as soon as they come in.
 - Debug - Current debug level (0-60)
 - LogFile - Current log file location (Default: [Non-Web Files]\Logs\MOVEit.Log)
 - MaxLogFileSize - The value of the maximum size of the debug log file. When the debug log file exceeds this value, a new one will be started and the old one will be renamed from *.Log to *.OL1.
- \SNICOMUtil
 - IPMasksToIgnoreDNS - A comma-separated list of IP addresses for which no attempts to look up DNS entries should be made. (Wildcards are allowed.) Use to optimize speed in environments where no internal DNS exists.
- \siLockFTPServer
 - AllowCCC - Whether CCC transfer mode is enabled on the FTP server. (0=no, 1=yes)
 - AllowNonSecure - Whether non-secure FTP sessions will be accepted by the FTP server. (0=no, 1=yes)
 - CertImplicitPort - The port number used by a implicit control port that requires client certificates.
 - CertIssuer - Issuer of the certificate being used by the FTP server.

- **CertPort** - The port number used by a explicit control port that requires client certificates.
- **CertSerial** - The serial number of the certificate being used by the FTP server.
- **ConnectionLimit** - Maximum number of connected FTP sessions (Default 32).
- **IdleTimeout** - Number of seconds after which an idle FTP session will be disconnected. (the FTP server only checks for idle connections every 30 seconds)
- **IgnoreCertProbs** - When set to 1, the FTP server (and SSH server) will ignore certificate problems when communicating with the MOVEit DMZ server. (useful when a test certificate is currently being used)
- **LocalPort** - The value of the port to listen on for standard FTP active data connections (Default 0x14, decimal 20)
- **LogMessages** - When set to 1, debug messages will be logged to the file specified in the **MsgLogFilename** key.
- **MaxLogSize** - The value of the maximum size of the debug log file. When the debug log file exceeds this value, a new one will be started and the old one will be renamed from *.log to *.old.
- **MoreCerts** - List of addition certificate-to-IPAddress mappings. Each mapping is of the format IPMask,CertSerial,CertIssuer. Mappings are separated by the pipe character |.
- **MsgLevel** - The value of the current debugging level (Default 0x2, decimal 2)
- **MsgLogFilename** - The location of the FTP server debug log file (Default c:\moveitdmz\logs\moveitdmzftp.log).
- **NATMappings** - List of NAT address mappings. Each mapping is of the format IPMask,IPMapTo. Mappings are separated by the pipe character |.
- **NonSecureIPs** - List of IP addresses allowed to do non-secure FTP to the FTP server.
- **PassivePortHigh** - The value of the highest port in a specified passive port range (Default 0x1388, decimal 5000)
- **PassivePortLow** - The value of the lowest port in a specified passive port range (Default 0x400, decimal 1024)
- **Port** - The value of the port to listen on for standard (explicit) FTP control connections (Default 0x15, decimal 21)
- **RequireClientCert** - This registry key is ignored. It is used to turn on the **require client certs on all FTP connections** feature, but that feature since been replaced with one that allows you to support clientcert and non-clientcert connections at the same time on different ports.
- **RequirePassive** - When set to 1, only passive data connections will be accepted.
- **RestrictedBindIP** - IP address for the FTP server to bind to. If blank or non-existent, FTP server will bind to all IP addresses on the server.
- **RestrictPassivePortRange** - When set to 1, the FTP server will only use ports in the range specified by the **PassivePortLow** and **PassivePortHigh** keys.

- **SecurePort** - The value of the port to listen on for implicit secure FTP control connections (Default 0x3DE, decimal 990)
- **StoreLocation** - Location of the certificate store where the certificate being used by the FTP server is located.
- **StoreName** - Name of the certificate store where the certificate being used by the FTP server is located.
- **Update** - An auto-incrementing number which the FTP server uses to determine if other registry entries have been updated.
- **\SQLServer** - This key contains database access settings for the SQL Server database. These values are only used when SQL Server is the database engine being used by MOVEit DMZ.
 - **Database** - Name of the SQL Server database.
 - **OptionA** - Primary SQL Server database connection string.
 - **OptionB** - First backup SQL Server database connection string.
 - **OptionC** - Second backup SQL Server database connection string.
 - **OptionN** - Non-pooled SQL Server database connection string.
 - **Password** - Encrypted copy of the password used to access the SQL Server database.
 - **RetryConnectCount** - Number of times to retry failed database connections (default 1).
 - **RetryConnectSleep** - Number of milliseconds to wait between retry attempts (default 750).
 - **Server** - Hostname or IP address of the SQL Server database.
 - **User** - Username used to access the SQL Server database.
- **\SSHServer**
 - **IdleTimeoutSecs** - Number of seconds after which an idle SFTP session will be disconnected; defaults to 600. Note: Independent of this setting, the SFTP server sends SSH keepalive messages if the session is idle for more than 30 seconds. If the client does not respond, the session is disconnected even if it has not been idle for IdleTimeoutSecs seconds.
 - **LogMessages** - When set to 1, debug messages will be logged to the file specified in the MsgLogFilename key.
 - **MaxLogSize** - The value of the maximum size of the debug log file. When the debug log file exceeds this value, a new one will be started and the old one will be renamed from *.log to *.old.
 - **MsgLevel** - The value of the current debugging level (Default 0x2, decimal 2)
 - **MsgLogFilename** - The location of the SSH server debug log file (Default c:\moveitdmz\logs\midmzssh.log).
 - **Port** - The value of the port to listen on for SSH connections (Default 0x16, decimal 22)
 - **PrivKey** - The (encrypted) private server key generated by the SSH server to be used for server identification.
 - **RestrictedBindIP** - IP address for the SSH server to bind to. If blank or non-existent, SSH server will bind to all IP addresses on the server.

- **Update** - An auto-incrementing number which the SSH server uses to determine if other registry entries have been updated.

Cookies

MOVEit DMZ sends the following cookies to web client browsers. Cookies marked Session are deleted when the browser is closed. Those marked Persistent will be saved between browser restarts, unless the browser is configured otherwise.

- **ASP.NET_SessionId** (Session) - The ASP.NET session identifier cookie. This is set by the ASP.NET environment and links the request to an existing session. For security reasons, this cookie will be marked as Secure when the current MOVEit DMZ organization is configured to require secure connections. This means the cookie will not be sent if the browser manages to access MOVEit DMZ via a non-secure page.
- **DesignModeTest** (Session) - Indicates whether the browser supports Design Mode for iframes. Used to determine whether to display the WYSIWYG secure message editor.
- **DMZCookieTest** (Session) - Indicates whether the browser supports cookies. If the user arrives from the signon screen without this cookie present, it generally means the browser does not support cookies, and an error message to that effect will be displayed.
- **FileListSortField** (Persistent) - Stores the user's file list sort field preference for ordinary MOVEit DMZ folders.
- **FileListSortOrder** (Persistent) - Stores the user's file list sort order preference for ordinary MOVEit DMZ folders.
- **InitialPage** (Persistent) - Stores the initial page the user should be directed to. Currently only set after a successful use of the automatic client certificate-based login page.
- **JavascriptTest** (Session) - Indicates whether the browser supports javascript. Used to determine whether to display certain portions of the MOVEit DMZ interface that require javascript, such as the MOVEit Wizard and the WYSIWYG secure message editor.
- **LongTermCookieExpireDate** (Session) - Indicates the computed persistent cookie expiration date based on the current date and the current configured persistent cookie expiration period. Used by some javascript code when writing out persistent cookies to the browser.
- **MessageListSortField** (Persistent) - Stores the user's message list sort field preference for MOVEit DMZ secure message mailboxes.
- **MessageListSortOrder** (Persistent) - Stores the user's message list sort order preference for MOVEit DMZ secure message mailboxes.
- **MIDMZLang** (Persistent) - Stores the language code of the most recently viewed language interface on the MOVEit DMZ server. Used to determine what language to display the initial signon screen in.
- **NoWiz** (Session) - Indicates which MOVEit Wizard applications are available for use. Used by some javascript code to determine which MOVEit Wizard interface portions to display.
- **siLockLongTermInstID** (Persistent) - Stores the ID of the most recently visited organization on the MOVEit DMZ server. Used to determine which organization's interface to display when the user arrives at the signon screen.

- **WebPostFileListSortField** (Persistent) - Stores the user's file list sort field preferences for MOVEit DMZ webpost folders.
- **WebPostFileListSortOrder** (Persistent) - Stores the user's file list sort order preferences for MOVEit DMZ webpost folders.
- **WizardVersions** (Session) - Indicates which versions of the ActiveX-based MOVEit Wizard application are available for use. Used by some javascript code to determine when to prompt the user to upgrade their current MOVEit Wizard object.
- **WizPrefPerm** (Persistent) - Stores the user's persistent MOVEit ActiveX Wizard preference - whether to use it or not.
- **WizPrefPermJava** (Persistent) - Stores the user's persistent MOVEit Java Wizard preference - whether to use it or not.
- **WizPrefSess** (Session) - Stores the user's single-session MOVEit ActiveX Wizard preference - whether to use it for this session or not.
- **WizPrefSessJava** (Session) - Stores the user's single-session MOVEit Java Wizard preference - whether to use it for this session or not.

Services

MOVEit DMZ services can be stopped and started by using the Windows Services program, or by using the DMZ Config program.

- **MOVEit DMZ FTP** - Provides secure FTP access to MOVEit DMZ files.
- **MOVEit DMZ Helper** - Helper for MOVEit DMZ web server nodes, providing miscellaneous functions.
- **MOVEit DMZ High Availability** - Provides high availability functions for MOVEit DMZ, such as stopping services when there is an error.
- **MOVEit DMZ SSH** - Provides secure SSH access to MOVEit DMZ files.
- **MOVEit SysStat** - Periodically gathers performance statistics about this server and the MOVEit products running on it.
- **MOVEit DMZ database** - the database server can be either MySQL or Microsoft SQL Server.

System Internals - Templates and Icons

Some SysAdmins would like to alter not only the custom banners, logos and stylesheets, but XSL templates and the stock icons used to display items such as users and groups. Changes to XSL templates can be placed in special custom folders which will take precedence over stock templates, but not be overwritten by upgrades. Custom templates can even be placed such that they are only used for specific organizations on the system. Changes to icons still affect the entire site, and will likely be overwritten during upgrades, so administrators will need to maintain a copy of any custom icons used, and be sure to re-apply them after upgrades.

Editing Stock Icons

Stock icons are stored in several locations.

Favorite Icon

MOVEit DMZ's favorite icon is used to display a pretty green icon next to the URL in the URL/Location bar, in tabbed browser windows and lists of favorites/shortcuts/bookmarks. This feature has been a part of MOVEit DMZ since version 2.3, but was enhanced in version 4.0 to take advantage of recent improvements in favorite icon display in IE 7.0.

- `\favicon.ico` - ICON format icon.

Images Folder

The main location of stock images. DO NOT change `null.gif` under any circumstances.

- `\images`

International Images Folders

While language-independent images are stored in the main Images Folder, language-dependant images (mostly button images that display text) are stored in subfolders of the main folder, each named with the language code it represents (en for English, fr for French, etc).

- `\images\en`
- `\images\fr`
- `\images\es`

Conventions:

- The phrase **icon** at the beginning of an image name often indicates that the icon is NON-clickable. (e.g., the face used to indicate a user).
- The phrase **imgbut** at the beginning of an image name often indicates that the icon IS clickable. (e.g., the white **find file** button).
- Icons with number 1 at the end are typically the small (12x12) version.
- Icons with number 2 at the end are typically the large (24x24) version.

Stock Bullets

- `\images\bullets`

Note that changing any of the stock bullets selections WILL NOT change bullets already selected.

Default Organization Logo and Bullet

Making changes to these images (also possible by changing the branding of Org#0 online) will change the default banner and bullet used by each new organization.

- `\images\InstLogos\bullet_0.gif`
- `\images\InstLogos\logobig_0.gif`

Editing Stock Templates

XSL templates are stored in the **templates** subdirectory of your **WebRoot** directory, in subfolders corresponding to the language of the template:

- `(WebRoot)\templates\en`
- `(WebRoot)\templates\fr`
- `(WebRoot)\templates\es`

DO NOT CHANGE THE TEMPLATES IN THESE FOLDERS! Any changes you make to these folders will be overwritten during the next MOVEit DMZ upgrade.

Instead, make sure a subfolder called **custom** exists and copy the template you would like to change into the **custom** folder. Templates in the **custom** folder override the default templates and will persist through future MOVEit DMZ upgrades. Be sure to test custom templates on a development system first before deploying them to a production server.

To change a template for all organizations:

- 1 Create a `templates\en` subfolder named **custom** if one does not already exist.
- 2 Copy the template you would like to change into the `templates\en\custom` subfolder if it does not already exist there.
- 3 Make changes to the `templates\en\custom` version of the template as desired.

To change a template for a particular organization:

- 1 Create a `templates\en` subfolder named `custom` if one does not already exist.
- 2 Create a `templates\en\custom` subfolder named after the ID of the particular organization if one does not already exist. (For example, if the Contractor organization has an ID of 1234, create a subfolder named 1234.)
- 3 Copy the template you would like to change into the `templates\en\custom\[OrgID]` subfolder if it does not already exist there.
- 4 Make changes to the `templates\en\custom\[OrgID]` version of the template as desired.

To test changed templates:

After a custom template has been modified, the webserver will need to be restarted to clear MOVEit DMZ's template cache. Otherwise, the changes made to your template will not be visible. To restart the webserver, log on as an administrator to the Windows server hosting MOVEit DMZ and run the `iisreset` command from a command-prompt.

However, it is possible to disable MOVEit DMZ's template cache by using the `NoXSLObjectCache` registry entry. See ***Advanced Topics - System Internals - Technical Reference*** (on page 764) for more information. Once the template cache has been disabled, it is no longer necessary to restart the IIS website, but the web interface will be slower. (The `NoXSLObjectCache` registry option should not be left on in production.)

To find the correct template:

The fastest way to find the correct template to edit is to find a key phrase on the template you want to change (e.g., Sign On) and search for that phrase in the *.xsl files in the various MOVEit templates folders. A complete list of templates and a short description of their use can be found in the online template folders in a file called `dmz_templates.txt`.

MOVEit DMZ also uses a master page template called `humanmain.xsl` that allows administrators to change the page title, change the favorite icon, import custom stylesheets, use custom refresh scripting, change the master table spacing, style or IDs, add custom headers and footers or perform other powerful formatting operations.

System Internals - Timeouts

Network-aware programs must deal with the case where the remote side has not responded to a message after a certain amount of time. Timeout is the term used to describe how much time a program will wait before giving up. While MOVEit DMZ allows some of its timeouts to be configured, others are fixed values. This document details some of the most commonly encountered MOVEit DMZ timeouts.

Web Interface and HTTPS Machine Interface

MOVEit DMZ's user-friendly web interface and its HTTPS machine interface (used by MOVEit Central, MOVEit DMZ API, MOVEit EZ, MOVEit Xfer, etc.) both use the same session timeout.

The value of this timeout can be changed by a Microsoft .NET configuration file called `Web.config`, which is located in the webroot of the MOVEitDMZ website (e.g. `C:\MOVEitDMZ\wwwroot`). Using Notepad or any other text editor, set the `timeout` attribute of the `sessionState` node in this file to set the timeout. This timeout is expressed in minutes. The default value is 20 minutes.

```
<sessionState mode="InProc" stateConnectionString="tcpip=127.0.0.1:42424"
sqlConnectionString="data source=127.0.0.1;user id=sa;password="
cookieless="false" timeout="20" />
```

You will not need to restart the server or any services after making a change to this value. The new value will apply to any new sessions.

MOVEit DMZ file transfer operations will automatically change the session timeout or individual sessions to a longer value during transfers to allow slow transfers to complete. The session timeout is reset to the shorter value (by default, 20 minutes) when a transfer is complete. The length of the long timeout can be configured the `MaxSessionTimeoutMinutes` registry key. Consult the *Technical Reference* (on page 764) for more information.

FTP Interface

One FTP timeout exposed to administrators is a value which allows them to control how long to wait for additional FTP commands from a still-connected-but-inactive FTP control connection before disconnecting. This timeout is expressed in seconds. The default value is 600 seconds.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Standard
Networks\siLock\siLockFTPServer\IdleTimeout
```

You will not need to restart the server or any services after making a change to this value. The new value will apply to any new sessions.

Email Client

The timeout used by the client that sends all of MOVEit DMZ's notifications is available in the MOVEit DMZ Config utility. By default, the email timeout is 30 seconds.

If you encounter ANY sort of timeout issues on a regular basis, we recommended you ***enable the local SMTP server*** (on page 712) and use it as queue and buffer against transient mail delivery problems.

RADIUS and LDAP Clients

These timeouts are configurable by administrators from the Web Interface. See the related RADIUS and LDAP sections for complete information.

System Internals - URL Crafting

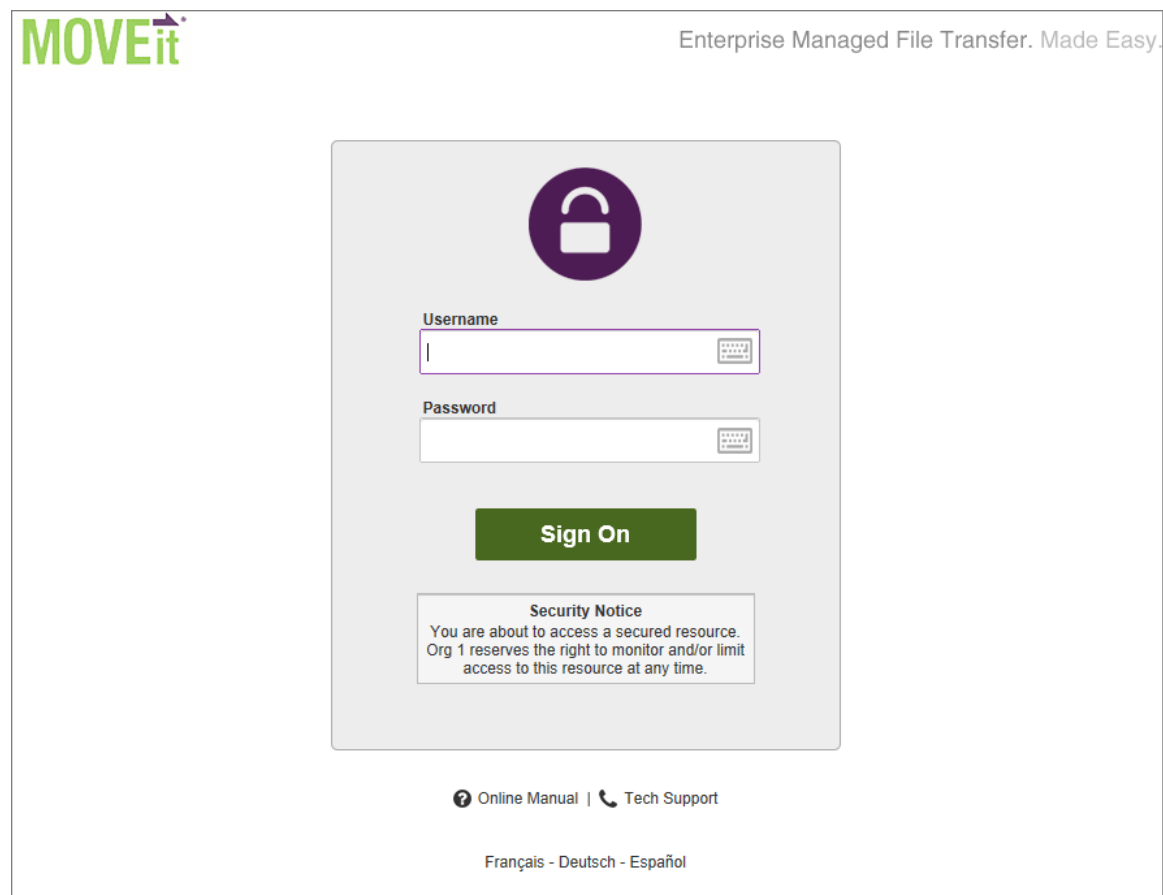
Multi-Organization Branding

Please also see *FTP Certs Tab* in **FTP - Configuration** (on page 577) and the *Multiple SSL Certificates* below if you plan on hosting multiple organizations with different SSL certificates on your MOVEit DMZ server.

The first page users will see depends on the link they followed to the signon page. For most users following links off an organization's main web site, the first page they will see will be their Home page. For users following links from notification emails, the first page will be a page with details about a specific file.

The Sign On page is presented in two different flavors:

Unbranded



The screenshot shows the unbranded signon page for MOVEit. The page has a white background with a light gray border. In the top left corner is the MOVEit logo. In the top right corner is the text "Enterprise Managed File Transfer. Made Easy." Below this is a central gray box containing a purple padlock icon. Under the icon are two input fields: "Username" and "Password". Below these fields is a green "Sign On" button. At the bottom of the gray box is a "Security Notice" box with the text: "Security Notice. You are about to access a secured resource. Org 1 reserves the right to monitor and/or limit access to this resource at any time." Below the gray box are links for "Online Manual" and "Tech Support". At the very bottom are the language options: "Français - Deutsch - Español".

Using the default MOVEit Gray scheme.

An unbranded Sign On page will display the MOVEit DMZ logo and contact information for the site provider. (This information has been configured by a SysAdmin.)

An unbranded Login page will be displayed by default unless particular Organizations take steps to brand this page. The URL to invoke this page is typically of this form: *http://moveit.nowhere.com*

Branded

The screenshot displays a branded login interface for Standard Networks. At the top left is the Standard Networks logo. A blue banner at the top right reads "POWERED BY... MOVEit". The central focus is a light gray box containing a purple padlock icon, a "Username" input field, a "Password" input field, and a blue "Sign On" button. Below the button is a "Welcome to Standard Networks" message. At the bottom of the gray box is a "Register and Send Files" button. The footer includes links for "Online Manual" and "Tech Support", and language options: "Français - Deutsch - Español".

STANDARD NETWORKS

POWERED BY... MOVEit

Username

Password

Sign On

Welcome to Standard Networks
This area exists to provide our clients and business partners with secure, immediate access to key resources. Anonymous

Don't have an account?
Register and Send Files

Online Manual | Tech Support

Français - Deutsch - Español

Using a customized scheme.

A branded Login page will display a particular Organization's logo, colors and contact information. (This information has been configured by an Administrator for that particular Organization through that Administrator's **Settings** page.)

A branded Login page will display in either of two cases:

- The user has just signed off the branding Organization.
- The Organization has provided its MOVEit DMZ users with a special URL which invokes branding based on that Organization's four-digit ID. For example, if the unbranded admin site URL is this:

`http://moveit.nowhere.com`

the branded admin site URL will be this:

`http://moveit.nowhere.com?OrgID=2345`

Most sites will probably want to bury this particular URL in a link to MOVEit DMZ from their main site.

Suppress Session Expired Messages

Particularly with older versions of MOVEit DMZ, you may have noticed that simply copying a URL for a specific user, folder, file or other MOVEit DMZ profile may cause MOVEit DMZ to sometimes display (correctly) that your session has timed out when you next try to access this URL. The display of this message, however, is often misleading, especially if you intend to use this URL in a permanent link tag on a public web site. (For example, Ipswitch provides a direct link to the support page from which customers and evaluators may download its software.)

To always suppress this session expired message, simply append the following code to any URL you wish to may publicly available:

`&quiet=true`

Content Only Display

Normal MOVEit DMZ pages include a header with banner logo, a user information bar, and a left-hand navigation section, all of which allow the user to navigate their way to different pages within the application. Some companies may wish to hide these sections, though, especially when DMZ is used in a single-signon system as part of a larger web application. To do so, the following code may be appended to the URL the user clicks to visit MOVEit DMZ:

`&contentonly=1`

This will cause the header, userbar, and left-hand navigation to be hidden for the rest of the session, or until the code above is repeated with a value of 0. Since the value is stored in the session, only the first MOVEit DMZ URL invoked by the portal application needs to have this code.

Since this feature is designed to allow MOVEit DMZ to be used within an existing web application via frames or iframes, when the contentonly flag is enabled, MOVEit DMZ will disable its normal cross-frame scripting protection code and allow the interface to be loaded by external framesets.

Return-To Link

Normal MOVEit DMZ pages include a Sign Out link in the upper right corner, allowing the user to discontinue their session. When used in a single-signon system as part of a larger web application, this is generally not a desirable feature. Instead, it is usually desirable to provide the user with a link back to the main web application. To have MOVEit DMZ replace the Sign Out link with a custom Return link, the following code may be appended to the URL the user clicks on to visit MOVEit DMZ:

`&returnto=<your URL>`

Replace `<your URL>` with the full URL of the web page you wish the user to return to. The URL must begin with either `http://` or `https://`. Since the value is stored in the session, only the first MOVEit DMZ URL invoked by the portal application needs to have this code. However, DMZ will always use the latest value provided to it for this option.

Simple Single Signon Support

In a situation where someone wants to set up a single signon to integrate MOVEit DMZ into an existing portal environment, you can submit an HTML form which silently prefills a username and password. To make this occur, you submit the form information, including the regular MOVEit DMZ URL using the POST method.

Note: Previous versions of MOVEit DMZ suggested using the HTTP GET method to send the session id. Security best practices call for using the POST method instead of the GET method. If your web integration uses HTTP GET, and you want to continue to use the GET method, you need to set the following registry entry to allow the continued use of this method.

Set the MOVEit DMZ registry value `AllowInsecureQueryStrings` to "1" to allow GET requests for sensitive transactions, and allow GET requests to include session IDs in `apilink.aspx`. For more information, see the **Registry Settings** (on page 764) section in the Technical Reference topic.

The original GET example suggested adding this snippet to the MOVEit DMZ URL:

&username=myusername&password=mypassword&transaction=signon

The following shows an example of the POST method:

```
<BODY onload="document.forms[0].submit();">
<FORM action="https://moveit.yourcompany.com" method="POST">
  <INPUT type="hidden" name="invisible-username" value="{myusername}"/>
  <INPUT type="hidden" name="invisible-password" value="{mypassword}"/>
  <NOSCRIPT>
    <P>Press this button to continue:</P>
    <INPUT type="submit" value="Continue"/>
  </NOSCRIPT>
</FORM>
</BODY>
```

Branded Redirect

Installations which wish to expose subfolder URLs without OrgIDs. (e.g., a site may want Woodstock Bank's users to access MOVEit as <https://www.myorg.com/woodstockbank> and let Bull Valley Credit Union's users access MOVEit as <https://www.myorg.com/bullvalley>). This arrangement is especially common at data centers where ownership wishes to minimize annual certificate costs by hosting many related sites on a single server.

To effect this configuration, perform the following steps for each subfolder you wish to configure.

- 1 Create a subfolder (on the SAME web server) for the bank or whatever. (e.g., <https://www.myorg.com/testbank>)
- 2 Create a new **default.aspx** file in that folder.
- 3 Make sure the IIS web site/folder properties recognize default.aspx as the default doc in that folder.
- 4 Copy/paste the following text into your new default.aspx file and make changes as necessary:

```
<% ' This redirect script sends users who type in "friendly" URLs  
' to MOVEit's front door with the appropriate parameters.
```

```
! * * * * *
```

```
' * Set your Organization's ID here!!!
```

```
Dim OrgID as String = "1234"
```

```
! * * * * *
```

```
' * Set the official URL of your MOVEit DMZ here!!!
```

```
' * (Make sure this URL has a VALID certificate.)
```

```
Dim URL as String = "https://moveit.stdnet.com"
```

```
! * * * * *
```

```
' * Do NOT modify the code below this line!!!
```

```
Response.Redirect(URL & "?OrgID=" & OrgID)
```

```
%>
```

Direct Download

By providing a special URL to end users, end users can be forced them to initiate a (non-Wizard) download immediately after signing on (if not already authenticated). This procedure is typically performed by a MOVEit DMZ API application which creates its own notifications or web pages, but the same technique can be used by any application which can create a link for a user to click.

Use the following syntax to initiate a direct download. Items to be filled in are in square brackets. Be sure your requests actually only use one line.

```
https://[MOVEitDMZ_Hostname]/human.aspx?
```

```
Username=[EndUser_Username]&arg01=[MOVEitDMZ_FileID]&
```

```
arg05=0/[DownloadAs_Filename]&arg12=downloaddirect&  
transaction=signon&quiet=true
```

The following example prepares to sign on as **Penguin** to download a file with ID#910286 as **dwn.gif**.
`https://dotnet.stdnet.com/human.aspx?`

```
Username=penguin&arg01=9102186&  
arg05=0/dwn.gif&arg12=downloaddirect&  
transaction=signon&quiet=true
```

This crafted URL may be used with other crafted URLs such as **Simple Single Signon Support** or **MOVEit DMZ API's session redirect** to ensure the user is signed on before attempting a transfer. (Otherwise, the user will be prompted for a username and password.)

Note: Sometimes different browsers will handle direct file downloads from MOVEit DMZ in different ways; sometimes files will be automatically opened by the browser using the default application for that filetype, while other times the user will be prompted to save the file before actually opening it. If the behavior the end users are experiencing is not the desired behavior, try adding the argument `noattach=0` to the direct download URL. This will cause MOVEit DMZ to add a **Content-Disposition: attachment** header to the direct download response, which will cause some browsers to treat the downloaded file differently than normal.

Multiple SSL Certificates

If you wish to support having different SSL certificates for different MOVEit DMZ organizations, you must have a unique IP address / port combination, and SSL certificate, for each organization. (IIS 7.0 on Windows 2008 does not require separate sites.) (See **Feature Focus - Multihoming** (on page 116) for more information.) If you are willing to share a named certificate across organizations, none of these extra steps are required.

For example, if SampleHoster wants to host `secure.acme.com` and `ftps.whammo.com` on the same MOVEit DMZ machine, each with a unique SSL certificate, then SampleHoster is **multihoming** (on page 116). However, if SampleHoster wants to host `vault.samplehoster.com` and allow access to `vault.samplehost.com/acme` and `vault.samplehost.com/whammo` (one, shared SSL certificate), SampleHoster needs only:

- Install MOVEit DMZ and the `secure.acme.com` SSL certificate. This will take care of one IIS site/SSL certificate.
- Create two organizations: one for `acme` and the other for `whammo`.
- Set up a **Branded Redirect** page for each organization as explained in this topic.

Both of these configurations have been deployed by data centers and MOVEit DMZ supports both equally well in production. The main reason cited for going with individual SSL certificates for each organization is that it completes the branding experience. The main reasons cited for going with single shared SSL certificate is that it reduces management hassle and SSL certificate costs.

System Internals - Remote Filesystem

MOVEit DMZ is capable of storing its encrypted files on a remote Windows fileshare. This is required for **Webfarms** (on page 661) configurations, but can also be used for standalone MOVEit DMZ servers. Storing the encrypted files on a remote location improves security by making it harder to access those files from a compromised webserver. This configuration can help MOVEit DMZ meet company requirements that no data reside in a DMZ network segment.

Using a Remote Fileshare

For standalone and webfarm-enabled MOVEit DMZ servers, follow these steps to configure a file server to provide remote filesystem support to MOVEit DMZ:

- 1** Create a `moveitdmz` user on the file server. This user will be used by MOVEit DMZ to access the file share. The account only needs to be present on the file server.
- 2** Create a `MOVEitDMZ` folder on the file server. This folder is where MOVEit DMZ's encrypted files will be stored.
- 3** Give the `moveitdmz` user full permissions to the `MOVEitDMZ` folder. Add the `moveitdmz` user to the list of access control entries through the **Security** tab on the folder's **Properties** dialog. Give the user full permissions to the folder.
- 4** Share the folder and give full permissions to remote users. Enable sharing on this folder through the **Sharing** tab on the folder's **Properties** dialog. Add the `moveitdmz` user to the share's permissions and give the user full control over the share (you may optionally remove all other users and/or groups from the share permissions list).

The shared folder may now be used as the MOVEit DMZ file store location. If you are configuring a standalone MOVEit DMZ server to use the shared folder, first shut down the MOVEit DMZ services and manually copy the contents of the existing \MOVEitDMZ\Files folder on the server to the new shared folder. Next, apply the new remote folder settings using the MOVEit DMZ Config program. Use the **Advanced** button on the **Paths** tab to enter the UNC path of the shared folder, as well as the username and password of the moveitdmz user configured above. Finally, start the MOVEit DMZ services and run the MOVEit DMZ Checker utility to make sure file transfers are working properly. If there are any errors, see the *Troubleshooting* section below.

Troubleshooting

When using a remote fileshare for its encrypted file store, MOVEit DMZ will mount the fileshare internally using the configured username and password. If MOVEit DMZ is unable to download or upload files after changing to a remote fileshare, the problem will usually be either an error mounting the share, or a permissions error with the share. Typically the error code and message that MOVEit DMZ encountered when it tried to access the share will be reported back to the client that is trying to upload or download a file. If this is not the case, see the DMZ_WEB.log file on the DMZ server for more details about the error.

This is a list of some errors that might be encountered when using a remote share, and how to resolve them:

- **Error mounting share: 1219** - Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.

This error occurs when two or more processes are trying to access the same share. Often this will happen when running the MOVEit DMZ Config program after accessing the remote fileshare using Windows Explorer. This can be fixed by disconnecting existing connections to the fileshare before running other programs that need to access it. To see if there are any connections open under the currently signed on user, open a command prompt window and type `net use`, then hit enter. Any existing connections to the fileshare being used by MOVEit DMZ should be disconnected by using the `net use /DELETE` command (for help with the net use command, type `net use /?` then hit enter).

- **Error mounting share: 1312** - A specified logon session does not exist. It may already have been terminated.

This error is usually caused by the program being run as the Local System account, which is not allowed to mount remote fileshares. This can be fixed by running the program as a regular user, or as the Network Service account. Normally the MOVEit DMZ install should automatically configure the services to run as either a custom service account, or the Network Service account. See the configuration for other MOVEit DMZ services if one of the services is having this problem.

- **Access is denied**

This error occurs when the permissions of the moveitdmz fileshare user are not correct on the share, or the folder itself. This can be fixed by making sure the user has full permissions on the folder, and full permissions on the share.

General Information

This section contains some supplemental information about MOVEit.

Client Support

The following list of clients includes those which have been tested against MOVEit by Ipswitch and our customers. However, because MOVEit conforms to HTTP, FTP, SSL and SSH standards, we continue to add to this list as new clients are discovered, developed and/or tested.

See also: *MOVEit Clients* <http://www.ipswitchft.com/Products/MOVEit/Clients.aspx>.

In several cases below, the terms "Linux" and "BSD" (two Unix variations) are used interchangeably; please consult the individual vendor's literature for the exact list of platforms supported. Likewise, "Windows" generally covers Microsoft's 32-bit operating systems from Windows 98 through Windows 7, but the exact list of supported operating systems should be obtained from the individual client vendor. (All MOVEit clients have been tested and approved for use under Windows 7.)

Supported Web Browsers

MOVEit has been tested against and fully supports the following major browsers:

- Microsoft Internet Explorer (IE) 9.0, 10.0 (on Windows only)
 - ✓ when using MOVEit Upload/Download Wizard (ActiveX or Java)
- Mozilla FireFox (FF): Latest version (on Windows, Macintosh and RedHat Linux)
 - ✓ when using MOVEit Upload/Download Wizard (Java - Windows/*nix/Mac OS X)
- Google Chrome: Latest version (on Windows only)
 - ✓ when using MOVEit Upload/Download Wizard (Java - Windows/*nix/Mac OS X)
- Apple Safari: Latest version (on Macintosh only)
 - ✓ when using MOVEit Upload/Download Wizard (Java Only)

✓ = Indicates this client ensures the integrity of transferred files and proves who uploaded and who downloaded a specific file (non-repudiation).

Use of the MOVEit Java Wizard on the Macintosh version of Firefox requires that you use the Java Preferences applet to select Java 6 or 7.

Supported Secure FTP/SSL Clients

MOVEit has been tested against and fully supports a large number of secure FTP clients using FTP over SSL:

- MOVEit Freely ✓ (free command-line)
- MOVEit Buddy ✓ (GUI)
- MOVEit Central ✓ (w/Admin)
- WS_FTP Professional and WS_FTP Home (GUI, version 7 and higher, Windows) (✓ version 12 and higher)
- SmartFTP ✓ (GUI, version 1.6 and higher, Windows)
- SmartFTP (free GUI, version 1.0 and higher, Windows)
- Cute FTP Pro (GUI, version 1.0 and higher, Windows)
- BitKinx (GUI, version 2.5 and higher, Windows)
- Glub FTP (GUI, Java 2.0 and higher)
- FlashFXP (GUI, version 3.0 and higher)
- IP*Works SSL (API, Windows, version 5.0)
- LFTP (free command-line, Linux, Unix, Solaris, AIX, etc.)
- NetKit (command-line, Linux, Unix, Solaris, etc.)
- SurgeFTP (command-line, FreeBSD, Linux, Macintosh, Windows, Solaris)
- C-Kermit (command-line; v8.0+, AIX, VMS, Linux, Unix, Solaris)
- AS/400 native FTPS client (OS/400 minicomputer)
- **z/OS Secure Sockets FTP client** (on page 601) (z/OS mainframe)
- TrailBlaxer ZMOD (OS/400 minicomputer)
- NetFinder (GUI, Apple)
- Sterling Commerce (batch, various)
- Tumbleweed SecureTransport (4.2+ on Windows, batch, various)
- Cleo Lexicom (batch, various)
- bTrade TDAccess (batch, AIX, AS/400, HP-UX, Linux, MVS, Solaris, Windows)
- **cURL** (on page 622) (command-line, AIX, HP-UX, Linux, QNX, Windows, AmigaOS, BeOS, Solaris, BSD and more)
- South River Technologies "WebDrive" (Windows "drive letter" - requires "passive, implicit and 'PROT P'" options)

- Stairways Software Pty Ltd. "Interarchy" (Mac "local drive" and GUI)

FTP Client Developers: Please consult the "FTP - Interoperability - Integrity Check How-To (on page 626)" documentation for information about how to support integrity checks with your FTP client too.

Supported Secure FTP/SSH (and SCP2) Clients

MOVEit has been tested against and fully supports the most popular secure FTP clients using FTP over SSH as well:

- **OpenSSH sftp for *nix** (<http://openssh.org/>) (free command-line, Unix - including Linux and BSD, password and client key modes)
- **OpenSSH for Windows** (<http://sshhwindows.sourceforge.net/>) (free command-line, Windows, password and client key modes)
- OpenSSH sftp for Mac (preinstalled command-line, Mac, password and client key modes)
- OpenSSH sftp for z/OS (part of "IBM Ported Tools for z/OS", z/OS 1.4+, password and client key modes)
- Putty PSFTP, (command-line, Windows, password and client key modes)
- WS_FTP (GUI, Windows, version 7.0 and higher; version 7.62 has a compression-related bug which prevents it from uploading large, highly compressible files)
- BitKinx (GUI, version 2.5 and higher, Windows)
- F-Secure SSH (command-line, 3.2.0 Client for Unix, password and client key modes)
- FileZilla (GUI, Windows)
- SSH Communications SSH Secure Shell FTP (GUI, Windows, password and client key modes; requires setting # of transfers to 1)
- SSH Tectia Connector (Windows)
- SSH Tectia Client (Windows,AIX,HP-UX,Linux,Solaris)
- J2SSH (free Java class - requires Java 1.3+)
- Net::SFTP - Net::SSH::Perl (free Perl module for Unix)
- MacSSH (GUI, Mac, password mode only)
- Fugu (free GUI, Mac, password mode only)
- Cyberduck (free GUI, Mac, password and client key modes)
- Rbrowser (GUI, Mac, password mode only)
- Transmit2 (GUI, Mac, password and client key modes)
- gftp (GUI, Linux, password and client key modes)
- Magnetk LLC sftpdriive (Windows "drive letter", password mode only)
- South River Technologies "WebDrive" (Windows "drive letter", password mode only)
- Cyclone Commerce Interchange (Solaris, client key mode only)
- Stairways Software Pty Ltd. "Interarchy" (Mac "local drive" and GUI, password mode only)

- Miklos Szeredi's "SSH FileSystem", a.k.a. "SSHFS" (*nix "mount file system" utility, password and client key modes; requires OpenSSH and FUSE)
- Tumbleweed SecureTransport (4.2+ on Windows, batch, various)

Note: Two of the clients above, (OpenSSH for Windows & SSH Communications), are capable of uploading files using multiple independent threads which may send blocks of data non-sequentially. This mode is not supported by MOVEit SSH and should be disabled using the "-R1" command-line option.

In addition to the SFTP clients listed above, MOVEit has limited support for some SCP clients. This list of clients is limited to those that implement the SCP2 protocol, which uses SFTP as its underlying transfer mechanism. MOVEit has been successfully tested with these SCP clients:

- PSCP, (command-line, Windows, password and client key modes)
- F-Secure SCP2 (command-line, 3.2.0 Client for Unix, password and client key modes)
- WinSCP (command-line; SFTP mode)

✓ = Indicates this client ensures the integrity of transferred files and proves who uploaded and who downloaded a specific file (non-repudiation).

MOVEit Central and MOVEit is the FIRST client and server solution to offer FTP over SSL (ftps) and FTP over SSH (sftp) support in a single product. MOVEit was also the first family of Windows-based products to support all three modes of FTP over SSL transport. Our commitment to full implementation of industry security standards ensures that a wide variety of clients using the FTP protocol over SSL or/and SSH can exchange files with MOVEit.

Additional FTP over SSL Information:

The three modes of FTP over SSL are:

- TLS-P (aka "Explicit, Always", "SSL" and "TLS")
- TLS-C (aka "Explicit, Negotiate")
- Implicit (usually connected over port 990)

Most administrators prefer their clients to connect to MOVEit using the IMPLICIT mode of FTP over SSL (TCP port 990). There are two advantages implicit mode enjoys over the other two modes due to its requirement to establish a secure channel before passing any commands at all. (The other two modes connect insecurely on TCP port 21, then build up a secure channel before passing sensitive information.)

- Implicit mode offers fewer interoperability problems because there are almost no options to haggle over during the connection.
- Implicit mode protects against the case where a fumble-fingered user or a poorly written script "leaks" a username, password or other information during the non-secure negotiation of the channel.

Please see the "FTP Server" section of this manual for additional information about supported FTP clients as well as a technical description of secure FTP and what a secure FTP client must do in general to be supported by MOVEit's secure FTP server.

Supported AS2/AS3 Clients

MOVEit supports any AS2 client that has been "Drummond" or "eBusinessReady" certified; the software MOVEit uses to handle incoming AS2 files and MDNs has itself been certified "eBusinessReady" under a program now managed by Drummond.



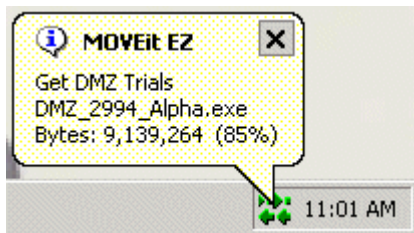
AS3 clients are just FTP/SSL clients as far as MOVEit is concerned. MOVEit Central handles the encryption/decryption, signing and verification of AS files in either case.

User Automation

MOVEit EZ is a Windows desktop client which automatically and securely moves files between MOVEit and a user's local machine or remote server. End users or applications simply copy files to a designated folder on their local machine and they are whisked away to MOVEit. Files which are uploaded for that user to MOVEit are automatically downloaded and placed on their local machine.

Note: ALL MOVEit EZ clients will need to be updated to MOVEit EZ V.6.5 or later to work with MOVEit V.6.5 or later. Because of problems with older MOVEit EZs unique handling of MOVEit folders, MOVEit will now prevent sign-ons from pre-6.5 versions of MOVEit EZ and will display a message to the end user telling them to upgrade to MOVEit EZ 6.5 or later.

MOVEit EZ normally runs as an icon in the tray of an end user, but it is often also installed as a service. During file transfers it will pop open status balloons like the one pictured below to let the end user know it is working. When new files have arrived, the MOVEit EZ icon will change (similar to an email client) to let the end user know something new has arrived.



MOVEit EZ supports the concept of guaranteed delivery, which means that it will only accept files which pass a cryptographic integrity check, will resume incomplete transfers and will retry failed transfers.

More information on MOVEit EZ is available on the **MOVEit EZ** (<http://www.ipswitchft.com/moveitez>) web site. 30-day, self-installing evaluations can be obtained from this page. Site licensing and customized redistribution options (including custom application name and icons) are also available.

Batch File Transfers Involving MOVEit

Many administrators like to use ".bat" scripts for FTP transfers. (.bat files are easy to debug, simple to read and can make use of the built-in ftp.exe client Microsoft ships with every operating system.)

Unfortunately, these batch files are limited by ftp.exe itself; specifically, ftp.exe lacks the ability to do passive FTP transfers (often necessary if transferring through firewalls) and secure FTP transfers (recommended for sensitive transmissions over the Internet or other untrusted networks).

MOVEit normally accepts only secure connections, so ftp.exe itself cannot be used to FTP files to and from MOVEit. However, the MOVEit family provides a free and secure alternative for ftp.exe called "MOVEit Freely" (aka "ftps.exe"). If you would prefer to use FTP over SSH transmissions, free scriptable clients are available for almost every version of Unix ever invented as well as most Windows operating systems from OpenSSH.

To avoid several all-too-common firewall issues with the FTP/SSL protocol, Ipswitch also offers a free HTTPS-based command-line utility called MOVEit Xfer that accepts the same syntax and commands as MOVEit Freely and Microsoft's ftp.exe client. Available in both Windows and Java 1.4.2+ versions, this scriptable utility provides single-port secure file transfer on a wide variety of platforms including *nix, Windows, Macintosh and some mainframes.

Copies of MOVEit Xfer and MOVEit Freely are available from the **MOVEit support site** (http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ) or from the MOVEit **product information site** (<http://www.ipswitchft.com/moveitfreely>).

Programmatic Control of MOVEit with MOVEit API

MOVEit offers two programming interfaces to Windows and Unix programmers.

MOVEit API Win(dows)

MOVEit API is a Windows COM object which lets developers build applications and scripts to exchange secure files with MOVEit servers, as well as administer folder settings, folder permissions, users and group membership.

MOVEit API Java (*nix, Windows, Macintosh, Mainframe, etc.)

MOVEit API Java is a Java class which lets developers build applications and scripts to exchange secure files with MOVEit servers, as well as administer folder settings, folder permissions, users and group membership.

As these products are separately licensed from MOVEit, you may **contact Ipswitch** (<mailto:moveitsales@ipswitch.com>) directly for more information about either of the MOVEit API products.

Scheduled and Audited File Transfers Involving MOVEit with MOVEit Central

MOVEit Central (<http://www.ipswitchft.com/moveitcentral>) is an enterprise file transfer manager capable of simultaneous file transfers to and from hundreds of Windows file systems, FTP/FTPS/SFTP servers, mail servers, web servers, MOVEit servers and AS1/AS2/AS3 partners.

Included are a full featured task scheduler, guaranteed delivery, instant (event-driven) transfers, multiple sources/destinations in a single task, the ability to run custom VBScripts against processed files in a fault-tolerant sandbox, and custom event log and/or email notification support. Security features include secure channels for remote control/configuration and AES encryption of configuration information, including remote host credentials.

Note: ALL MOVEit Central clients will need to be updated to the following patched versions of the most recent releases to work with MOVEit V.6.5 or later. Because of problems with older MOVEit Centrals using the improved folder structure added in MOVEit V.6.5, MOVEit will now prevent sign-ons from older versions and will display a message to the end user telling them to upgrade to one of the following patched versions.

- If you are running version 6.0.0.0 or version 6.0.0.1, you will need to upgrade to version 6.0.0.2 or later to access MOVEit 6.5 or later.
- If you were given a special version of MOVEit Central, please contact MOVEit Support for an appropriate upgrade version.
- All other releases of MOVEit Central should upgrade to version 7.0.2.0 or later to access MOVEit 6.5 or later.

Security

The following security features are functions of the MOVEit software and exist in addition to the hardening of the operating system and associated application services.

Transport Encryption

During transport MOVEit uses SSL or SSH to encrypt communications. The minimum strength of the encryption used during web transport (e.g., 128-bit) is configurable within the MOVEit interface.

This value is configurable by organization. To configure this value for any particular organization, sign on as a SysAdmin, view the organization for which this value should be set, and click the "Change Req" link to set the value.

Note: If you set the minimum encryption value of the "System" organization (#0), you will be given the chance to apply your setting to ALL organizations in the system.

Storage Encryption

MOVEit stores all files on disk using FIPS 140-2 validated 256-bit AES (<http://csrc.nist.gov/encryption/aes> (<http://csrc.nist.gov/encryption/aes>)), the US federal standard for encryption. MOVEit Crypto, the encryption engine on which MOVEit relies, is only the tenth product to have been vetted, validated and certified by the United States and Canadian governments for cryptographic fitness under the rigorous FIPS 140-2 guidelines.

MOVEit also overwrites just-deleted files with random bytes to prevent even encrypted files from lingering on a physical disk after users thought them to have been destroyed.

Precautions Taken During Transport-Storage Exchange

If files received by MOVEit were simply copied to a large cleartext memory buffer, trojan programs could potentially "sniff" sensitive files out of these spaces.

Instead MOVEit spools pieces of files received into much smaller buffers, encrypts them and writes them to disk almost immediately. Spooling files in this manner reduces overall exposure in two ways: 1) reduces amount of information exposed and 2) reduces time information is exposed. (This technique also yields some important performance gains.)

(A frequently asked question regarding this issue is "why not just store the file using SSL or SSH" - a short answer to this question is: SSL or SSH uses temporary keys which are renegotiated each time a client establishes a new connection, and we need "more permanent" keys for storage.)

Integrity Checking

When certain file transfer clients are used with a MOVEit server, the integrity of transferred files will be confirmed. All MOVEit secure FTP, API and web-based clients (including the upload/download Wizard) support integrity checking. Other FTP clients can also take advantage of integrity checks; see "**FTP - Interoperability - Integrity Check How-To** (on page 626)" for more information.

To perform an integrity check, both the client and the server obtain a cryptographic hash of the transferred file as part of the last step of the transfer. If the values agree, both sides "know" that the file transferred is completely identical to the original. The results of any integrity check are not only displayed to the user of the file transfer client but stored for ready access on the MOVEit server.

Immediate Transfer off Server

When used with MOVEit Central, MOVEit supports "event-driven" transfers which allow files to begin spooling to internal servers as soon as they land on an Internet-facing MOVEit server. This prevents even encrypted files from remaining on the server for longer than absolutely necessary.

Transfer Resume

MOVEit supports file transfer resume on both its HTTPS and FTPS interfaces. In addition to being useful during transfers of multi-gigabyte file, this feature is also a secure feature in the sense that it makes large file transfers less susceptible to denial-of-service attacks.

Folder Quotas

Enforceable folder size quotas can be set on various folders to prevent system storage from being exhausted.

User Quotas

Enforceable user size quotas can be set on various users to prevent them from exhausting system storage.

Delegation of Authority

Individual end-user members of a group can be designated as Group Admins. These users then are able to administrate the users, folder permissions and address books in their group, subject to various parameters set by organization administrators.

Administrative Alerts

Email notifications are sent to administrators when users are locked out, when the internal consistency checker notices something amiss with the database, etc.

One-Way Workflows

MOVEit can be configured to never allow users to download what they have just uploaded into the system. This configuration alone can prevent users from misusing MOVEit as a repository of personal or restricted materials. (Another common way to handle this scenario is through the use of IP restrictions.)

Password Aging

Users can be forced to change their passwords periodically with MOVEit's password aging features. Users will also be warned (via email) several days in advance of actual expiration, and notified again when their password expires.

Password History

MOVEit can be configured to remember a certain number of passwords and prevent users from reusing those passwords.

Password Strength Requirements

Various password complexity requirements can be set on MOVEit, including number/letter, dictionary word and length requirements.

Account Lockout

If someone attempts to sign on to a valid account with an incorrect password too many times, their account can be locked out and administrators will be notified via email.

IP Lockout

A very real concern of administrators of any authenticated resource which supports account lockouts is that someone will get a list of valid usernames and lock all of them out. To mitigate this risk, MOVEit offers a feature which will prevent a machine with a specific IP address from making any further requests of the system if MOVEit sees too many bad signon attempts. Administrators will also be notified via email when this occurs.

Restricted IP/Hostname Access

Specific users or classes of users can be restricted to certain ranges of IP addresses and/or hostnames.

Detailed, Tamper-Evident Audit Logging

MOVEit logs not only signon and signoff events, but permission changes, new user additions and other actions which directly affect the security of the system. Realtime views of this audit trail as well as detailed query tools are available on the Logs and Report pages. All log entries are cryptographically chained together in a way that makes any tampering (add, delete, change) of audit logs evident.

Remote Authentication

MOVEit's RADIUS and LDAP clients support any standard RADIUS and LDAP servers, including Microsoft's Internet Authentication Server, Novell's BorderManager, Microsoft Active Directory, Novell eDirectory, Sun iPlanet and IBM Tivoli Access Manager (SecureWay).

Obscured Product and Version Identity

MOVEit does not reveal its product name to unauthorized users via the SSH and FTP interfaces and can be configured to hide this information from web users as well. Version numbers are also only available to authorized users. Obscuring this information prevents hackers from figuring out what they are attacking without doing a fair amount of research.

Client Certificates and Client Keys

All major interfaces of MOVEit (SFTP, FTPS, HTTPS) support the use of SSL (X.509) client certificates and SSH client keys. SSL client certs and SSH client keys are usually installed on individual machines, but SSL client certificates are also available as hardware tokens.

Multiple Factor Authentication

When used with a username, IP addresses, passwords and client keys/certs offer one-, two- or three-factor authentication.

External Authentication

Organizations worried about storing username-hash combinations on MOVEit's protected database can use the External Authentication feature and move all non-administrative usernames and passwords to RADIUS or LDAP servers. (Access to the remaining administrative usernames can be locked to specific, internal-only IP addresses.)

Not-In-DMZ Storage Option

There is a way to store MOVEit encrypted files in a location that is not in a DMZ. It is to deploy MOVEit on a piece of an existing storage area network (SAN).

Web Browser "Clickable Keyboard" Keystroke Logging Protection

To prevent keystroke logging software and hardware from capturing the keystrokes used to sign on to a MOVEit using a web browser, a clickable keyboard is provided as an alternate method of data entry. The same keyboard also protects other password fields used throughout the application to protect other users as well.

Cross-Frame Scripting Protection

To help prevent cross-frame scripting attacks against MOVEit, the web interface will prevent itself from being loaded in a frame or iframe window. This can be overridden using the "contentonly" flag, if the goal is to integrate MOVEit with an existing portal application using frames. See the ***URL Crafting*** (on page 783) doc page for further details.

Regulations Overview

MOVEit DMZ is used by a wide variety of health care, insurance, financial service and pharmaceutical organizations to satisfy data integrity, auditing and privacy concerns raised by HIPAA, FDIC, OCC, G-L-B Act, California SB 1386, Canadian PIPEDA Payment Card Industry ("PCI"), Sarbanes-Oxley (a.k.a. "SARBOX") and other regulations. Although a particular organization's fitness with regards to major industry-specific federal regulations is usually determined on a site-by-site basis by a dedicated auditing team, the ***"Privacy/Security/Auditing" guide*** (on page 805) in this section will help answer some "entry-level" questions regarding MOVEit DMZ's expected conformance.

If you are branch or agency of the U.S. federal government, you may be required to only purchase cryptography which is FIPS 140 validated. MOVEit DMZ meets this requirement with its own FIPS 140-2 validated MOVEit Crypto module, the heart of MOVEit DMZ and MOVEit Central. (MOVEit Crypto has been approved for use with information designated up through the Classified level.)

Certain agencies, vendors or providers may also be required to conform to other federal requirements such as those issued by the ***Food and Drug Administration ("FDA")*** (on page 807) or mandated by the ***Americans with Disabilities Act ("ADA")*** (on page 809) . As these requirements are frequently NOT the subject of their own audits, the applicable regulations and MOVEit DMZ's compliance statements are detailed in their own sections for easy inclusion into most conformance reports.

If you have a question about compliance with a specific regulation not specified above, please contact Ipswitch MOVEit compliance officer at ***moveitsales@ipswitch.com (mailto:moveitsales@ipswitch.com)***.

Privacy/Security/Auditing Requirements

This section answers some questions regarding MOVEit's expected conformance to HIPAA, FDIC, OCC, G-L-B Act, California SB 1386, Canadian PIPEDA, Payment Card Industry ("PCI"), Sarbanes-Oxley (a.k.a. "SARBOX") and other regulations. Please consult with Ipswitch for the latest information about how MOVEit helps its security-conscious customers achieve their file transfer and storage privacy and security standards as well as relevant contractual, industry and regulatory requirements.

- "Data at Rest" - MOVEit satisfies this requirement by encrypting all files stored on disk with FIPS 140-2 validated 256-bit AES encryption. MOVEit Crypto (the encryption module which powers MOVEit) is only the tenth product to have been vetted, validated and certified by the United States and Canadian governments for cryptographic fitness under the rigorous FIPS 140-2 guidelines.
- "Data in Motion" - MOVEit satisfies this requirement by using encrypted channels (SSL or SSH) when sending or receiving data.
- "Tamper-Evident Audit Trail" - MOVEit maintains a full audit trail of not only every file transfer but every administrative action as well. All entries are cryptographically chained in a way that makes log tampering (i.e., adding, deleting or changing entries) evident. Scheduled "tamper checks" are run automatically and may also be run manually whenever needed.
- "Integrity Checking" - MOVEit and MOVEit file transfer clients including the Upload/Download Wizard, EZ, Xfer, Freely, Central, API Windows and API Java use cryptographic hashes to verify the integrity of files throughout the transfer chain.
- "Non-repudiation" - MOVEit authentication and integrity checking allows people to prove that certain people transmitted and/or received specific files.
- "Guaranteed Delivery" - When MOVEit non-repudiation is combined with MOVEit transfer restart and transfer resume features, it satisfies the requirements for a conglomerate concept called "guaranteed delivery".
- "Obsolete Data Destruction" - MOVEit overwrites all deleted files with cryptographic-quality random data to prevent any future access. Specifically, MOVEit meets the requirements of NIST SP800-88 (data erasure).
- "Need-To-Know Access Only" - MOVEit user/group permissions allow specific access to only those materials users should access.
- "Good Password Protection" - MOVEit requires tough passwords, prevents users from reusing passwords and periodically forces users to change their passwords.
- "Good Encryption" - MOVEit uses SSL to communicate across networks. This "negotiated" protocol can be enforced to connect with 128-bit strength, the maximum currently available. MOVEit uses MOVEit Crypto's FIPS 140-2 validated 256-bit AES to store data on disk. (This algorithm has been selected by NIST to replace DES, and is faster and more secure than Triple-DES.)

- "Denial of Service Protection" - MOVEit is resilient to DOS attacks caused by resource exhaustion through credential checks or other resources available to anonymous users. ("Nuisance" IP addresses will be locked out.)
- "Hardening" - Installation of MOVEit involves a multi-step (and FULLY documented) hardening procedure which covers the operating system, web service environment, permissions and extraneous applications.
- "Firewall" - MOVEit comes with a detailed firewall configuration guide to minimize confusion on the part of firewall administrators. MOVEit also supports the use of native IPSec as a "poor-man's" (packet filtering) firewall as a second line of defense.
- "Code Escrow" - The complete source code and build instructions of major (i.e. "3.2") versions of MOVEit are escrowed with a third-party.
- "Code Review and Regression Testing" - All MOVEit code passes through a code review and change control is maintained with the help of Microsoft's SourceSafe application. Regression testing is performed on each release with an ever-increasing test battery which now includes several thousand tests.
- "Multiple Factor Authentication" - When used with a username, IP addresses, passwords and client keys/certs offer one-, two- or three-factor authentication.

Regulations FDA

MOVEit is fully compliant with Food and Drug Administration (FDA) standards for timestamps as related to the auditing of medical information which may be transmitted via or placed at rest on MOVEit DMZ.

MOVEit DMZ's complete compliance statement follows.

Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures

(Maintained online here: http://www.fda.gov/ora/compliance_ref/part11/
(http://www.fda.gov/ora/compliance_ref/part11/))

Timestamp Draft Sections 5.1-5.2

N/A (MOVEit DMZ is not responsible for administrator/auditor training or the operating-system level synchronization of machine clocks.)

Timestamp Draft Section 5.3

"You should implement time stamps with a clear understanding of what time zone reference you use. Systems documentation should explain time zone references as well as zone acronyms or other naming conventions. For example, the time zone reference might be a central point like Greenwich Mean Time, a point local to the computer where the activity linked to the time stamp occurs, or a point where the time stamp clock (e.g., a time stamp server) is located."

If enabled, MOVEit DMZ displays the difference between the server's time and Greenwich Mean Time (commonly expressed as GMT +/- HH:MM). This field is visible on the LOWER LEFT side of the screen in the web interface and as a "welcome banner" when signing onto the web server.



Timestamp Draft Section 5.4

"You should take steps to ensure that date and time expressions are clearly understood throughout an organization."

MOVEit DMZ uses AM/PM to designate times and uses a date format of "MM/DD/YYYY"

Timestamp Draft Section 5.5

"Audit trail and signature time stamps should be precise to the hour and minute."

MOVEit DMZ is accurate not only to the minute but the second in its audit trail.

Regulations ADA

MOVEit is fully compliant with Americans with Disabilities Act (ADA) standards for web and windows application design.

MOVEit DMZ's complete compliance statement follows.

Section 508 Standards for Electronic and Information Technology

(Maintained online here: <http://www.access-board.gov/sec508/guide/>
(<http://www.access-board.gov/sec508/guide/>))

SubSection 1194.21 Software Applications and Operating Systems

- a) Keyboard Access: All "GUI" configuration can be performed with the use of a keyboard.
- b) Non-Disruptive: None of the components of MOVEit DMZ interfere with the performance of existing accessibility features in any way.
- c) Current Focus: Current focus is always clearly indicated using the normal Windows conventions.
- d) Sufficient Interface Elements: User Interface Elements are always clearly associated with labels.
- e) Bitmap Meaning: N/A (Bitmaps are currently not being used by MOVEit DMZ's non-web components.)
- f) Text Methods: MOVEit DMZ components use standard Windows text calls.
- g) Color Override: MOVEit DMZ components do not override user color selections.
- h) Animation: N/A (MOVEit DMZ does not use animation.)
- i) Color Significance: Colors are used to highlight special conditions, but are never used as the sole method of indicating significance.
- j) Color Contrast: N/A (MOVEit DMZ uses Windows color selections.)
- k) Flickering Images: N/A (MOVEit DMZ does not use flickering images.)
- l) Label Association: User Interface Elements are always clearly associated with labels.

SubSection 1194.22 Web-based Intranet and Internet Information and Applications

- a) Text Equivalents: All significant images, including logos and folder/file/user icons, make use of "alt" attributes.
- b) Multimedia Equivalents: N/A (MOVEit DMZ does not use "Multimedia")
- c) Color Significance: Colors are used to highlight special conditions, but are never used as the sole method of indicating significance.
- d) Stylesheet Requirements: Stylesheets are not required to properly format the application. In addition, all element styles may be overridden by user-specific stylesheets.
- e) Image Map Links: N/A (MOVEit DMZ does not use "Image Maps")
- f) Server-Side/Client-Side Image Maps: N/A (MOVEit DMZ does not use "Image Maps")
- g) Table Row and Column Identification: All rows and columns make use of the "scope" attribute.
- h) Additional Markup for Complex Tables: N/A (MOVEit DMZ does not use "Complex Tables")
- i) Frame Titles: Frames (used only when displaying help) make use of the "title" attribute.
- j) Flickering Elements: N/A (MOVEit DMZ does not use flickering images.)
- k) Text-Only Page: N/A (MOVEit DMZ is compliant w/o having to resort to this style of page)
- l) JavaScript Titles: JavaScript links make use of the "title" attribute.
- m) Compliant Plug-ins: N/A (No plug-ins are required to view MOVEit DMZ content. Nevertheless, MOVEit DMZ's Upload Wizard - an alternative method of uploading files - is SubSection 1194.21 compliant.)
- n) Form Labels: All form fields use "explicit", "label" attributes.
- o) Skip Repetitive Links: MOVEit DMZ offers a "Skip Repetitive Links" option which allows users to skip directly to the dynamically generated content on each page. When enabled, the "Skip Repetitive Links" link appears as the first item on each and every page.



p) Timed Response: MOVEit DMZ allows the contents of fields from "expired" forms to "pass through" after the user is challenged for his or her username and password again.

Regulations Export

The high quality cryptography provided by Ipswitch FIPS 140-2 validated MOVEit Crypto and its integral use in MOVEit DMZ makes MOVEit DMZ subject to cryptography export controls. Long story short, it is currently legal to install and use MOVEit DMZ from any country which is not one of countries covered in the **U.S. Department of Commerce**

(<http://www.bis.doc.gov/policiesandregulations/regionalconsiderations.htm>) "Regional Considerations" documents.

The remainder of this document is an abbreviated response to "**Control Policy--CCL Based Controls**", "**Supplement No. 6 to part 742**", "**Export Administration Regulations**".

(<http://www.access.gpo.gov/bis/ear/pdf/742.pdf>) (The full document is on file with the Commerce Department.) By request, it was last updated on May 15, 2002.

Section a - Name of item

MOVEit DMZ and MOVEit Central.

Section b - Duplicate copy

Section c - Commodity or software

1. MOVEit DMZ uses:

- Standard SSL (Secure Socket Layer) encryption, as provided by Microsoft. The product does not install any SSL encryption software; it simply uses the SSL implementation already present on the computer. The key lengths and algorithms are determined by what is already installed on the computer. Microsoft Windows is required.
- AES, aka Rijndael. 256-bit keys are used, with cipher block chaining.

MOVEit Central also uses a simple stream cipher to protect passwords stored locally. This is a rotor-based scheme specifically designed to be exportable back around 1990, when regulations were more restrictive.

Aside from the SSL implementation supplied by Microsoft, the products do not use asymmetric encryption.

2. MOVEit DMZ encrypts files with a 256-bit key.

The key management algorithms for SSL are well-documented, and will not be discussed here.

3. The AES algorithm is not proprietary; in fact, it has been FIPS 197 validated to work exactly the way NIST and CSE insist it will work in their public documents.

(Source code has been inspected as part of the FIPS 140-2 validation process.)

The rotor-based algorithm works this way:

- Create an additive linear congruential pseudorandom number generator using the time-of-day and the user-supplied password.
- Create a 256-byte array that maps 0->0, 1->1, and so on.
- Using the PRNG, permute the array to make a pseudorandom "rotor".
- Encipher each byte:
 `ranbyte = next number from PRNG`
 `cipherbyte = rotorArray[plainbyte + prevcipherbyte] % 256 ^ ranbyte;`
- Printably encode the result using RFC 1113 encoding.

4. No pre-processing is applied to the data before encryption.
5. For the AES cipher, the ciphertext is prefixed with a 128-byte header used to store a message hash, original message size and other information which cannot be stored using the underlying operating system file structure alone.

For the simple rotor-based scheme, as described above, RFC 1113-style printable encoding is applied.

6. TCP and SSL are supported. We rely upon standard Microsoft software already installed on the user's computer.
7. We implement two APIs; both are internal only.

These methods encrypt and decrypt files without having to read the entire file into memory.

Unfortunately, to accommodate both the ASP and ASP.NET versions of Response.BinaryWrite, we have had to implement both BSTR and SafeArray of Byte versions.

8. The API which uses AES is implemented both by static linking, and by a COM object, which is dynamically linked. The same source code is used in either case.

We also use *TCP/IP Enterprise Edition* from Dundas Software. This software supplies some code in a static library, and some in a dynamic library named UTSecureLayer.dll. The actual encryption code is not supplied by us or Dundas; instead, Microsoft's CRYPT32.dll is used. CRYPT32.dll is dynamically linked and must already be present on the user's computer. (MOVEit products do not install CRYPT32.dll.)

9. We do not use Java byte code.
10. The product is supplied as compiled and linked Microsoft .exe and .dll files. No special checksumming or obfuscation is used to prevent binary editing of the files.

Section d - Components

1. - 4. Not applicable - we are not selling components.

Section e - Source code

1. - 3. Not applicable - we are not attempting to distribute source code.

User's Guide

Introduction

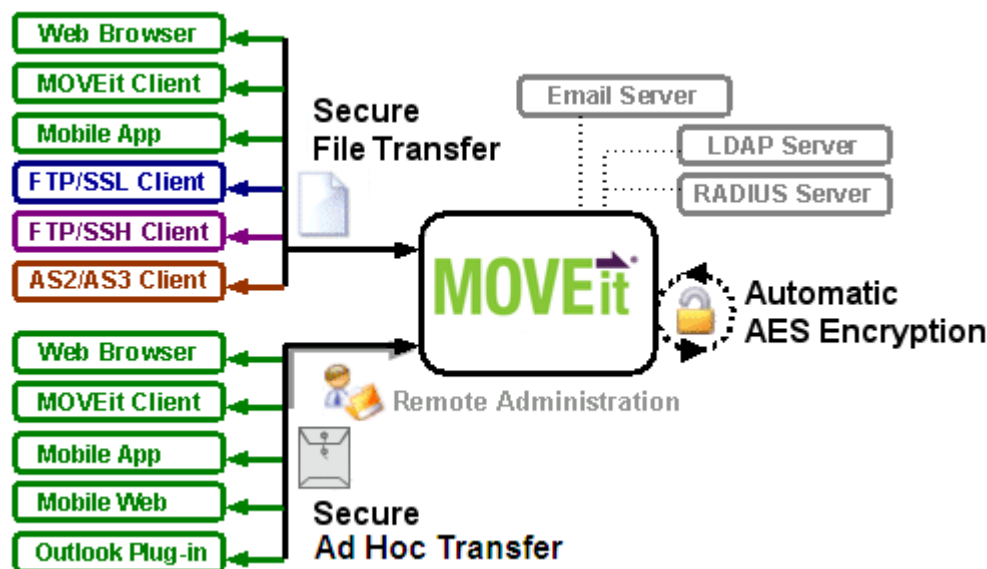
This section provides an overview of the MOVEit secure transfer server capabilities and also provides contact information for getting technical support within your organization.

Overview

Web browsers and no cost/low cost secure FTP clients can quickly, easily, and securely exchange files with MOVEit over encrypted connections using the HTTP over SSL (https), FTP over SSL (ftps) and FTP over SSH (sftp) protocols. And all files received by MOVEit are securely stored using FIPS 140-2 validated AES encryption, the U.S. Federal and Canadian government encryption standard.

In addition, a web interface offers easy online administration and monitoring of MOVEit activities while a programmable interface (via MOVEit API Windows and MOVEit API Java) makes MOVEit accessible to custom applications.

MOVEit includes an optional MOVEit Wizard plug-in that works with Internet Explorer, Firefox and Mozilla to help web-based users to quickly upload and download large and/or multiple files and folder trees to and from MOVEit. There is also a Microsoft Outlook plug-in that users can use for Ad Hoc Transfer.



Encryption and Validation

Encryption capabilities throughout the MOVEit product line are provided by MOVEit Crypto, a compact and fast dynamically-linked library. The AES encryption in MOVEit Crypto has been FIPS 197 validated. The entire cryptographic module has been FIPS 140-2 validated after rigorous examination by cryptographic specialists in the United States' National Institute of Standards and Technology (NIST) and Canada's Communications Security Establishment (CSE).



MOVEit also has an approved Certificate of Networkiness (CoN) from the United States Army. This certification involves a review of how MOVEit meets Army requirements for network security, integration, interoperability, and ease of management and support.

Physical Specifications

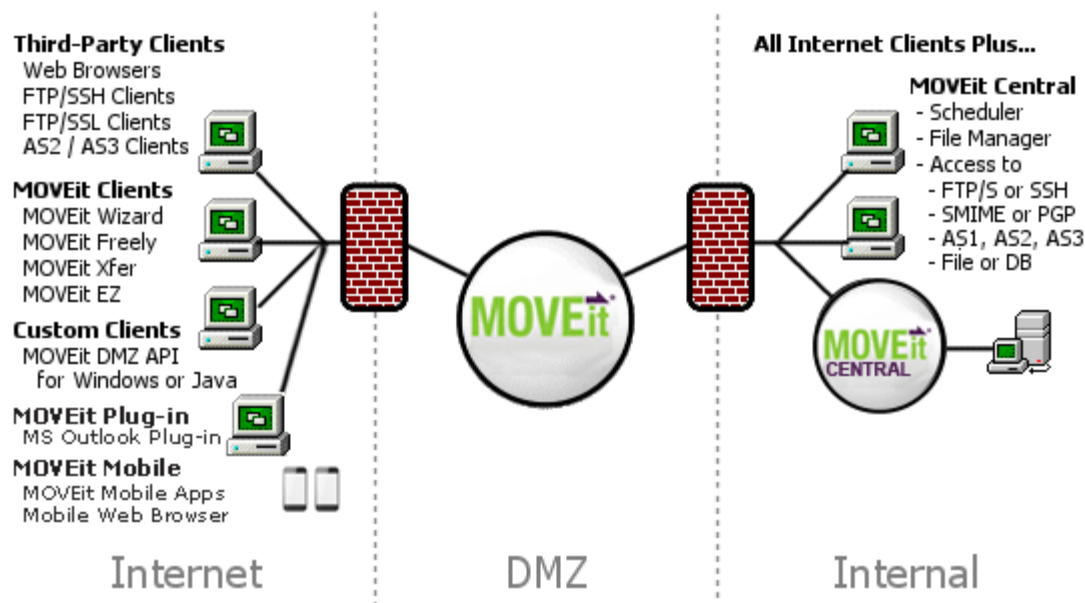
The MOVEit software itself resides on a Microsoft Windows Server platform hardened against threats from the Internet and trusted networks. Organizations that need to support very large volumes of file transfers and/or many users may require additional hardware, but for many organizations the minimum recommended specifications of a MOVEit should suffice:

- 2 GHz Pentium-compatible CPU
- 80 GB SATA or SAS Hard Drive
- 1 GB RAM
- 100/1000 Mb TCP/IP-capable ethernet interface

The latest production recommendations can be found in the **online Support Knowledge Base** (http://ipswitchft.force.com/kb/knowledgeProduct?c=MOVEit_DMZ).

Network Specifications

In a typical network topology MOVEit is best located on a secured "DMZ" segment accessible to both internal and external users. "DMZ" is short for DeMilitarized Zone - a network "no man's land" where both internal and internet hosts are allowed to connect. By default, connections originating from a DMZ network segment are not to be trusted and are usually not allowed unless there is a compelling case to allow a particular service through.



Web and secure FTP clients can upload and download files to MOVEit from internal and external networks. For security reasons, MOVEit is NOT permitted to establish connections with or push files to systems on either your internal network or on an external network. (If a "proxy push" or "proxy store-and-forward" solution is desired, MOVEit Central can be used with MOVEit to fill this role.)

MOVEit's Security Advantages Over Other "Secure FTP" Solutions

There are three areas where files are at risk when transferred between an external network (such as the Internet) and your internal network:

- When transferred over the Internet to a system in your DMZ.
- When temporarily stored on a system in your DMZ.
- When transferred from the system in your DMZ to a system on your internal network.

Most secure Web and FTP file transfer products reside on a system in a DMZ and use industry-standard SSL or SSH to provide secure transfers between the Internet and DMZ. (MOVEit does as well.)

Unfortunately, that is as far as most products go; they fail to secure files stored on the DMZ (at risk if the DMZ box gets hacked) and fail to secure files being transferred between DMZ and MY ORG (at risk if a hacker sets up a sniffer inside the DMZ).

MOVEit secures all three areas by using SSL/SSH-encrypted transfers for ALL transfers and by using FIPS 140-2 validated AES encryption to secure files on disk.

In addition, only MOVEit offers complete end-to-end file integrity over FTP. In other words, files transferred with secure FTP or web clients which support file integrity checks through the MOVEit system can be proven to be 100% identical to their source files through the use of SHA-1 cryptographic hashes. (When combined with authentication, complete file integrity provides non-repudiation.)

Get Technical Support

The technical support page provides information about and a point of contact for technical support at your organization. (People who may reset your password, find out why a particular file was not delivered, etc.)

Technical Support

Information

This page directs you to technical support.

Contact

Main Contact(s): KE

Email Address: name@company.com
WARNING: Messages sent to this address may not be encrypted. Use Ad Hoc Transfer, a secure web form or other secure channel if your inquiry is sensitive.

Current Environment

IP Address: 172.0.0.0

Server Application Version: MOVEit DMZ Enterprise 8.0.9.172

Server Name: 08R2DOC

Server .NET Framework Version: 4.0.30319.17929

Browser: Firefox Browser 27.0

Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0

The Current Environment section provides specific information about the site software, your browser and your address which may be useful to your local technical support personnel.

Note: The Server Application Version is only visible to authenticated users. The Server Name and Server .NET Framework Version are only visible to authenticated Admins and SysAdmins.

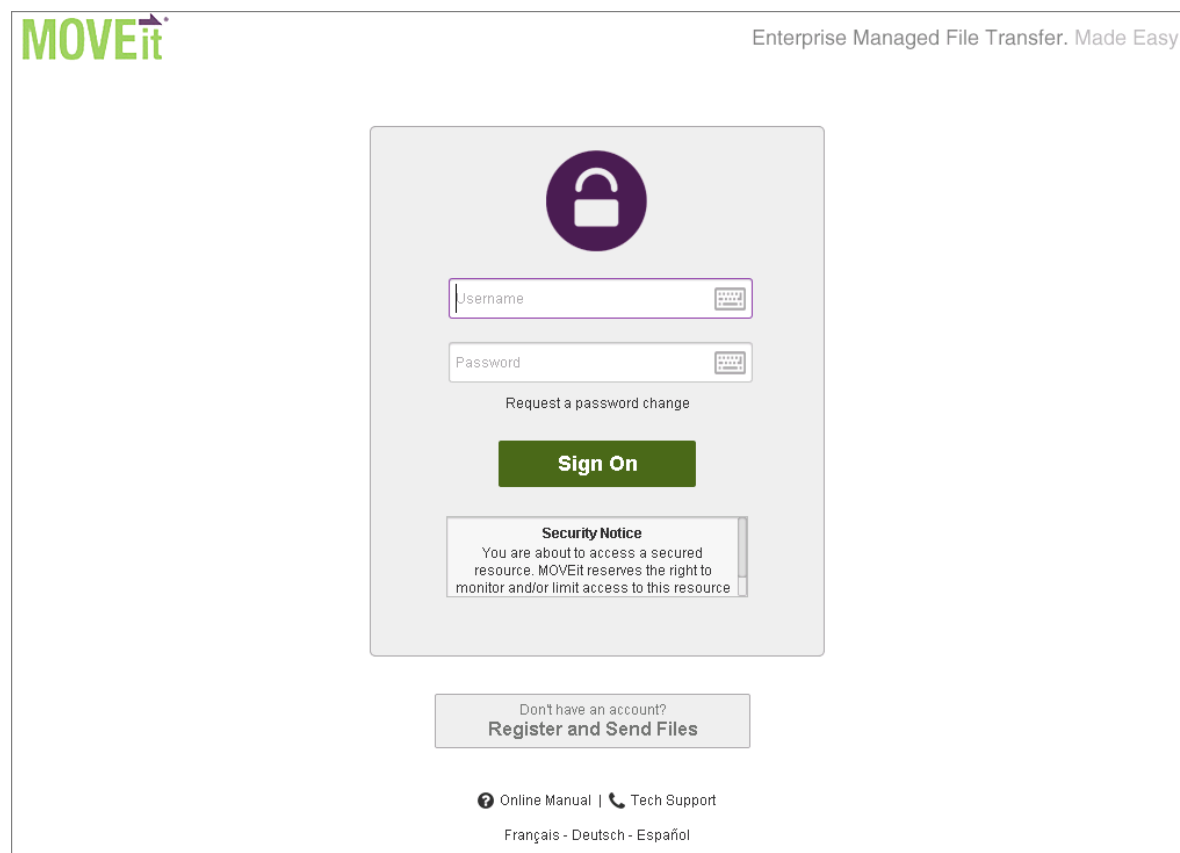
Note: ADMINs ONLY – You can change the information on the Technical Support page online. On the Home page, click the Settings link, then, in the Appearance section, click the Tech Support link to edit this information. Typically, the values here should help point end users to your help desk.

Get Started

This section helps you sign on, install the Upload/Download Wizard, and gives you a brief overview of the workspace.

Sign On

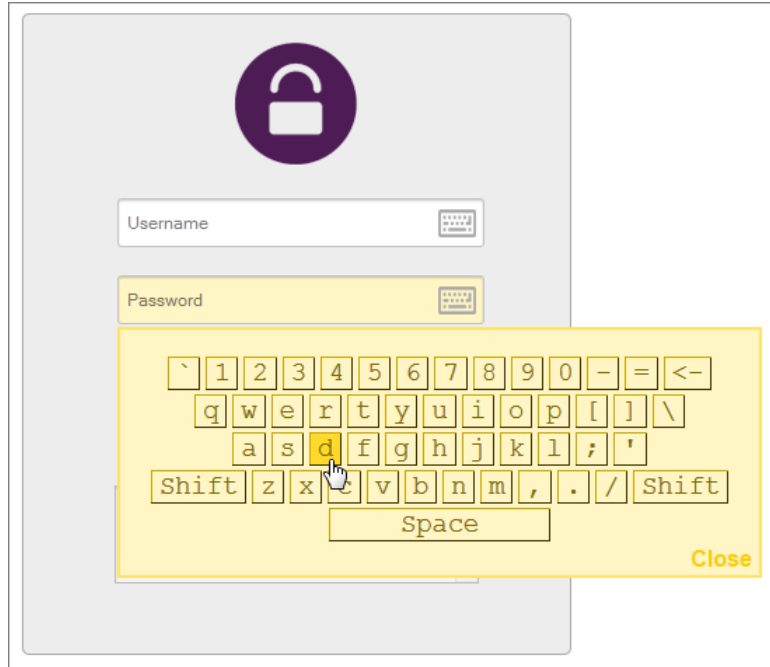
The Sign On page is the first page you see on the MOVEit site. This page contains fields for your Username and Password and a Sign On button to send this information to MOVEit.



The screenshot shows the MOVEit Sign On page. At the top left is the MOVEit logo, and at the top right is the tagline "Enterprise Managed File Transfer. Made Easy." The main content area is a light gray box containing a dark purple padlock icon. Below the icon are two input fields: "Username" and "Password". Below the password field is a link "Request a password change". A large green "Sign On" button is centered below these fields. Below the button is a "Security Notice" box with the text: "You are about to access a secured resource. MOVEit reserves the right to monitor and/or limit access to this resource". At the bottom of the sign-on box is a link "Don't have an account? Register and Send Files". At the very bottom of the page are links for "Online Manual" and "Tech Support", followed by language options: "Français - Deutsch - Español".

Protect Against Keystroke Loggers

Clicking on the keyboard icons next to the **Username** and **Password** fields will open a clickable keyboard which can be used to enter your authentication information. Using the clickable keyboard can help thwart keystroke loggers. If you are logging on to the MOVEit site from a public computer, it is highly recommended you use the clickable keyboard to enter your Username and Password.



When you click **Sign On**, your username and password are transmitted securely (via HTTPS) to MOVEit. If your sign on attempt fails, you will see an error message. If you attempt to sign on too many times in a short period of time you may get locked out of the system altogether. If you need assistance, use the **Tech Support** link on the Sign On page to contact someone who can help you.

Invalid username/password or not allowed to sign on from this location.

If your sign on succeeds you will be rewarded with a success message.

Welcome to TestOrg! Please watch this area for important messages.

The page you will see immediately after signing on depends on how you got to the sign on page in the first place. If you clicked a link from your web browser or typed a short URL into your browser, you are now most likely at the Home Page. If you clicked a link from an email notification, you are now either looking at a package or file.

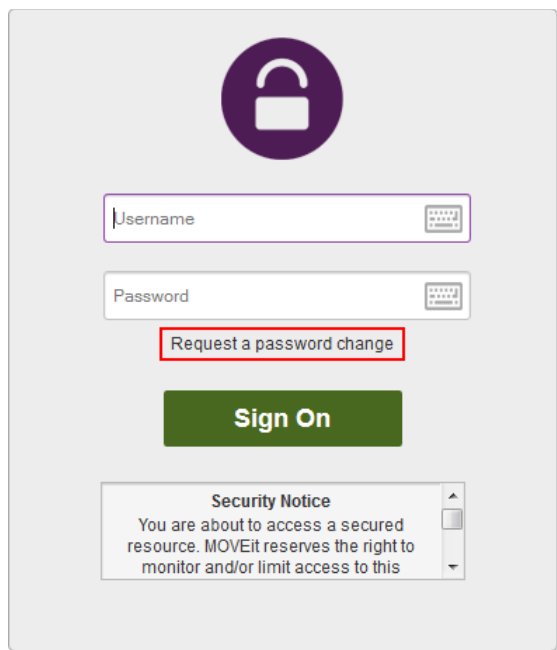
Common Reasons Access is Denied

For security reasons, the *same* message is displayed to anyone who fails to sign on for any of the following reasons. (You will only be told *that* access was denied, not *why* access was denied.)

- Username is incorrect
- Password is incorrect
- Account has been suspended (for too many bad signon attempts, password aging, or manual administrator action)
- Account is not allowed to sign on from this IP address
- IP address has been locked out (for too many bad signon attempts, often with different usernames)
- Client certificate has not been provided when one is required, or a bad client certificate has been provided.

Request a Password Change

Some organizations may allow you to request an automatic password change if you have forgotten your password, to avoid a round trip though technical support staff. If this option is enabled, a **Request a password change** link will be present at the bottom of the Sign On page.



The screenshot shows a sign-on interface with a purple padlock icon at the top. Below it are two input fields: 'Username' and 'Password', each with a small 'Remember Me' checkbox to its right. A red rectangular box highlights the 'Request a password change' link located below the password field. Below this link is a green 'Sign On' button. At the bottom, there is a 'Security Notice' section with a scrollable text area containing the message: 'You are about to access a secured resource. MOVEit reserves the right to monitor and/or limit access to this'.

Clicking this link opens the Password Change Request page. This page will prompt you for your Username and provide instructions for completing the password change process. Once you enter your Username and click the **Request Password Change** button, an email will be sent to your registered email address, if your account has one, either with instructions for completing the password change, or a notice that the password change was denied.

Request a Password Change

This page is displayed if you click a **Request a password change** link at the bottom of the signon page.

Forget Your Password?

Password Change Request

Please enter your username below and then click the "Request Password Change" button. An email message with more information about the password reset process will be sent to your registered email address. This message may ask you to click on a link to reset your password. If it does, you have 30 minutes to do so before the link expires. If no link is provided in the message, or if you do not receive a message within 15 minutes, you will need to contact your administrator to reset your password.

Username:

Request Password Change

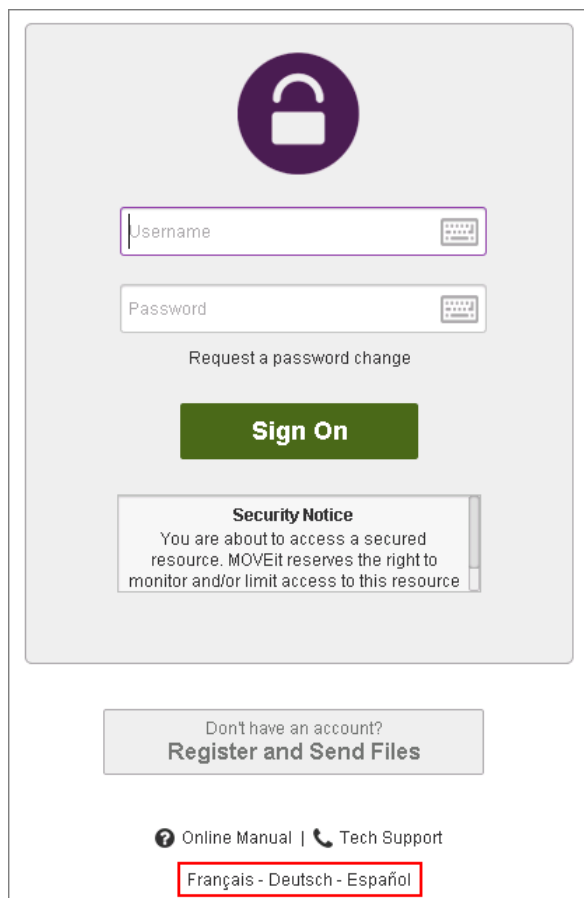
[Return to the sign on page](#)

Enter your **Username** in the field and then click the **Request Password Change** button.

An email message with more information about the password reset process will be sent to your registered email address. This message may ask you to click on a link to reset your password. If it does, you will have the specified amount of time to do so before the link expires. If no link is provided in the message, or if you do not receive a message within 15 minutes, you will need to contact your administrator to reset your password.

Change Languages

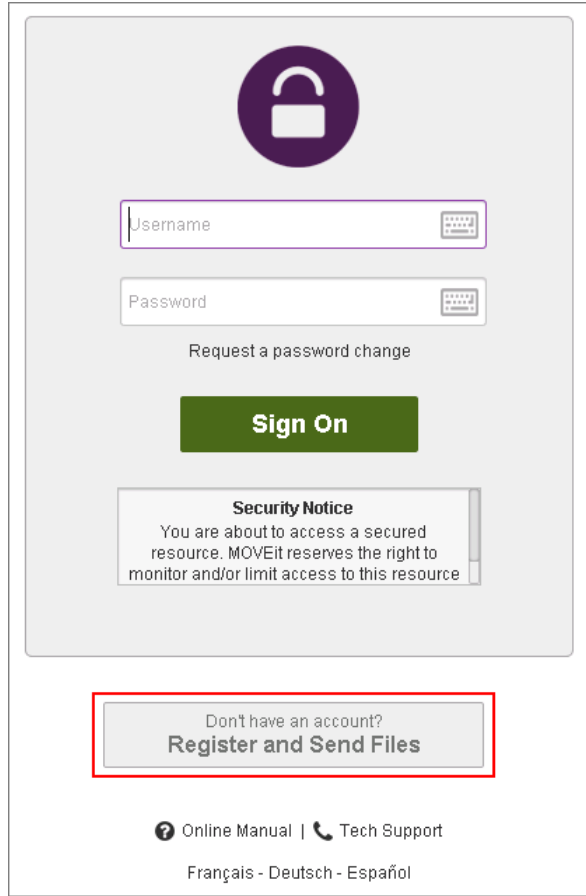
If your organization gives the option to change languages before signing on, MOVEit will provide links to switch the displayed language. Clicking one of the links will change the Sign On page to display in that language, and set a cookie so your language choice is used the next time you sign on.



The screenshot shows the MOVEit Sign On page. At the top is a purple circular icon with a white padlock. Below it are two input fields: 'Username' and 'Password', each with a small 'Show/Hide' button to its right. Under the password field is a link that says 'Request a password change'. Below that is a large green button labeled 'Sign On'. Underneath the 'Sign On' button is a 'Security Notice' box with the text: 'You are about to access a secured resource. MOVEit reserves the right to monitor and/or limit access to this resource'. Below the security notice is a button that says 'Don't have an account? Register and Send Files'. At the bottom of the page, there are links for 'Online Manual' and 'Tech Support', and a language selection box containing 'Français - Deutsch - Español'.

Register and Send Files

Some organizations may allow you to self-register in order to send a package. Self-registering users are handled according to the organization's configuration as either one-time guest users or limited-time temporary users. If this option is enabled, a Register and Send Files link will be present at the bottom of the Sign On page.



The screenshot shows the MOVEit Sign On interface. At the top is a purple padlock icon. Below it are two input fields: 'Username' and 'Password', each with a small icon to its right. Under the password field is a link that says 'Request a password change'. Below that is a green 'Sign On' button. Further down is a 'Security Notice' box with the text: 'You are about to access a secured resource. MOVEit reserves the right to monitor and/or limit access to this resource'. At the bottom of the main content area, a link is highlighted with a red rectangle; it says 'Don't have an account?' followed by 'Register and Send Files' in bold. At the very bottom of the page are links for 'Online Manual' and 'Tech Support', and a language selection bar showing 'Français - Deutsch - Español'.

Clicking this link will open the Register and Send Files page. This page has fields for your recipient's email address as well as for your email address.

Register and Send Files

Separate multiple emails with a comma

Recipient Email(s):

Your Email:

[Register and Send Files](#)

Security Notice
You are about to access a secured resource. MOVEit reserves the right to monitor and/or limit access to this resource at any time. You are about to access a secured resource. MOVEit reserves the right to monitor and/or limit access to this resource at any time.

[Return to the sign on page](#)

Need Help? [Tech Support](#)

Forget your password? [Request a password change](#)

Depending on how the organization has set this up, the page might also offer a "Captcha" box to provide verification that you are a person and not an automated process.

Register and Send Files

Separate multiple emails with a comma

Recipient Email(s):

Your Email:

Answer Question:



Type the text

[Privacy & Terms](#)

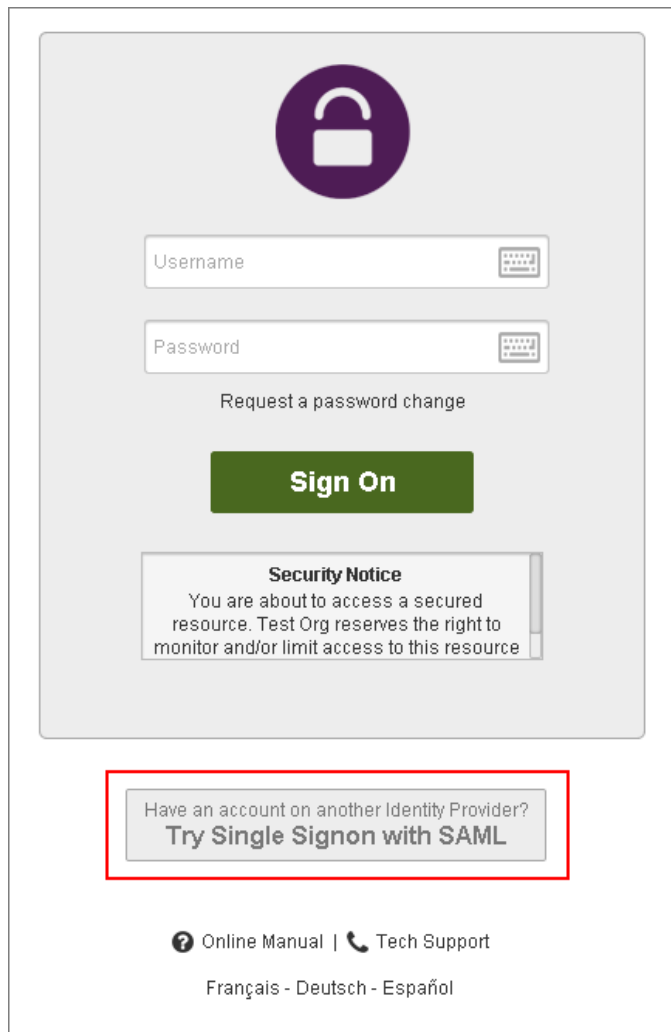


[Register and Send Files](#)

Once you enter the requested information and click the **Register and Send Files** button, you will either be signed in immediately or you will receive a page explaining that an email is being sent to your email address with information and instructions for completing the registration.

Single Signon

If your organization gives the option to use Single Signon, MOVEit will provide a link to show your sign on options.



The screenshot displays the MOVEit login page. At the top is a purple padlock icon. Below it are input fields for 'Username' and 'Password', each with a small icon to its right. A link 'Request a password change' is positioned below the password field. A green 'Sign On' button is centered below the links. A 'Security Notice' box contains the text: 'You are about to access a secured resource. Test Org reserves the right to monitor and/or limit access to this resource'. Below this, a red rectangular box highlights a link that reads: 'Have an account on another Identity Provider? Try Single Signon with SAML'. At the bottom, there are links for 'Online Manual' and 'Tech Support', and a language selection bar showing 'Français - Deutsch - Español'.

Username

Password

[Request a password change](#)

Sign On

Security Notice
You are about to access a secured resource. Test Org reserves the right to monitor and/or limit access to this resource

Have an account on another Identity Provider?
Try Single Signon with SAML

[? Online Manual](#) | [Tech Support](#)

Français - Deutsch - Español

Single Signon lets you sign on using an account with an Identity Provider. Your organization may be configured to use an Identity Provider that can authenticate your username and password and sign you on to multiple applications, including MOVEit.

Click **Try single signon with SAML**. If there are multiple Identity Providers for your organization, you are prompted to select one.

Select Identity Provider

Several SAML Identity Providers are supported by this organization. Please select the one you wish to authenticate to. If you do not know, leave the default choice selected.

You may also select the "Remember" checkbox to have this server remember your selection going forward.

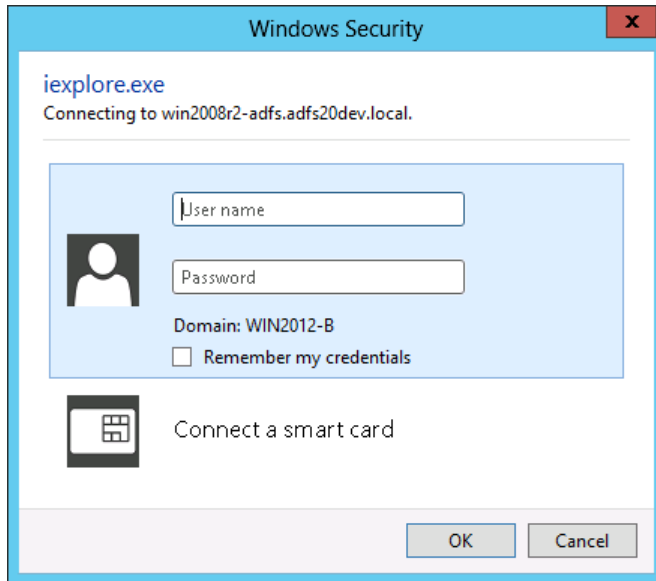
- ☒ ADFS IdP #1
<http://Win2008R2-ADFS.adfs20dev.local/adfs/services/trust>
- ☐ Multiple IdP Selection Test; Do Not Use
<http://sts.ipswitch.com/adfs/services/trust>

☐ Remember selection

Continue

Optionally, select **Remember selection** so that you can bypass the Select Identity Provider step on your next signon.

Click **Continue**. The Identity Provider's sign on screen opens.



Enter your username and password and click **OK**. Provided your account information is valid, the Identity Provider authenticates you and sends the information to MOVEit. Your MOVEit Home page opens.

On subsequent signons, if you are already authenticated (via your Identity Provider) from MOVEit or another application, corporate, or network account, when you open MOVEit, you will go directly to your Home page.

Note: If you click **Cancel** on the Identity Provider's signon page, an error page is displayed. To sign on, you must restart your MOVEit web interface session.

Client Certificates

Your organization may require you to authenticate to MOVEit with an SSL (X.509) client certificate ("client cert"). This is common when "two-factor authentication" is required.

All client certs are either "self-signed" or "CA-signed". The "CA-" indicates that a "Certificate Authority" has signed the client cert and vouches for the identity of the bearer. Furthermore, CAs are divided into "commercial CAs" that sell client cert issue and signing services to the general public (e.g., Thawte, GeoTrust, etc.) and "corporate CAs" that perform the same client cert functions for their own users.

MOVEit supports self-signed certs, commercial CA-signed certs and corporate CA-signed certs, but only your organization can tell you which client certs it will accept for authentication. Your client cert may be delivered to you as a "*.pfx" file with a password or it may be your responsibility to request a client cert from a CA; again only your organization knows the details of this process.

Various browsers have different ways to install client certs. Internet Explorer (IE) uses the Windows Certificate Store; you can install and manage client certs through IE's "Certificate" dialog. Windows will also launch a client cert import wizard that will automatically install most client certs into IE if you just double-click "*.pfx" client cert file.

The Mozilla/Firefox line of browsers uses its own client cert store. To install client certs in these browsers you must use their "Certificate Manager".

Various browsers also have different ways to select client certs for authentication. The most common way is for the browser to simply ask you (via a pop-up dialog) about which client cert to use. When connecting to a MOVEit server, you may be prompted through your browser to select a client cert after you fill in your username and password or before you view the sign on screen.

However, most browsers also have options to automatically present a client cert if you only have one installed or not ask you about picking a client cert if you did not present one. In these cases you may be using client cert authentication behind the scenes (in the "one cert, so don't ask" case) or not at all (in the "no certs installed, so don't ask" case).

Finally, the private key on your client cert may be password protected. If this is the case you may need to type in the password you created when you opted to protect this client cert or key store as well. (Usually, such prompting takes place once per session.)

Next, see Tour the Interface.

Install the Upload/Download Wizard

Depending on how your system is configured, the first time you sign on to MOVEit you may see the Upload/Download Wizard page. The Upload/Download Wizard is a useful browser add-on tool that helps you transfer files faster and more efficiently. It is recommended that you install the Wizard. The benefits include:

- No maximum size (files larger than 2 gigabytes are allowed)
- Faster uploads due to compression on the fly (ActiveX only)
- Cryptographic quality (FIPS 140-2 SHA-1) integrity check
- Transfer resume avoids resending lost pieces of large files
- Option to zip multiple files into a single file before transferring
- Option to send multiple files in single transfer session

If you do not see the Upload/Download Wizard page or do not wish to install it at this time, proceed to **Tour the Interface** (on page 21).

You may still be able to install the Wizard by going to **My Account > Edit Your Upload/Download Wizard Settings**. See the sections that follow for browser-specific Wizard instructions.

Internet Explorer

Internet Explorer users will see the ActiveX Wizard Installation page, which gives options to install the ActiveX Wizard (if it's not installed yet), enable the Wizard, enable the Wizard for this session only, or disable it the Wizard.

ActiveX Upload/Download Wizard

The Upload/Download Wizard is a browser add-on that allows you to:

- Transfer files faster
- Transfer files greater than 2GB
- Transfer multiple files at once
- Perform automatic integrity checking to ensure file non-repudiation
- Compress/Uncompress data on the fly
- Add files via drag-and-drop

The ActiveX version of the Upload/Download Wizard requires Internet Explorer.

The ActiveX Upload/Download Wizard is NOT Installed and is Disabled

 **Install the Upload/Download Wizard (ActiveX)**

~ OR ~ [Return to My Account](#)

 You will NOT be able to install the ActiveX Wizard on some computers.

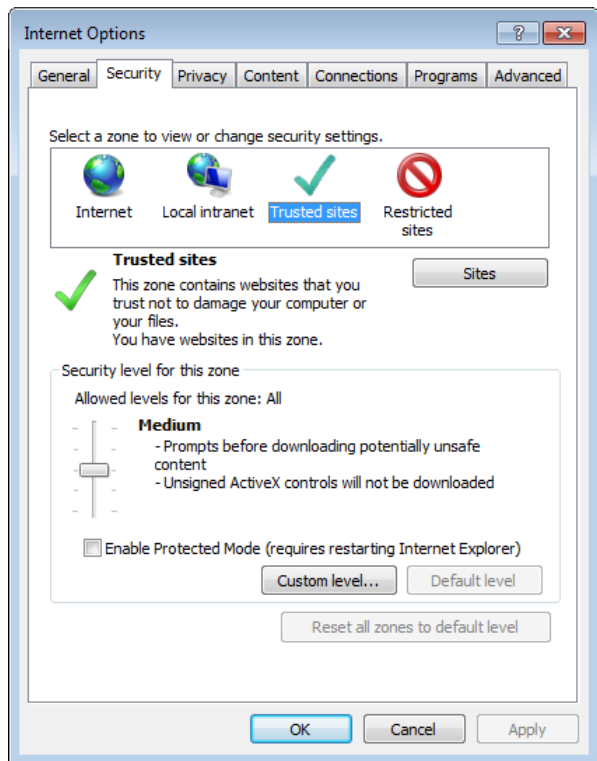
- You must have administrative privileges on your machine to install the ActiveX Wizard. (Many users, especially home users, already enjoy these rights. Most 'public terminal' users, however, will not have these rights. Ask your IT department if you are unsure.)
- Internet Explorer must be configured to allow you to install SIGNED ActiveX controls. (This right has been the default for some time, but some recent versions of IE have been restricting this right to 'Trusted' or 'Intranet' sites only. If this is the case, please add this site to your list of 'Trusted' or 'Intranet' sites.)

If you choose **Install the Upload/Download Wizard (ActiveX)**, you will be sent to a page which will attempt to download the ActiveX control. This may take several seconds. You may need to alter your browser's security settings to permit signed ActiveX controls to be installed in order to successfully complete the process.

If you choose **Disable the Wizard**, you will not be prompted to install the ActiveX Wizard again unless you explicitly request it via the Account Options page. If you choose **Disable the Wizard (for this session only)**, during the next browser session, you will be shown a link to install the Wizard.

If you are running Internet Explorer, you may have to perform an extra step before you can use all the features of the Wizard, such as the ability to download multiple files at once. This extra step is to add any MOVEit site you communicate with into your Internet Explorer list of "Trusted Sites".

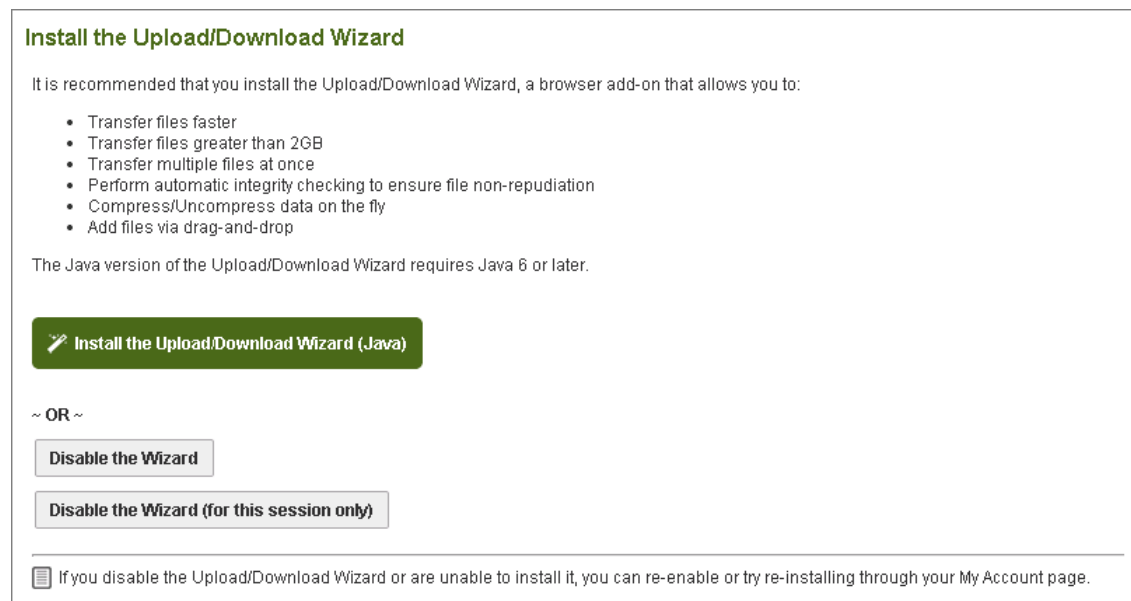
To change your security settings in this way, from the **Tools** menu select **Internet Options** and then select the **Security** tab.



Click the **Trusted Sites** icon (the green check mark) and then click the **Sites** button. A list of existing trusted sites will appear and your MOVEit site should be listed in the **Add this website to the zone** text box. Click **Add** to finish trusting your MOVEit site, and then click **Close**.

Other Browsers

The first time a user signs on to MOVEit with a browser other than Internet Explorer (e.g., Firefox), MOVEit will display a slightly different page with a link to install the Java Upload/Download Wizard. The Java Upload/Download Wizard is a component very similar to the ActiveX Wizard, designed for environments that can't run ActiveX controls.



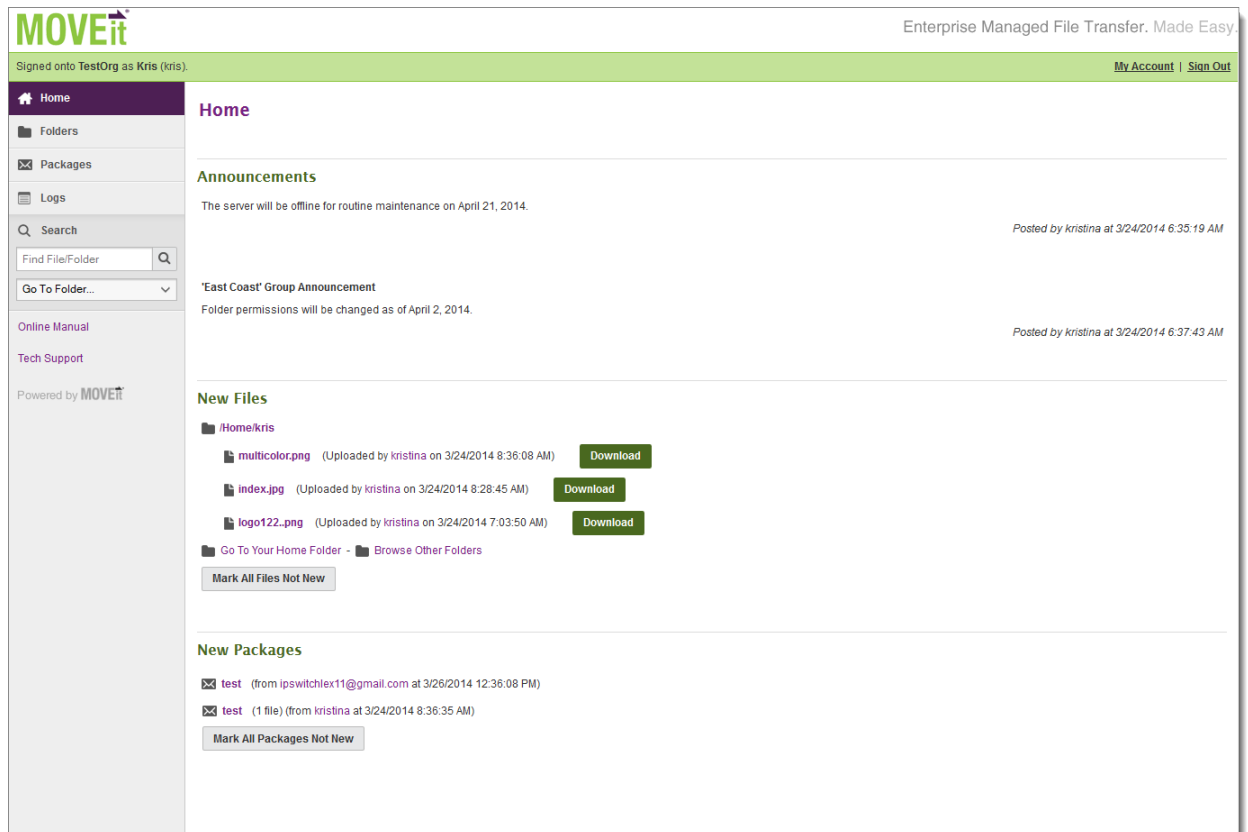
The choices are similar to those for the ActiveX Wizard. If Java is not installed, the user can simply choose **Disable** to avoid being prompted to install the Java Wizard in subsequent sessions.

Java can be downloaded from **Sun's Java website** (<http://java.sun.com/j2se/desktopjava/jre/index.jsp>).

Next, see ***Tour the Interface*** (on page 21).

Tour the Interface

When you first sign on, you see the main workspace:



Note: Depending on your organization's setup, you may not see all areas depicted in this tour.

The following topics introduce you to each area of the workspace:

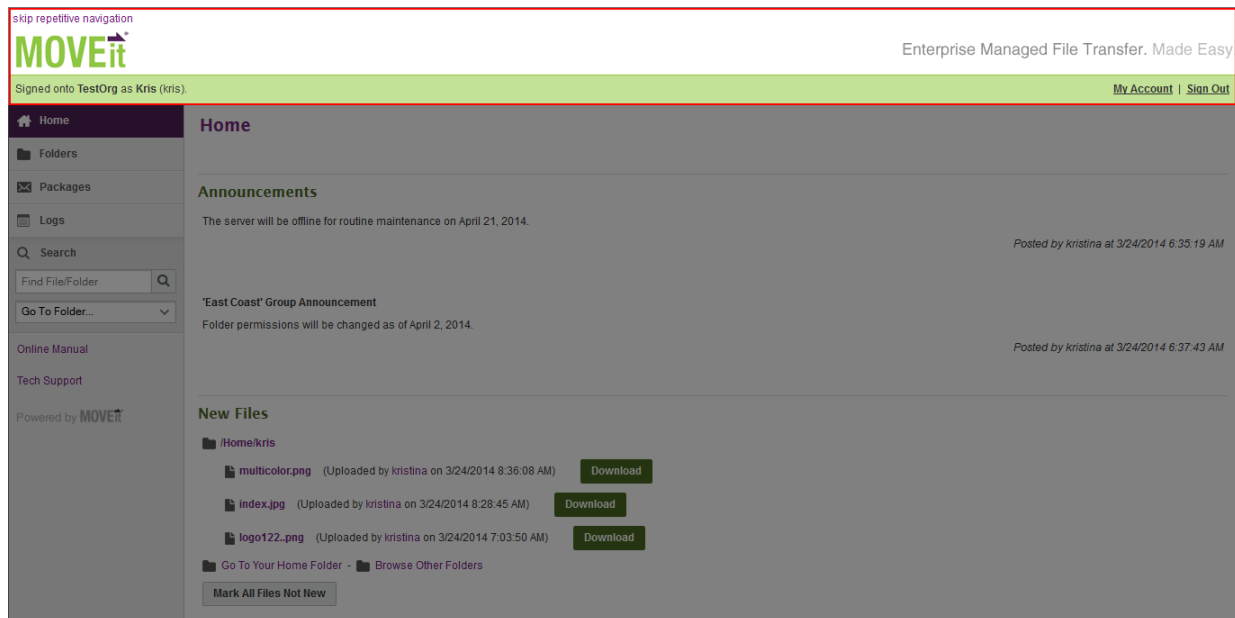
Top Banner (on page 22)

Left Navigation (on page 23)

Main Workspace (on page 25)

Top Banner

Organizational branding and information about your account fill the top of every screen.



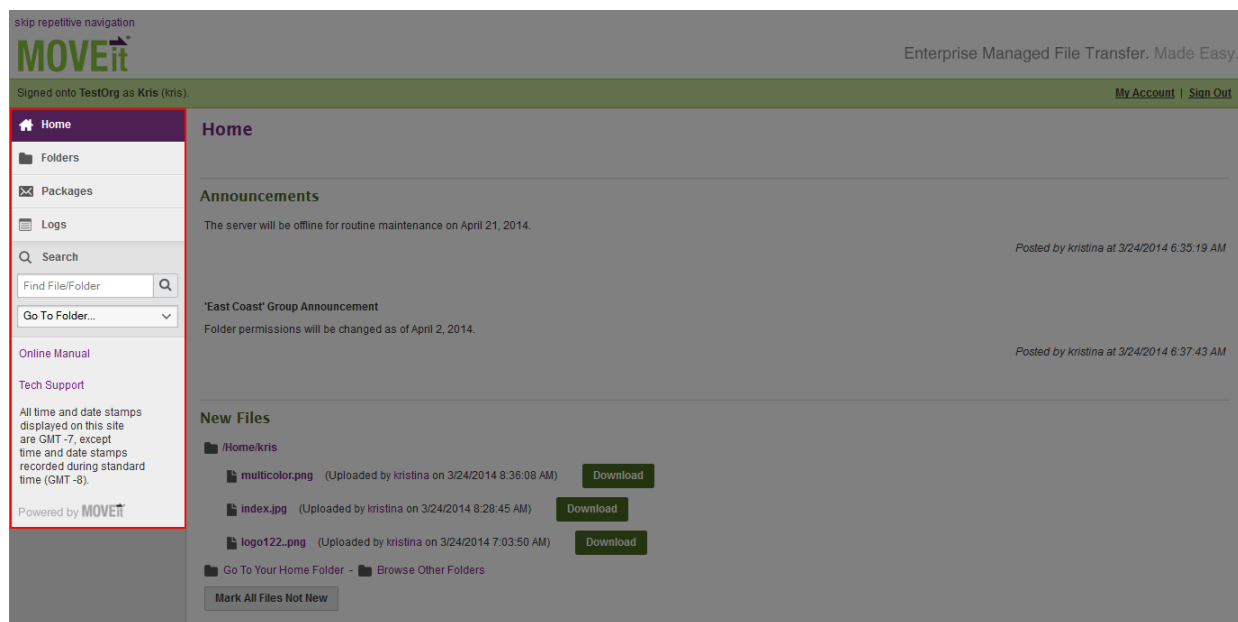
The top banner contains the following information:

- **Skip Repetitive Navigation Link** - An optional link that allows disabled readers to skip past the common top and side links to get to "the page content."
- **Identity Message** - A brief "signed onto [Organization Name] as [Full Name]" message reminds users who they are (especially those with multiple accounts on the same machine). If your username is different than your full name, the username will be displayed in parenthesis here as well.
- **My Account** (on page 109) - An optional link to your account page where you can view your user expiration details, change your password, change the language, edit your package delivery options, and install or disable the Upload/Download Wizard.
- **Sign Out** (on page 114) - A link that lets you sign out.

Next, see **Left Navigation** (on page 23).

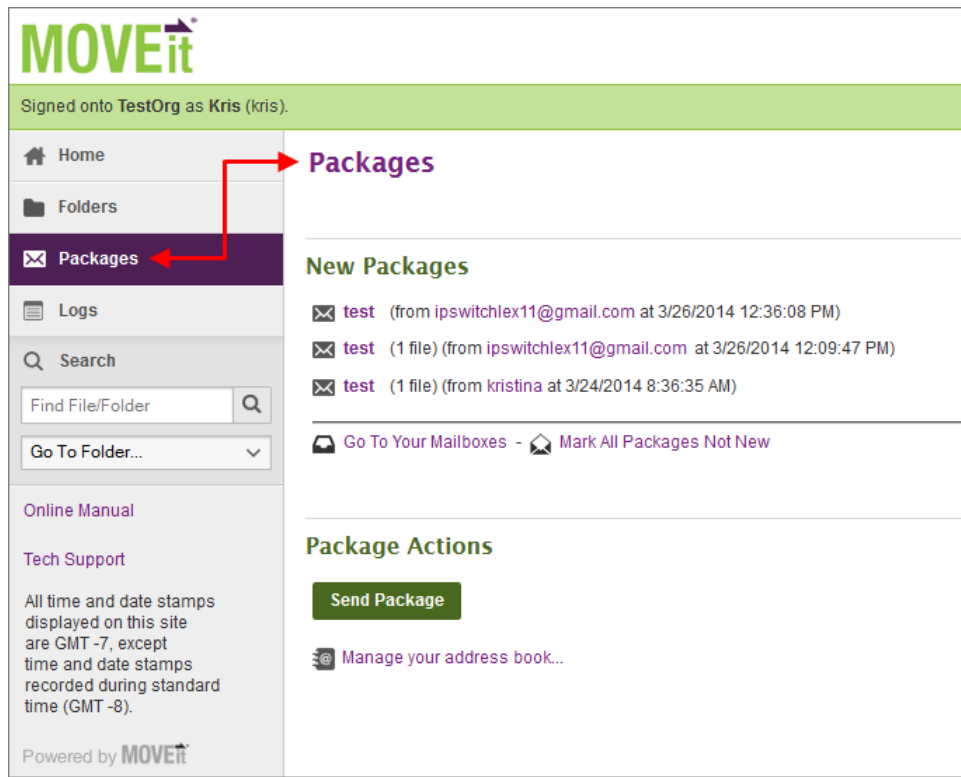
Left Navigation

The left side of the screen contains links that let you jump to different pages, such as your Home page, the Folders page, the Packages page, and Logs:



Note: Depending on your organization's setup, you may not see the left navigation area, or may see only some of the items displayed in the example.

Use the left navigation menu to control what displays in the main workspace. The currently page highlights purple in the left menu.



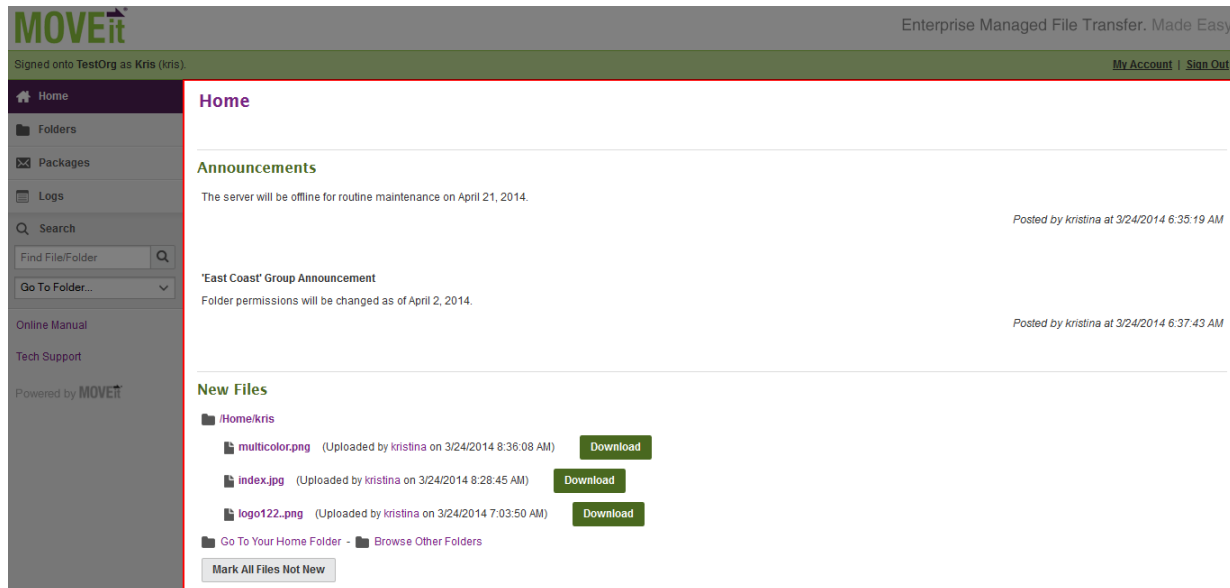
The left navigation area also contains:

- A Search box to help you find files and folders.
- A Go To Folder selector that lets you go quickly to a specific folder to view its contents.
- An Online Manual link that opens helpful documentation. Your organization may also include a custom help link here.
- A Tech Support (on page 5) link that tells you how to get more help if you need it.
- A GMT time zone offset statement that allows users in any timezone to reconcile timestamps displayed here with any other audit materials they may have available locally.

Next, see **Main Workspace** (on page 25).

Main Workspace

The main workspace is where you do most of your work. You control what displays in the main workspace by selecting an item from the **left navigation** (on page 23) menu.



The main workspace displays the item you select in the left navigation. Depending on your permissions, the main workspace may display the following pages:

Home page (on page 26)

Folders (on page 30)

Packages (on page 37)

Home Page

Your **Home** page displays initially. It is a friendly starting point for both administrators and users. From this page you can see any new files which have been uploaded or posted for you, browse to various folders to retrieve old files, or upload a file into the system. If Ad Hoc Transfer is enabled, you can also send a file package to one or more individuals, and you will see any new packages sent to you.

Note: The items on your **Home** page may vary depending on your organization's setup.

The screenshot displays the MOVEit Home page. At the top, the MOVEit logo is on the left, and the tagline "Enterprise Managed File Transfer. Made Easy" is on the right. Below the logo, a green bar indicates the user is "Signed onto Org 1 as Lynn (lynn)". To the right of this bar are links for "My Account" and "Sign Out".

A left-hand navigation menu contains the following items: "Home" (selected), "Folders", "Packages", "Logs", "Search", "Online Manual", and "Tech Support". Below the menu, a note states: "All time and date stamps displayed on this site are GMT -7, except time and date stamps recorded during standard time (GMT -8)." At the bottom of the menu area, it says "Powered by MOVEit".

The main content area is titled "Home". It features a section "Browse Files and Folders" with instructions on how to search for a file. Below this are links for "Go To Your Home Folder" and "Browse Other Folders".

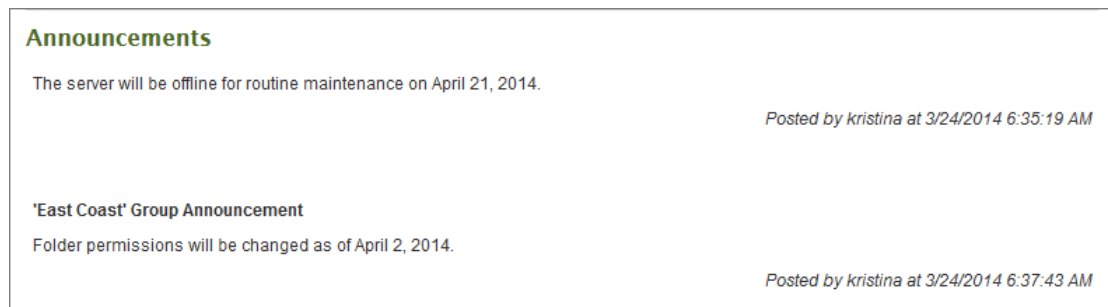
The "New Packages" section lists two packages: "test 2" and "test 1", both from "kristina" at 8:01:54 AM and 8:01:46 AM respectively. A button "Mark All Packages Not New" is provided.

The "Upload a File" section includes a folder selection dropdown (currently showing "/ Home / lynn"), a "Choose a file" button (with "No file chosen" text), a text box for "Enter any notes:", and an "Upload" button.

The "Package Actions" section at the bottom contains a "Send Package" button and a link "Manage your address book..." with a small icon.

Announcements

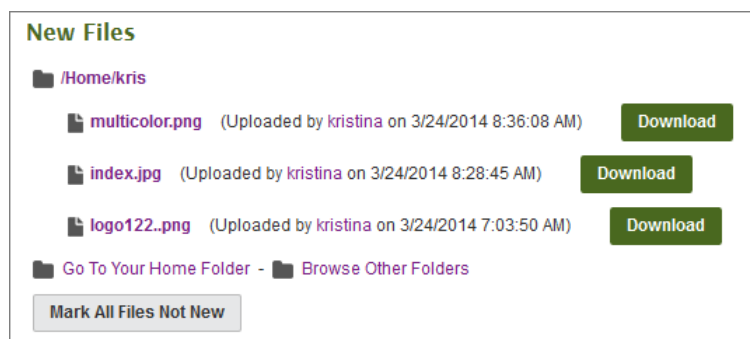
Some organizations will post an announcement for all users to see after they sign on. The name of the person who posted the announcement as well of the time of the announcement will appear immediately below the announcement itself.



Groups may also post announcements to their members. Group announcements will appear here along with the name of the group the announcement belongs to. As with the organization announcement, the name of the person who posted the announcement as well as the time of the announcement will appear immediately below the announcement itself.

New Files

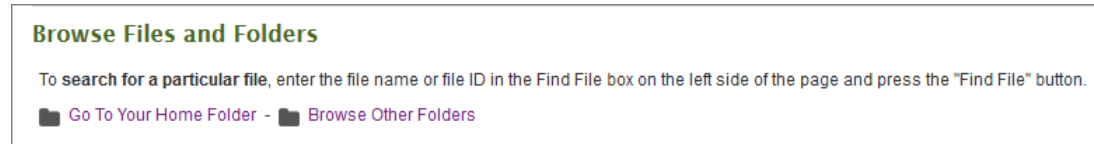
If any new files have been uploaded recently, they will be listed in this section. New files will be organized by folder (clicking on a folder will take you to the folder view). Clicking on the file name will take you to the file view. Clicking on the name of the person who uploaded the file will take you to a brief user profile. Clicking on the **Download** link will pop up a "Save as..." dialog which lets you save the file to your local hard drive. Several links are also shown. One link will take you to your home folder, another will take you to the main folder list. The third link will mark all the new files listed as Not New, so that they will no longer appear in this list.



See **Work With Files and Folders** (on page 42).

Browse Files and Folders...

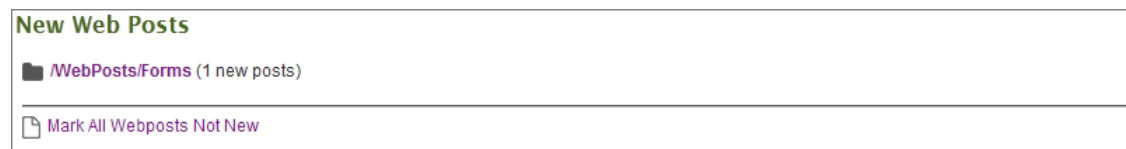
If you currently have no new files to download, the "Browse Files and Folders..." section will be displayed instead. This section provides a hint about using the Find File box to locate files and two links. One link will take you to your home folder, the other will take you to the main folder list.



See **Work With Files and Folders** (on page 42).

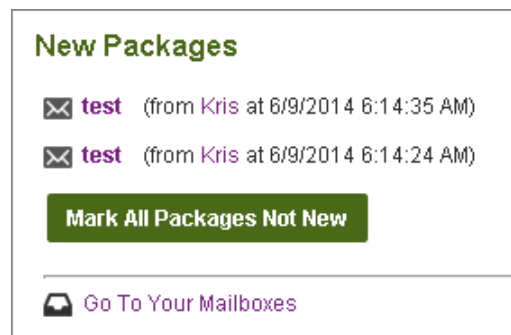
New Web Posts

If you are interested in the collected results in a webpost folder, all folders with new webposts will be listed in this section. Clicking on a folder link will take you to the folder view, from which you may select to download or view the new web posts. A link is also available that will mark all the new webposts listed as Not New, so that they will no longer appear in this list.



New Packages

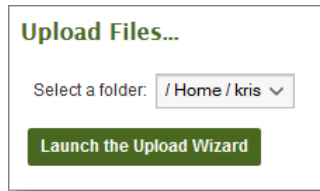
If Ad Hoc Transfer is enabled, any new packages for you will appear in this section. A package can contain a secure note (message) and/or attached files. This list will include any unviewed packages that are not currently located in your Trash mailbox. Clicking on the package subject will take you to the package view, where you can view the package and then perform an action on it, such as downloading files, or moving or replying to the package.



See **View Packages** (on page 90).

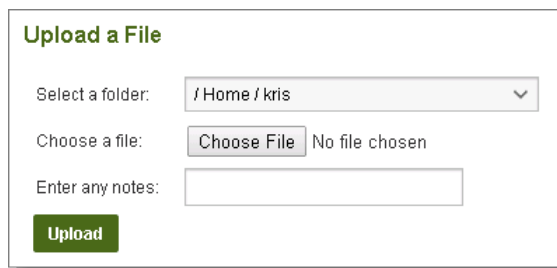
Upload Files...

The form in this section lets you upload files with minimum hassle.

A screenshot of a web form titled "Upload Files...". It features a dropdown menu labeled "Select a folder:" with the text "/ Home / kris" and a downward arrow. Below the dropdown is a green button with the text "Launch the Upload Wizard".

If you have not yet installed the Upload/Download Wizard, visit My Account to install it. The Upload/Download Wizard is a tool that makes web transfers faster and adds the ability to collect several files in a single archive before transfer. See **Upload Files Using the Wizard** (on page 69).

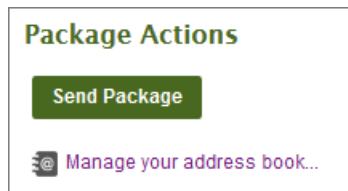
If you choose not to install the Upload/Download Wizard, the following dialog will display instead:

A screenshot of a web form titled "Upload a File". It contains a dropdown menu labeled "Select a folder:" with the text "/ Home / kris" and a downward arrow. Below this is a section labeled "Choose a file:" with a button labeled "Choose File" and the text "No file chosen". Underneath is a text input field labeled "Enter any notes:". At the bottom is a green button labeled "Upload".

Simply follow the steps (notes are optional) and click the Upload button to upload a file into the system. See **Upload a File Without the Wizard** (on page 81).

Package Actions

From this section, you can click Send Package (on page 98) to display the form that lets you create a new package.

A screenshot of a web form titled "Package Actions". It features a green button labeled "Send Package". Below the button is a link with a small icon and the text "Manage your address book...".

You can also click Manage your address book... (on page 107) to view and edit your list of contacts.

Folders

The **Folders** page displays a table that shows all of the contents of a single folder. The initial folder that you view depends on your organization's setup. You can also display other folders to which you have access. Your home folder will usually have your username as its title, and will be located in the organization's top-level Home folder.

The example below shows the contents of the "kris" folder. The name of the folder you are currently viewing displays at the top of the page. "/" is the root folder for your organization.

Folders

/ Home/ kris/

Go To Folder... ▾

☐ ▾	Name	Created	Size/Contents	Creator	⬇	☑		
	↑ Parent Folder							
☐	Test Folder 4	6/6/2014 8:26:10 AM	3					
☐	bootprompt.txt ☑	6/4/2014 8:07:30 AM	3 KB	Kris	-	☑		
☐	index.gif	6/6/2014 7:01:08 AM	14.7 KB	kristina	-			
☐	index_435.gif ☑	6/6/2014 8:25:23 AM	14.7 KB	Kris	1	☑		
☐	logo122.gif	6/6/2014 7:01:27 AM	14.7 KB	kristina	-			
☐	multicolor.gif	6/6/2014 7:01:18 AM	14.7 KB	kristina	-			

Thumbnail File List

Selected File/Folder Actions:

Delete

Send

Download

Destination folder... ▾

Copy

Move

[Advanced Copy/Move Options >>](#)

Upload Files...

Select a folder: / Home / kris ▾

Launch the Upload Wizard

You can quickly view other folders by using the **Go to Folder** (on page 44) drop-down menu, or if you want to search for a folder, use the **Find File/Folder** (on page 45) tool.

The screenshot displays the MOVEit Administrator's Guide interface. On the left sidebar, the 'Go To Folder...' dropdown menu is highlighted with a red box. The main content area shows the path '/ Home/ kris/' and a table of files with columns for Name and Created. The 'Go To Folder...' dropdown menu is highlighted with a red box.

	Name	Created
↑	Parent Folder	
☐	bootprompt.txt	6/4/2014 8:07:30 AM
☐	index.jpg.gif	6/4/2014 10:16:59 AM
☐	logo122.jpg.gif	6/4/2014 10:16:54 AM

A list of the currently selected folder's contents display in a large table. Each line in the table contains a file, a subfolder or a virtual folder. If you have proper permission, you can **Add a Folder** (on page 53) to create sub-folders.

The number of items that display on a single page is set by your administrator. Page navigation links display if the number of items exceeds the per page limit.

The table contains details about each file, subfolder and virtual folder. See **View Folders** (on page 43) for a description of each field.

Click any column header to sort the list by the values in that column.

Depending on your permissions, you may also see action buttons in each row:

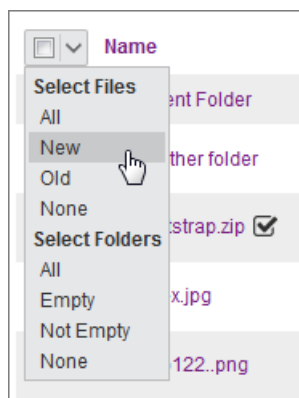
☐	Name	Created	Size/Contents	Creator	↓	✓
	↑ Parent Folder					
☐	Test Folder	6/4/2014 1:15:17 PM	1 2			
☐	bootprompt.txt ✓	6/4/2014 8:07:30 AM	3 KB	kris	-	
☐	index.jpg.gif	6/4/2014 10:16:59 AM	14.7 KB	kristina	2	
☐	logo122.jpg.gif	6/4/2014 10:16:54 AM	14.7 KB	kristina	-	
☐	multicolor.png.gif	6/4/2014 10:17:07 AM	14.7 KB	kristina	-	

Delete (on page 66) a folder or file

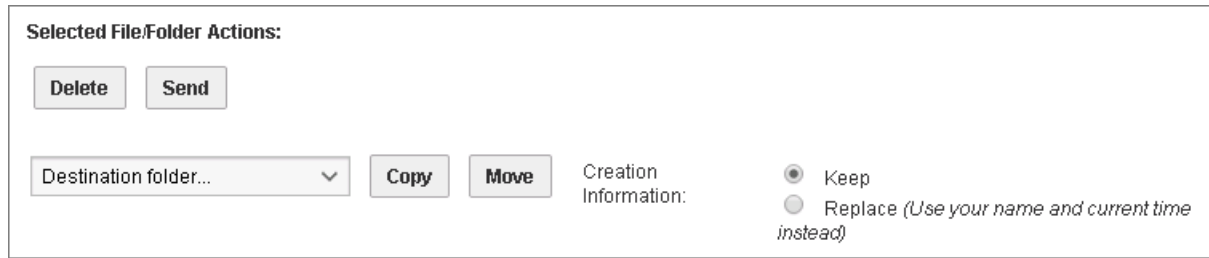
Edit a folder's permissions and settings (available only to users with proper permissions)

Download (on page 83) a file

Use the selector tool at the top of the table to quickly select **All** files, only **New** files, only **Old** files, or **None** to deselect all files. Similarly, you can select **All** folders, only **Empty** folders, only **Not Empty** folders, or **None** to deselect all folders.



After selecting folders and files, you can perform the following actions using the buttons beneath the table, depending on your permissions:



Selected File/Folder Actions:

Delete Send

Destination folder... ▼ Copy Move

Creation Information: ☒ Keep ☐ Replace (*Use your name and current time instead*)

- Delete (on page 66) selected folders and/or files after a short confirmation.
- Send (on page 98) selected files in a new package.
- Download (on page 83) selected folders and/or files using the MOVEit Download Wizard; not available unless the Wizard is installed. If folders are checked, these folders and all their subfolders and all files in these folders will also be downloaded.

Note: For WebPost and Archived Logs folders, selected files will download as a single bundle file using the As Format option to determine the format of the resulting file. This download process does not use the MOVEit Download Wizard.

- **Download All** webpost files in the folder as a single bundle file using the **As Format** option to determine the format of the resulting file. This download process does not use the MOVEit Download Wizard.
- **Copy** (on page 66) selected folders and/or files to another folder (the originals remain intact), or to the same parent folder (the copy will be created with a new name, appending "Copy" to the old name, to differentiate it from the original). Click **Advanced Copy/Move Options** for more control over how folders and files copy.
- **Move** (on page 67) selected folders and/or files to another folder. Click **Advanced Copy/Move Options** for more control over how folders and files move.

A **Thumbnail File List** button may display beneath the table, which allows you to switch to a thumbnail view of the folder's contents:

☐	Name	Created	Size/Contents	Creator	↓	✓
	↑ Parent Folder					
☐	Test Folder	6/4/2014 1:15:17 PM	1 2		✕	⚙
☐	bootprompt.bt ✓	6/4/2014 8:07:30 AM	3 KB	Kris	-	✓
☐	index.gif	6/6/2014 7:01:08 AM	14.7 KB	kristina	-	
☐	index_435.gif ✓	6/6/2014 8:25:23 AM	14.7 KB	Kris	1	✓
☐	logo122.gif	6/6/2014 7:01:27 AM	14.7 KB	kristina	-	
☐	multicolor.gif	6/6/2014 7:01:18 AM	14.7 KB	kristina	-	

Thumbnail File List

After clicking **Thumbnail File List**, you see files display in thumbnail view:

/Home/kris/

Thumbnail File List - Return to Normal View

Thumbnails



index.jpg
Open - View Full Size



logo122.png
Open - View Full Size



multicolore01.png
Open - View Full Size

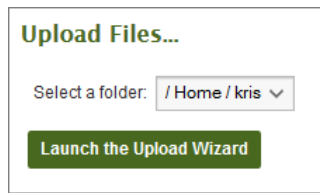
Under each thumbnail, the name of the file displays along with two links:

- **Open** pulls up the normal file view
- **View Full Size** downloads the complete file and renders it in the browser

Click **Return to Normal View** to return to the text-only file list.

Upload a File

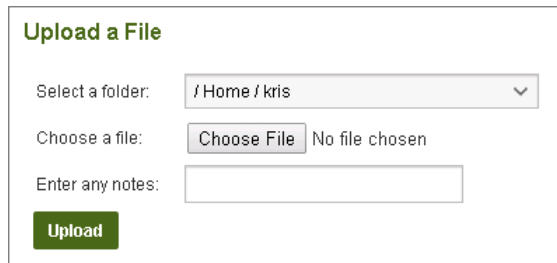
Depending on your permissions, you may also be able to **Upload a File** from the bottom of the page. If you have installed the Upload Wizard (ActiveX or Java), you will see an upload section similar to this:



The screenshot shows a dialog box titled "Upload Files...". It contains a "Select a folder:" label followed by a dropdown menu showing "/ Home / kris". Below this is a green button labeled "Launch the Upload Wizard".

See ***Upload Files Using the Wizard*** (on page 18).

If the Upload Wizard is not installed, you will see an upload section similar to this:



The screenshot shows a form titled "Upload a File". It includes a "Select a folder:" label with a dropdown menu showing "/ Home / kris". Below this is a "Choose a file:" label with a "Choose File" button and the text "No file chosen". There is also a text input field labeled "Enter any notes:". At the bottom left is a green button labeled "Upload".

See ***Upload a File Without the Wizard*** (on page 81).

See also ***Work with Files and Folders*** (on page 42).

Packages

Packages are similar to email messages. A package contains a note and optionally one or more file attachments, and is sent to specific people or groups. Files that are sent as package attachments are uploaded to a MOVEit server, and a new package notification email is sent to the recipients to inform them that a package is waiting for them. Recipients can click on the web link in this notification, sign on to MOVEit and view the package, where they can download the files.

Packages are located within mailboxes.

Click the **Packages** link in the left-navigation to display the Packages page, which contains a list of your mailboxes and the **Package Actions** section.

Packages

Mailbox	✉ New Packages	✉ All Packages
 Drafts	-	-
 Inbox	3	4
 Sent	-	4
 Templates	-	-
 Trash	1	1



Add Box...

Package Actions

Send Package

 Manage your address book...

New Packages might display initially on your Packages page if you have any unread packages. Simply click [Go To My Mailboxes](#) to view your mailboxes

Packages

New Packages

 **update** (from [Kris](#) at 6/6/2014 9:03:08 AM)

 **test** (from [Lynn](#) at 6/4/2014 10:16:04 AM)

 **test** (from [kristina](#) at 6/4/2014 10:15:34 AM)

[Mark All Packages Not New](#)

 [Go To Your Mailboxes](#)

Package Actions

[Send Package](#)

 [Manage your address book...](#)

There are five standard mailboxes (depending on the organization settings): **Inbox**, **Drafts**, **Templates**, **Sent**, and **Trash**, but you can also create custom mailboxes. Custom mailboxes can be nested like folders.

For each mailbox, the number of new packages (✉), and the number of total packages (📁) display. Mailboxes that contain new packages are **bold**.

Click **Empty**  to delete all packages in the **Trash** mailbox.

For custom mailboxes, the following actions are available:

-  **Delete**: Deletes the mailbox and any packages and mailboxes contained within it. Confirmation will be asked for.
-  **Rename**: Allows the user to change the name of the mailbox.
-  **Add Box**: Adds a mailbox within the selected mailbox.

If the organization is configured to clean up old packages, a note will be displayed indicating the age limit for old packages before they are deleted, and whether or not the packages will be archived before they are deleted.

Mailbox Contents

Click on any mailbox to display a list of packages in that mailbox. The **Subject**, **Sender**, number of **Files** in the package, total **Size** of files, and **Date/Time** sent are displayed for each package, as well as a short list of actions that can be performed on that package.

Packages

/ Inbox/

Go To Mailbox... ▾

☐	Subject	Files	Size	From	Date/Time	
☐	✉ Report 88	-	1 KB	Kris	6/6/2014 9:13:57 AM	
☐	✉ 145	1	3.5 KB	Kris	6/6/2014 9:10:30 AM	
☐	✉ update	-	1 KB	Kris	6/6/2014 9:03:08 AM	
☐	✉ test	-	1 KB	Lynn	6/4/2014 10:16:04 AM	
☐	✉ test	-	1 KB	kristina	6/4/2014 10:15:34 AM	
☐	✉ test package	-	1 KB	Kris	6/4/2014 8:07:12 AM	

[Return to Mailboxes](#)

Checked Package Options:

Click a column header to sort the list by the values in that column.

Click on a package to **view that package's details** (on page 90).

To change mailboxes, select the desired mailbox from the **Go To Mailbox** drop-down menu at the top of the page.

Packages

/ Inbox/

▾

- /Drafts
- /Inbox
- /Sent**
- /Templates
- /Trash

Files

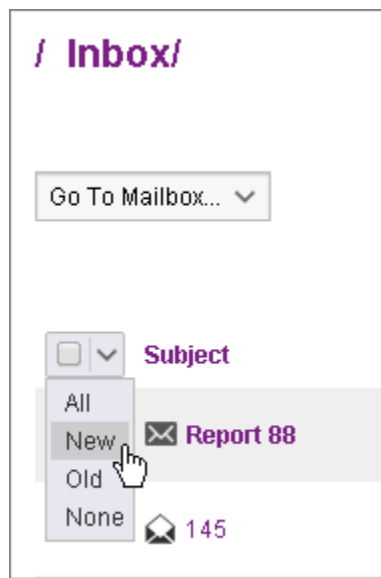
☐	✉ Report 88	-
☐	✉ 145	1
☐	✉ update	-

To place a package in the **Trash** mailbox where it can be permanently removed, click  in that package row. You can also select multiple packages and click the **Trash** button beneath the table.

To mark one or more packages as new, select the package(s) and click **Mark As New**. To mark one or more packages as not new, select the package(s) and click **Mark As Not New**.

To move one or more packages to a different mailbox, select the **Destination Mailbox** from the drop-down selector and then click **Move**.

To quickly select **All** packages, only **New** packages, only **Old** packages, or **None** to deselect all packages, use the package selector tool at the top of the table:



The Sent mailbox displays these additional columns:

- Read Status (): One of three read status icons will display:
 -  All recipients of the package have viewed the package.
 -  Some but not all of the recipients of the package have viewed the package.
 -  None of the recipients of the package have viewed the package.

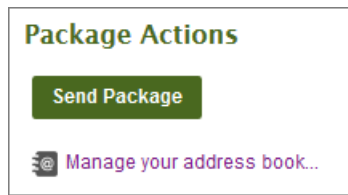
- **To:** Replaces the usual From column, and lists the major recipients of the package.

When you open a Sent package, you can also **recall** (on page 106) it so it is not available for download by recipients.

The **Drafts** and **Templates** mailboxes let you edit  and permanently delete  items there.

Package Actions

Click the **Send Package** (on page 98) link at the bottom of the Packages page to create a new package.



Click **Manage your address book...** (on page 107) to view and manage the contacts in your address book.

Work with Files and Folders

This section describes the MOVEit folder structure and helps you work with files and folders, including uploading and downloading files and folders.

View Folders

Click the **Folders** link in the left navigation to view folders to which you have access:

Folders

/ Home/ kris/

Go To Folder...

☐	Name	Created	Size/Contents	Creator	Download	Integrity
☐	Parent Folder					
☐	Test Folder	6/4/2014 1:15:17 PM	1 2			
☐	bootprompt.bt	6/4/2014 8:07:30 AM	3 KB	Kris		☒
☐	index.gif	6/6/2014 7:01:08 AM	14.7 KB	kristina		
☐	index_435.gif	6/6/2014 8:25:23 AM	14.7 KB	Kris	1	☒
☐	logo122.gif	6/6/2014 7:01:27 AM	14.7 KB	kristina		

Thumbnail File List

Selected File/Folder Actions:

Delete Send Download

Destination folder... Copy Move Advanced Copy/Move Options >>

The name of the currently viewed folder displays at the top of the screen (/ Home/ in the example above). A list of the files and sub-folders contained within that folder display in the table.

The table contains the following information about each item:

- (Checkbox): Selects a folder or file in preparation for an action in the **Selected File/Folder Actions** section.
- **Name:** The name of the folder or file. New files are bold. Files whose integrity was verified during upload are marked with the integrity icon ☒. Click a folder name to open that folder; click a file name to either open the file view or download the file, depending on the organization settings.

Note: If content scanning is enabled, files that pass the content scan (Anti-Virus and/or Data Loss Prevention (DLP) scans) are marked with this icon . Files that fail the scan are marked with a warning icon .

- **File ID:** The unique ID of the file. (WebPost filelists will see this column in place of the Name column)
- **Created:** The date the folder was created or the file was uploaded
- **Size/Contents:** For folders, the number of subfolders and/or files in the folder will be shown, if any exist. For files, the byte count of the file will be shown.
- **Creator:** The user who created the folder or uploaded the file
- **Uploading IP/Agent:** (WebPosts only) The IP address and agent (often a browser) used to upload this file
- **Downloads (↓):** The number of times the file has been downloaded

Note: Even though someone else has downloaded a certain file, it may still be "new to you") This statistic is often used to quickly see what the most popular downloads in a given folder are.

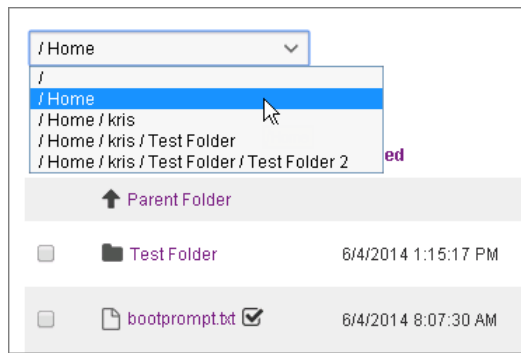
- **Integrity (✓):** If this file was uploaded with integrity checking, an icon is displayed here.

You may also select another folder to view from the **Go to Folder** drop-down menu.

See **Folders** (on page 30) for a description of all items on this page.

Go to a Folder

The **Go To Folder** box (typically located in a colored box on the left side of the screen) lets you quickly jump to your favorite folders. If you have a home or default folder defined, and have permissions to that folder, it will automatically be pre-selected here.

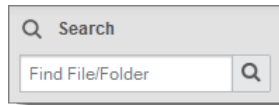


When the **Go To** button is pressed, a view of the selected folder (including a list of any subfolders and files, if applicable) will be displayed.

If you have access to a large number of folders, the **Go To Folder** drop-down will not be displayed. Instead, you can type in the first few letters of the folder you are looking for into the **Find File/Folder** box.

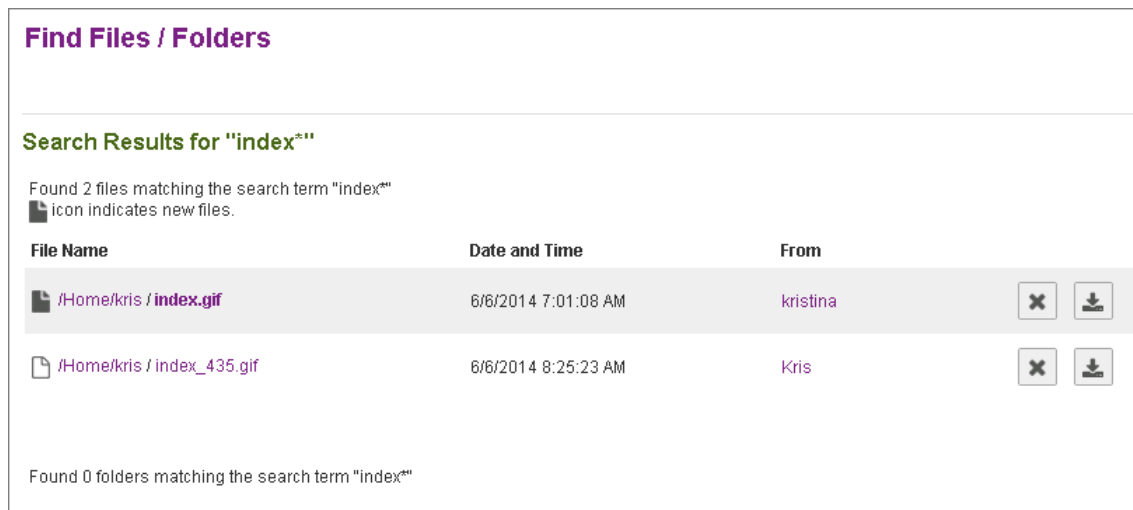
Find Files and Folders

The Find File/Folder box (typically located in a colored box on the left side of the screen) lets you search the MOVEit system for files and folders using either an ID (e.g., "1234567") or a name (e.g., "myfile.txt").



Name wildcards ("*") are allowed and their use is encouraged. For example, you may wish to search for "*.pdf", "myfile*.txt" or "Home/John Smith/*".

Results from searches are displayed as soon as the Find File button is pressed.



The resulting file list has several columns:

- **File Name:** The folderpath and name of the file. If the folderpath is clicked, the user will be taken to a view of this folder. If the name of the file is clicked, the user will be taken to a view of the file.
- **Date and Time:** When the file was uploaded (or created).
- **From:** The full name of the person (or device) who uploaded or created this file. If clicked, this link will go to a view of this user.
- **Action:**
 - **Download:** Downloads this file (in its original format)
 - **Delete:** Deletes this file

The resulting folder list has only one column, containing the full path of the folders matching the search string. Clicking on a folder path will take you to a view of the folder.

Automatic Wildcards

There are two cases where wildcard characters will automatically be added to a search term in order to find results:

- If a search term does not return any results, an asterisk wildcard character will automatically be appended to the search term if one does not already exist, and the search will be retried.
- If a search term containing a slash ("/") does not return any results, and the same search term with an asterisk appended also does not return any results, an asterisk will be prepended to the search term if one does not already exist, and the search will be retried. This allows users to search for partial folderpaths and successfully find them.

View Restricted Folders

Restricted folders are created by the MOVEit installation, and can be one of following types:

- **Archive** - The Archive folder contains folders in which various archived materials are kept. The Logs subfolder collects log extracts automatically generated before online logs are purged. The Packages subfolder collects package archives automatically generated before attached files are purged.
- **WebPosts** - Webpost folders are used to collect data posted from various non-MOVEit web forms by anonymous users. MOVEit offers online preview and individual or collective extraction of these posts as CSV or XML files.
- **AS2** - AS2 folders collect incoming messages and MDNs from AS2 trading partners. (Read more in "***Advanced Topics - AS2 and AS3***" (on page 676).)

These folders are displayed at the "root" level when someone clicks on the "Folders" link on the left side of the page. If a Distribution folder was created, it is also displayed. Archive, WebPosts, and AS2 folders are displayed with an orange folder icon to indicate their "restricted access" status.

View Web Posts

Below is the alternate file list used when viewing web posts; the file list of the built-in Archive folders will also have a different layout. Note the different types of "agents" logged. (From top: Google Chrome, Internet Explorer, Firefox.)

/ WebPosts/ Forms/

Go To Folder... ▾

	File ID	Created	Size/Contents	Uploading IP / Agent		
↑ Parent Folder						
	 987203917	4/7/2014 4:10:44 PM	1 KB	172.16.0.190 /  33.0.1750.154	-	
	 987211809	4/7/2014 4:09:59 PM	1 KB	172.16.0.190 /  9.0	-	
	 987167761	4/7/2014 4:08:04 PM	1 KB	172.16.0.190 /  28.0	-	

Permissions and Settings

View Files

File view pages display current and historical information about a specific file as well as provide links to download it.

(Links from email new file notifications and upload confirmations will also frequently point to file view pages.)

/Home/kris/multicolor.gif
(ID # 103168718)

File Actions
[Download](#) [View Online](#) [Mark As Viewed](#) [Send As Attachment](#)
[Delete](#) [Rename](#) [Renew](#)

File Information
Uploaded by [kristina \(kristina\)](#) at 6/6/2014 10:47:53 AM from 127.0.0.1 via [Mi](#) MOVEit Wizard Java 8.1.0.0
File Size: 15,027 bytes **# of Downloads:** 1
Integrity Verified: Yes ☒ A SHA-1 hash has automatically been used to confirm this file is identical to the original file from which it was uploaded.
Thumbnail:  [View Online](#)

File Log

Time/Date	User	Action
6/6/2014 10:48:39 AM	kristina	Copied file to folder 985735448
6/6/2014 10:48:11 AM	kristina	File downloaded previously at 2014-06-06 10:48:11 integrity checked
6/6/2014 10:48:11 AM	kristina	Downloaded as raw file from 127.0.0.1
6/6/2014 10:47:53 AM	kristina	Uploaded file "multicolor.gif" from 127.0.0.1; integrity verified; upload took 0.047 seconds (319,723 bytes/second)

File Actions

Several different links may appear in this section:

- **Download** - The standard "download this now" link. Downloads the file to your local machine.
- **Download as XML (WebPosts & Logs only)** - Downloads this file in XML format.
- **Download as CSV (WebPosts & Logs only)** - Downloads this file in comma-separated format.
- **Mark as Read (WebPosts & Logs only)** - Makes this file "not new" to you and logs an entry noted you viewed the file online without downloading it to your hard drive.
- **Mark as Viewed (Image files with Thumbnail Previews only)** - Makes this file "not new" to you and logs an entry noted you viewed the file online without downloading it to your hard drive.
- **View Online (Image files with Thumbnail Previews only)** - Displays the image file in the current browser window. An online view counts as a single download of the image.
- **Send As Attachment** - If the Ad Hoc Transfer option is enabled, opens the Compose page and attaches the selected file.
- **Delete** - Deletes this file after a brief confirmation.
- **Rename** - Renames this file.
- **Renew** - Allows an administrator to edit the list of users to whom this file appears marked "New". Renewing a file for a MOVEit EZ user (or MOVEit Central version earlier than 3.2) will cause the file to be downloaded again if the client is configured to only download new files. This allows administrators to "re-queue" a file transfer that has already occurred without having to re-upload the file.
- **Clear DLP Policy Violations** - Allows an administrator to remove the file from quarantine and allow downloads of the file.

File Information

The file information consists of a brief sentence describing how the file was created or uploaded, as well as the file size and number of times it has been downloaded.

A file integrity section notes whether or not MOVEit has authoritatively determined if its copy of this file is identical to the original. (This is an important element of non-repudiation.) This field will normally display a value of NO if a non-IE web browser was used to upload the file, a non-MOVEit FTP client was used to upload the file, or the upload was made through a version of MOVEit before 2.4.

If Content Scanning is enabled, the notes may identify whether the file was scanned for viruses and/or for data loss prevention (DLP). With DLP, file names and the Notes field (associated with an upload) are also scanned for data policy violations.

If any comments were provided while the file was uploaded, they will appear in the lower half of this section below a small dividing line.

If this file is an image file and a thumbnail for it exists on disk, this image will also be displayed here.

File Log

The file log displays a complete history of events regarding this file. When a file is deleted, the file log is the only section still available to display the history of a particular file.

End users will usually see less information displayed here than admins would when the folder's Hide History option is enabled. Usernames, full names, and email addresses of uploaders, downloaders, and users who performed other actions on the file will be hidden in various circumstances to ensure security.

WebPosts

The File View page for a WebPost file is slightly different; see the sample below. Note the additional "File Preview" section and the choice of file formats in the download section (which are also available for Audit Log archive files). Also notice the "Print and Mark as Read for All" link. Clicking this will initiate a Print Page operation in the browser (provided JavaScript is enabled), and then clear all New File entries for this file.

/WebPosts/Forms/
 (ID # 987198821)

File Actions

Download as XML
Download as CSV
Mark As Read

Print and Mark as Read For All

Delete
Renew

File Information
 Posted by (Anonymous) at 4/7/2014 4:37:51 PM from 172.16.0.190 via Firefox Browser 28.0
 File Size: 33 bytes # of Downloads: 0

File Preview

Field Name	Value
email	= helga@ipswitch.com

File Log

Time/Date	User	Action
4/7/2014 4:37:51 PM	Anonymous	Posted from 172.16.0.190

View File Thumbnails

A Thumbnail File List button may display beneath the table, which allows you to switch to a thumbnail view of the folder's contents:

☐	Name	Created	Size/Contents	Creator	☐	☐
↑ Parent Folder						
☐	Test Folder	6/4/2014 1:15:17 PM	1 2		☐	☐
☐	bootprompt.bt ☒	6/4/2014 8:07:30 AM	3 KB	Kris	-	☒
☐	index.gif	6/6/2014 7:01:08 AM	14.7 KB	kristina	-	☐
☐	index_435.gif ☒	6/6/2014 8:25:23 AM	14.7 KB	Kris	1	☒
☐	logo122.gif	6/6/2014 7:01:27 AM	14.7 KB	kristina	-	☐
☐	multicolor.gif	6/6/2014 7:01:18 AM	14.7 KB	kristina	-	☐

Thumbnail File List

After clicking Thumbnail File List, you see files display in thumbnail view:

/Home/kris/

Thumbnail File List - Return to Normal View

Thumbnails



index.jpg
Open - View Full Size



logo122.png
Open - View Full Size



multicolore01.png
Open - View Full Size

Under each thumbnail, the name of the file displays along with two links:

- Open pulls up the normal file view
- View Full Size downloads the complete file and renders it in the browser

Click Return to Normal View to return to the text-only file list.

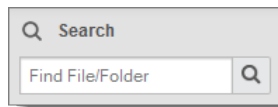
View Partial Files

When a file is still in the process of being uploaded, it will be displayed in a directory listing as a partial file . While a file is in the partial state, it may continue to receive appending content (i.e., grow larger), but only the original user who began the upload will be allowed to add this content. (Once a file is closed and made ready for download, no additional content may be appended, not even by the original uploader.)

Partial files may not be downloaded by anyone, and will be hidden from some file list views, including FTP directory lists performed by users other than the original uploader. Partial files may be deleted, however, if the user viewing the partial file entry has sufficient permissions. Partial files will also usually be deleted from the system within 24 hours. (In other words, broken uploads must be resumed without 24 hours; otherwise there will be no file on the server for a client to resume an upload to.)

Find Files and Folders

The Find File/Folder box (typically located in a colored box on the left side of the screen) lets you search the MOVEit system for files and folders using either an ID (e.g., "1234567") or a name (e.g., "myfile.txt").



Name wildcards ("*") are allowed and their use is encouraged. For example, you may wish to search for "*.pdf", "myfile*.*" or "Home/John Smith/*".

Results from searches are displayed as soon as the Find File button is pressed.

Find Files / Folders

Search Results for "index"

Found 2 files matching the search term "index"

 icon indicates new files.

File Name	Date and Time	From		
 /Home/kris / index.gif	6/6/2014 7:01:08 AM	kristina		
 /Home/kris / index_435.gif	6/6/2014 8:25:23 AM	Kris		

Found 0 folders matching the search term "index"

The resulting file list has several columns:

- **File Name:** The folderpath and name of the file. If the folderpath is clicked, the user will be taken to a view of this folder. If the name of the file is clicked, the user will be taken to a view of the file.
- **Date and Time:** When the file was uploaded (or created).
- **From:** The full name of the person (or device) who uploaded or created this file. If clicked, this link will go to a view of this user.
- **Action:**
 - **Download:** Downloads this file (in its original format)
 - **Delete:** Deletes this file

The resulting folder list has only one column, containing the full path of the folders matching the search string. Clicking on a folder path will take you to a view of the folder.

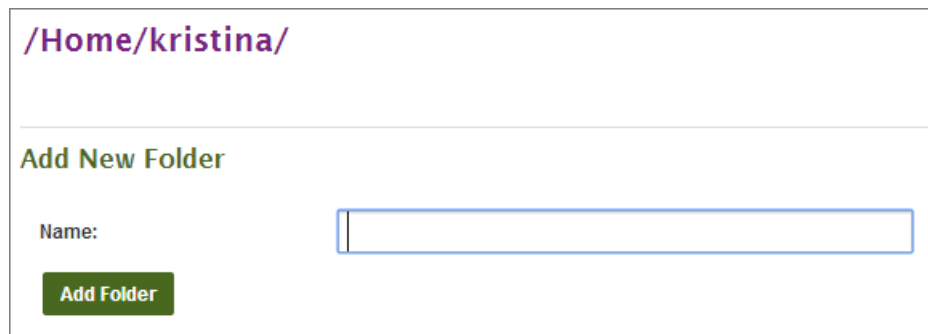
Automatic Wildcards

There are two cases where wildcard characters will automatically be added to a search term in order to find results:

- If a search term does not return any results, an asterisk wildcard character will automatically be appended to the search term if one does not already exist, and the search will be retried.
- If a search term containing a slash ("/") does not return any results, and the same search term with an asterisk appended also does not return any results, an asterisk will be prepended to the search term if one does not already exist, and the search will be retried. This allows users to search for partial folderpaths and successfully find them.

Add a Folder

If you have proper permissions, you can add a folder to the current folder by clicking **Add Folder** beneath the table. Enter a name for the new folder. If the parent folder is not a root folder, you will also be prompted to decide how the new folder should inherit any explicit permissions from the parent. Most other folder settings will be automatically copied from the parent to the new folder.



/Home/kristina/

Add New Folder

Name:

Add Folder

The three inheritance options are:

- **Always inherit from parent:** This option turns on the Inherit Access From Parent option on the new folder. This will cause the new folder to inherit existing and future explicit permissions from the parent.
- **Copy from parent but do not inherit future changes from parent:** This option causes the existing explicit permissions on the parent folder to be copied to the new folder, but does not turn on the Inherit Access From Parent option. This will cause the new folder to inherit existing explicit permissions from the parent, but not be affected by future changes to the parent's permissions.
- **Clear and do not inherit future changes from parent:** This option causes the new folder to be created without copying any permissions from the parent, and without turning on the Inherit Access From Parent option.

Add a Virtual Folder

A Virtual folder is a folder that links to another real folder in the MOVEit folder tree, allowing a user to see the contents of the target folder in a different location.

Click the "Add Virtual" link to open the Add New Virtual Folder page.

Add New Virtual Folder

Name:

Permissions: Always inherit from parent ▼

Target: /Home/kris ▼

Add Virtual Folder

~ OR ~ [Return to the folder list](#)

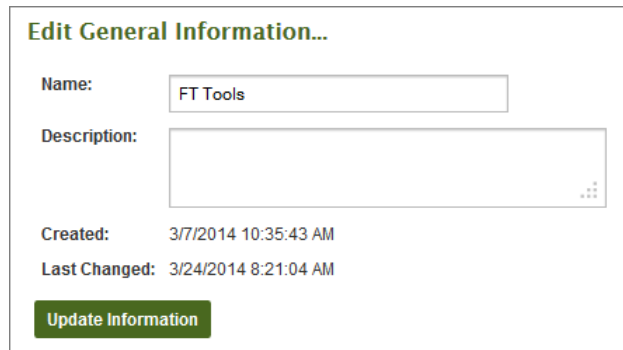
- **Name:** Enter a name for the new folder.
- **Permissions:** The three inheritance options are the same as described above for a normal folder.
- **Target:** This option shows the available folders (for the current user, based on permissions) which can be selected as the target for the virtual folder. The contents of the target folder will appear in the folder tree under the folder name selected for the virtual folder. (For performance reasons, if the current user is an admin user, the virtual folder will instead show a link to the target folder.) Navigation of the target folder and any subfolders will be relative to the virtual path.

Note: To create a virtual folder, the current user needs to have administrative permissions on the target folder. Also, "Subs" permissions are required in the folder where the virtual folder is created.

Edit Folder Settings

Admins, FileAdmins and Users/Groups with explicit folder Admin permissions have the power to make changes to the way folders behave through the folder settings page.

Edit General Information...



The screenshot shows a dialog box titled "Edit General Information...". It contains the following fields and information:

- Name:** A text input field containing "FT Tools".
- Description:** A large text area, currently empty.
- Created:** 3/7/2014 10:35:43 AM
- Last Changed:** 3/24/2014 8:21:04 AM
- Update Information:** A green button at the bottom left.

The folder name and description may be changed here, and the folder's creation and last change timestamps are shown. Note that changing a folder's name **MAY** cause certain external automated procedures to break if the automated client is looking for specific folder names.

All characters in the ISO-Latin-1 (ISO/IEC 8859-1) set are allowed in folder names, with the exception of the following:

\\ / " < > |

Also, folder names must be less than 256 characters long.

Note: Folder names may not begin with the characters "@!", for internal reasons.

If the folder is a virtual folder, a user with administrative permissions can also change the target folder, which will be shown under Edit General Information.

Edit Folder Access...

Edit Folder Access...

Explicit permissions can be granted to various other users. (As noted, Admins and FileAdmins always have "full permission.")

☐ Inherit Access From Parent
 Change Value

User	Read	Write	Delete	List	Notify	Subs	Admin	Action
(FileAdmins/Administrators)	X	X	X	X		X	X	
Home: Kris (kris)	X	X	X	X	X			Override
GROUP: East Coast	X			X	X			Edit - Remove
another test (another test) Kris (kris) kristina (kristina) Steve (steve) test (test) yet another test (yet another test) GROUP: Human Resources	☐	☐	☐	☐	☐	☐	☐	Add Access

Specific access to various folders may be granted. The types of access which may be granted are:

- Read: Allows this user/group to read files from this folder.
- Write: Allows this user/group to upload files into this folder.
- Delete: Allows this user/group to delete files from this folder.
- List: Allows this user/group to list which files are in this folder.
- Notify: Sends an email notification to this user/group if new files are uploaded to this folder. Notify permissions work a little differently if used on home folders: files uploaded to home folders are only considered new to non-owners if they are uploaded by folder owners. For example, if "George" uploads a file into "Fred's" home folder and "Jane" has notify permission, "Jane" will not get a notification. However, if Fred uploads a file into his home folder, "Jane" will get a notification.
- Subs: Allows this user/group to add, rename, and remove subfolders in this folder.
- Admin: Allows this user/group to manage the settings of this folder. If you wish to delegate the ability to designate who should be able to access this folder (i.e., change folder permissions) to particular users, you must also promote those users to GroupAdmins.

"Extra Delete Permission" Rule: Although DELETE permissions can be explicitly assigned, they are often enjoyed as derived permissions instead. The following rule is used to award additional delete permissions:

- If a user is granted ADMIN permission to a folder, that user or group will be granted DELETE permissions as well.

"Limited List Permission" Rule: Although LIST permissions can be explicitly assigned, they are also enjoyed as derived permissions instead. The following rule is used to award additional LIST permissions on "write-only" folders:

- If a user is granted WRITE permission to a folder (and only write permission), that user or group will be granted limited LIST permission to that folder as well. Specifically, the limited LIST permission granted on the folder in this case allows users to see all files that user has uploaded, but no files that anyone else has uploaded. This behavior may be turned off on a user-by-user basis by checking the "shared" flag on any user account; when the user-level "shared" setting is checked, the related user will never enjoy limited LIST permissions.

Implicit permissions will be shown without any actions available, as they cannot be changed or removed. Explicit permissions have two possible actions. The Edit link allows you to change the permissions assigned to that user or group. The Remove link allows you to remove the permissions assigned to that user or group.

Note: Instead of granting USERS permission, you can also grant GROUPs permission. In fact, the preferred method of granting access is to set up groups, add users to groups and grant folder permissions to groups.

If multiple type of access to a folder are granted to a single user (for example, through user AND a group), file permissions will be combined.

Edit Folder Access...

Explicit permissions can be granted to various other users. (As noted, Admins and FileAdmins always have "full permission.")

☒ Inherit Access From Parent

Change Value

Subfolders may have an "Inherit Access From Parent" option. When checked, this option will cause access to this folder to be completely controlled by the access settings of this folder's parent folder. (i.e. "ActiveHEAT\Release" access might be controlled by "ActiveHEAT" access rules.) This option **MUST** be **UNCHECKED** (if available) if subfolder permissions should override parent folder permissions.

Home Folder Permissions Override**Edit Folder Access...**

Explicit permissions can be granted to various other users. (As noted, Admins and FileAdmins always have "full permission.")

☒ Inherit Access From Parent

Change Value

User	Read	Write	Delete	List	Notify	Subs	Admin	Action
(FileAdmins/Administrators)	X	X	X	X		X	X	
Home: Kris (kris)	X	X	X	X	X			Override
GROUP: East Coast	X			X	X			Edit - Remove
another test (another test) Kris (kris) kristina (kristina) Steve (steve) test (test) yet another test (yet another test) GROUP: Human Resources	☐	☐	☐	☐	☐	☐	☐	Add Access

The default permissions applied by the organization to a home folder owner can be added to or overridden for individual users. The Edit Folder Access section for home folders will display the current default permissions for the home folder owner, along with a link to override those permissions.

Edit Folder Access...

Set the desired permissions for this user or group, then click the Change Permissions button.

User	Read	Write	Delete	List	Notify	Subs	Admin
Kris (kris)	☒	☒	☒	☒	☒	☐	☐

Permission Behavior:

☒ Override inherited permissions ☐ Add to inherited permissions

Change Permissions

Clicking the Override link will create an explicit set of permissions for the owner for their home folder, and prompt the user to edit that permissions entry. The explicit permissions entry will supplement the default organization permissions if the "Add to inherited permissions" option is selected, or replace the default organization permissions if the "Override inherited permissions" option is selected.

Note: If all permissions are removed here, the user will NOT be able to upload to, download from, or even see their home folder.

Change Miscellaneous Settings...

Change Miscellaneous Settings....

The "hide history" setting prevents people from viewing information about other people who have downloaded files from this folder in file histories. (This setting applies only to Users, not to FileAdmins or Admins.)

Hide History: ☐ No ☒ Yes

Set the "create thumbnails" setting to "Yes" to have MOVEit DMZ create thumbnail images of any images that are uploaded to this folder. For users with read access to this folder, a separate "Thumbnail File List" link will appear which will show the thumbnails of the images in this folder.

Create Thumbnails: ☐ No ☒ Yes

Set the "enforce unique filenames" setting to "Yes" to have MOVEit DMZ check for an existing file with the same name during file uploads. Folders with this setting enabled will look more normal to an FTP client, as the FileID will not be appended to the file name in a directory listing.

Enforce Unique Filenames: ☐ No ☒ Yes

Set the "allow file overwrite" setting to "Yes" to allow users to overwrite existing files on upload. This setting only has an effect when "enforce unique filenames" is set to "Yes" as well. If a file exists in a folder with the same name as that which is being uploaded, this setting will cause the old file to be deleted, and the new file to be allowed to upload successfully.

Allow File Overwrite: ☒ No ☐ Yes

When a custom sort field is selected for this folder, that selection will override users' normal folder sorting preferences, causing items in the folder to be sorted the selected way regardless of how other folders appear to the user. Users will still be able to override this value by clicking a column header in the folder list to sort by that column.

Custom Sort Field:

Update Miscellaneous Settings

Hide History: Information about user downloads and viewings may be hidden from end users using this feature. When set to "Yes", end users will not be shown usernames and IP addresses of those users who have downloaded or viewed a specific file in the folder under that file's History heading. (This setting is YES by default.)

Create Thumbnails: Allows MOVEit to detect "image file" uploads into this folder and to make thumbnails for image files. The following image formats are supported: BMP, GIF, JPG, PNG, TIF. (Thumbnails are always created as JPG images.) After this setting is changed to YES or NO, an additional page will ask if you want to delete all existing thumbnails (if NO) or create new thumbnail for all existing images (if YES). (This setting is NO by default.)

Enforce Unique Filenames: When set to "YES" prevents users from uploading multiple files of the same name into this folder. This setting also affects the display of filenames via the FTP and SSH interfaces:

- "NO" - Format is "[Filename]_[FileID].[FileExt]" - i.e. "readme_1234567.txt"
- "YES" - Format is "[Filename].[FileExt]" - i.e. "readme.txt"

Allow File Overwrite: When set to "YES" and if Enforce Unique Filenames is enabled, if a user tries to upload a file with the same name as a file already in the folder, the file in the folder will be deleted, and the new file allowed to upload. This can be beneficial for FTP users, as it makes MOVEit behave like other FTP servers. When set to "NO", files will not be overwritten, and an error will be issued if a user tries to upload a file with the same name as an existing file.

Custom Sort Field: By default, Distribution and Home folders are sorted based on the organization's default folder sort setting. Users may then re-sort folders to a different method, which is remembered in a cookie for the user. Sometimes, however, an individual folder may need to be sorted differently than the default, and than the user's normal sorting selection. This setting allows a folder to be sorted in a way which overrides the organization and user selections. Users may still choose to sort the contents of the folder differently by clicking one of the column headers, but this choice will not be remembered between sessions. Custom sort field options are:

- None - Do not use any custom sorting for this folder. This is the default option.
- Name - Sort folder contents by name in ascending order.
- Created - Sort folder contents by creation timestamp in descending order.
- Size/Contents - Sort folder contents by size (files) or contents (subfolders) in ascending order.
- Creator - Sort folder contents by creator username in ascending order.
- Download Count - Sort files in folder by number of times downloaded in descending order.

Change Notification...

Change Notification...

The Notification Style setting determines whom notifications are sent to when a new file is uploaded.

Notification Style: ☒ Normal ☐ Inbox/Outbox

A "sender" is someone who uploads a file into this directory; senders get "upload confirmation" notices. A "recipient" is an owner or someone with NOTIFY permission to this folder; recipients get "new file" notices. "Delivery Receipt" sends an email message back to the "sender" when someone first downloads or deletes a file they uploaded.

Upload Confirmation to Sender:

☒ No ☐ Yes (immediately)
☐ Yes (include in upload summary after minutes)

New File Alert to Recipient:

☐ No ☐ Yes (immediately)
☒ Yes (include in upload summary after minutes)

Delivery Receipt to Sender:

☒ No ☐ Yes (immediately)

Alert Sender if File is Not Downloaded:

☒ No ☐ Yes (after)

Update Notification Settings

Notification settings control how "new file" and "upload confirmation" messages are sent for this folder. Note that these notifications also work with virtual folders.

"Notification style" determines who notifications are sent to when a new file is uploaded:

- Normal - Notifications about new files uploaded by someone other than the folder owner are sent to the folder owner and the recipients.
- Inbox/Outbox - Notifications about new files uploaded by someone other than the folder owner are sent to the folder owner only.

Senders are people who upload into this folder; they get "upload confirmations." Recipients are people/groups with NOTIFY permissions to this folder; they get "new file" notices.

Two more types of automated messages can be sent back to users who upload files. The first, called a "Delivery Receipt", is sent when another user downloads a file (delivery receipts are also sent back to the user who uploaded a file if the file was deleted from MOVEit before being read). The second, controlled by the "Alert Sender if File is Not Downloaded" option, is sent after the specified period of time if no users have downloaded a file.

Notification messages are sent one of several ways:

- No - These messages are never sent. (Good if a "user" is really an automated procedure.)
- Yes (immediately) - Messages are sent as soon as a file is successfully uploaded. (Ideal for most "human users.")
- Yes (include in Upload Summary after X Minutes) - Every X minutes, an automated process looks for new messages and collects a list of them in a single email message. (Best for extremely busy folders - often webposts.)
- Yes (after X (Days|Hours|Minutes)) - The message is sent after the configured number of days, hours, or minutes. This method is only available for alerts if the file is not downloaded.

Change Automated Maintenance Settings...

Change Automated Maintenance Settings...

Cleanup: ☐ Enabled

Delete old files after days

Delete empty subfolders after days

Display New Files: For days

Folder Quota: ☒ KB ☐ MB

☐ Quota applies to files in sub folders

Update Maintenance Settings

Maintenance settings control the cleanup of old files, empty subfolders, the aging of "new" files, and the file quota of the folder. Automated cleanups take place as part of the scheduled "nightly" tasks; quotas are always live and enforced immediately.

Old files (defined as being "not new" to everyone in the folder) can be deleted automatically after a certain number of days. The old file cleanup option is available on all folder types.

Empty subfolders can also be deleted automatically after a separately configurable number of days. The empty subfolder cleanup option is available on the Distribution and WebPosts root folders, and Distribution and Home subfolders. Setting a value of 0 for the "Delete empty subfolders after" setting will disable this feature, even while the Cleanup option is enabled. Folders are deleted after they have been empty for a period of time greater than the configured number of days in this setting. Every time a file or subfolder is added or removed from a folder, an internal timestamp is updated. Thus, folders will only be automatically deleted when they are empty and their internal "last activity" timestamp is older than the configured setting value.

New files remain new for each user until that user downloads (or marks as read) that file OR a certain number of days have passed since the file was uploaded. The number of days setting is controlled here.

A file quota may be configured for general use folders, including user home folders. The file quota can be set to a given number of kilobytes, or megabytes. File uploads, copies to, and moves to will generate errors if they would exceed the configured quota. Set the quota level to zero (0) to disable the quota.

Change Allowed File Masks...

Change Allowed File Masks...

Enter a comma-delimited list of filemasks below. Each file uploaded, moved, or copied into this folder will be checked against the list of filemasks. (e.g., *.mp3, report*, data???.ach) Depending on the mask rule setting, matched files will either be allowed or denied. Filemask comparisons are case insensitive. The macro text [USERNAME] will be replaced by the username of each user that uploads a file to this folder.

Mask Rule:

☒ Allow All Files Except...

☐ Deny All Files Except...

Folders can be configured to allow or deny files matching certain filemasks. Filemasks using the "*" multi-select or "?" single-select wildcard characters may be entered in this section as a comma-delimited list. Any instances of the macro string [USERNAME] will be replaced by the uploading user's username during filemask checking. The Mask Rule setting determines whether files that match at least one of the masks are allowed or denied.

Change File and Folder Name Character Restrictions

Change File and Folder Name Character Restrictions...

Change this setting to restrict characters allowed in file and folder names to the selected character set. Whenever a file or folder is uploaded, moved, or copied into this folder, the name will be checked for illegal characters. By default, file and folder names are not restricted (exception: the characters \ are never allowed in file names and the characters \ "<>| are never allowed in folder names, for internal reasons).

Character Set:

- ☒ Do not restrict file and folder names
- ☐ Allow only valid Windows NTFS characters in file and folder names, i.e. don't allow \ "<>|:?*
- ☐ Use a custom defined character set

Update Character Restrictions

Windows clients can have difficulty reconciling illegal (for NTFS) characters in filenames when downloading from MOVEit, which has fewer restrictions when it comes to filenames.

You can use these folder-level settings for enforcing Windows NTFS characters in file/folder names. You can also use these options for defining a custom character set. If a user attempts to upload/copy/move/rename a file or folder that contains illegal characters, an error will be returned. Enabling character restrictions on a folder will also check all existing immediate files/sub folders for illegal characters, and if found, will prompt the user if they want to automatically replace illegal characters (this is for existing files/folders only, there is no auto replacement for incoming files/folders).

When defining a custom character set, folder and file names can be configured to allow or deny matching characters.

Change Web Post Response... (WebPosts Only)

Change Web Post Response...

When a web form is submitted to this folder, by default users will see this organization's logo and a brief message. The "web response" settings allow these defaults to be overridden with a form-specific banner, thank you message, and URL to which the user will be redirected.

URL:

Redirect:

☐ Go to (URL) immediately.

☒ Go to (URL) after seconds.

Subject:

Package:



[Update Web Response Settings](#)

After customizing your web response settings, press the "Update Web Response Settings" button above BEFORE selecting and uploading your custom response banner. (You may also "reset" your banner to the organizational logo by pressing the "Clear Banner" button.)

Current Banner:  (scaled)

Step 1: Select a *.gif file: No file selected.

Step 2: [Upload Custom Banner](#)

~ OR ~

These settings are used to control the content returned in response to web form posts (webposts). More information on these settings can be found in the **WebPosts Feature Focus** (on page 92) page.

The URL, Response Subject, and Response Message fields support *intra-string language tags* (on page 57).

After customizing your web response settings, press the "Update Web Response Settings" button above BEFORE selecting and uploading your custom response banner. (You may also "reset" your banner to the organizational logo by pressing the "Clear Banner" button.)

Current Banner:    (scaled)

Step 1: Select a *.gif file:

Step 2:

~ OR ~

Delete Folders and Files

To delete one or more folders and/or files:

- 1 Select the **Folders** menu.
- 2 Navigate to the location of the folder(s) or file(s) you wish to delete.
- 3 Do one of the following:
 - Click  next to the folder or file.
 - Select one or more folder(s) and/or file(s) and click the **Delete** button at the bottom of the table.



After confirming the deletion, the folder or file will be deleted.

Copy Folders and Files

To copy one or more folders and/or files:

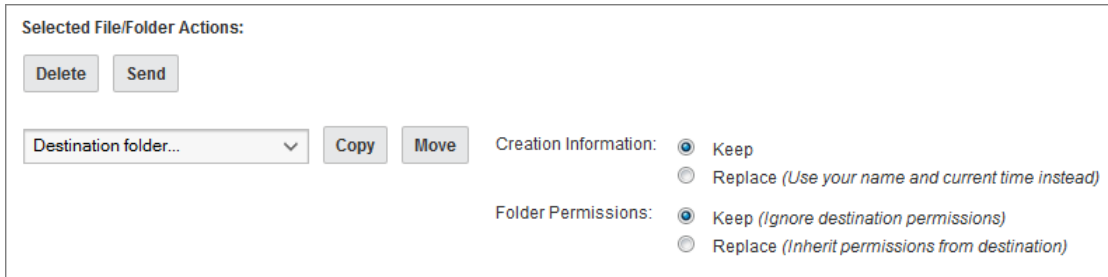
- 1 Select the **Folders** menu.
- 2 Navigate to the location of the folder(s) or file(s) you wish to copy.
- 3 Select the folder(s) and/or file(s).



- 4 Select a **Destination Folder** from the drop-down list. This is where a copy of the folder(s) and/or file(s) will be placed.

A screenshot of a user interface element. It features a text box with the placeholder text "Destination folder..." and a downward-pointing arrow on the right side, indicating a dropdown menu. To the right of the text box is a button labeled "Copy".

- 5 Click **Advanced Copy/Move Options** to specify copy details:

A screenshot of a dialog box titled "Selected File/Folder Actions:". Inside the dialog, there are two buttons at the top: "Delete" and "Send". Below these is a "Destination folder..." dropdown menu, followed by "Copy" and "Move" buttons. To the right of these buttons are two sections: "Creation Information:" with radio buttons for "Keep" (selected) and "Replace (Use your name and current time instead)"; and "Folder Permissions:" with radio buttons for "Keep (Ignore destination permissions)" (selected) and "Replace (Inherit permissions from destination)".

The following options apply to Copy operations only for most folders. For WebPost folders, the **AS Format** option also applies when downloading multiple files.

- **As Format** (WebPost and Archived Logs folders only): This option defines how the selected webpost or log files will be copied, moved, or downloaded. Available formats are:
 - **Single XML Bundle:** Selected files will be converted into a single XML file containing the data from each file in a separate node.
 - **Single CSV Bundle:** Selected files will be converted into a single Comma Separated Value (CSV) text file containing the data from each file in a separate row.
 - **Individual XML files:** Selected files will be individually copied or moved to the target folder as XML files. This option is not allowed when downloading multiple files.
 - **Individual CSV files:** Selected files will be individually copied or moved to the target folder as CSV text files. This option is not allowed when downloading multiple files.
 - **Creation Information:** These options define whether the original uploader information is kept with the file, or replaced by the current user's information. Note that folder creation information is not retained.
 - **Folder Permissions:** For copied or moved folders, these options define whether the existing permissions are retained, or whether the permissions of the new parent folder are applied. Note: This feature may not be available for all users.
- 6 Click **Copy**. A copy of each folder and/or file is placed in the destination folder.

Move Folders and Files

To move one or more folders and/or files:

- 1 Select the **Folders** menu.
- 2 Navigate to the location of the folder(s) or file(s) you wish to move.

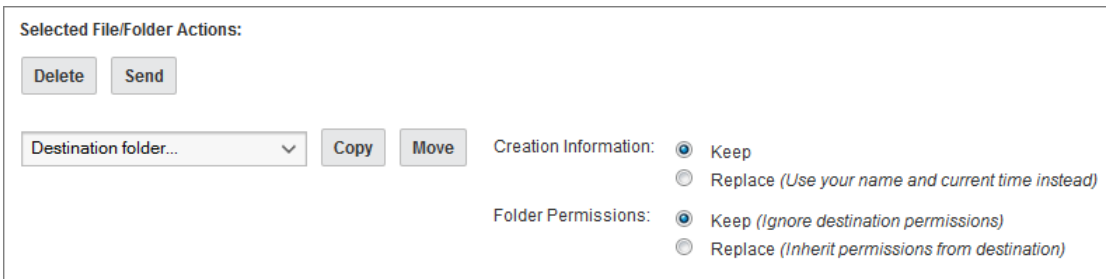
- 3 Select the folder(s) and/or file(s).



- 4 Select a Destination Folder from the drop-down list. This is where the selected folder(s) and/or file(s) will be moved. The original folder and/or file will be removed from its current location.



- 5 Click Advanced Copy/Move Options to specify move details:



The following options apply to Copy operations only for most folders. For WebPost folders, the **As Format** option also applies when downloading multiple files.

- **As Format** (WebPost and Archived Logs folders only): This option defines how the selected webpost or log files will be copied, moved, or downloaded. Available formats are:
 - **Single XML Bundle:** Selected files will be converted into a single XML file containing the data from each file in a separate node.
 - **Single CSV Bundle:** Selected files will be converted into a single Comma Separated Value (CSV) text file containing the data from each file in a separate row.
 - **Individual XML files:** Selected files will be individually copied or moved to the target folder as XML files. This option is not allowed when downloading multiple files.
 - **Individual CSV files:** Selected files will be individually copied or moved to the target folder as CSV text files. This option is not allowed when downloading multiple files.
 - **Creation Information:** These options define whether the original uploader information is kept with the file, or replaced by the current user's information. Note that folder creation information is not retained.
 - **Folder Permissions:** For copied or moved folders, these options define whether the existing permissions are retained, or whether the permissions of the new parent folder are applied.
- 6 Click **Move**. The selected folder and/or file is moved to the destination folder.

Upload Files Using the Wizard

The MOVEit Upload Wizard affords web users a faster method to transfer files over the web than the usual web transfers performed via the built-in "upload" button, through the use of compression-on-the-fly. It also offers the ability to upload entire folder trees or bundle multiple files into a ZIP archive before transfer, and displays transfers using a progress bar instead of the usual "spinning icon" in the corner of your web browser. Finally, the Upload Wizard provides integrity checking; it proves that the file or files which were just uploaded to the server are exactly the same as the files which exist on your local hard drive.

As discussed below, there are two versions of the Wizard: ActiveX and Java. However, they look and act very similarly.

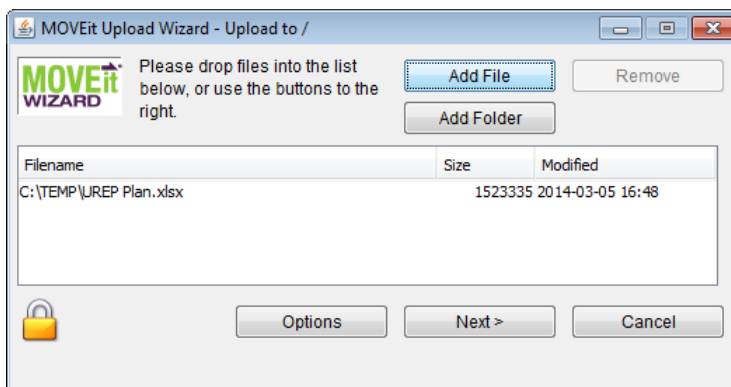
1 Start the Upload Wizard.

The MOVEit Upload Wizard will be presented as an option to users who have enabled it via the My Account page. It will appear on all pages from which uploads are normally permitted.

To start the Wizard:

- a) Select the folder into which you would like to upload files.
- b) Click the [CLICK HERE to Launch the Upload/Download Wizard...](#) link.

2 Select Files to Be Uploaded to MOVEit.



Files to be uploaded may be selected several different ways.

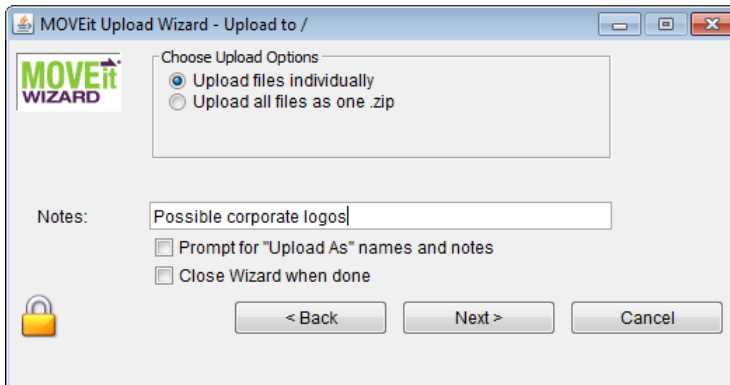
- Drag-and-drop files and/or folders from an Explorer window onto the list of files in the Wizard.
- Click **Add File** and "double-click" files from the navigation to select individual files.
- Click **Add File** and "CTRL-click" files from the navigation to select multiple files from the same folder.
- Click **Add Folder** and select a folder to recursively upload.

The files do NOT have to be from the same directory - the Upload Wizard can handle files from several different directories (or even drives) at the same time.

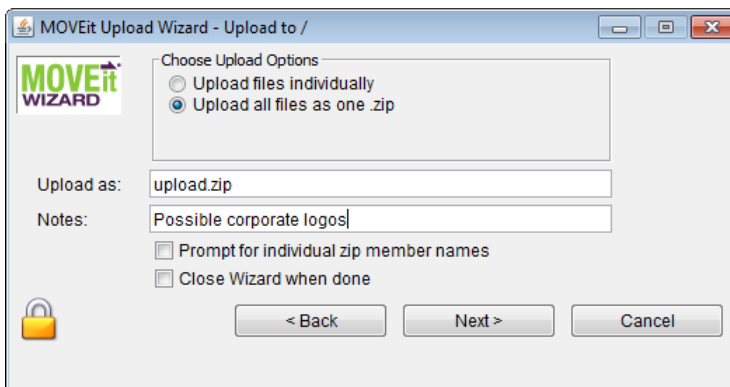
3 Press **Next >** to continue...

4 Choose your Upload Options. You may choose to upload your selected file(s) in one of two different ways:

- You may upload each file individually, in which case each file will be logged on the MOVEit with a separate file ID.



- Because each entry will retain its own notes, you ALSO have the ability to check the "Prompt for 'Upload As' names and notes" box and fill out custom notes for each and every file uploaded in the collection.
 - The "Ignore Subfolders" box will cause all files to be uploaded to the same folder, even if they are in different folders on your computer.
 - The "Close Wizard when Done" box will cause the Wizard to close itself when the transfer is complete.
- Alternatively, you may upload all files as a ZIP archive bundle, in which case each file will become a member of a new zip file.

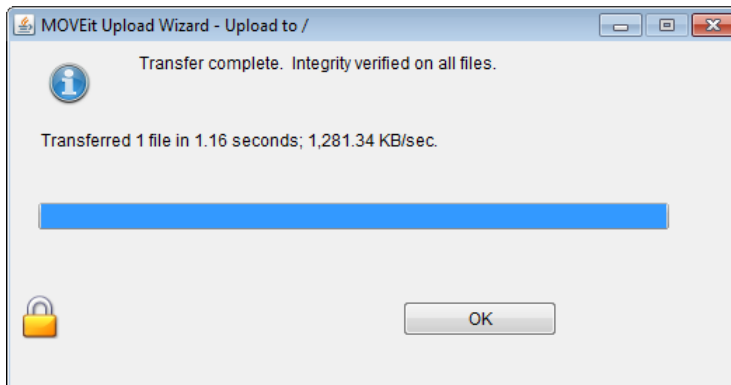


Note: The .zip file format cannot accommodate zipfiles larger than 4GB, so the Wizard will refuse to create a .zip file if the total size of the data files is greater than about 4 billion bytes.

- **Prompt for individual zip member names** Although you only have the opportunity to specify the upload notes for the zip file itself, you do have the opportunity to change the names the files stored in the archive will use if the "Prompt for individual zip member names" button is checked.
- The "Ignore Subfolders" box will cause no subfolder names to be included in the zip file, even if the files are in different folders on your computer.
- The "Close Wizard when Done" box will cause the Wizard to close itself when the transfer is complete.

5 Press the "Next >" button to begin the transfer.

As soon as the transfer begins, a progress bar will appear to show you how much of your transfer has been completed. (The same information will also be displayed in a short text area nearby.) When it is complete, you will see a transfer summary displayed.



6 Click OK to leave the Wizard.

Upload Wizard Transfer Report

When you click the OK button to leave the Wizard, you may see an Upload Wizard Transfer Report which provides more information about and links to the folders and files affected or created by the upload. This report is displayed only if you are uploading files from your home page; if you are already viewing the folder into which you uploaded your files the page view will simply refresh to show the files you uploaded.

After transferring files individually, your Upload Wizard Transfer Report will resemble this example:

<i>Upload Wizard Transfer Report</i>	
Local File	Status
 C:\MOVEitCentral_Install.log 	Uploaded to / Home / kristina OK (ID #984059345)
 C:\MOVEitDMZ_Install.log 	Uploaded to / Home / kristina OK (ID #983959650)

If you cancel the upload wizard before attempting to transfer any files, your Upload Wizard Transfer Report will resemble this example:

Upload Wizard Transfer Report
The upload was cancelled before any transfers began.

Content Scanning for Viruses and Data Loss Prevention

If your administrator has enabled content scanning, and a virus or data policy violation is detected in a file you selected for upload, the Upload Wizard will display an error and either block or quarantine the file. If you selected multiple files for upload, the Upload Wizard will upload all but the infected (or policy violating) file. Filenames and entries in the Notes field are also scanned for data policy violations. The Upload Wizard Transfer Report will show that the content scan was successful or resulted in an error, similar to these examples:

If the scan is successful:

Upload Wizard Transfer Report	
Local File	Status
 C:\MOVEitCentral_Install.log  	Uploaded to / Home / helga OK (ID #993705423)

If the scan results in a file being blocked:

Upload Wizard Transfer Report	
Some files were not uploaded. Blocked for DLP Violation.	
Local File	Status
 C:\DLP test\SSN.txt	Not uploaded: Blocked for DLP Violation.

If the scan results in the file being quarantined (meaning downloads not allowed):

Upload Wizard Transfer Report	
Local File	Status
 C:\DLP test\SSN.txt  	Uploaded to / Home / helga OK (ID #993630502)

Download Wizard

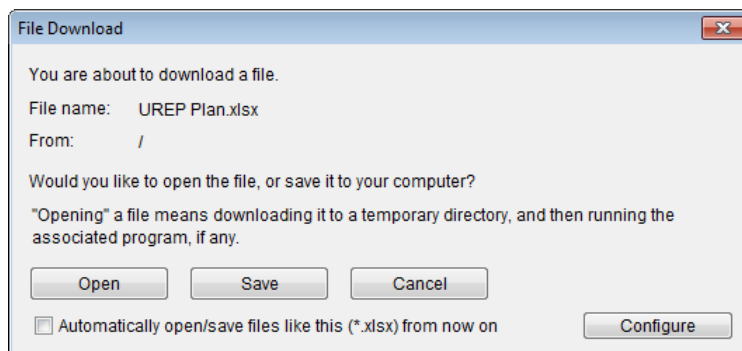
The MOVEit Download Wizard affords web users a faster method to transfer files over the web than the usual web transfers performed via built-in download facilities, through the use of compression-on-the-fly. It also provides the ability for a user to download more than one file at one time and download entire folders, using the Advanced File List page. In addition, the Download Wizard displays the progress of transfers using a progress bar and provides Open File, Open Folder and Unzip File buttons when transfers are complete. Finally, the Download Wizard provides integrity checking; it proves that the file or files which were just downloaded from the server are exactly the same as the files which exist on the server.

1 Start the Download Wizard.

The MOVEit Download Wizard is automatically invoked when a Download link is chosen. It is also invoked when clicking the Download button on the File List page.

2 Click Open or Save.

The first dialog you see will ask whether to open or save the file. "Opening" the file means the file will be downloaded to a temporary directory, and after successful completion, the associated application (based on file extension) will be run without any further prompting. "Saving" the file means that you will be prompted for a directory into which the file should be placed. The associated application will not be run automatically.



- If you choose "Automatically open/save files like this from now on, in the future, this dialog will not appear for files with the same extension as this one.
- The **Configure** button allows you to change your mind regarding what should be done with files with a given extension. The configuration dialog is also available via the Account Options page.

3 Select Download Destination.

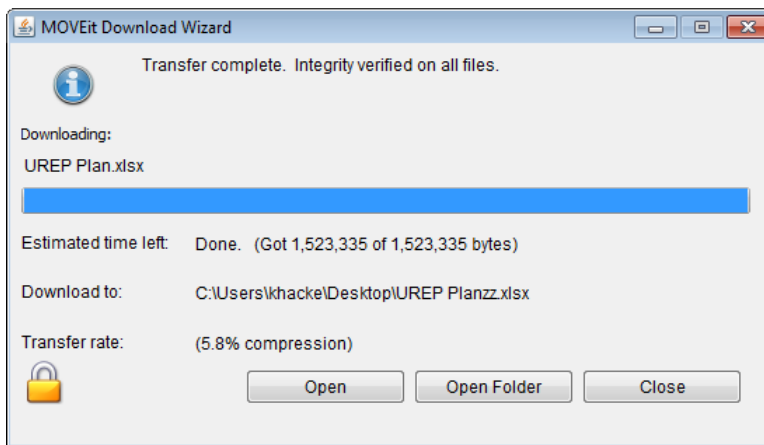
If you are saving, the download wizard asks into which folder the download should be saved as well as what filename to use. (If an existing file of the same name already exists in this location, you will be asked if you want to overwrite the existing file.)

4 Click Save.

The download wizard will display a progress bar, the size of the download, the amount currently downloaded, an estimate of the transfer speed and an estimate of the amount of time required to complete the download while the download is occurring.

When complete, the integrity of the downloaded file will be checked. (This ensures that the file just downloaded is completely identical to the file on the server.) At least three buttons will also be displayed if the transfer was successful:

- **Open:** Opens the file just downloaded, using any file associations currently available.
- **Open Folder:** "Browses" to the folder into which the file was just downloaded.
- **Close:** Closes the download wizard immediately.
- **Unzip:** ZIP file downloads only. Pops up an additional dialog which allows you to choose into which folder the Download Wizard should expand the contents of the ZIP archive.



Upload Confirmation: You may get an email message called an "upload confirmation" when you upload your file. (This option is turned off by default.)

New File Notification: Other users may get an email message called a "new file notification" when you upload your file. (This option is turned on by default.) However, you will NOT get a new file notification if you upload a file into your OWN home folder.

Delivery Receipt: When someone downloads your file from MOVEit, you may also get a "delivery receipt" message. (This option is turned off by default.)

File "Not Downloaded" Warning: If your file has not been downloaded within a set amount of time, you may also get a "not downloaded yet" message to warn you that the person or process you expected to pick up your file has not yet picked it up. (This option is turned off by default.)

Delivery Notification: If Ad Hoc Transfer is enabled, you may get an email message called a "delivery notification" when a recipient reads a package or downloads a file from the package.

Wizard Requirements

The Upload/Download Wizard comes in two versions: an ActiveX control, which is only usable by Internet Explorer running on Windows, and a Java Applet, which can be run on most browsers that support java applets.

The ActiveX version of Upload/Download Wizard is available only when using Internet Explorer. In addition, Internet Explorer MUST be configured to accept SIGNED ActiveX controls and run JavaScript, and the end user working with Internet Explorer must manually click a "Yes" button to download/accept/install the Upload/Download Wizard ActiveX control. The ActiveX version also requires the end user to ***mark their MOVEit site as an IE Trusted Site*** (on page 18) to take full advantage of Wizard capabilities such as multiple file download.

The Java version of Upload/Download Wizard requires Sun's Java2 version 1.5 or higher runtime environment. Java applet support MUST be enabled in the browser, as well as JavaScript support. Finally, the end user must click the "Yes" or "Always" button when asked whether they wish to trust the Upload/Download Wizard applet. (Warning: the Java version does not currently run under IE7 on Windows Vista; use the ActiveX version instead here.)

Install/Uninstall the Wizard

The Upload Wizard and Download Wizard are really two interfaces of the same program. This means that, when using the ActiveX version of the Wizard, there is only one control to install and uninstall. When using the Java version, there is only one JAR file to download.

Install the ActiveX Wizard

When a user visits their Home page on the MOVEit server for the first time, they will be prompted to install the Upload Wizard or disable it, provided their browser meets the requirements above.

ActiveX Upload/Download Wizard

The Upload/Download Wizard is a browser add-on that allows you to:

- Transfer files faster
- Transfer files greater than 2GB
- Transfer multiple files at once
- Perform automatic integrity checking to ensure file non-repudiation
- Compress/Uncompress data on the fly
- Add files via drag-and-drop

The ActiveX version of the Upload/Download Wizard requires Internet Explorer.

The ActiveX Upload/Download Wizard is NOT Installed and is Disabled

 **Install the Upload/Download Wizard (ActiveX)**

~ OR ~ [Return to My Account](#)

 You will NOT be able to install the ActiveX Wizard on some computers.

- You must have administrative privileges on your machine to install the ActiveX Wizard. (Many users, especially home users, already enjoy these rights. Most 'public terminal' users, however, will not have these rights. Ask your IT department if you are unsure.)
- Internet Explorer must be configured to allow you to install SIGNED ActiveX controls. (This right has been the default for some time, but some recent versions of IE have been restricting this right to 'Trusted' or 'Intranet' sites only. If this is the case, please add this site to your list of 'Trusted' or 'Intranet' sites.)

Clicking on the installation link will take the user to the Upload/Download Wizard installation page.

At this point, the Upload/Download Wizard will be installed, and the user will be notified when the process is complete. The user will then be returned back to their Home page, where they can continue on to other things. Upload/Download Wizard can also be re-installed or configured from the My Account page if necessary. See the **My Account** (on page 109) manual page for further details.

Please see additional installation/trust instructions in "**Web Interface - Home Page - Wizard Install** (on page 18)" topic.

Install the Java Wizard

The first time a user signs on to MOVEit with a browser other than Internet Explorer (e.g., Firefox), MOVEit will display a slightly different page with a link to install the Java Upload/Download Wizard. The Java Upload/Download Wizard is a component very similar to the ActiveX Wizard, designed for environments that can't run ActiveX controls.

Install the Upload/Download Wizard

It is recommended that you install the Upload/Download Wizard, a browser add-on that allows you to:

- Transfer files faster
- Transfer files greater than 2GB
- Transfer multiple files at once
- Perform automatic integrity checking to ensure file non-repudiation
- Compress/Uncompress data on the fly
- Add files via drag-and-drop

The Java version of the Upload/Download Wizard requires Java 6 or later.

 **Install the Upload/Download Wizard (Java)**

~ OR ~

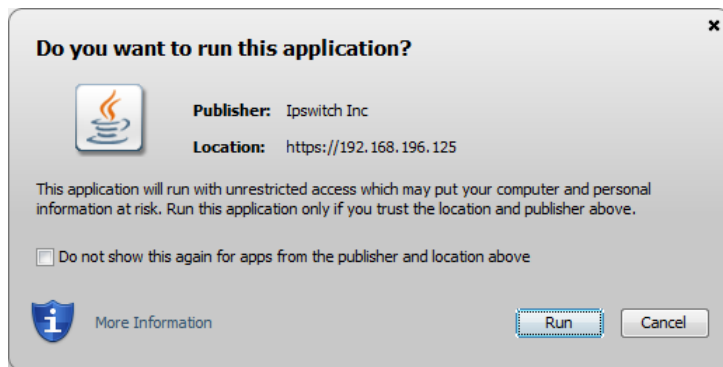
Disable the Wizard

Disable the Wizard (for this session only)

 If you disable the Upload/Download Wizard or are unable to install it, you can re-enable or try re-installing through your My Account page.

The choices are similar to those for the ActiveX Wizard. If Java is not installed, the user can simply choose Disable to avoid being prompted to install the Java Wizard in subsequent sessions.

Clicking on the installation link will open the following window, asking if the user wants to run the applet. The user should click "Run" here to allow the Java Wizard to run. Checking the **Always trust content...** box is also recommended.



Note: You might be presented a dialog box saying The Wizard has not downloaded yet. Continue waiting? OK | Cancel.

- If you also received the Do you want to run the application? window, click OK.
- If you never received the Do you want to run the application? window:
Click Cancel to stop waiting. Next, click OK in the Failed to upload... dialog. Then, to enable Java through your Web browser, follow the instructions at the following link:
http://java.com/en/download/help/enable_browser.xml
http://java.com/en/download/help/enable_browser.xml. Once you have enabled Java, start installation of the Java wizard again from the My Account page.

"Pre-Install" the Wizard

Windows administrators may "pre-install" the Upload/Download Wizard on selected Windows platforms by downloading the appropriate Upload/Download Wizard "MSI" (MicroSoft Installer - "*.msi") package from the MOVEit support site and distributing it using standard MSI utilities.

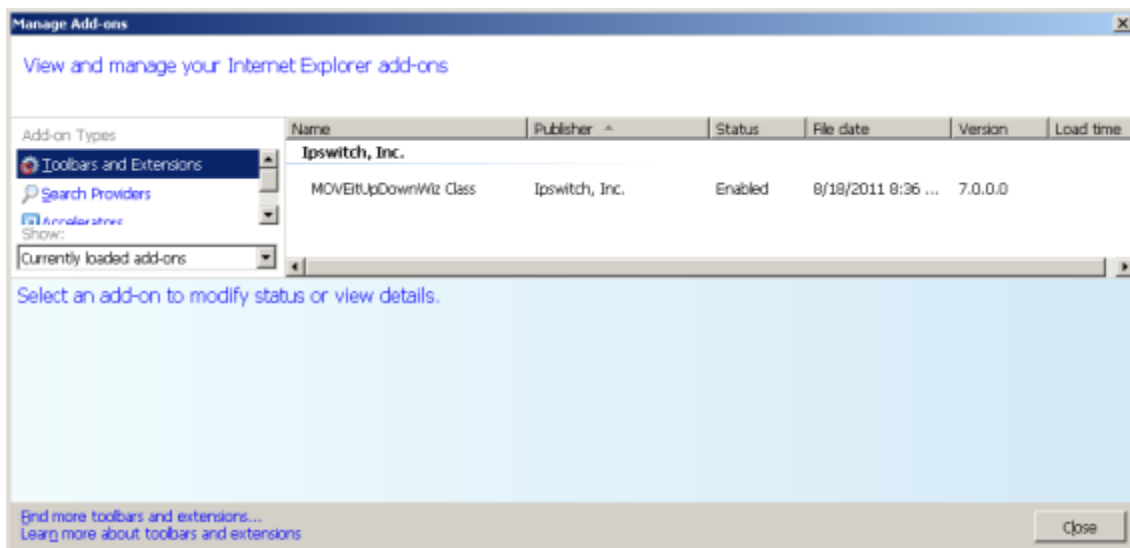
Uninstall the Wizard - Manually

Uninstallation of the Upload/Download Wizard is only necessary for the ActiveX version. The Java version is not actually installed on the local machine, so it never needs to be uninstalled.

To uninstall the ActiveX Wizard using Internet Explorer 9...

- 1** Click Tools | Manage Add-Ons

2 Select Currently loaded add-ons



3 Select the MOVEitUpDownWiz Class and click the Delete button.

If you want to reinstall the wizard, restart Internet Explorer and sign on to MOVEit again - on the first page with upload options the MOVEit Upload Wizard will be downloaded and automatically installed again.

Configuring the Wizard

The Upload/Download Wizard can be configured by choosing **My Account**, then **Change Wizard Status (ActiveX or Java)**. See **My Account** (on page 109). Both Wizards allow you to configure the default action, per file extension, for downloaded files.

Both Wizards will automatically read the settings from **supported browsers** (on page 793), so there is no need to configure settings for HTTP/S proxy and client certificates.

Wizard Technical Hints

- After launching the Upload Wizard, hold down the CTRL key while you click the **Next >** button to get version information.
- After launching the Upload Wizard, hold down the SHIFT key while you click the **Next >** button to get an additional "debugging" window.
- To ensure that the Wizard is made available to all Internet Explorer users, make sure the Content Expiration value is set to no less than 30 days on the COM web folder in your IIS settings. A setting of "Immediately" in this folder has been known to keep end users from downloading and installing the Upload/Download Wizard.
- Starting in version 3.2, Upload/Download Wizard gained the ability to remember whether files with certain extensions should be opened or saved automatically. These settings are stored in two different places depending on whether the Java or ActiveX versions of the Wizard are used. The Java settings are stored in a file called ".miwizrc" in an end user's home folder. (On Windows, this is the path listed in the "USERPROFILE" variable, e.g. "C:\Documents and Settings\JSmith") The ActiveX settings are stored in the registry key "HKEY_CURRENT_USER\SOFTWARE\Standard Networks\MOVEitUploadWizard\ExtensionHandling". (This is a unique tree for each user.)

- **Advanced hint:** Some firewalls or proxy servers block the "Transfer-Encoding: chunked" header used by the Upload Wizard. When the Upload Wizard detects this situation, it reverts to a different upload protocol. (This alternative protocol is not used by default, because it does not allow compression or the creation of .zip files.) If you have software or network devices that block "Transfer-Encoding: chunked" headers, and find that the MOVEit Wizard is not able to detect this, you can force the Upload Wizard to use the alternative protocol by creating a value in the registry of the computer that is running Internet Explorer.

Run RegEdit and navigate to HKEY_CURRENT_USER\Software\Standard Networks\MOVEitUploadWizard. (If this key does not exist, create it.) Then create a DWORD value named ForceNonLumpHashMode and give it a value of 1. This will force the Upload Wizard to use the less efficient but more widely-accepted alternative upload protocol.

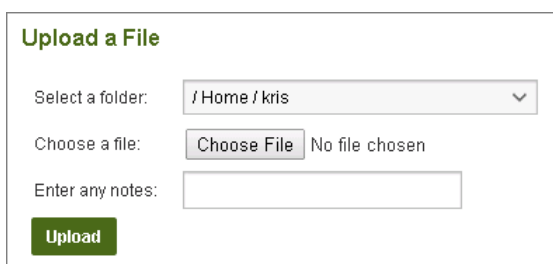
This must be done on every end-user's computer. Setting this value on the MOVEit server itself has no effect unless you actually use Internet Explorer on the server.

Organizations that wish to predistribute the ActiveX version of the Wizard or want to allow the control to be "preinstalled" for all users by an Administrator account through a "normal" installation package can obtain a simple Upload/Download Wizard "ActiveX" installation package from the MOVEit support site.

Upload a File Without the Wizard

To upload a single file without using the *Upload/Download Wizard* (on page 18):

- 1 Go to either the Home page or the Folders page and locate the Upload Files... area.



Upload a File

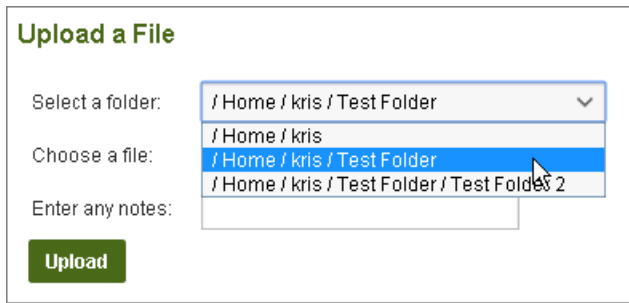
Select a folder: / Home / kris

Choose a file: Choose File No file chosen

Enter any notes:

Upload

- 2 Select the folder to which you want to upload one or more files by using the drop-down selector.



- 3 Click **Browse** to locate and select the file you want to upload. After making your selection, the file name appears next to the Browse button.
- 4 Enter any optional notes.
- 5 Click **Upload**. A confirmation message appears in the top banner:

Uploaded new file with ID #984539883 OK.

Upload Confirmation: You may get an email message called an "upload confirmation" when you upload your file. (This option is turned off by default.)

New File Notification: Other users may get an email message called a "new file notification" when you upload your file. (This option is turned on by default.) However, you will NOT get a new file notification if you upload a file into your OWN home folder.

Delivery Receipt: When someone downloads your file from MOVEit, you may also get a "delivery receipt" message. (This option is turned off by default.)

File "Not Downloaded" Warning: If your file has not been downloaded within a set amount of time, you may also get a "not downloaded yet" message to warn you that the person or process you expected to pick up your file has not yet picked it up. (This option is turned off by default.)

Delivery Notification: If Ad Hoc Transfer is enabled, you may get an email message called a "delivery notification" when a recipient reads a package or downloads a file from the package.

Content Scanning for Viruses and Data Loss Prevention

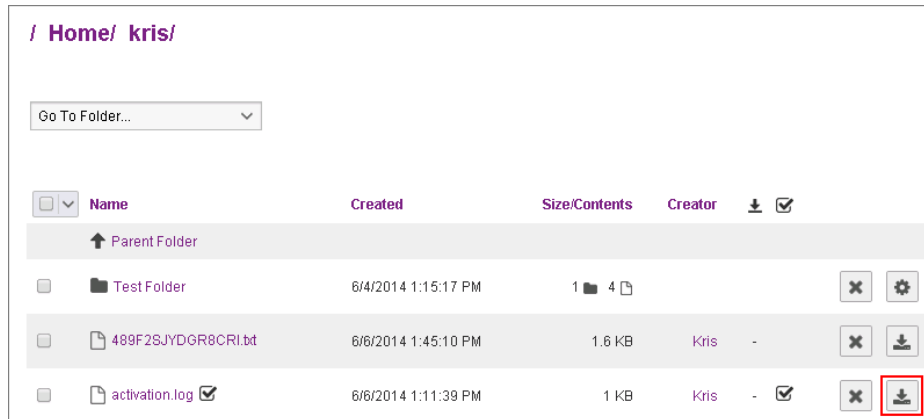
If your administrator has enabled content scanning, and a virus or data policy violation is detected in a file you selected for upload, the browser will display an error and either block or quarantine the file.

Filenames and entries in the Notes field are also scanned for data policy violations. If the content scan results in a file being quarantined, it will be uploaded, but the file will not be available for download. If the content scan results in a file being blocked, you will see a message similar to this one:

Blocked for DLP Violation.

Download Files

There are several ways to download files from MOVEit through the web interface. The general rule of thumb is to click the "Download" link next to or under the file you wish to download. If installed, the MOVEit Download Wizard will automatically help download your selected file; otherwise your browser will handle it directly.



There are several ways to find the file you need to download:

- If you received a new file notification, click (or copy into your browser) the link sent in the email. This link will take you directly to the file referenced in the email. (After signing on, if necessary.)
- If you received a new package notification, click (or copy into your browser) the link sent in the email. This link will take you directly to the package referenced in the email. (After signing on, if necessary.) See **Getting Started - Viewing Packages** (on page 90) for more information.
- If you know the name of the folder in which your file is located, click the Folders link and navigate to the appropriate folder. A list of files will be displayed - download the one you are interested in.
- If you do not know where the file is, type EITHER the NAME of the file (i.e. "readme.txt") or the FILEID (e.g., "1234567") into the Find File/Folder box on the LEFT side of the page and click the "Find File" button.

Work with Packages

This section describes packages and the mailboxes where packages are stored, and how to send, view, and manage packages.

View Mailboxes

Packages are located inside of mailboxes. Click **Packages** in the left navigation menu to display the Packages page...

Packages

Mailbox	 New Packages	 All Packages
 Drafts	-	-
 Inbox	3	4
 Sent	-	4
 Templates	-	-
 Trash	1	1



Add Box...

Package Actions

Send Package

 Manage your address book...

...then select a mailbox to view the packages in that mailbox.

Packages

/ Inbox/

Go To Mailbox... ▾

☐	Subject	Files	Size	From	Date/Time	
☐	✉ Report 88	-	1 KB	Kris	6/6/2014 9:13:57 AM	
☐	✉ 145	1	3.5 KB	Kris	6/6/2014 9:10:30 AM	
☐	✉ update	-	1 KB	Kris	6/6/2014 9:03:08 AM	
☐	✉ test	-	1 KB	Lynn	6/4/2014 10:16:04 AM	
☐	✉ test	-	1 KB	kristina	6/4/2014 10:15:34 AM	
☐	✉ test package	-	1 KB	Kris	6/4/2014 8:07:12 AM	

[Return to Mailboxes](#)

Checked Package Options:

New Packages might display initially on your Packages page if you have any unread packages. Simply click [Go To My Mailboxes](#) to view your mailboxes.

Packages

New Packages

 **update** (from [Kris](#) at 6/6/2014 9:03:08 AM)

 **test** (from [Lynn](#) at 6/4/2014 10:16:04 AM)

 **test** (from [kristina](#) at 6/4/2014 10:15:34 AM)

[Mark All Packages Not New](#)

 [Go To Your Mailboxes](#)

Package Actions

[Send Package](#)

 [Manage your address book...](#)

There are five standard mailboxes (depending on the organization settings): **Inbox**, **Drafts**, **Templates**, **Sent**, and **Trash**, but you can also create custom mailboxes. Custom mailboxes can be nested like folders.

For each mailbox, the number of new packages (✉), and the number of total packages (📁) display. Mailboxes that contain new packages are **bold**.

Click **Empty**  to delete all packages in the **Trash** mailbox.

For custom mailboxes, the following actions are available:

-  **Delete**: Deletes the mailbox and any packages and mailboxes contained within it. Confirmation will be asked for.
-  **Rename**: Allows the user to change the name of the mailbox.
-  **Add Box**: Adds a mailbox within the selected mailbox.

If the organization is configured to clean up old packages, a note will be displayed indicating the age limit for old packages before they are deleted, and whether or not the packages will be archived before they are deleted.

Click on any mailbox to display a list of packages in that mailbox. The **Subject**, **Sender**, number of **Files** in the package, total **Size** of files, and **Date/Time** sent are displayed for each package, as well as a short list of actions that can be performed on that package.

Packages

/ **Inbox** /

Go To Mailbox... ▾

☐	Subject	Files	Size	From	Date/Time	
☐	✉ Report 88	-	1 KB	Kris	6/6/2014 9:13:57 AM	
☐	✉ 145	1	3.5 KB	Kris	6/6/2014 9:10:30 AM	
☐	✉ update	-	1 KB	Kris	6/6/2014 9:03:08 AM	
☐	✉ test	-	1 KB	Lynn	6/4/2014 10:16:04 AM	
☐	✉ test	-	1 KB	kristina	6/4/2014 10:15:34 AM	
☐	✉ test package	-	1 KB	Kris	6/4/2014 8:07:12 AM	

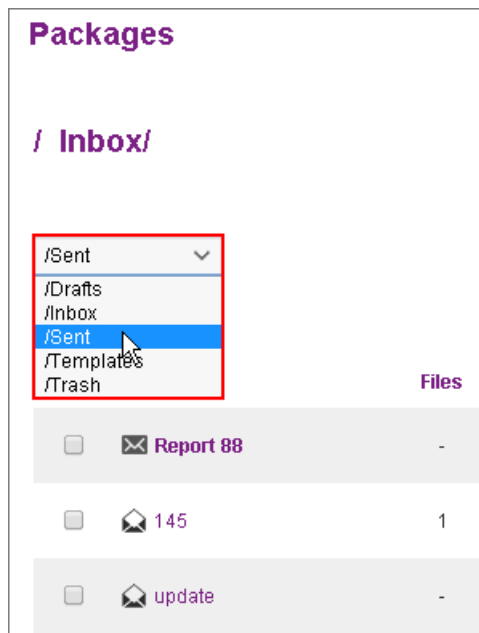
[Return to Mailboxes](#)

Checked Package Options:

Click a column header to sort the list by the values in that column.

Click on a package to **view *that package's details*** (on page 90).

To change mailboxes, select the desired mailbox from the **Go To Mailbox** drop-down menu at the top of the page.

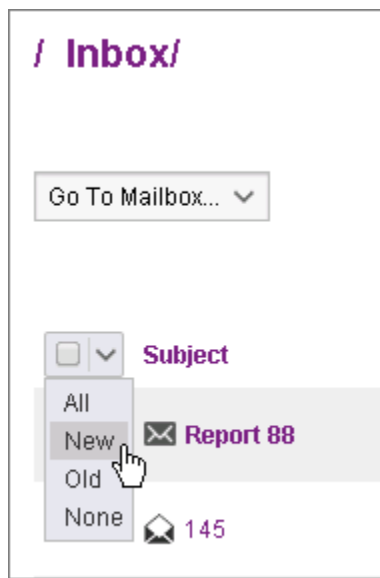


To place a package in the **Trash** mailbox where it can be permanently removed, click  in that package row. You can also select multiple packages and click the **Trash** button beneath the table.

To mark one or more packages as new, select the package(s) and click **Mark As New**. To mark one or more packages as not new, select the package(s) and click **Mark As Not New**.

To move one or more packages to a different mailbox, select the **Destination Mailbox** from the drop-down selector and then click **Move**.

To quickly select **All** packages, only **New** packages, only **Old** packages, or **None** to deselect all packages, use the package selector tool at the top of the table:



The **Sent** mailbox displays these additional columns:

- **Read Status** (): One of three read status icons will display:
 -  All recipients of the package have viewed the package.
 -  Some but not all of the recipients of the package have viewed the package.
 -  None of the recipients of the package have viewed the package.
- **To:** Replaces the usual **From** column, and lists the major recipients of the package.

When you open a **Sent** package, you can also **recall** (on page 106) it so it is not available for download by recipients.

The **Drafts** and **Templates** mailboxes let you edit  and permanently delete  items there.

To **view a package** (on page 90), click on the title of the package.

View Packages

To view your packages, click the **Packages** link in the left navigation menu.

If you have any new packages, they will display on the Packages page.

New Packages

 **test** (from **Kris** at 6/9/2014 6:14:35 AM)

 **test** (from **Kris** at 6/9/2014 6:14:24 AM)

[Mark All Packages Not New](#)

 [Go To Your Mailboxes](#)

You can also click **Go To Your Mailboxes**. Mailboxes that contain new packages are bold and show a count under the **New Packages** column.

Packages		
Mailbox	 New Packages	 All Packages
 Drafts	-	-
 Inbox	2	8
 Sent	-	8
 Templates	-	-
 Trash	-	1 
Add Box...		

Once you open a mailbox, new packages display in bold next to a new package icon .

/ **Inbox**

Go To Mailbox... ▾

☐	Subject	Files	Size	From	Date/Time	
☐	 test	-	1 KB	Kris	6/9/2014 6:14:35 AM	
☐	 test	-	1 KB	Kris	6/9/2014 6:14:24 AM	
☐	 Report 88	-	1 KB	Kris	6/6/2014 9:13:57 AM	
☐	 145	1	3.5 KB	Kris	6/6/2014 9:10:30 AM	
☐	 update	-	1 KB	Kris	6/6/2014 9:03:08 AM	
☐	 test	-	1 KB	Lynn	6/4/2014 10:16:04 AM	
☐	 test	-	1 KB	kristina	6/4/2014 10:15:34 AM	
☐	 test package	-	1 KB	Kris	6/4/2014 8:07:12 AM	

New Package Notifications

You may receive an email notification when you receive a new package. Click (or copy into your browser) the link provided in the email. Sign on to MOVEit with your username and password (registered users) or with the credentials provided by email (unregistered users) to view the package and download any attached files. If enabled, you can also reply to a package and send additional attachments, which will also be uploaded to the file transfer server. The organization administrator sets options that determine who can send and receive packages, enforces user- and package-level quotas, and controls package expiration and download limits.

Click on a package subject to read the package.

Package Contents

When you select a package to view, you see the contents of the package. A package header contains information such as the **Sender**, the **Recipients**, the **Subject**, and the current **Mailbox**.

Package to Kris

[Trash](#) [Forward](#) [Save As Template](#)

To: Mary
From: Kris at 6/9/2014 6:32:23 AM
Subject: Report 89

Mailbox: /Inbox/ **Read Status:** ☐ ☐ Read by no recipients [\(More\)](#) [Recall](#)

This is a package for you.

Files:

 [Report 89.gif](#) (14.7 KB) [Download](#)

Total: 14.7 KB

[Trash](#) [Forward](#) [Save As Template](#)

[View Send Receipt](#) - [View Package History](#) - [View Print Friendly](#)

Below that, the note (message body) is shown, followed by a list of file attachments, if there are any. Clicking on an attachment name will lead to a page with information about the attachment file. A **Download** button is provided, along with a **Download All** button if the Upload/Download Wizard is installed and enabled.

If Content Scanning is enabled, a note may identify whether the file was scanned for viruses and/or for data loss prevention (DLP). With DLP, file names and the Notes field (associated with an upload) are also scanned for data policy violations.

Buttons and links display actions that can be performed on the current package. These actions will include some or all of the following:

- **Trash** - Move the package to the Trash mailbox.
- **Delete** - Only available to packages in the Trash mailbox, this permanently removes the current package from the Trash mailbox.
- **Reply** - Start composing a new package to the sender of the current package. The body of the current package will be retained and each line marked with the ">" character.
- **Reply All** - Start composing a new package to the sender of the current package, as well as the recipients of the current package. As with Reply, the body of the current package will be retained and each line marked with the ">" character.
- **Forward** - Start composing a new package with no recipient. As with Reply and Reply All, the body of the current package will be retained and each line marked with the ">" character. Unlike Reply and Reply All, any attachments in the current package will be copied to the new package.
- **Move/Restore** - In all mailboxes except Trash, this will be "Move". In Trash, it will be "Restore". They both function the same way, allowing the user to select a mailbox to move the current package to.
- **View Send Receipt** - View the Send Receipt, which shows the subject, sent date and time, recipients, any attached files, and any options, such as expiration and quota, set for this package.
- **View Package History** - View any audit log entries associated with the current package.
- **View Print Friendly** - View the package in a printer friendly format. (Navigation is suppressed and the package is forced into a 660 pixel-wide page.)

Check a Package's Read Status

To see who has read a package that you have sent:

- 1** Click **Packages** from the left navigation menu
- 2** Go to your **Sent** mailbox.
- 3** Locate the package and open it.

- 4 In the package header, look for **Read Status**. This is a quick indicator of how many of the package recipients have viewed the package. The possible status indicators are All, Some, or None.

Package to kristina

Trash Forward Save As Template

To: kristina
From: kristina at 3/17/2014 9:30:47 AM
Subject: A package for you

Mailbox: /Inbox/ **Read Status: ●● Read by all recipients (More)** Recall

Sending a package with that file you wanted.

Joe

Files:

ph-10135.jpg (60.2 KB) Download

Total: 60.2 KB

Trash Forward Save As Template

View Send Receipt - View Package History - View Print Friendly

- 5 Click **More** to view all recipients of the package, including members of groups marked as "Expansion Allowed" in the sender's address book, along with whether or not they have viewed the package.

Package Recipient List

Recipient List for "sample package"

Recipient	Read Status
ipswitch11lex@gmail.com	
East Coast (Expansion Not Allowed)	
Kris	
kristina	
Test Group	
kristina	

[Return to Package](#)

- All recipients of the package have viewed the package.
- Some but not all of the recipients of the package have viewed the package.
- None of the recipients of the package have viewed the package.

View Package Receipt

To view the package receipt of a package that you sent:

- 1 Click **Packages** from the left navigation menu
- 2 Go to your **Sent** mailbox.
- 3 Locate the package and open it.

- 4 At the bottom of the package page, click **View Send Receipt**. The Send Receipt page shows the Subject, Sent date and time, Recipients, any Attachments, and any Options, such as expiration and quota, set for this package.

Package

Send Receipt

Subject:	report 90
Sent:	6/9/2014 7:03:23 AM
Registered Recipients:	To:  Kris  East Coast  Administrators  Lynn
Attachments:	 UREP Plan.xlsx (280.2 KB) Total: 280.2 KB
Options:	The note was sent securely.

[!\[\]\(f1081ae2c74a1a6942b1c15eeb9a3248_img.jpg\) Return to Package](#)

View Package History

To view the package history of a package that you sent, including each time the package was viewed and attachments were downloaded:

- 1 Click **Packages** from the left navigation menu
- 2 Go to your **Sent** mailbox.
- 3 Locate the package and open it.

- 4 At the bottom of the package page, click **View Package History**. A list of events related to the package display, including the original package posting event, any notifications that were sent out, and any views of the package or any of its attachments.

"report 90"

Package History

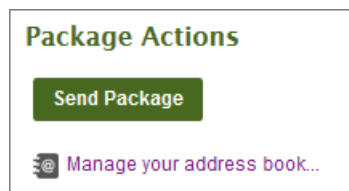
Time	Entry
6/9/2014 7:03:23 AM	Attachment added to Package
6/9/2014 7:03:23 AM	Sent new package notification to Recipient Annie
6/9/2014 7:03:24 AM	Sent new package notification to Recipient Fred
6/9/2014 7:03:24 AM	Sent new package notification to Recipient kristina
6/9/2014 7:03:24 AM	Sent new package notification to Recipient Lynn
6/9/2014 7:03:24 AM	Package posted by Kris
6/9/2014 7:03:26 AM	Viewed by Kris
6/9/2014 7:04:10 AM	Viewed by Kris
6/9/2014 7:04:43 AM	Viewed by Kris
6/9/2014 7:05:15 AM	Viewed by Kris
6/9/2014 7:05:53 AM	Viewed by Kris
6/9/2014 7:06:02 AM	Viewed by Kris
6/9/2014 7:06:07 AM	Attachment downloaded by Kris
6/9/2014 7:06:26 AM	Viewed by Kris
6/9/2014 7:06:27 AM	Attachment downloaded by Kris

 [Return to Package](#)

The **Package History** page will be available to all recipients of the package. However, only the sender will be able to see all the events. Recipients will only see the events that pertain to them, though all recipients will see the initial package posting event.

Send Packages

Sending a package is like sending an email with attachments. As such, it is a familiar process, and uses a form similar to a compose email form. The **Package Actions** section may appear on the **Home** page and/or the **Packages** page:



1 To get started, click **Send Package**. The **New Package** page opens.

- 2 Enter email address(es) in the To field. Separate multiple entries with a comma. As with conventional email, a recipient can be classified as "To", "CC", or "BCC". BCC recipients are "hidden" recipients: only the package sender can see them; none of the recipients can see or reply to any of the BCC recipients. If your administrator has configured it, you may also see the **Address Book** option for adding recipients. This option lets you click on the "To", "CC", or "BCC", then select an address from a list of contacts. You can add yourself as a recipient.
- 3 Enter a **Subject**, a description of the package (the subject will usually be included in the 'new package notification' email). It is also used to identify the package in package lists.

- 4 Enter a **Note** in the message body. The note may be optional depending on the organization settings. "Optional" may display to the left.

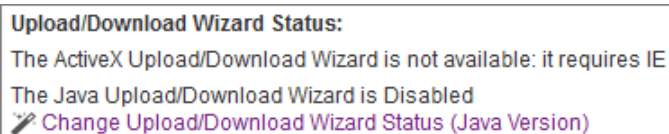
Rich Text Editor: You may see a rich text editor where you can type your note. In this editor, buttons above the editing box let you change the font, size, style, alignment, indentation, and even color of the text you enter. You can also enter links and lists. Two editors are available depending on the user's browser and that browser's configuration. Users of Internet Explorer, Firefox or Mozilla browsers with JavaScript enabled, will be able to use a rich text HTML editor. This editor lets you add color, change fonts, and add bold, underlined, and/or italicized text to your note and see what it will look like immediately. A **Clear Formatting** link is also provided to remove all HTML formatting, to facilitate copying in content from various different sources, and making it all look the same. Users who are not able to use the rich text editor will be provided a standard text box in which they may edit their package. This text box allows the entry of standard HTML tags for use of color, bold, underlines, and italics, but the text will all appear plain.

Check Spelling: You may also have a **Check Spelling** button available, which will check the spelling of both the package subject and the note. Misspelled words will be highlighted and you may use your left mouse button to select appropriate replacements as well as options to ignore that specific word, or all instances of that word. Click **Finish** to finish the spell-checker.

Note: The spell-checker will not run against notes that contain one or more sequences of characters that are longer than 1,000 characters and are not separated by spaces. If such sequences are detected, an error message will be returned and the spell-check will be aborted.

- 5 The padlock icon to the left of the **Note** box is shown either open or locked depending upon the **Secure the Note** default set by the administrator. (You might have a per package override checkbox in **Options** below.)
- If the padlock is locked, this note will appear in the package, but it will not appear as part of a new package notification email.
 - If the padlock is unlocked, the note will be included in the new package notification email.
- 6 Optionally click the **Preview** button to see what your note will look like to your recipient(s). Click the **Edit** button from the Preview page to continue working on your note.
- 7 Add files to your package. Click either **Browse** or **Launch the Upload Wizard** to locate the file(s) to upload.

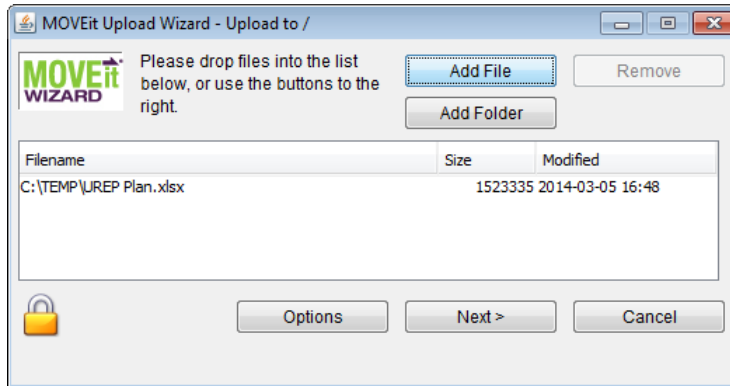
Note: Depending how your system is configured, you may see the **Upload/Download Wizard Status** at the bottom of the page.

A screenshot of a status message box with a light blue border and a drop shadow. The text inside is as follows:

Upload/Download Wizard Status:
The ActiveX Upload/Download Wizard is not available: it requires IE
The Java Upload/Download Wizard is Disabled
[Change Upload/Download Wizard Status \(Java Version\)](#)

See **Install the Upload/Download Wizard** (on page 18) for information on how to install the wizard to upload files easier and more securely.

- If you click **Browse**, locate a file and then click **Upload**. Proceed to step 13.
- If you click **Launch the Upload Wizard**, the Upload Wizard window opens:



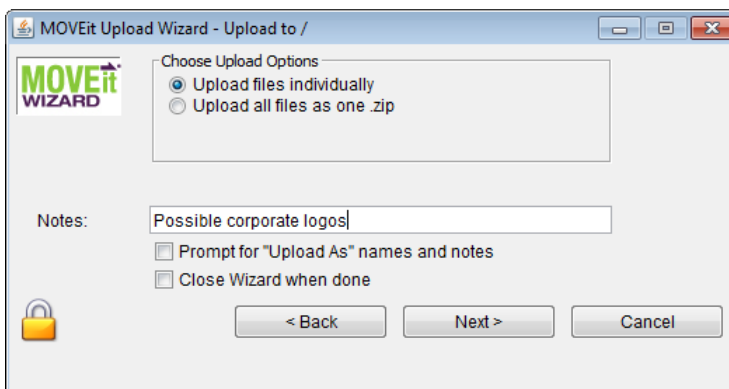
Proceed to step 8.

8 You may upload files several different ways.

- Drag-and-drop files and/or folders from an Explorer window onto the list of files in the Wizard.
- Click **Add File** and double-click files from the navigation to select individual files.
- Click **Add File** and CTRL-click files from the navigation to select multiple files from the same folder.
- Click **Add Folder** and select a folder to recursively upload.

The files do NOT have to be from the same directory. The Upload Wizard can handle files from several different directories (or even drives) at the same time.

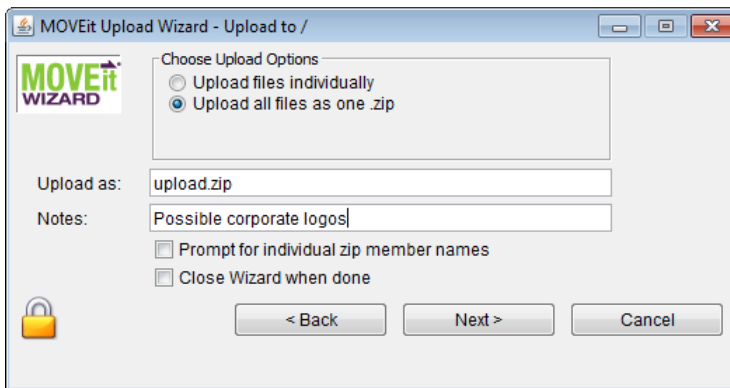
9 Press **Next >** to continue. The **Upload to /** window displays.



10 Choose how you want to upload:

- **Upload files individually:** uploads each file individually; each file will be logged on the MOVEit with a separate file ID.

- **Prompt for 'Upload As' names and notes:** Lets you add custom notes for each and every file uploaded in the collection.
- **Ignore Subfolders:** Causes all files to be uploaded to the same folder, even if they are in different folders on your computer.
- **Close Wizard when Done:** Causes the Wizard to close itself when the transfer is complete.
- **Upload all files as one .zip:** uploads all files in one zip bundle; each file will become a member of a new zip file.

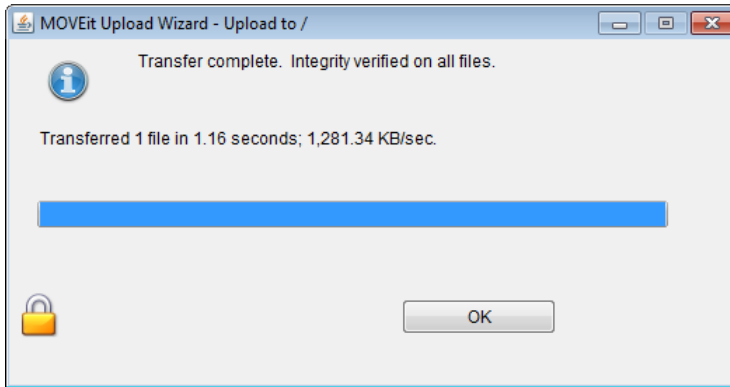


Note: The .zip file format cannot accommodate zipfiles larger than 4GB, so the Wizard will refuse to create a .zip file if the total size of the data files is greater than about 4 billion bytes.

- **Prompt for individual zip member names** Although you only have the opportunity to specify the upload notes for the zip file itself, you do have the opportunity to change the names the files stored in the archive will use if the "Prompt for individual zip member names" button is checked.
- **Ignore Subfolders:** Causes no subfolder names to be included in the zip file, even if the files are in different folders on your computer.
- **Close Wizard when Done:** Causes the Wizard to close itself when the transfer is complete.

11 Press **Next >** to begin the transfer.

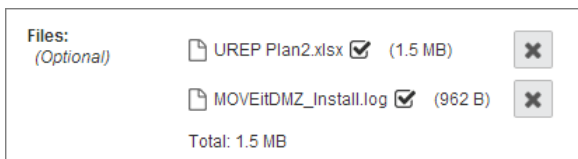
As soon as the transfer begins, a progress bar will display how much of your transfer has been completed. (The same information will also be displayed in a short text area nearby.) When it is complete, you will see a transfer summary displayed.



Note: If your administrator has enabled content scanning, and a virus or data policy violation is detected in a file you selected for upload, the Upload Wizard will display an error and either block or quarantine the file. If you selected multiple files for upload, the Upload Wizard will upload all but the infected (or policy violating) file. Filenames and entries in the Notes field are also scanned for data policy violations.

12 Click OK to leave the Wizard.

13 After you have uploaded a file it will appear in the files list, showing the size of each attached file and the total size for all attached files. If per package quotas have been set by the administrator, the quota for file size per package will also be shown. If the quota for total packages on the server is set, the lower of this quota and the per package quota is shown.



Note: When a file is added to the package, the file is uploaded to the MOVEit Server. If you click **Cancel** to stop composing the package, the file is removed from the server. If you click **Save as draft** or **Save as template** the file remains on the server.

14 Select any of the following options at the bottom of the new package page:

- **Delivery Receipt(s)** - Select this option to receive a notification email when each recipient of your package reads the package for the first time, and when a recipient downloads a file.
- **Prevent "Reply All"** - Select this option if you do not want the recipients of your package to be able to reply to all recipients of the package. This can be useful for administrators who want to send information to a large group of people, but do not want that group messaging each other.

- **Prevent all replies** - Select this option if you do not want the recipients of your package to be able to reply to the package.
- **Limit downloads to nn per file** - Sets the maximum number of times recipients can download a given transferred file. The maximum that you can specify is also shown.
- **Package will expire after nn days** - Sets the number of days that the package will be available to recipients.

Note: If an option has been 'locked' by the administrator, the value will be displayed, but you will not be able to change it.

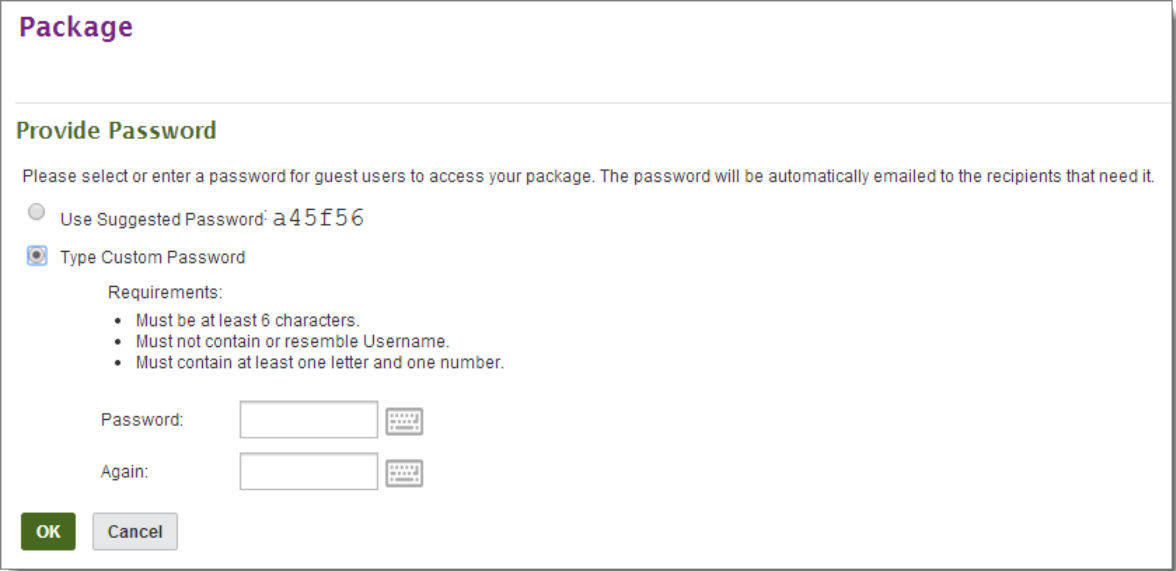
15 Optionally click any of the following:

- **Check Recipients:** Verifies that the email addresses you have entered in the **To**, **CC**, and **BCC** fields are valid addresses. This action will automatically try a wildcard search if an exact match was not found on a recipient. Specifically, if a recipient in the list has no matches, and doesn't already have a wildcard (*), email (@) or leading quote (") character, it will search again with a leading and trailing wildcard (*).
- **Save As Draft:** Saves the current package as a draft. Drafts can be opened later from the **Drafts** mailbox. You can edit a draft or send it. Once a draft has been sent, it is deleted from the Drafts mailbox. After a draft is saved, use the "click here to return to packages" link to quit editing the current draft (and save it for later) or continue editing and send the package to remove the draft.
- **Save As Template:** Saves the current package as a template in the **Templates** mailbox. You can open a template later, edit it, and send it. The original template will remain in the Templates mailbox unaltered.

16 When you are done composing your package and uploading attachments, click **Send** to send the package. Once sent, a copy is saved to your **Sent** mailbox for future reference.

A 'new package notification' email will be sent to your recipients, to inform them that a package is waiting for them. Recipients can click on the web link in this notification to connect to the site and view the package.

Sending to Unregistered Recipients: If you sent the package to an unregistered recipient (recipients that are not MOVEit users), you may be prompted to provide a password, as shown:



The screenshot shows a dialog box titled "Package". Inside, there is a section titled "Provide Password" with the instruction: "Please select or enter a password for guest users to access your package. The password will be automatically emailed to the recipients that need it." There are two radio buttons: "Use Suggested Password: a45f56" (which is unselected) and "Type Custom Password" (which is selected). Below the radio buttons, there are "Requirements:" listed as: "Must be at least 6 characters.", "Must not contain or resemble Username.", and "Must contain at least one letter and one number." There are two text input fields labeled "Password:" and "Again:", each with a small icon to its right. At the bottom left are "OK" and "Cancel" buttons.

In this case, you will need to open the sent package to view the password, which you will need to provide to unregistered recipients by sending it as a separate email, a phone call, fax, etc. in accordance with your organization's security policy. If you are a registered user, this MOVEit help contains another topic with more detail about the password options. See [Web Interface - Packages - Sending](#).

Recipient Reconciliation

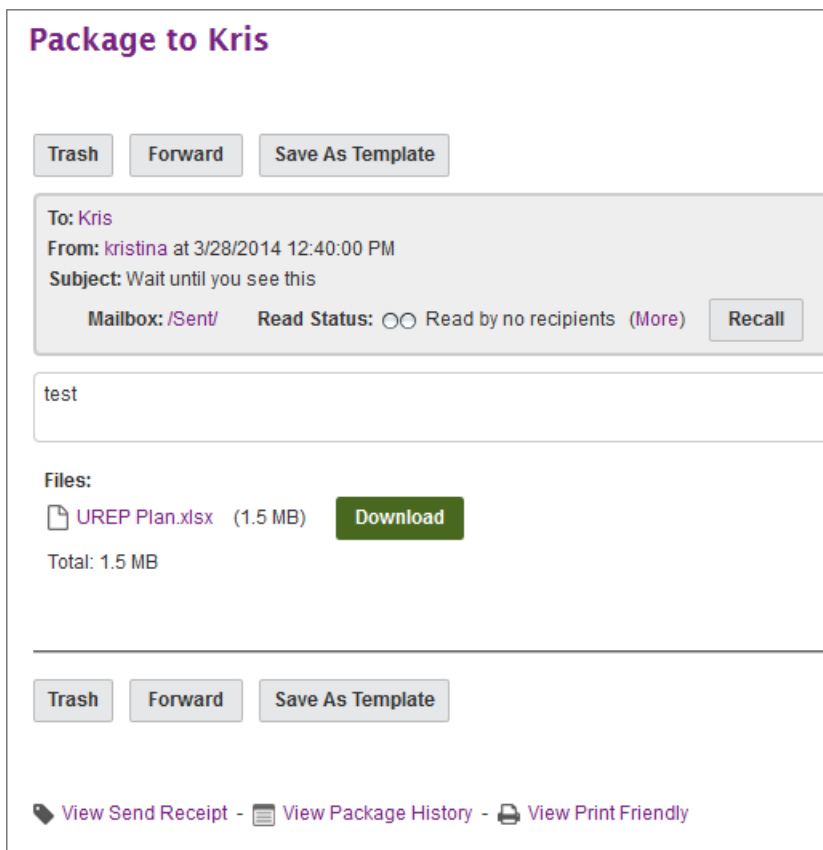
When the **Send** button is clicked, MOVEit will attempt to reconcile the email address(es) into an existing user, using the following rules:

- If two or more users reconcile to the same email address, a page will be presented asking to select the user to send a package to. If only one such user is found, that user will be silently added as a recipient to the package.
- If no registered users in the user's address book are found to match the given email address, but a temporary user is found, that temporary user will be silently copied in as the recipient of the package.
- In all of the above cases, only users who are active will be selectable as a recipient. If one or more registered or temporary users are found that match the search term, but are not currently active, an error message will be displayed indicating this fact.
- If no existing user is found matching the given email address, MOVEit creates a temporary user based on that email address. By default, passwords are automatically generated and emailed to the user, "full names" are initially assumed to be the same as the email address, and the language of the recipient is initially assumed to be the same as the sender.

Recall a Package

To recall a package that you sent so it is no longer available to the recipients:

- 1 Click **Packages** from the left navigation menu
- 2 Go to your **Sent** mailbox.
- 3 Locate the package and open it.
- 4 In the package header, click **Recall**.



- 5 Confirm your selection.

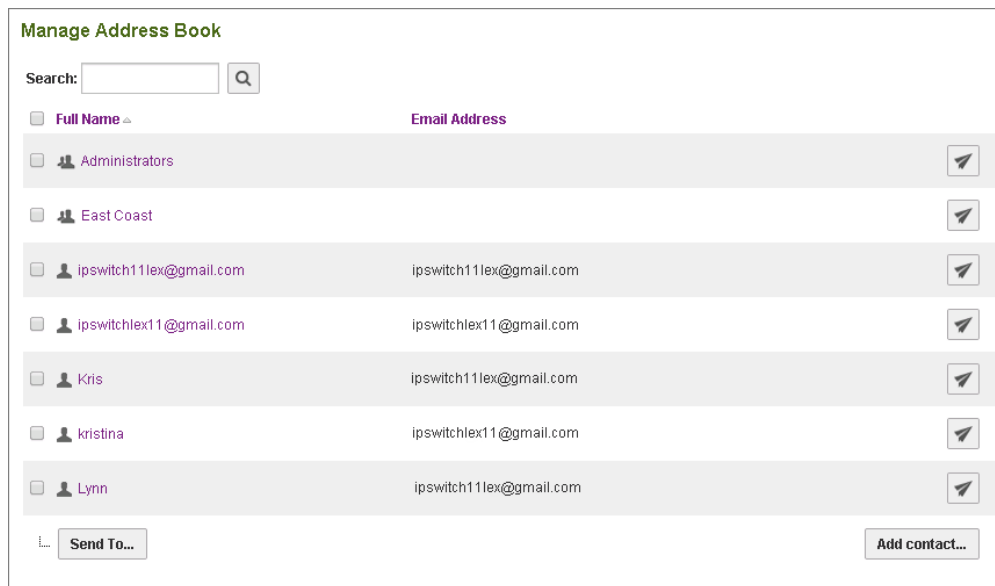
The recalled package will be removed from the MOVEit server and will not be available for download by the recipients. Recalled packages will still appear in the Sent mailbox where they can be viewed, trashed or resent with edits.

Note: Recalling a package has no affect on package quotas, so cannot be used to "recover" quota

Manage Your Address Book

Your address book contains a list of users and groups to whom you may send packages. If enabled, you can also send packages to registered users not in your Address Book, and also to unregistered users, in which case MOVEit creates a temporary user.

To view your address book, from the Home page or the Packages page, click the Manage your address book... link. The Manage Address Book page displays:



The screenshot shows the 'Manage Address Book' interface. At the top, there is a search bar with a magnifying glass icon. Below it, a table lists contacts. Each row has a checkbox on the left, a name or group name in the middle, and an email address on the right. A paper plane icon is at the end of each row. At the bottom left, there is a 'Send To...' button. At the bottom right, there is an 'Add contact...' button.

	Full Name	Email Address	
☐	Administrators		
☐	East Coast		
☐	ipswitch11lex@gmail.com	ipswitch11lex@gmail.com	
☐	ipswitchlex11@gmail.com	ipswitchlex11@gmail.com	
☐	Kris	ipswitch11lex@gmail.com	
☐	kristina	ipswitchlex11@gmail.com	
☐	Lynn	ipswitch11lex@gmail.com	

...

This page shows a list of all contacts in your address book. Groups may also have address books, and the entries in a group's address book are automatically available to the members of that group.

Note: Inactive, suspended, or expired users will not be available as package recipients, even if they are present in a user or group address book.

Click Send  to send a package to that user.

Click on any user name to view the User Profile:



User Profile (ipswitchlex11@gmail.com)

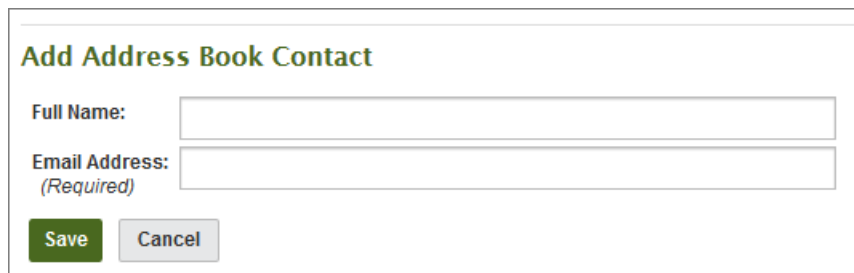
Information

Username: ipswitchlex11@gmail.com
Full Name: ipswitchlex11@gmail.com

Select an Activity...

 [Send Package to ipswitchlex11@gmail.com](#)

Click **Add contact...** to add a contact to your address book. Enter a name and email address for the new contact and click **Save**:



Add Address Book Contact

Full Name:

Email Address:
(Required)

Note: If you send a package to a user who is not in your address book, an entry will be added to your address book so that replies are possible. Another option lets users send packages to an unregistered user with a "package password," in which case, a temporary user is not created. A "package password" provides access to the package sent only, and can be used for a one-time, or infrequent, correspondence with recipient(s).

Manage My Account

Note: The My Account link may not display depending on your organization's setup.

The My Account page lets you change your password or email address without having to contact an administrator. It also provides a place to edit personal display settings, such as how many files or folders are shown on file/folder list pages, and whether or not to use the **Upload/Download Wizard** (on page 18) for uploading and downloading files. If Ad Hoc Transfer is enabled, you can select to always receive a delivery receipt, and you can enter a signature for packages. The page can be accessed from the user bar which appears at the top of each and every screen.

Manage Your Expiration Details

To view your expiration details, click My Account in the top banner. Locate the Expiration Details section.

Expiration Details...

Your account will expire...

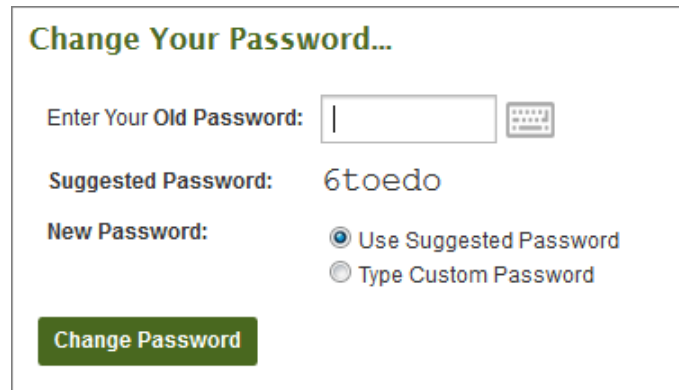
on 3/31/2014 6:15:31 AM unless account is used again (7 day(s) after last signon)

If an expiration policy is assigned to your user account, the details of when the user account will expire will be shown here. An information string states when the user account will be expired according to the current policy.

Note: This section will not appear if no expiration policy is assigned to the user.

Change Your Password

To change your password, click **My Account** in the top banner. Locate the **Change Your Password...** section.



The screenshot shows a web form titled "Change Your Password...". It contains the following elements:

- A label "Enter Your Old Password:" followed by a text input field and a password strength indicator icon.
- A label "Suggested Password:" followed by the text "6toedo".
- A label "New Password:" followed by two radio button options: "Use Suggested Password" (which is selected) and "Type Custom Password".
- A green button labeled "Change Password" at the bottom left.

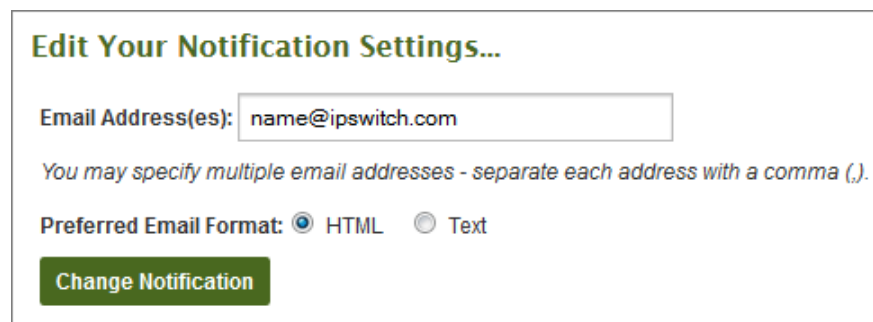
Enter your old password where prompted, and either select the suggested password or choose to enter a custom password, and then press the **Change Password** button. If password aging has been enabled, an additional aging status message will be displayed to show how long it has been since the last password change and note when you must change your password.

Note: This section will not appear if the Disallow User Password Changing feature has been enabled. Please see the "Settings" help page for more information.

Note: You need to read the password rules shown here (and also shown when an attempt to change your password fails). Depending on site specifics, passwords may be disallowed because they are too short, contain variations of the username, contain common words or are otherwise too easy to guess or crack.

Edit Your Notification Settings

To edit the email address where you receive notification, click **My Account** in the top banner. Locate the **Edit Your Notification Settings...** section.



The screenshot shows a web form titled "Edit Your Notification Settings...". It contains the following elements:

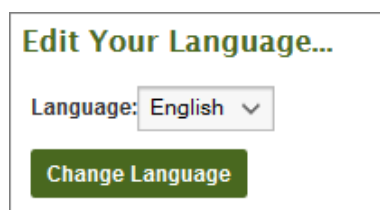
- A label "Email Address(es):" followed by a text input field containing "name@ipswitch.com".
- A note below the input field: "You may specify multiple email addresses - separate each address with a comma (,)."
- A label "Preferred Email Format:" followed by two radio button options: "HTML" (which is selected) and "Text".
- A green button labeled "Change Notification" at the bottom left.

Enter an email address where you want to receive new package and new file notifications. You may specify multiple email addresses for a single account by separating email addresses with commas.

You may also change your preferred format for notification emails that you receive. Available formats are HTML and Text.

Edit Your Language

To edit the language displayed in the current session, click **My Account** in the top banner. Locate the **Edit Your Language...** section.

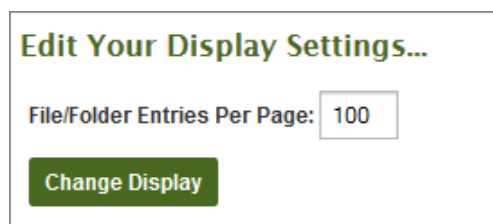


Select the desired language and click **Change Language**. The new language is saved in your profile, and the current session changes to the new language.

Note: Only Registered users and Temporary users may change their language.

Edit Number of Folders/Files Shown Per Page

To edit the number of files and folders that display per page, click **My Account** in the top banner. Locate the **Edit Your Display Settings...** section.

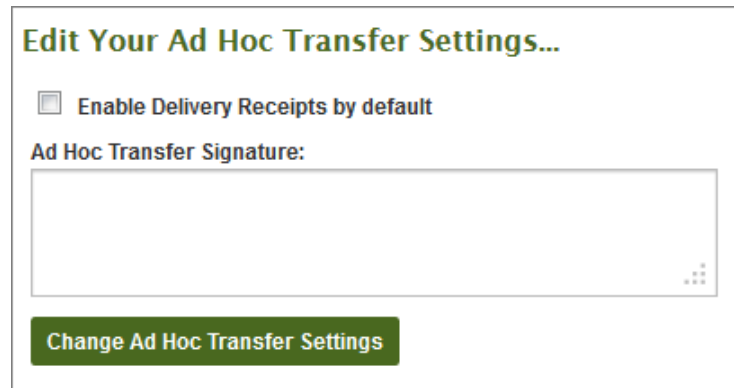


Enter a number between 5 and 200, then click **Change Display**.

If more than this number of files or folders existing, page navigation links will appear on the Folders page.

Edit Your Ad Hoc (Package) Transfer Settings

To enable or disable Delivery Receipts by default in all packages you send, or to add a signature by default to all new packages, click **My Account** in the top banner. Locate the **Edit Your Ad Hoc Transfer Settings...** section.



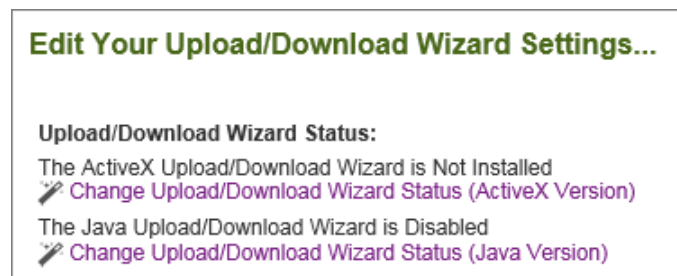
The screenshot shows a dialog box titled "Edit Your Ad Hoc Transfer Settings...". It contains a checkbox labeled "Enable Delivery Receipts by default". Below this is a text input field labeled "Ad Hoc Transfer Signature:". At the bottom of the dialog is a green button labeled "Change Ad Hoc Transfer Settings".

Check **Enable Delivery Receipts by default** to have all new, replied or forwarded packages show the Delivery Receipts box checked by default. You may still uncheck Delivery Receipts manually within any new package.

Enter a signature in the Ad Hoc Transfer Signature box to append to all new packages that you create.

Edit Your Upload/Download Wizard Settings

To view or change the Upload/Download Wizard status, click **My Account** in the top banner. Locate the **Edit Your Upload/Download Wizard Settings...** section.



The screenshot shows a dialog box titled "Edit Your Upload/Download Wizard Settings...". It contains the following text:

- Upload/Download Wizard Status:**
- The ActiveX Upload/Download Wizard is Not Installed
 [Change Upload/Download Wizard Status \(ActiveX Version\)](#)
- The Java Upload/Download Wizard is Disabled
 [Change Upload/Download Wizard Status \(Java Version\)](#)

There are two versions of the Wizard: ActiveX and Java. The ActiveX version is available only to users of Internet Explorer. The Java version is available only if Java 6 or later is installed on your computer.

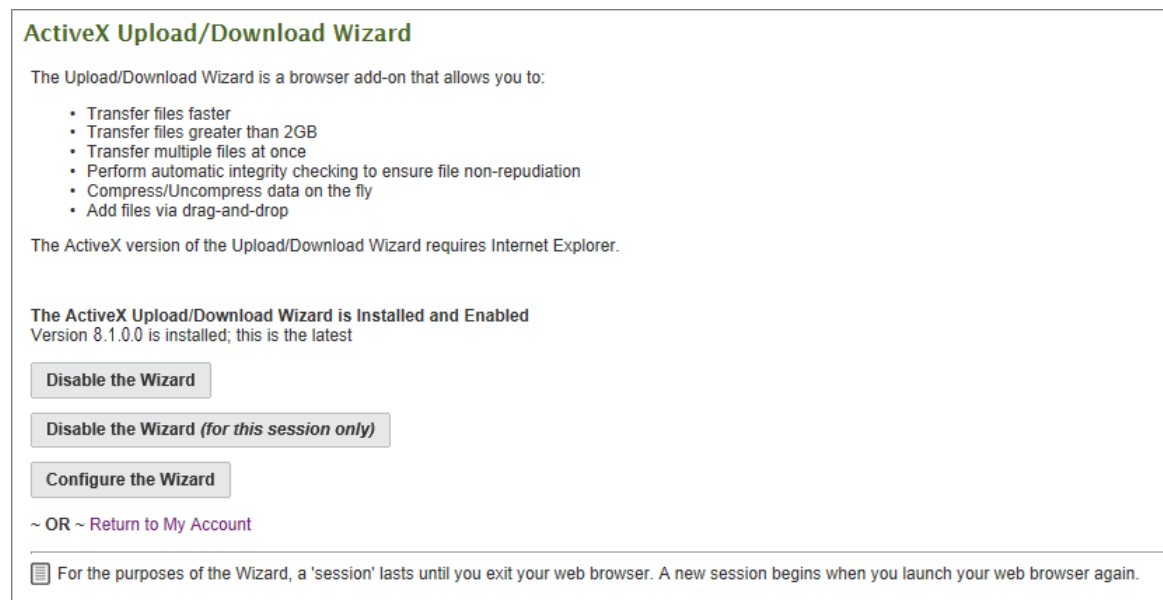
Click **Change Upload/Download Wizard Status** for the desired version (ActiveX or Java). Separate but similar configuration pages display for the ActiveX and Java Wizards.

Wizard Not Installed

If the Wizard is not installed on the current browser, you'll see a link to a page where the Wizard can be installed.

Wizard Already Installed

If the Wizard is already installed and enabled, you'll see the following options:



ActiveX Upload/Download Wizard

The Upload/Download Wizard is a browser add-on that allows you to:

- Transfer files faster
- Transfer files greater than 2GB
- Transfer multiple files at once
- Perform automatic integrity checking to ensure file non-repudiation
- Compress/Uncompress data on the fly
- Add files via drag-and-drop

The ActiveX version of the Upload/Download Wizard requires Internet Explorer.

The ActiveX Upload/Download Wizard is Installed and Enabled
Version 8.1.0.0 is installed; this is the latest

[Disable the Wizard](#)

[Disable the Wizard \(for this session only\)](#)

[Configure the Wizard](#)

~ OR ~ [Return to My Account](#)

 For the purposes of the Wizard, a 'session' lasts until you exit your web browser. A new session begins when you launch your web browser again.

Java Upload/Download Wizard

The Upload/Download Wizard is a browser add-on that allows you to:

- Transfer files faster
- Transfer files greater than 2GB
- Transfer multiple files at once
- Perform automatic integrity checking to ensure file non-repudiation
- Compress/Uncompress data on the fly
- Add files via drag-and-drop

The Java version of the Upload/Download Wizard requires Java 6 or later.

The Java Upload/Download Wizard is Installed and Enabled

Disable the Wizard

Disable the Wizard (*for this session only*)

Configure the Wizard

~ OR ~ [Return to My Account](#)

 For the purposes of the Wizard, a 'session' lasts until you exit your web browser. A new session begins when you launch your web browser again.

- **Disable the Wizard:** Disables use of the Wizard for all future sessions. You can still enable the Wizard by going to My Account and clicking the **Change Upload/Download Wizard Status** link.
- **Disable the Wizard (*for this session only*):** Disables the Wizard for this session only. You will be asked at the beginning of the next session whether you want to enable the Wizard or not.
- **Configure the Wizard:** Displays a dialog that lets you edit the default download actions for each type of file. The Wizard allows you to specify that all files with a given extension be saved to a temporary directory and immediately opened, OR saved to a user-specified directory with no further action taken. The Configure the Wizard option allows you to later change your mind regarding what actions should be taken for different file extensions.

Note: The Configure the Java Wizard option also gives the option of configuring proxy settings. The ActiveX Wizard gets its proxy settings directly from Internet Explorer.

Sign Out

You may be signed off for one of four reasons:

- You clicked the **Sign Off** link found near the top of the page. Typically, a "Signed off successfully" message will appear at the top of the screen to confirm a proper sign off.

Signed off successfully.

-
- You have done NOTHING for the last XX minutes (usually, 20 minutes) and you were signed off automatically for security reasons. Often, a "signout by timeout" will result in less friendly "You already signed off" or "Session has expired" messages at the top of the screen.
 - An administrator terminated your session.
 - You signed off from your Single Signon account. If your organization is set up to use SAML Single Signon, when you sign off from your corporate or network account, you may also be signed off from MOVEit.

Most often, when you are signed off the system, you will be returned to the Sign On page. If you attempt to "re- sign on" from this page, you will usually be returned to the page you were viewing before you signed off. Also, with few exceptions, pressing the "BACK" button on your browser will not allow you to see MOVEit content unless you sign back on.

Signing out from a SAML Single Signon Session

If you are using Single Signon, and you select to sign off from MOVEit, you will be asked if you want to sign out of your Identity Provider session as well. If you click **Yes**, you will initiate a Single Logout process, which means you will be logged out of your MOVEit session as well as any other applications to which your Single Signon provides access. You are returned to the MOVEit Single Signon page. To sign on again, you will need to supply your username and password.

Note: If your organization has multiple identity providers, you will be asked to choose one in order to re-signon, if you did not click the **Remember selection** option on the Sign On page.

If you click **No**, you will be signed out of the MOVEit session only. You are returned to the Single Signon page. To sign on to MOVEit again, you do not have to enter your username and password, as you are still authenticated through the identity provider.

If you click **Cancel**, the sign out is canceled and you are returned to your MOVEit home page.

Index
