

Getting Started - Sign On

The Sign On page is the first page you will see from the MOVEit DMZ site. This page contains fields for a your Username and Password, a "Sign On" button to send this information to MOVEit DMZ and a "Reset" button to clear it.

The screenshot shows the 'Sign On' section of the MOVEit DMZ site. It includes a 'Username:' field, a 'Password:' field, and two buttons: 'Sign On' and 'Reset'. To the right of the fields is a 'Security Notice' box with the text: 'You are about to access a secured resource. MOVEit Sample reserves the right to monitor and/or limit access to this resource at any time.'

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 DMZ site from a public computer, it is highly recommended you use the clickable keyboard to enter your username and password.

This screenshot shows the same 'Sign On' page as above, but with a yellow 'clickable keyboard' overlay. The keyboard has four rows of keys: the first row contains backslash, numbers 1-0, hyphen/underscore, equals, and left arrow; the second row contains letters q-w, e-r, t-y, u-i, o-p, left bracket, right bracket, and backslash; the third row contains letters a-s, d-f, g-h, j-k, l, semicolon/apostrophe; the fourth row contains left shift, letters z-x, c-v, b-n, m, comma/semicolon, period/slash, and right shift. A 'SPACE' key is centered below the fourth row. A 'Close' button is in the bottom right corner of the keyboard overlay.

If your organization supports multiple languages, MOVEit DMZ 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.

Connexion

Nom d'utilisateur:

Mot de passe:

Connexion

Réinitialiser

Avis de sécurité

Vous êtes sur le point d'accéder à une ressource sécurisée. MOVEit Sample se réserve le droit de surveiller et/ou limiter l'accès à cette ressource à tout moment.

When you press the Sign On button, your username and password are transmitted securely (via HTTPS) to MOVEit DMZ. 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 you 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 MOVEit Sample! 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 secure message 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!)

1. Username is incorrect
2. Password is incorrect
3. Account has been suspended (for too many bad sign-on attempts, password aging, or manual administrator action)
4. Account is not allowed to sign on from this IP address
5. IP address has been locked out (for too many bad sign-on attempts, often with different usernames)
6. Client certificate has not been provided when one is required, or a bad client certificate has been provided.

Requesting 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 through 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.



Sign On

Username:

Password:

Sign On

Reset

Security Notice

You are about to access a secured resource. MOVEit Sample reserves the right to monitor and/or limit access to this resource at any time.

Need Help? [Tech Support](#) - [Online Manual](#)

Forget your password? [Request a password change](#)

Clicking this link will open 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.

Client Certificates

Your organization may require you to authenticate to MOVEit DMZ 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 DMZ 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 either install and manage client certs through IE's "Certificate" dialog (located on the "Content" tab under IE7's "Tools" menu). 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". In Mozilla (1.7), this facility is found in the "Privacy & Security" options tree. In Firefox (2.0), this facility is found in the "Encryption" options tab ("View Certificates" button).

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 DMZ 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.)

Getting Started - Uploading Files

There are 2 quick ways to upload files to MOVEit DMZ through the web interface:

Upload Wizard (*Internet Explorer, Mozilla, Firefox, Netscape or Safari only*):

Upload Form (*If not using the MOVEit Upload Wizard*):

The upload wizard and/or form are available in two different locations:

1. Your **Home page**. Click on the "Home" link on the left side of the screen. Scroll down to the "Upload" section on your Home page and pick the person/folder the file should go to.
2. Any **folder view page** into which you are allowed to upload. If it is available, click the "Folders" link on the left side of the screen and then "click into" the folders displayed until you find the folder into which you would like to upload your file. Scroll down to the "Upload" section on this Folder's page.

File Notifications

Upload Confirmation: You may get an email message called an "upload confirmation" when you upload your file. (This option is turned off by default.)



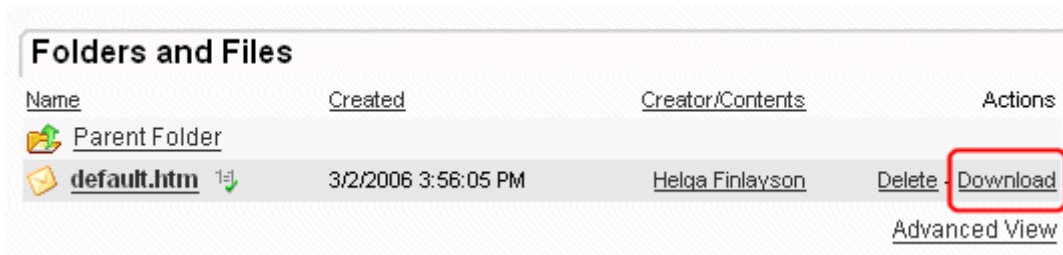
New File Notification: Other users may get an email message called a "new file notification" when you upload your file. (This option is turned on by default.) However, you will NOT get a new file notification if you upload a file into your OWN home folder.

Delivery Receipt: When someone downloads your file from MOVEit DMZ, 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.)

Getting Started - Downloading Files

There are several ways to download files from MOVEit DMZ 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:

1. 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.)
2. 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.
3. 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.

Getting Started - Sign Off

You may be signed off for one of two 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.



- You have done NOTHING for the last XX minutes (usually, 20 minutes) and you were signed off automatically for security reasons. Often, a "sign-out by timeout" will result in less friendly "You already signed off" or "Session has expired" messages at the top of the screen.



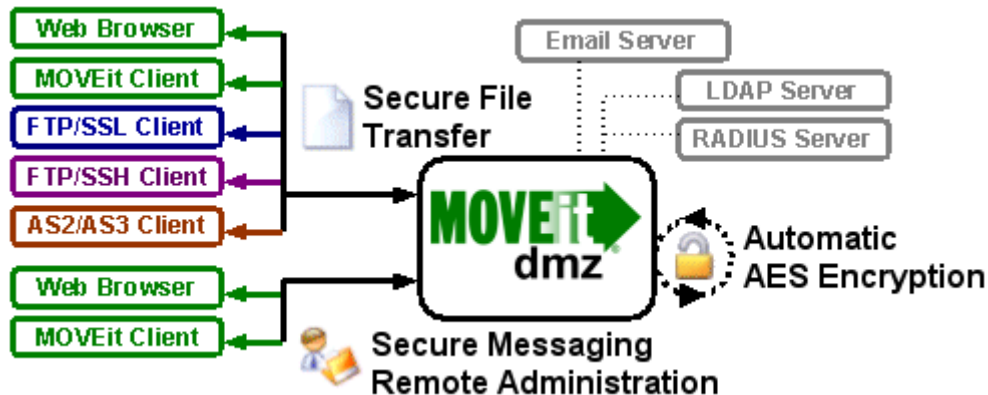
- An administrator "kicked" you off the system.

No matter how 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 to see MOVEit DMZ content unless you sign back on.

Detailed information on why WellCare chose to utilize this product

Introduction

MOVEit® DMZ is a secure file transfer and secure message server. It is a vital component of the [MOVEit® family](#) of secure file processing, storage, and transfer products developed by [Ipswitch, Inc.](#). These products provide comprehensive, integrated, standards-based solutions for secure handling of sensitive information, including financial files, medical records, legal documents, and personal data.



MOVEit DMZ safely and securely collects, stores, manages, and distributes sensitive information between your organization and external entities. Web browsers and no cost/low cost secure FTP clients can quickly, easily, and securely exchange files with MOVEit DMZ 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 DMZ 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 DMZ activities while a programmable interface (via [MOVEit DMZ API Windows](#) and [MOVEit DMZ API Java](#)) makes MOVEit DMZ accessible to custom applications.

MOVEit DMZ 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 DMZ.

Encryption capabilities throughout the MOVEit product line are provided by [MOVEit Crypto](#). 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).



Physical Specifications

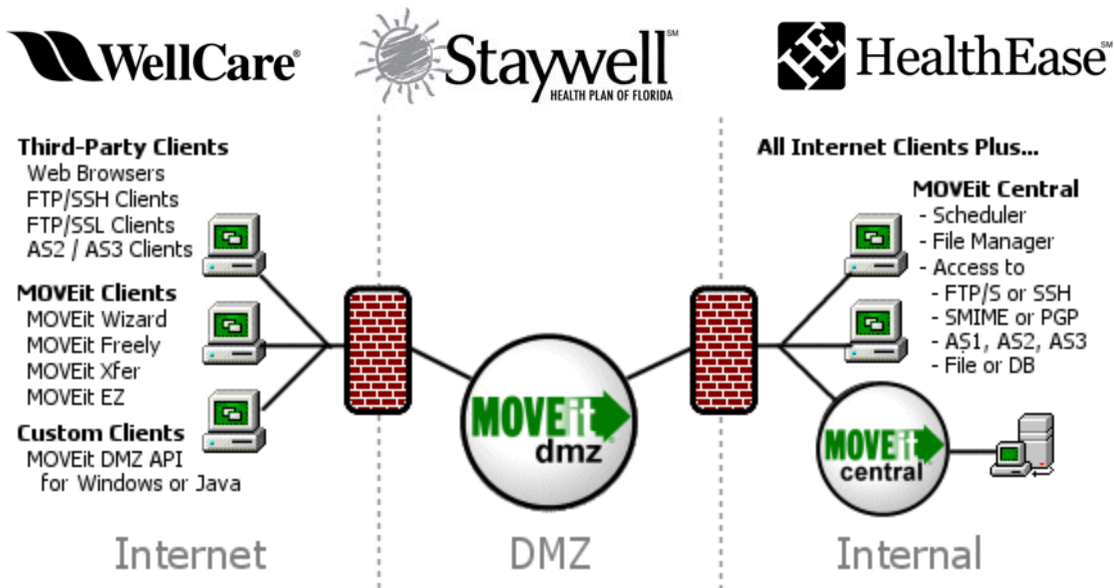
The MOVEit DMZ software itself resides on a Microsoft Windows Server 2003 platform hardened against threats from the Internet and trusted networks. Organizations that need to support very large volumes of file transfers and/or many users may require additional hardware, but for many organizations the minimum recommended specifications of a MOVEit DMZ 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](#).

Network Specifications

In a typical network topology MOVEit DMZ 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 DMZ from internal and external networks. For security reasons, MOVEit DMZ 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 DMZ to fill this role.)

MOVEit DMZ'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 DMZ 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 DMZ 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 DMZ 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.)

Accessing MOVEit DMZ

"Client" access to MOVEit DMZ 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 (i.e. Internet Explorer, Firefox, Netscape, Mozilla, Safari and/or Opera). Authorized administrators may configure the MOVEit DMZ server from authorized locations while customers and partners use a simpler portal to move files in and out of the MOVEit DMZ system.

Also available through the web interface, the optional MOVEit Upload/Download Wizard 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.

A secure FTP interface is also available on the MOVEit DMZ server for people or programs with secure FTP clients. The MOVEit family offers two free, scriptable command-line clients, [MOVEit Freely](#) (FTP) and [MOVEit Xfer](#) (HTTPS) both of which support file integrity checking. Many third-party companies manufacture secure FTP clients for desktops and servers which will also interface with MOVEit DMZ's secure FTP over SSL and FTP over SSH servers.

For IT departments who desire more control over the MOVEit DMZ environment than the FTP protocol can provide, the [MOVEit DMZ API](#) products provide easy access to and control of MOVEit DMZ via a COM object (for Windows) or Java classes (for *nix, Windows, IBM, etc.). MOVEit DMZ 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 DMZ as a local folder is desired, consider using [MOVEit EZ](#). MOVEit EZ is a "tray icon application" which synchronizes content between a user's desktop and MOVEit DMZ and schedules transfers.

When coupled with MOVEit Central and the appropriate licensing, [MOVEit DMZ supports AS2 and AS3 file transfer](#). (MOVEit DMZ 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 DMZ can be found in the ["Client Support" document](#).