
MOVEit DMZ

Getting Started Guide

Version 8.3



Install - Check Prerequisites

License file: Save the license file that is attached to the MOVEit DMZ thank you email. MOVEit DMZ requires a license file to install and operate. For details, go to the Ipswitch Knowledge Base and search for this topic [*How do I download my MOVEit license file.*](#)

The installation program first checks for required software and displays a message if any of the required software is missing.

For complete list of requirements see *System Requirements* (<http://www.ipswitchft.com/products/moveit/systemrequirements.aspx>)

Microsoft .NET 4.5 is required

When installing on Windows 2012, Microsoft .NET 4.5 is already installed with the operating system.

When installing on Windows 2008 R2, if the install program detects that you do not have Microsoft .NET 4.5, you are prompted to download and install it.

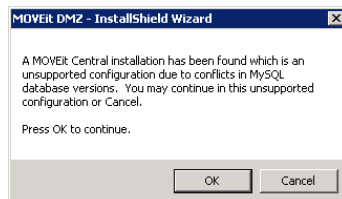
Note: You must have internet connectivity for this step.



Click **Yes** to download and install the .NET 4.5 software. This can take several minutes to complete. When complete, the Welcome dialog opens.

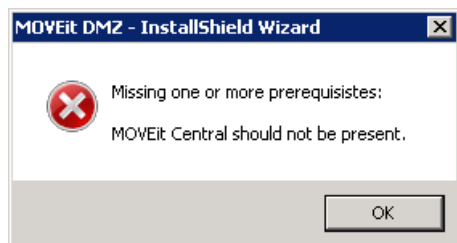
Unsupported Configuration: MOVEit Central installed on same machine

Running MOVEit DMZ and MOVEit Central on the same machine is not supported. If a MOVEit Central is installed on the machine, a message informs you of this:



Cancel the install, and either move your MOVEit Central installation or find another machine for the MOVEit DMZ installation.

When you click **Cancel**, a second dialog opens.



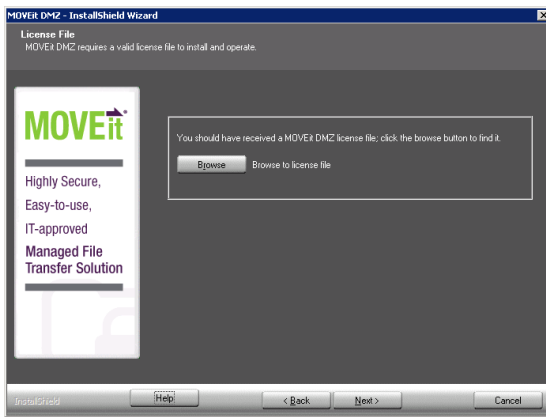
Click **OK** to close the installation program.

MOVEit DMZ Installation

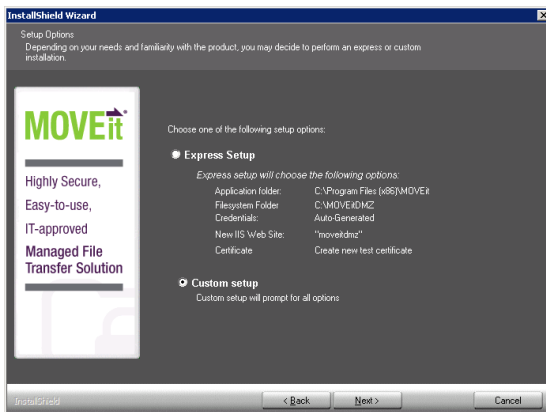
This installation program installs MOVEit DMZ and its services on a server. These services include:

- Web Application (HTTP - HTTPS)
- FTP Server (FTP - FTPS)
- SSH Server (SFTP)
- MySQL Database Server - **Express Setup**, the default selection, installs MySQL on the local machine.

1. This Welcome screen opens. Click **Next**. The License File screen opens.
2. Read and accept the license agreement. Click **Next**.
3. Click **Browse** and select the license file, which was attached to the MOVEit DMZ thank you email. Click **Next**.



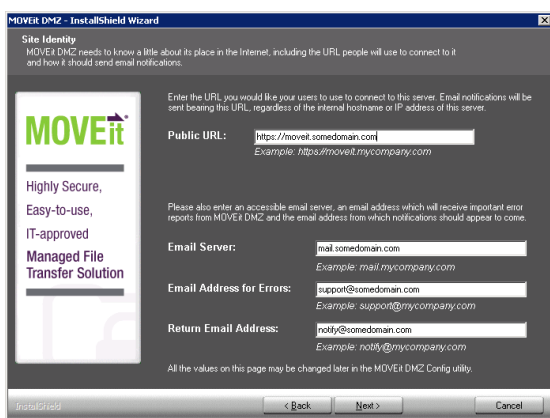
4. On the Setup Options screen, select **Express Setup** for an evaluation installation.



Express Setup uses the default values for the following items:

- Application Folder: C:\Program Files\MOVEit
- Filesystem Folder: E:\MOVEitDMZ (largest local drive)
- Credentials: Use Suggested (automatically generated)
- New IIS Web Site: MOVEitDMZ
- Certificate: Create New Test Certificate

5. On Site Identify screen, specify the URL for users to connect to MOVEit DMZ and how MOVEit DMZ sends email notifications.



Site Identity Options:

- **Public URL:** The URL for users to connect to this server. Email notifications will be sent with this URL, regardless of the internal hostname or IP address of this server.

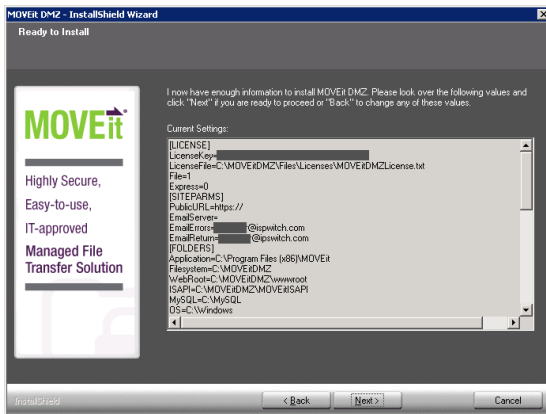
Note: IP addresses and hostnames are valid, but should only be used for testing and evaluation purposes.

Examples:

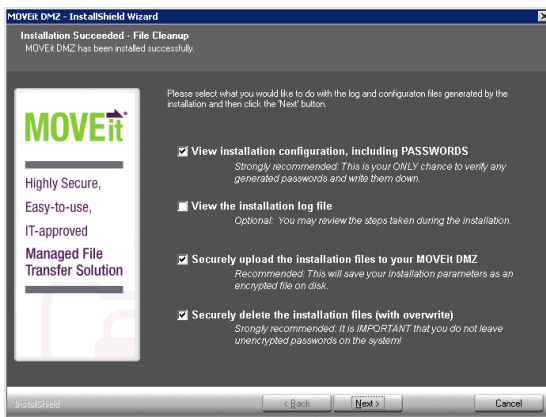
- Installing into a regular folder: **https://moveit.somedomain.com.**
- Installing into a virtual folder: **https://www.somedomain.com/moveit.**
- **Email Server:** The email server that MOVEit DMZ will use to relay email. An IP address is a valid entry. For example, **mail.somedomain.com**
- **Email Address for Errors:** Occasionally MOVEit DMZ will send errors and other administrative notices using this address. It's highly recommended that this address be a valid address that is checked regularly. For example, **support@somedomain.com**
- **Return Email Address:** The "From" address that will be used on all email notifications. It's recommended this be a valid address as end-users may reply to this address. For example, **notify@somedomain.com**

All of these values can be changed later in the MOVEit DMZ Config Utility.

6. On the Ready to install screen, review your selections and click **Next**.



7. Installation complete screen: MOVEit DMZ has been installed successfully.



8. View successful install options

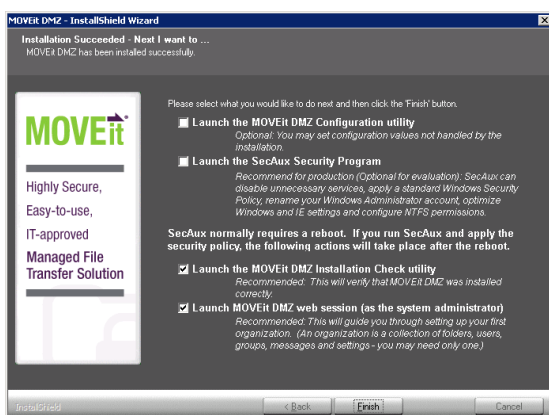
- **View Installation configuration, including Passwords:** Opens a text document with all the configuration settings and passwords that have been used. This will be the only chance to verify any suggested passwords.

Important: Be sure to view the Installation configuration and write down the password for the **sysadmin** account. You need this password to log into MOVEit and set up your organization, users, and other settings.

- **View the installation log file:** A file containing all the install steps. Useful for debugging installation issues.
- **Securely upload the installation files to your MOVEit DMZ:** Saves your installation parameters as an encrypted file on disk. Only SysAdmins can view these files.
- **Securely delete the installation files (with overwrite):** Deletes all configuration files that were generated during the install. This step is highly recommended so that unencrypted passwords do not remain on the DMZ server.

If you choose either of the first two options, you must close the text document before continuing to the next installation screen.

9. On the MOVEit DMZ has been installed successfully screen, select the Finished Installation options.



Finished Installation Options:

- **Launch the MOVEit DMZ Configuration Utility:** Launches the utility that allows you to make changes to your MOVEit DMZ system. You can set configuration values that are not handled by the installation.
- **Launch SecAux Security Program:** Launches the security program to further harden your operating system.

Highly recommended: Run the SecAux program on production servers that will be made available on the internet.

SecAux can disable unnecessary services, apply a Windows Security Policy, rename your Windows Administrator account, optimize Windows and IE settings and configure NTFS permissions.

- **Launch the MOVEit DMZ Installation Check Utility:** Launches the MOVEit DMZ Check Utility which is used to test various components of the MOVEit DMZ system and verify that they are in working order.
- **Launch MOVEit DMZ web session (as the SysAdmin):** This will start you with adding a new organization and adding additional users. This step is highly recommended.

If you select multiple options here, each program/utility is displayed after the current one is closed.

After you close any open program/utility, the setup program prompts you to delete the installation configuration and log files. Doing this provides an extra measure of security.

MOVEit DMZ Configuration

After you sign in to the MOVEit DMZ server for the first time, your first task will be to create an Organization that will contain your users, groups, folders, and files.

The Add a New Organization wizard opens.

Step 1 - Name, Passphrase, and Technical Contact

- **Name** - The name your organization will be displayed with. The name is visible to users when they are signed in to the system. Suggestion: use a name that is similar or even identical to your company name, as this name will be visible to your users when they are signed on to the system. This value can be changed after the organization has been created.

This organization's name should not be an "internal" designation, but rather something which will make sense to the people accessing this system remotely. Only the following characters are allowed in the organization name (including uppercase letters):

abcdefghijklmnopqrstuvwxyz1234567890 . , ! ? * # @ _ = + () : ` ~ % ^ & [{] ;

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.

Short Name:

- **Passphrase** - The passphrase is used to generate the encryption keys that will protect the files that are uploaded to your organization.

Recommended: Use the automatically-generated passphrase. It is guaranteed to meet the strength requirements imposed by the system

An automatically-generated 16-character passphrase is provided by MOVEit DMZ. It is recommended that you use this passphrase, because it is guaranteed to meet the strength requirements imposed by the system. If you do not approve of the automatically generated passphrase, you can refresh the page to generate a new one. To create your own passphrase, select User Own Passphrase and provide the passphrase. It must meet the following requirements: It should be a relatively long sequence of characters, as random as possible, and must contain at least one letter and one number.

Important: The passphrase cannot be changed once the organization has been created, and it cannot be recovered if lost. MAKE SURE YOU WRITE DOWN THIS PASSPHRASE AND/OR PRINT THIS PAGE.

Each organization uses a unique key based on a passphrase to protect information. You may choose to accept the autogenerated passphrase or specify one of your own. If you choose to use the autogenerated passphrase, please **write it down** and/or print this page before proceeding.

Autogenerated Passphrase:

./%5 SbTY !D.B cgj8 b5s8

Use Autogenerated Passphrase

Use Own Passphrase

Enter passphrase:

Confirm passphrase:

- **Technical Contact** - The name, phone number, and email address of the primary technical support contact for your organization, such as your helpdesk group, or customer service team. This information will be provided to users in notification emails, and on the Tech Support page. These values can be changed after the organization has been created.

Please fill in the name, phone number and email address of this organization's help desk or customer service team. This information will be used to direct end users to the first line of local technical support (e.g., the group normally responsible for resetting passwords).

Tech Contact:

Tech Phone:

Email:

Click the "Continue" button below to add a new organization and continue configuration.

Before you continue, you must confirm that you have written down and/or printed your organization passphrase and safely stored it.

Step 2 - Host Access Rules

Host access rules define the hosts and IP addresses where your users and administrators can log on to the system. More rules can be added at a later time.

- **Allow (End) Users to Connect From** - Defines hosts where your end users can initially log on to MOVEit DMZ. Most organizations will want to allow end users to connect from anywhere, so the default mask here is "*.*.*.*.".

Allow (End) Users to Connect From
(Enter "*.*.*.*" to allow access from anywhere on the Internet)

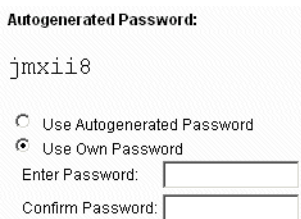
- **Allow Administrators to Connect From** - Defines the hosts where your administrator users can initially log on to MOVEit DMZ. The default mask here is "10.*.*.*", which allows administrators to connect from their internal network

Allow Administrators to Connect From
(Enter "10.*.*.*" or a more appropriate Internal address range)

Step 3 - Add an Administrator

This step allows you to create your first administrator account in your new organization. The username cannot be changed after the account is created, but the password and email address can.

- **Username** - The login name of the new administrator account. The username cannot be changed once the account is created, but more accounts can be created and this one deleted at a later time, if necessary.
- **Password** - Use the recommended automatically-generated password, or select the Use Own Password option and enter your own. The password for this account may be changed at a later time.



Autogenerated Password:
jmxii8

Use Autogenerated Password
 Use Own Password

Enter Password:
Confirm Password:

- **Email Address** - The email address is used to send notifications for this administrator account will be sent to, or leave this field blank if you do not want the account to receive notifications. If you do provide an email address, notifications of events such as user and IP lockouts, and user expirations will be sent to it when they occur. The email address for this account can be changed at a later time.



Email Address:

Step 4 - Finished

Your organization is created, along with your initial host access rules and your new administrator account. Click Finish. You are returned to the Sign On screen with your new administrator username prefilled. Enter the account password and click Sign On.

On your home page, hints are provided regarding what you should do next, including uploading a logo image for your organization, choosing a color scheme, and adding user accounts.