MOVEit DMZ

Installation Guide

This document was published on Tuesday, September 23, 2014 at 11:32.

Contents

CHAPTER 1

Overview

In This Chapter

The MOVEit DMZ Installation Program

The MOVEit DMZ installation program will install, upgrade, repair or uninstall MOVEit DMZ. Although a single package performs all these operations, not all choices will be available to at all times.

- **Install** - The installation program will automatically attempt to install MOVEit DMZ when it detects that MOVEit DMZ is not present on the system.
- **Upgrade** - The installation program will automatically attempt to upgrade MOVEit DMZ when it detects that an older version of MOVEit DMZ is present on the system. New versions of MOVEit DMZ components and applications will be upgraded and database changes/conversions will automatically be implemented during the upgrade operation.
- **Repair** - This option will only be available if the installation detects that the most recent version of MOVEit DMZ is already present on the system. Various MOVEit DMZ components and applications will be replaced with known, good copies but no database changes/conversions will be performed during the repair operation.
- **Modify** - This option will only be available if the installation detects that the most recent version of MOVEit DMZ is already present on the system. Various MOVEit DMZ components and applications may be added or removed and database changes/conversions may be performed during the modify operation. You should only use this option under the direct supervision of Ipswitch MOVEit support.
- **Uninstall/Remove** - This option will be available if the installation detects that the most recent version of MOVEit DMZ is already present on the system. It is also available from the "Add/Remove Programs" section of the Control Panel.

Before you perform an upgrade or repair option, you should use the included DMZBackup utility or a trusted backup tool to make a good backup of your existing MOVEit DMZ configuration.

The installation program runs the SecAuxNET utility, which is used to prepare a Windows Server platform running the MOVEit DMZ application for deployment on Internet-exposed network segment. SecAuxNET offers the installer/operator several different options to optimize and lock down the server, including :

- Optimize Windows and Internet Explorer
- Disable unneeded services and applications
- Apply recommended NTFS Windows security settings
- Apply recommended NTFS permissions
- Enable FIPS compliance mode
- Rename Administrator account
- Configure IIS
- Configure SMB Signing

System Requirements

This version of MOVEit has the following system requirements:

- **Supported Operating Systems for MOVEit File Transfer (DMZ) and Modules:**
  - Windows Server 2012, Windows Server 2008 R2 (64-bit English)
  - Windows Server 2008 (32-bit and 64-bit English and 32-bit German)
- **Supported Operating Systems for API and Wizard (end user computers):**
  - Windows 8
  - Windows 7 (32-bit and 64-bit English)
  - Windows Vista (32-bit and 64-bit English)
  - Windows Server 2012, Windows Server 2008R2
  - Windows Server 2008 (32-bit and 64-bit English)
  - Java version: RHEL 5.6 and 6.1, Ubuntu 11.0.4, MacOS 10.7 and 10.8
- **Supported Virtualization Environments:** Support for virtual servers running on:
  - VMware ESX (32-bit and 64-bit guest servers)
  - Microsoft Hyper-V (32-bit and 64-bit guest servers)
- **Supported Browsers (end user computers):**
  - Internet Explorer 9 and 10 (Windows only)
  - Mozilla Firefox (Windows, Mac and RedHat Linux)
  - Chrome (Windows only)
  - Safari (Mac only)

- **Support for Ad Hoc Transfer module Outlook plug-in (end user computers)**
  - Outlook: Outlook 2013 (English, German, French and Spanish), Outlook 2010 (32-bit and 64-bit English, German, French and Spanish) and Outlook 2007 (32-bit English, German, French and Spanish)
  - Mail or Exchange Server: Outlook plug-in is compatible with a variety of mail servers, such as Exchange Server 2013, Exchange Server 2010 (32-bit and 64-bit English and German), Exchange Server 2007 (32-bit English and German) or Ipswitch IMail 11 (using SMTP). When Outlook & Exchange used together, Cached Exchange Mode will be supported but is not required
  - Operating System: Microsoft Windows 8, Windows 7 (32-bit and 64-bit English and German) and Windows Vista (32-bit English, German, French and Spanish)
- **Microsoft Runtime Environment and Libraries:**
  - Microsoft ASP.NET (via IIS) and .NET 3.0 for MOVEit File Transfer (DMZ)
  - Sun Java J2SE 6.0 and 7.0 for MOVEit Wizard for Java
- **Supported Database:**
  - MySQL 5.5
  - Microsoft SQL Server 2012; Microsoft SQL Server 2008 R2; Microsoft SQL Server 2008; Microsoft SQL Server 2005; Enterprise/Standard Editions
- **Hardware:** 2GB RAM, 40GB HD; Dual-core or faster processor. Production systems will benefit from additional resources, including faster, additional and multicore processors (single or dual quad-core processors are common), more RAM (4GB is common), hard drive capacity and speed (1TB SAS is common) and SSL accelerator hardware

Install Notes

- If you will use the MySQL database, any local non-MOVEit MySQL versions should be removed prior to installing MOVEit DMZ on the server. A "clean" server is recommended for installations. The MOVEit DMZ installation program will install the MySQL database.
- The MOVEit DMZ installation can activate "Roles and Features" for many of the prerequisites needed.
- The installation program will create exceptions in the Windows Firewall to permit connections to MOVEit DMZ FTP and SSH.
- Finally, in order to support installation on Domain Controllers, a network service called "File and Printer Sharing" must be installed on the system.

If any of these requirements have not yet been met, MOVEit DMZ will recommend (to the best of its ability) the installation/registration of these various components before allowing you to proceed with the installation.

Upgrade Notes

- If you are using a license file in your current installation, you will need to provide an 8.0-compatible license file during the upgrade process. If you are not sure whether you are using a license file, please refer to this ***knowledge base article*** (***http://ipswitchft.force.com/kb/articles/FAQ/How-do-I-locate-my-current-MOVEit-DMZ-license-file-or-serial-number***).
- Upgrades generally require you to upgrade the underlying database. This can be time consuming if you have a large "log" table or if the drive is heavily fragmented. It's suggested that you defragment on a regular basis for performance and prior to an upgrade could be beneficial.
- Currently signed-on accounts may need to sign-on again after an upgrade as their sessions may need to be rebuilt. MOVEit Central will automatically do this.
- The upgrade routine does not prompt you to run SecAux (secuirty wizard) after the upgrade. Since this version of MOVEit DMZ has new hardening options in SecAux (see the Configure IIS and Configure SMB Signing sections), you may want to run it manually after the upgrade process. You can usually find SecAux here: C:\Program Files (x86)\MOVEit\SecAuxNET.exe
- For Microsoft SQL Server databases, entering the 'sa' password should no longer be required during the upgrade. Instead, the upgrade process will use the normal database user account. As long as this user has db_owner permissions to the appropriate database (it will if the user was originally created by the MOVEit DMZ installer), this change in behavior should not disrupt the upgrade process.

CHAPTER 2

Install

This installation program will install MOVEit DMZ and its services on a computer running the ***required Windows server software*** (***http://www.ipswitchft.com/products/moveit/systemrequirements.aspx***).

In This Chapter

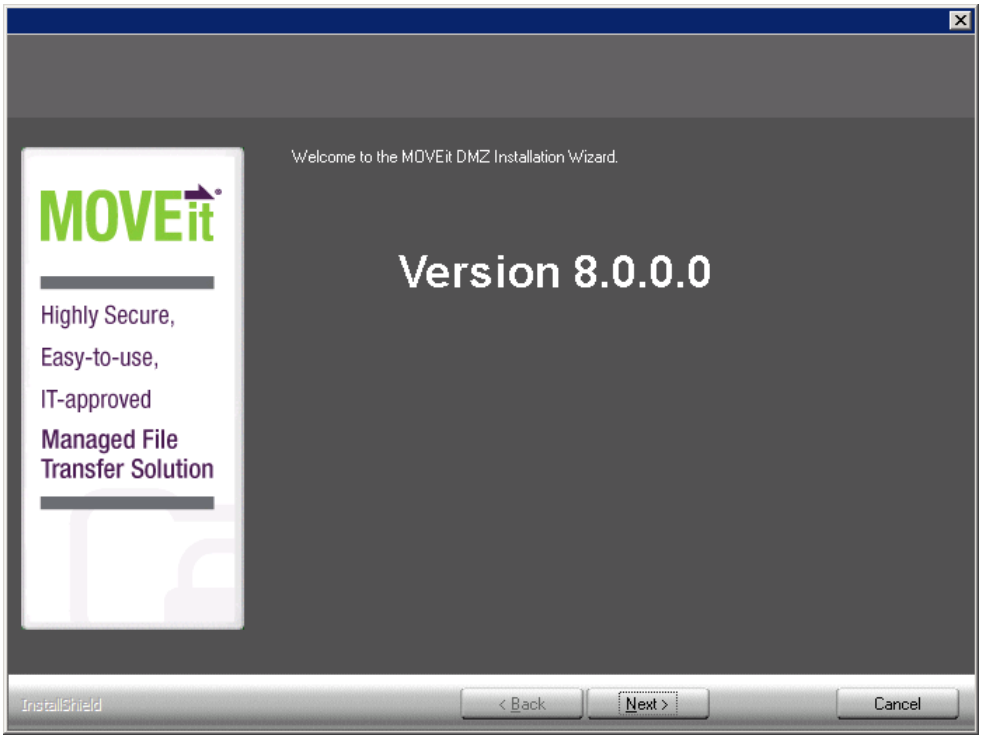
Install - Welcome Dialog

This installation program will install MOVEit DMZ and its services on a computer running the ***required Windows server software*** (***http://www.ipswitchft.com/products/moveit/systemrequirements.aspx***).

. Some of the services which this program installs 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. To use an existing Microsoft SQL Server database instead, select Custom Setup during installation.

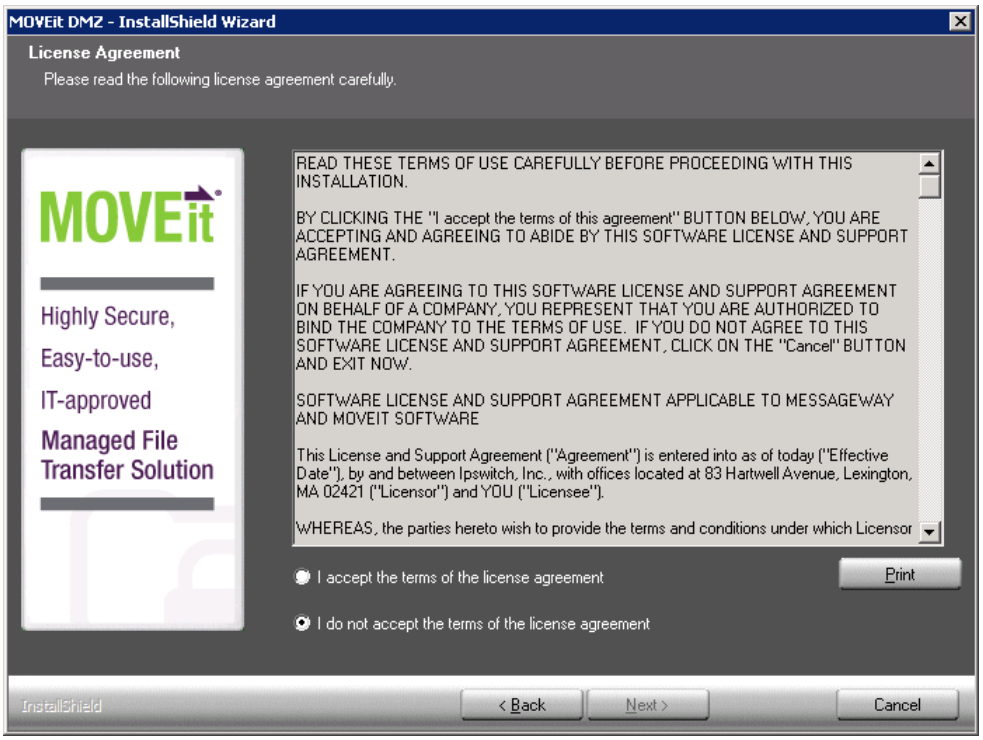
A single copy of the installation can be used to install a fresh copy of MOVEit DMZ or upgrade an existing copy of MOVEit DMZ from a previous version.



Initial Welcome screen for MOVEit DMZ Install, click **Next** to continue or **Cancel** to quit.

Install - License Agreement Dialog

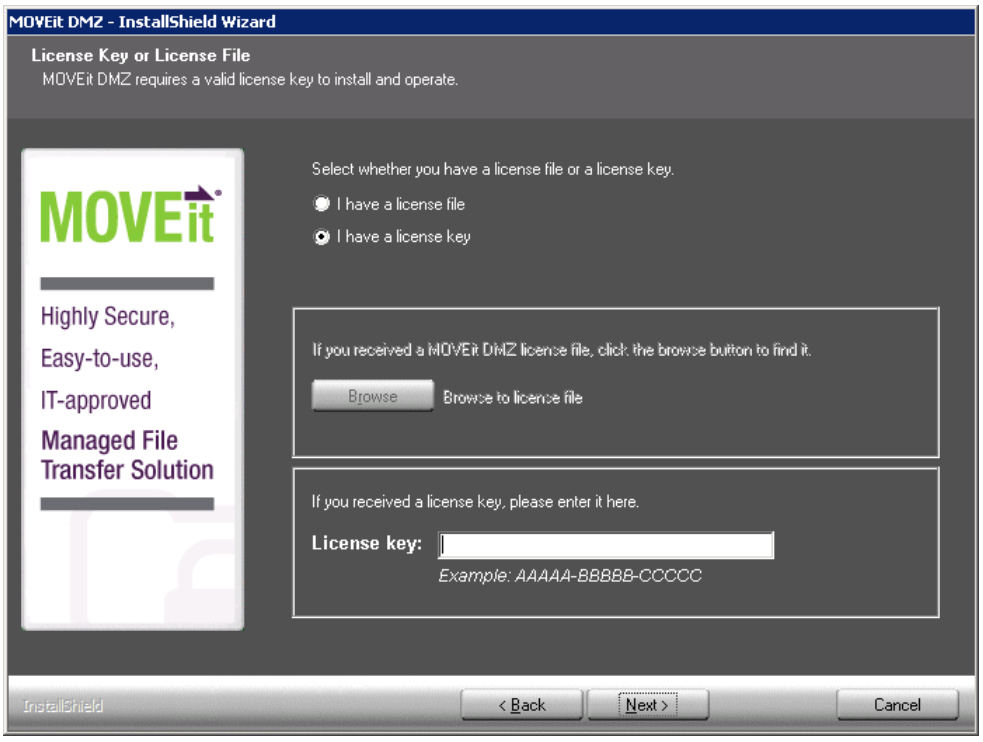
The MOVEit DMZ License Agreement, please read carefully.



Choose "I Accept the Terms of License Agreement" to proceed.

Install - License Key or File Dialog

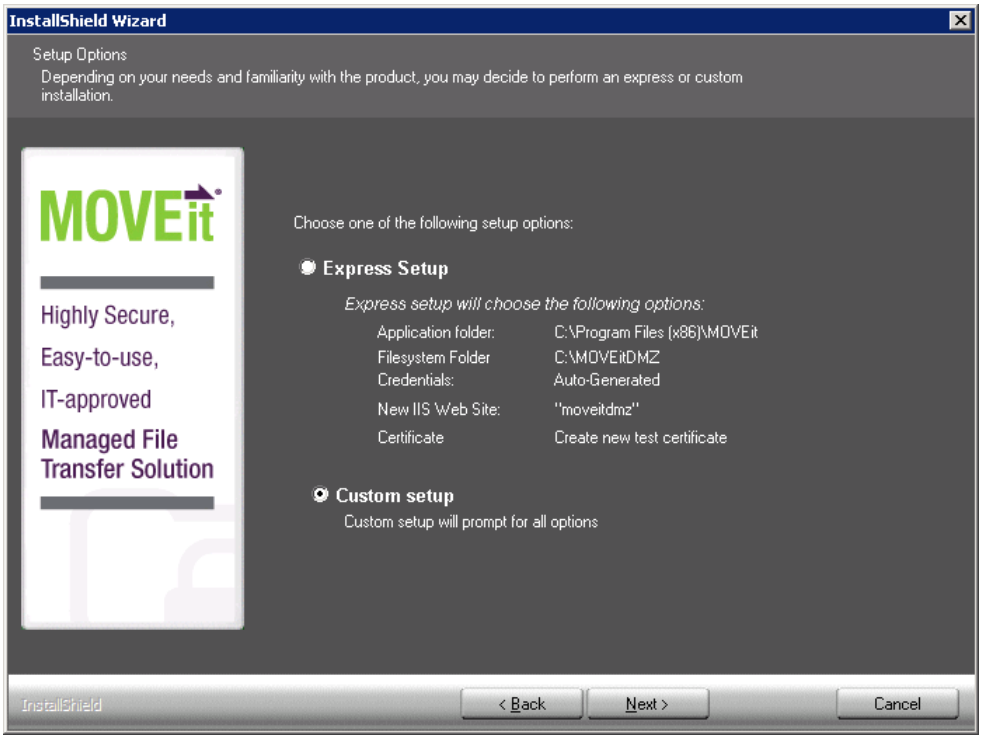
MOVEit DMZ requires a valid license key or file to install and operate.



- Select file or key option:
  - I have a license file - Use this option if you have downloaded a MOVEit license file and want to use this to activate your software.
  - I have a license key - Use this option if you have a MOVEit license key. (This is a 16-digit alphanumeric code.)
- Browse to license file - If you selected "I have a license file," click the Browse button to find and select the file.
- License key - Enter your 16-digit alphanumeric code to activate your MOVEit license.

Install - Setup Options Dialog

You can choose to use Express Setup or the Custom Setup options. This choice will determine which installation screens will be presented to you.

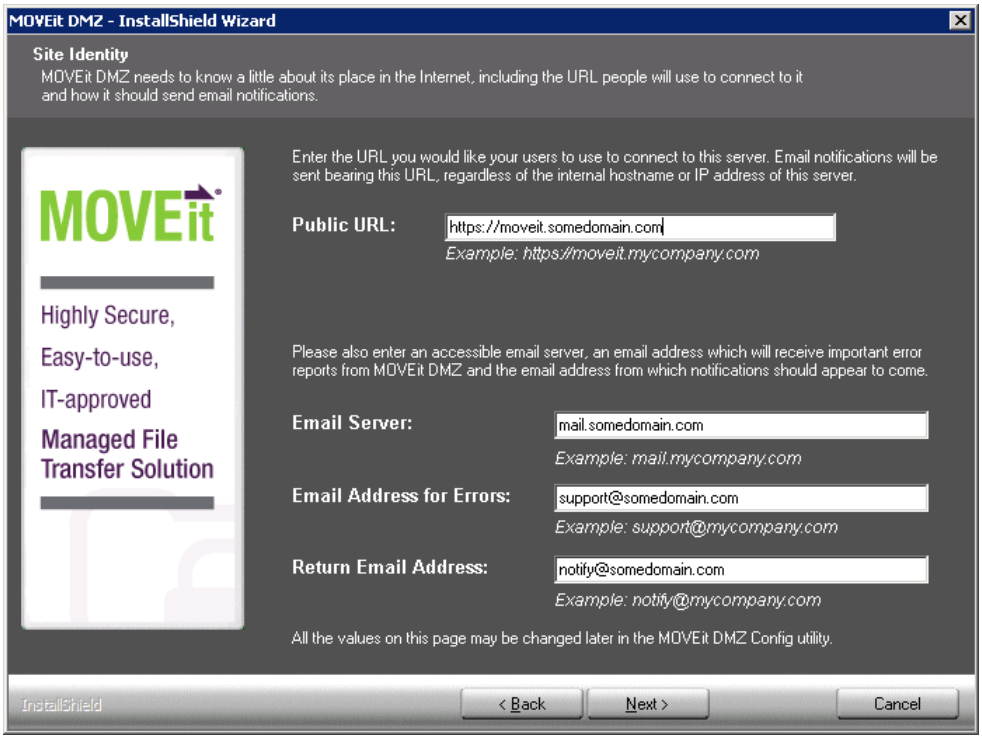


Setup Options

- **Express Setup** - Pick this option if you are setting up an evaluation server or looking to install MOVEit DMZ in a timely fashion. The express options will make the following choices for you:
  - Application Folder: C:\Program Files\MOVEit
  - Filesystem Folder: E:\MOVEitDMZ (*largest local drive*)
  - Credentials: Use Suggested (*automatically generated*)
  - New IIS Web Site: MOVEitDMZ
  - SecAux Security Hardening: Not Run
  - Certificate: Create New Test Certificate
- **Custom Setup** - Pick this option and the setup will prompt for all options. If you want to use an existing Microsoft SQL Server database, instead of MySQL, you must select this option. For more information on the database settings, see the "Custom Setup " topics.

Install - Site Identity Dialog

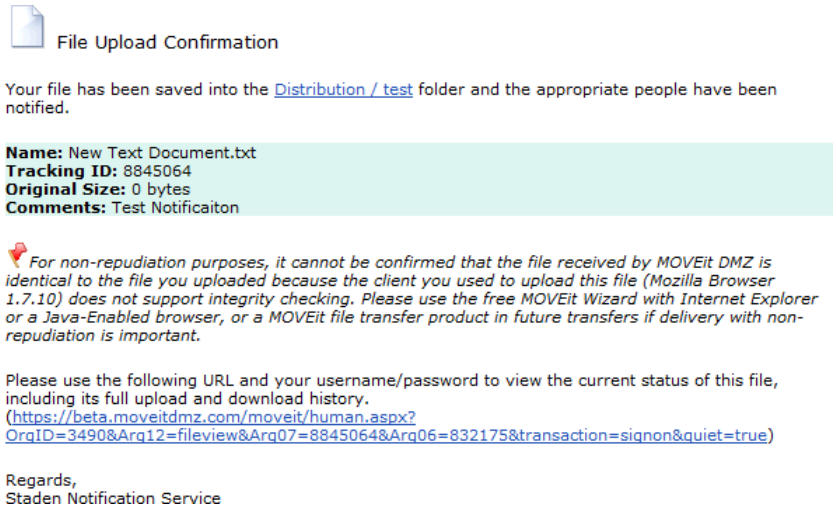
MOVEit DMZ needs to know a little about its place in the Internet, including the URL people will use to connect to it and how it should send email notifications.



Site Identity Options

- **Public URL**
  - The URL you would like users to use to connect to this server. Email notifications will be sent bearing this URL, regardless of the internal hostname or IP address of this server. IP addresses and hostnames are valid, but should only be used for testing and evaluation purposes.
  - An example of an install into a regular folder would be: **https://moveit.somedomain.com.**

- An example of an install into a virtual folder would be: **https://www.somedomain.com/moveit**.
- A new file notification will use the base URL (beta.moveitdmz.com) as shown in the example below.



File Upload Confirmation

Your file has been saved into the Distribution / test folder and the appropriate people have been notified.

Name: New Text Document.txt
Tracking ID: 8845064
Original Size: 0 bytes
Comments: Test Notificaiton

For non-repudiation purposes, it cannot be confirmed that the file received by MOVEit DMZ is identical to the file you uploaded because the client you used to upload this file (Mozilla Browser 1.7.10) does not support integrity checking. Please use the free MOVEit Wizard with Internet Explorer or a Java-Enabled browser, or a MOVEit file transfer product in future transfers if delivery with non-repudiation is important.

Please use the following URL and your username/password to view the current status of this file, including its full upload and download history.
(https://beta.moveitdmz.com/moveit/human.aspx?OrgID=3490&Arg12=fileview&Arg07=8845064&Arg06=832175&transaction=signon&quiet=true)

Regards,
Staden Notification Service

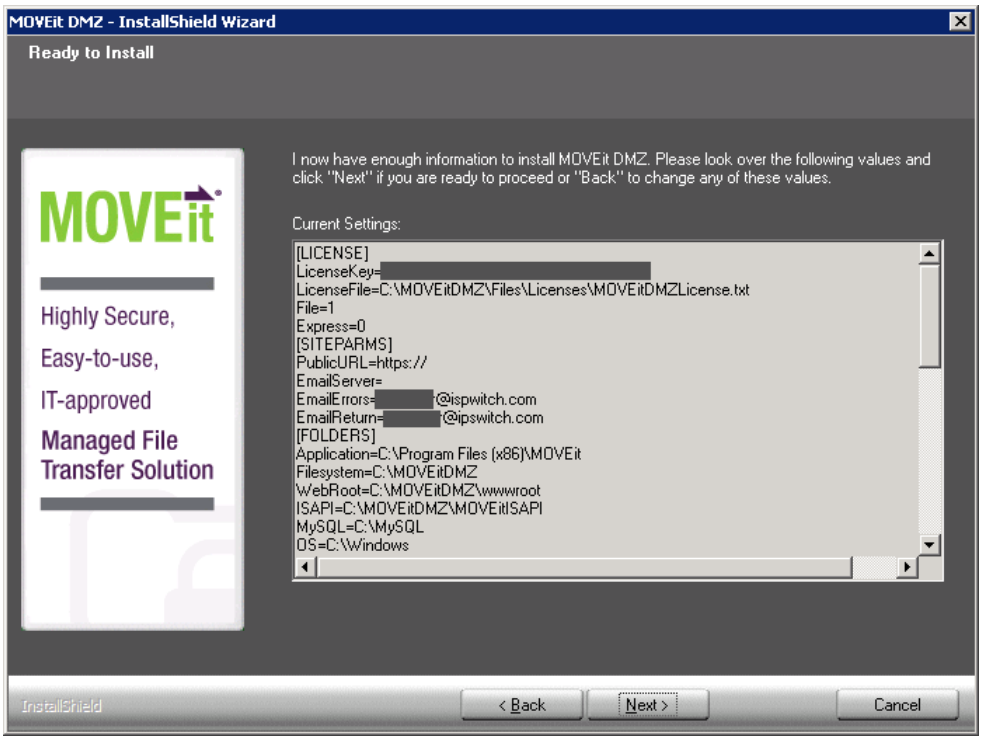
- **Email Server**
  - The email server that MOVEit DMZ will use to relay email. An IP address is a valid entry.
  - For example, **mail.somedomain.com**
- **Email Address for Errors**
  - Occasionally MOVEit DMZ will send errors and other administrative notices using this address. It's highly recommended 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 may be changed later in the MOVEit DMZ Config Utility.

If you are doing a custom install, you will see the dialogs described in the Custom Setup section, starting with the ***Database Type.*** (on page 20)

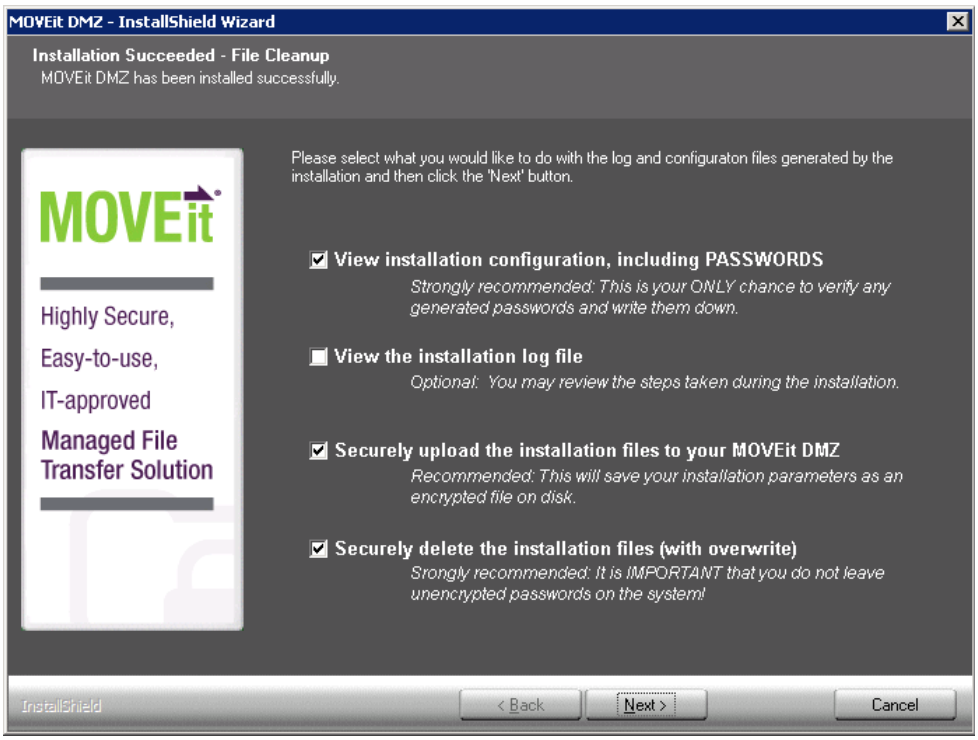
Install - Ready to Install Dialog

MOVEit DMZ is ready to install with the options you have selected.



Install - Installation Complete Dialog

MOVEit DMZ has been installed successfully.



Successful Install Options

- **View Installation configuration, including Passwords**

  This will display 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.

- **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**

  This will save your installation parameters as an encrypted file on disk. Only SysAdmins will be able to view these files.

- **Securely delete the installation files (with overwrite)**

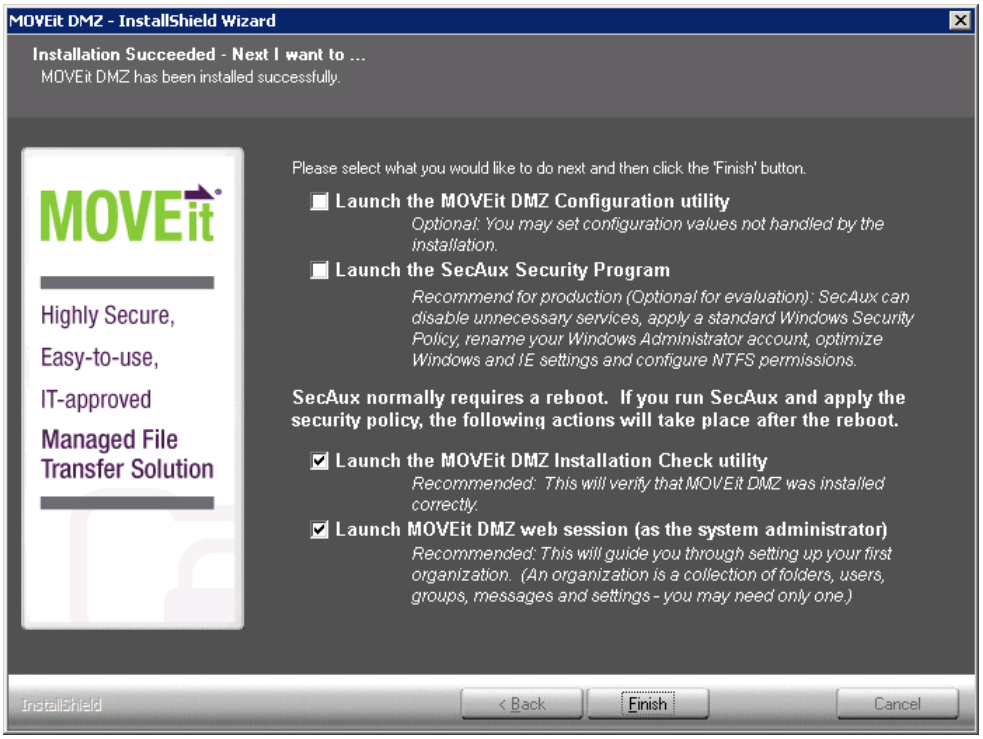
  This will securely delete all configuration files that were generated during the install. This step is highly recommended as to not leave unencrypted passwords on the DMZ server.

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

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

Install - Installation Finished Dialog

MOVEit DMZ has been installed successfully.



Finished Installation Options

- **Launch the MOVEit DMZ Configuration Utility**

  This will launch the utility that allows you to make changes to your MOVEit DMZ system. You may set configuration values not handled by the installation.

- **Launch SecAux Security Program**

  This will launch the security program to further harden your operating system. SecAux can disable unnecessary services, apply a Windows Security Policy, rename your Windows Administrator account, optimize Windows and IE settings and configure NTFS permissions. Running the SecAux program is highly recommended on production servers that will be made available on the internet.

- **Launch the MOVEit DMZ Installation Check Utility**

  This will launch 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 will be displayed after the current one is closed.

When you have closed any open program/utility, the setup program will prompt you to delete the installation configuration and log files. Doing this provides an extra measure of security.

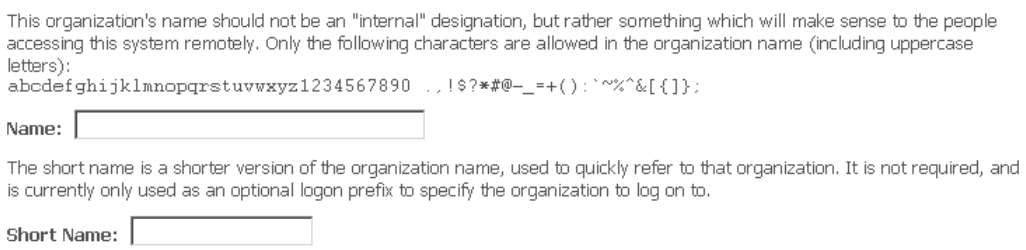
Install - Creating an Organization

After signing in to the MOVEit DMZ server for the first time, your first task will be to create an Organization which will contain your users, groups, folders, and files. As such, you will be taken to the Add a New Organization wizard once you have signed on to the system.

Step 1 - Name, Passphrase, and Technical Contact

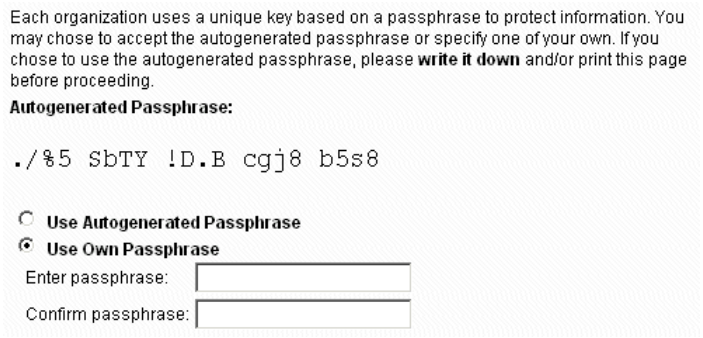
The first step in the Add a New Organization wizard allows you to select a name for your organization, a passphrase which will be used to generate encryption keys, and the technical contact information which will be presented to users in notifications and on the Tech Support page.

- **Name** - The name your organization will be displayed with. This should generally be 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 may be changed after the organization has been created.

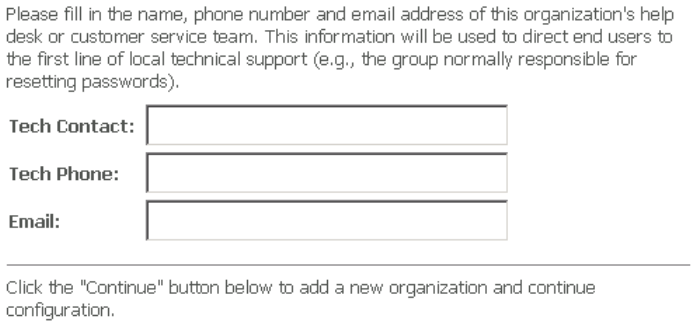


- **Passphrase** - The passphrase is used to generate the encryption keys that will protect the files that are uploaded to your organization. It should be a relatively long sequence of characters, as random as possible, and must contain at least one letter and one number. An automatically-generated 16-character passphrase is provided by MOVEit DMZ, and it is recommended that you use this passphrase, as 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.

  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.



- **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 may be changed after the organization has been created.



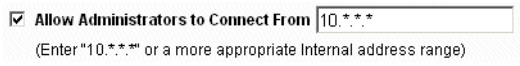
To stress the importance of writing down and/or printing your organization passphrase and safely storing it, you are required to check the checkbox at the bottom of the page, indicating that you have done so, whether you have used the suggested passphrase, or you have chosen to enter a custom passphrase. You will not be allowed to continue until you have made this indication.

Step 2 - Host Access Rules

The next step in the Add a New Organization wizard allows you to set some initial host access rules for your new organization. These rules define which hosts and IP addresses your users and your administrators may log on to the system from. More rules can be added at a later time.

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

- **Allow Administrators to Connect From** - This mask will define which hosts your administrator users may initially log on to MOVEit DMZ from. Most organizations will want to restrict their administrators to only connect from their internal network, so the default mask here is "10.*.*.*".

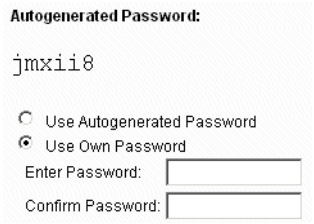


Step 3 - Add an Administrator

This step allows you to create your first administrator account in your new organization. Enter a username for the new account, select the automatically-generated password, or enter a password of your own, and enter an email address (or leave the email address field blank) to create the account. The username can not be changed once 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** - You can either choose to 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.



- **Email Address** - Enter the email address that 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 may be changed at a later time.

Step 4 - Finished

Your organization should now be created, along with your initial host access rules and your new administrator account. To continue setting up your new organization, click the Finish button to log out. You will be returned to the Sign On screen with your new administrator username prefilled. Enter the account password and click the Sign On button, and you will be signed on to your new organization. Hints will be provided on your home page informing you what you should do next. Tasks you will need to carry out at this point include uploading a logo image for your organization, choosing a color scheme, and adding user accounts.

CHAPTER 3

Install - Custom Setup

If you chose the Custom Setup option, the setup program lets you enter the settings for the following:

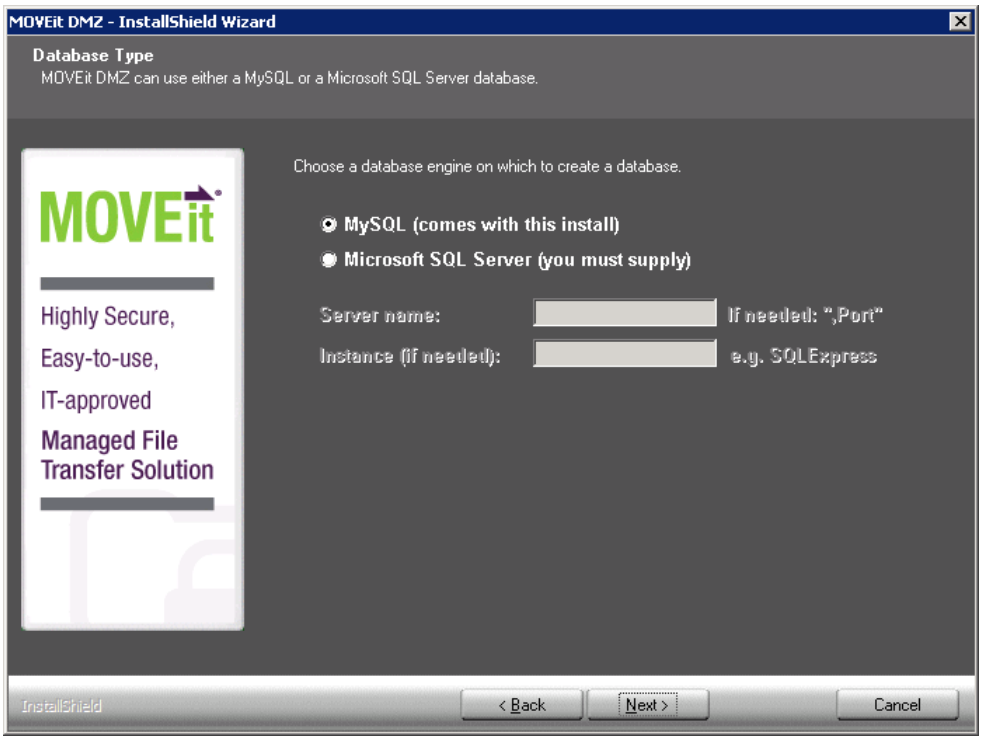
- Database Type, Name (MySQL or Microsoft SQL Server)
- Folders for the MOVEit application, filesystem and database
- Credentials for the MOVEit SysAdmin, Windows Services User, and database
- Web Site settings for MicroSoft IIS
- Certificate for SSL server

If you chose the Express install option, the setup program uses default values for these settings.

In This Chapter

Install - Custom Setup - Database Type

Choose the database engine that MOVEit DMZ should use.



- **MySQL**: a small-footprint database engine that MOVEit DMZ will install and administer.
- **Microsoft SQL Server**: a widely-used database engine. You must supply a pre-installed instance of SQL Server if you choose this option.

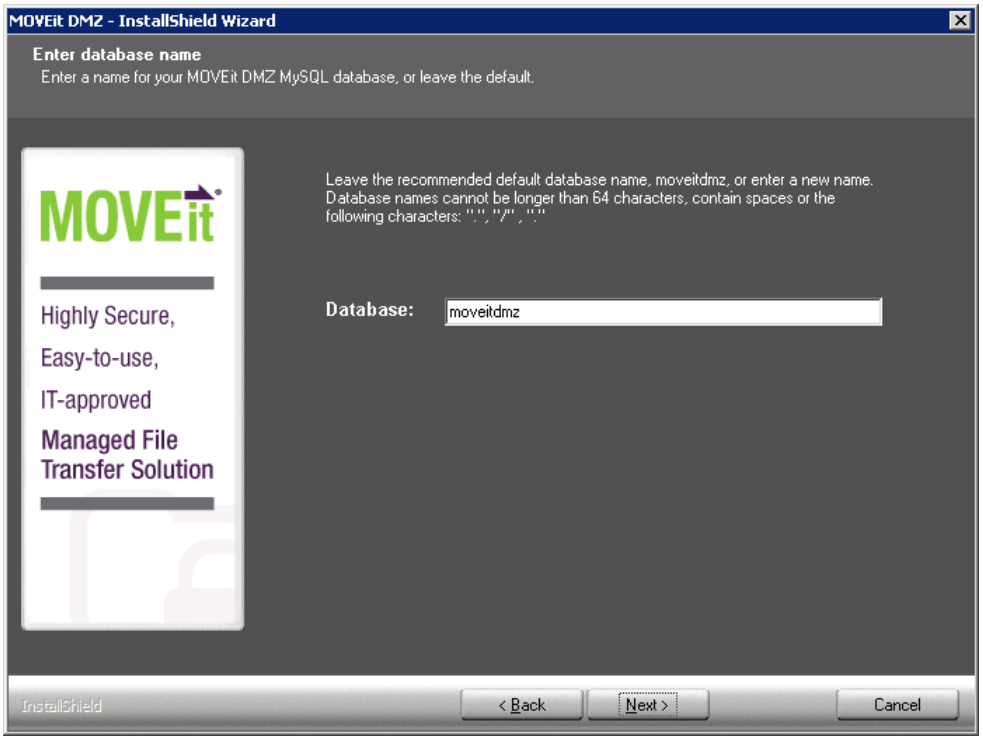
If you select Microsoft SQL Server, you must provide these pieces of information:

- The hostname or IP address of the server. If the server is listening on a non-standard port, add a comma followed by the port number after the hostname.
- The "instance name". If the MOVEit DMZ database is the default instance, this is typically blank. In a shared environment, this is the name that identifies the MOVEit DMZ database on the SQL Server, for example: **HOST1\midmzdb**

Depending on the database type selected, you will see one of the following screens:

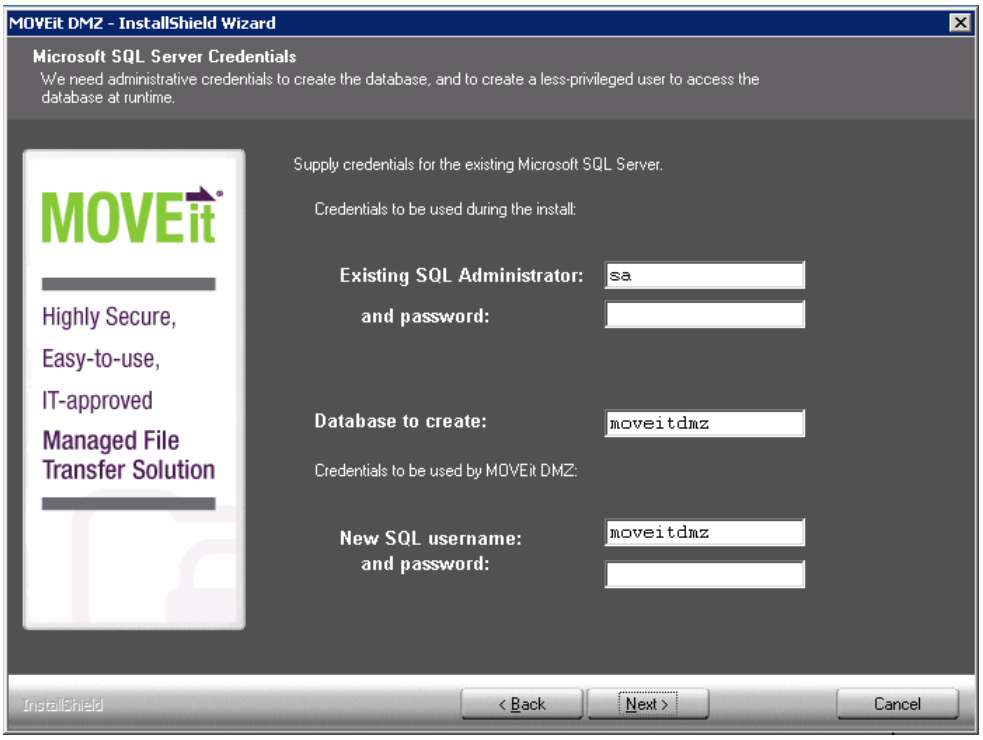
Install - Custom Setup - MySQL Database Name

Choose the database name that MOVEit DMZ should use. For most installations, you should use the default database name: 'moveitdmz' Database names cannot be longer than 64 characters, contain spaces or the following characters: "." "," "/"



Install - Custom Setup - MS SQL Server Credentials

Provide credentials to be used to access the existing instance of Microsoft SQL Server.

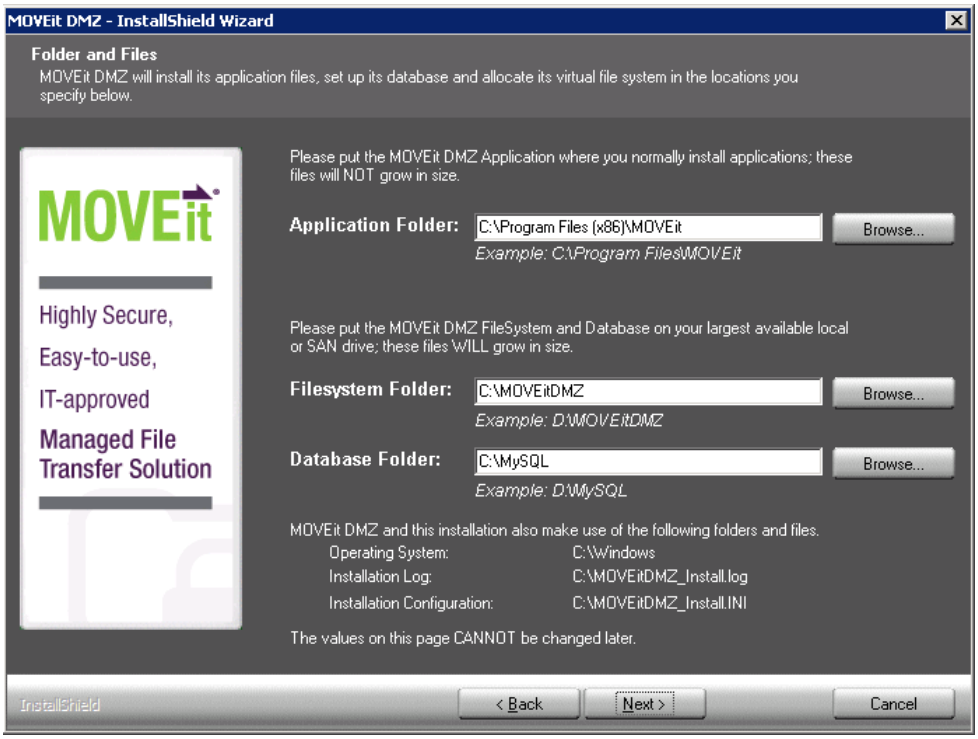


SQL Server Credentials

- **Credentials to be used during the install** - Specify an existing SQL Server username and password.
- **Database to create** - In most cases you should simply accept the suggested default.
- **Credentials to be used by MOVEit DMZ** - Specify a SQL Server username and password to be created by the install program.

Install - Custom Setup - Folders Dialog

MOVEit DMZ will install its application files, set up its database and allocate its virtual file system in the locations you specify below.



Folder and File Options

- **Application Folder**

  The folder where MOVEit DMZ executables and supporting .dll's are stored. These files rarely grow in size therefore this folder requires a small amount of space.

- **FileSystem Folder**

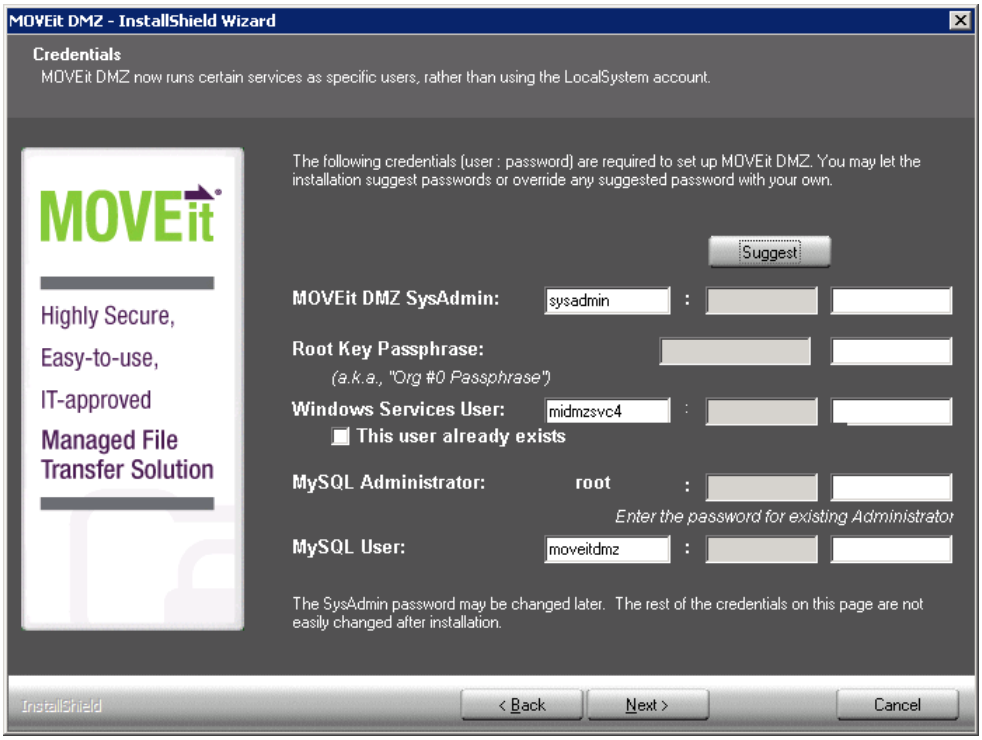
  The folder where MOVEit DMZ stores the encrypted files, logs, logos, schemes and utilities. This folder WILL grow in size so be sure to select the largest drive as it is difficult to change directories.

- **Database Folder**

  The folder where the MySQL database files will be installed. MySQL stores the configuration and logs for MOVEit DMZ. This destination will grow, so be sure to select the largest drive as it is difficult to change directories.

Install - Custom Setup - Credentials Dialog

MOVEit DMZ Default Credentials. Please make sure to write down this information. Ipswitch recommends making each password as strong as possible. The SysAdmin password may be changed later; however, all other credentials are not easily changed after installation.



Credentials Description

- **MOVEit DMZ SysAdmin**
  - This is the initial user account created on your MOVEit DMZ system.
  - Caution: The next two settings are the System Administrator (SysAdmin) username and password. This account will have complete access to the MOVEit DMZ system and will be used to initially configure MOVEit DMZ. Once you have created a new organization and an administrator account in that organization, the SysAdmin account should be used only if required. However, this account has no access to files. Please keep this username and password in a safe place.
  - Password Requirement: SysAdmin password must be at least 8 characters long. SysAdmin password must have numbers, upper and lower case letters.
- **Root Key Passphrase**
  - Used to generate the encryption key for the default System Org (Org #0)
  - Password Requirement: Root key must be at least 12 characters long. Root key must have numbers, upper and lower case letters

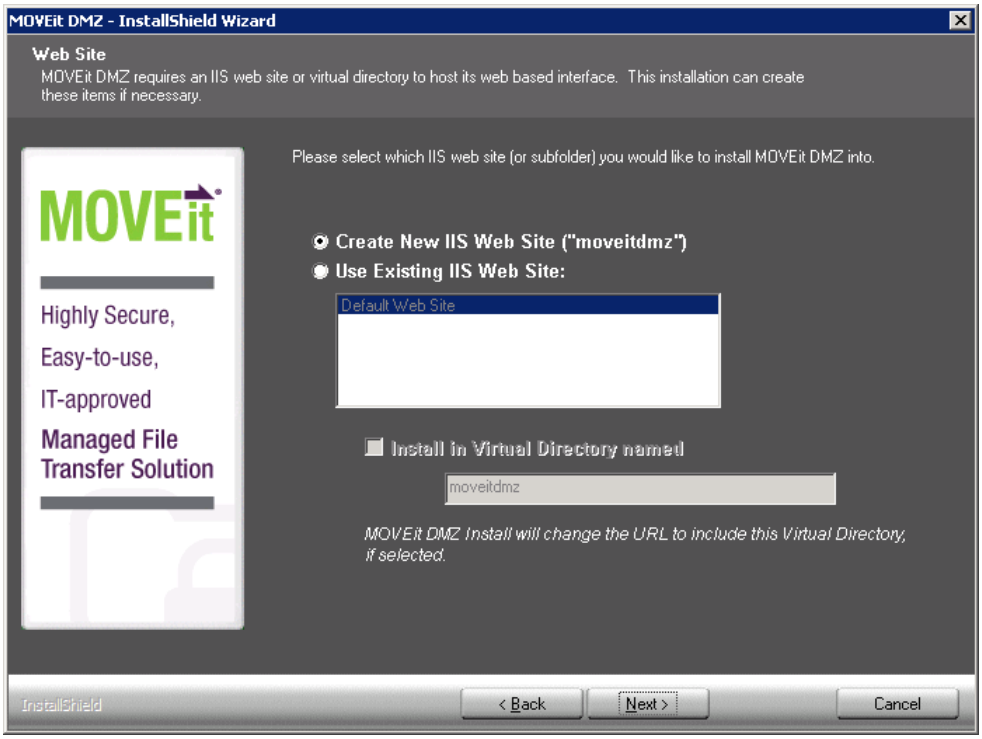
- **Windows Services User**
  - This is the Windows account that the DMZ services will run under.
  - **This user already exists** - Check this box to use an existing Windows account with the name specified for Windows Services User.
  - Password Requirement: Windows Services password requirements are determined by the Windows security policy.
- **MySQL Administrator**
  - The master account for accessing the MySQL server.
  - Password Requirement: MySQL Administrator password must be at least 8 characters long. MySQL Administrator password must have numbers, upper and lower case letters.
- **MySQL User**
  - This is the MySQL username that MOVEit uses to log on to MySQL to access the database.
  - Password Requirement: MySQL User password must be at least 8 characters long. MySQL User password must have numbers, upper and lower case letters.

Suggest Button Description

The suggest button will suggest passwords that fit the complexity requirements. Any suggested password may be overwritten with by typing in a password in the adjoining box.

Install - Custom Setup - Web Site Dialog

MOVEit DMZ requires an IIS web site or virtual directory to host its web based interface. This installation will create these items if necessary.



Web Site Options

- Create New IIS Web Site ("moveitdmz")

  This will create a new web site in IIS called moveitdmz. This is the recommended option for MOVEit DMZ installations.

- Use Existing IIS Web site

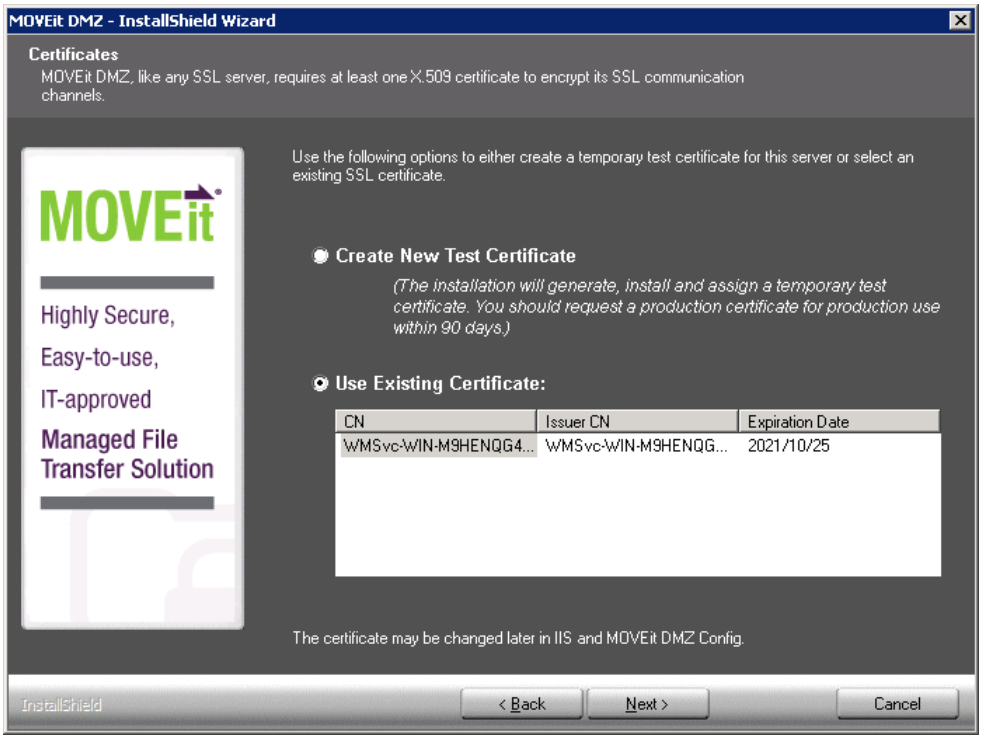
  This will use an existing web site to install/upgrade MOVEit DMZ. Please be sure to select the appropriate site name.

- Install in Virtual Directory named

  This will install MOVEit DMZ into a virtual directory and also set the Base URL to the appropriate virtual directory. The existing site option needs to be selected before you can proceed with this option.

Install - Custom Setup - Certificate Dialog

MOVEit DMZ, like any SSL server, requires at least one X.509 server certificate to encrypt its SSL communication channels.



- **Create New Test Certificate**

  This will install a test certificate and should only be used for evaluation and testing purposes. The certificate will expire after 90 days.

- **Use Existing Certificate**

  This will use an existing certificate from the Microsoft Local Machine certificate store.

* The selected certificate will be automatically installed and configured in IIS (for the MOVEit DMZ web site) and DMZ Config (for the MOVEit DMZ FTP Server).

* The certificate(s) may be changed anytime in IIS and the DMZ Config.

When you click Next, the installer displays the ***Ready to Install dialog*** (on page 12).

CHAPTER 4

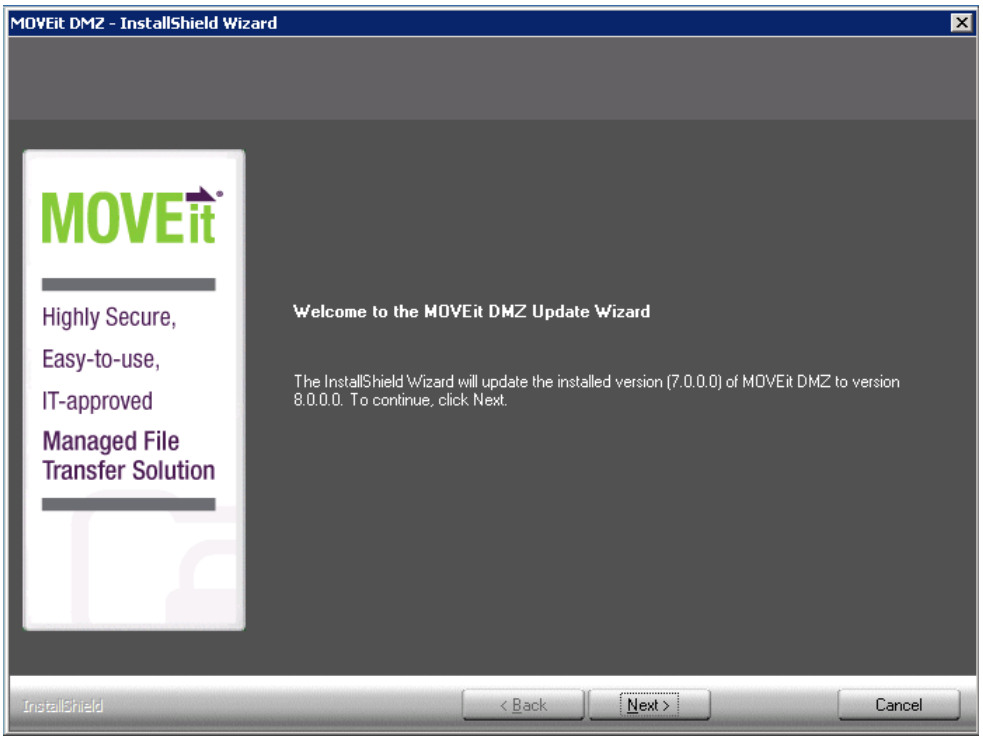
Upgrade

When upgrading the MOVEit DMZ software to a newer version, you will see some or all of these dialogs.

In This Chapter

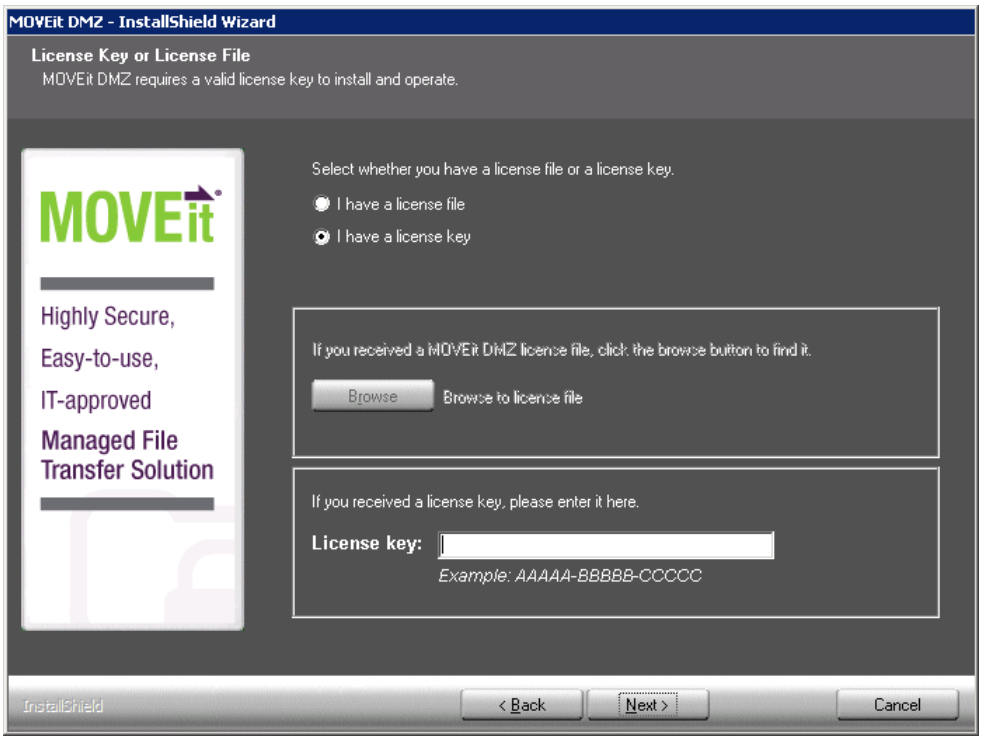
Upgrade - Welcome

The Upgrade Welcome screen starts the upgrade sequence.

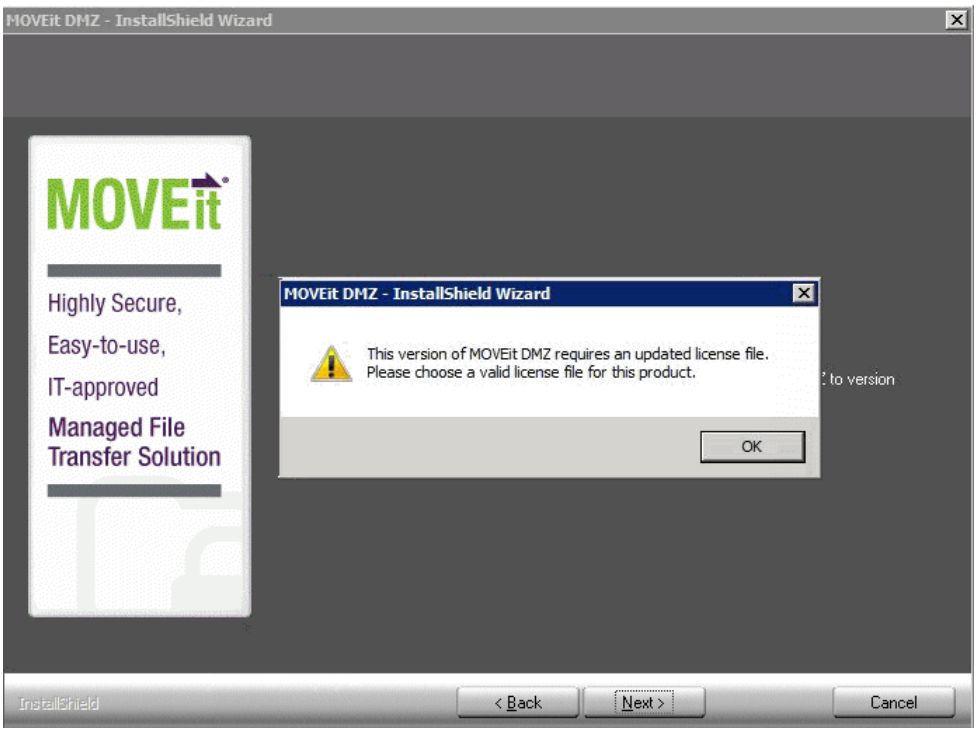


Upgrade - License File Dialog

MOVEit DMZ displays the License Key or License File dialog.



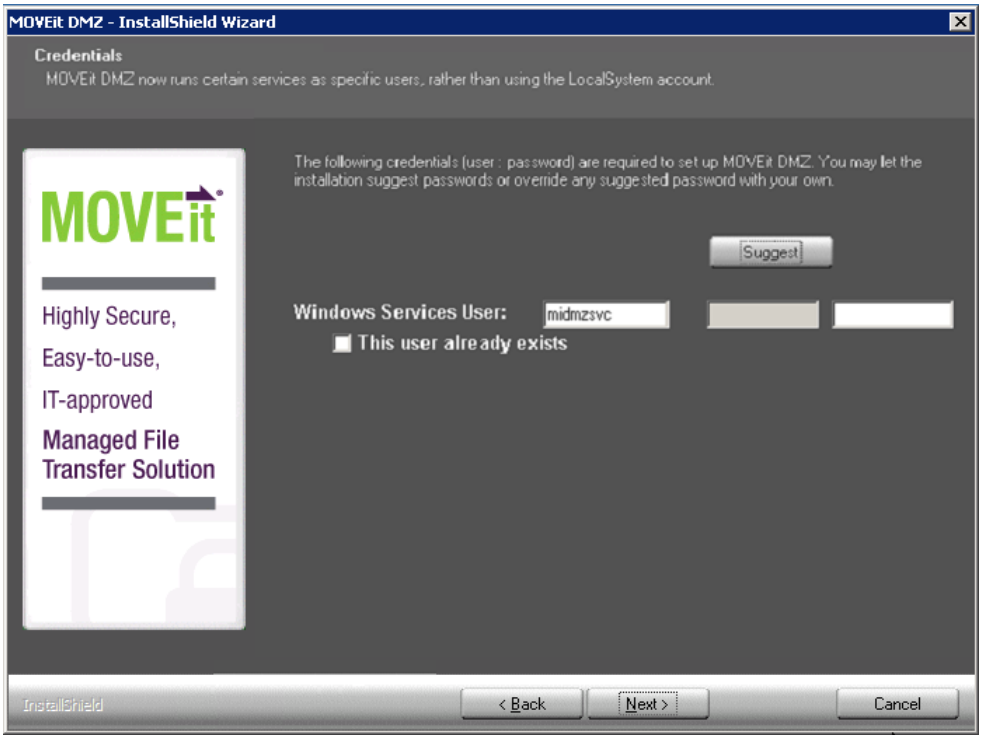
If you are using a license file (rather than a license key), to upgrade, you must obtain a new license file. A license file from a pre-v.8.0 version will not work due to changes made to support new licensing options. If your license file does not meet this requirement, you will see the following message:



To get a new license file, please follow the steps documented in the Upgrade section of the ***MOVEit Release Notes*** (***http://docs.ipswitch.com/Moveit/DMZ8.0/ReleaseNotes/MOVEit%20Release%20Notes.pdf***), (also available on the MOVEit Support site).

Upgrade - Windows Services User Dialog

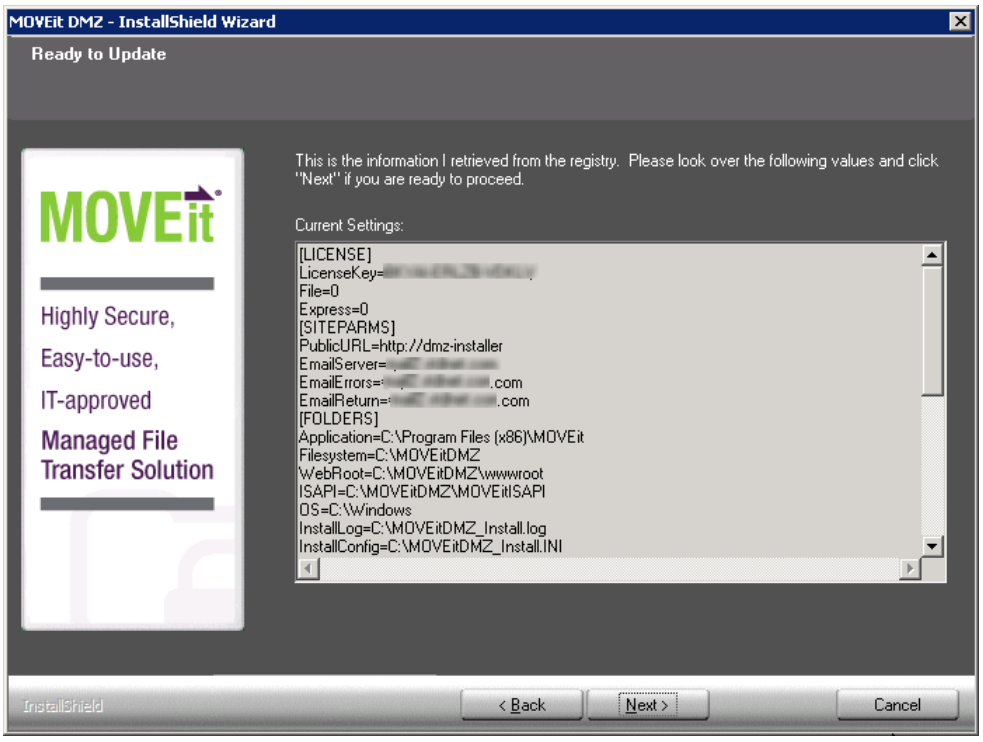
Displays the Windows Services User Dialog. Please make sure to write down this information. Ipswitch recommends making each password as strong as possible. Credentials are not easily changed after installation.



- **Windows Services User**: This is the Windows account that the DMZ services will run under.
- **This user already exists**: Check this box to use an existing Windows account with the name specified for Windows Services User.
- **Password Requirement**: Windows Services password requirements are determined by the Windows security policy.

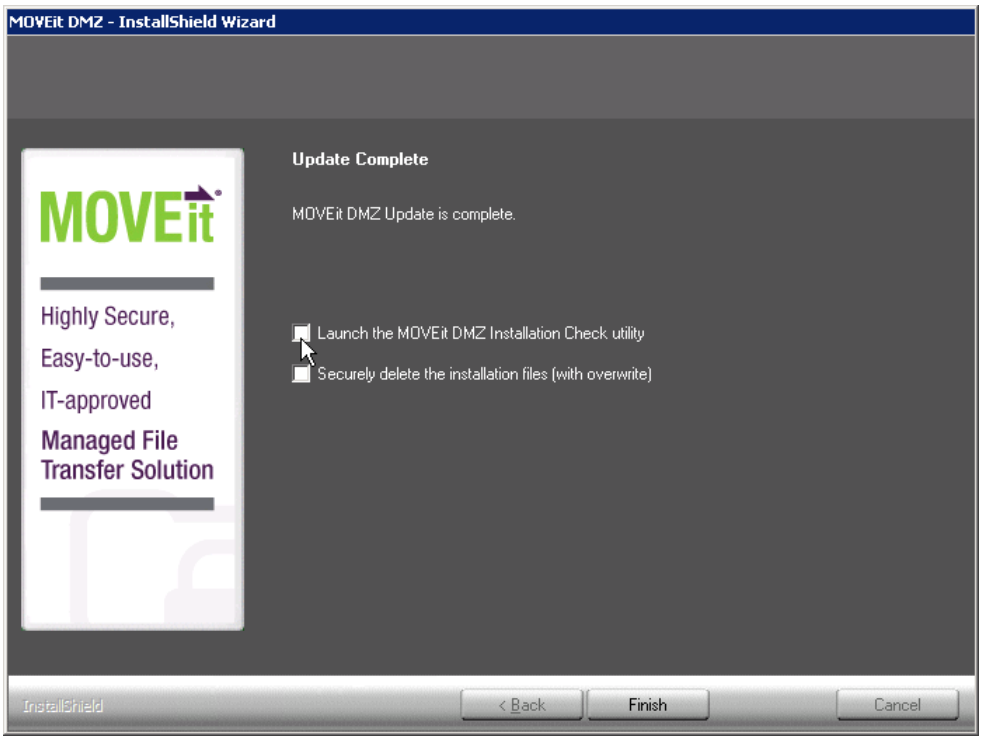
Upgrade - Ready to Upgrade Dialog

Displays current MOVEit DMZ Settings. Review the information and click Next to continue.



Upgrade - Complete Dialog

Displays post-install options. Click "Finish" to finalize the upgrade.



- **Launch the MOVEit DMZ Installation Check Utility**

  This option will run the MOVEit DMZ checker to verify settings.

- **Securely delete the installation files (with overwrite)**

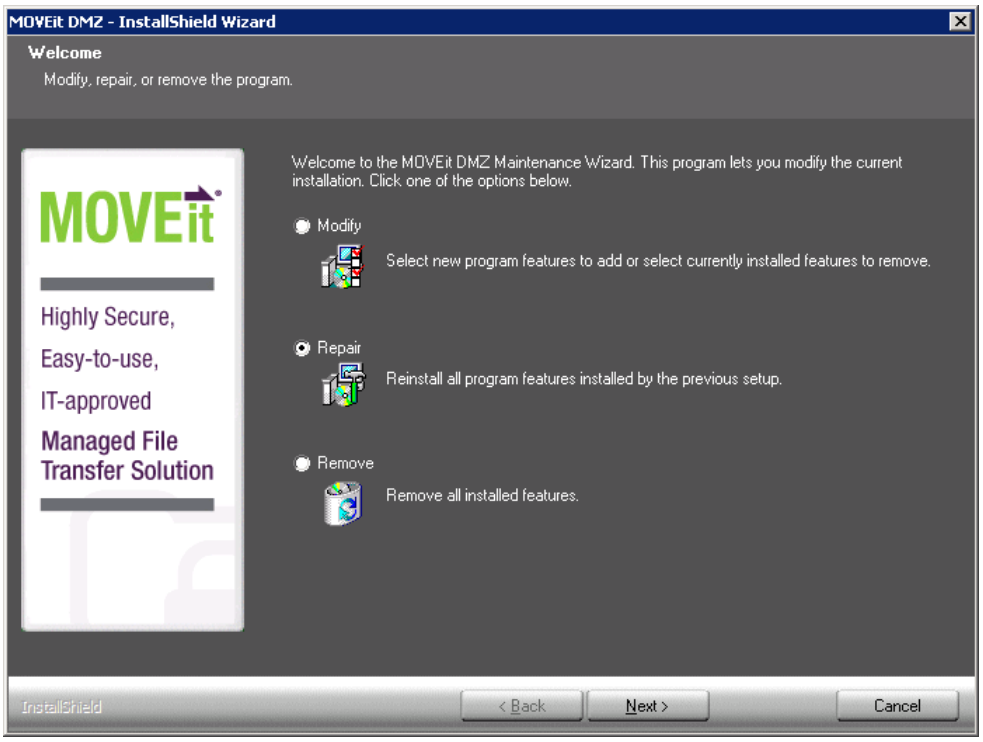
  This will securely delete the install files that contain configuration settings and passwords.

CHAPTER 5

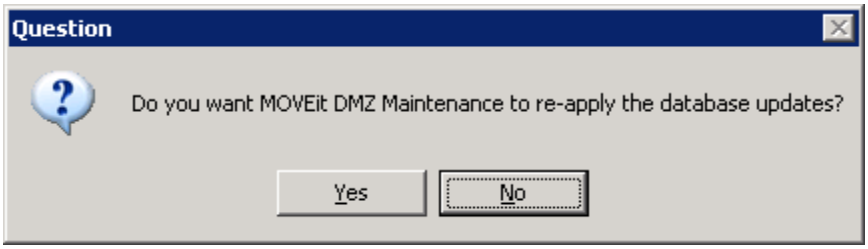
Repair - Repair Dialog

This option will re-install all components that were originally installed with the identical version.

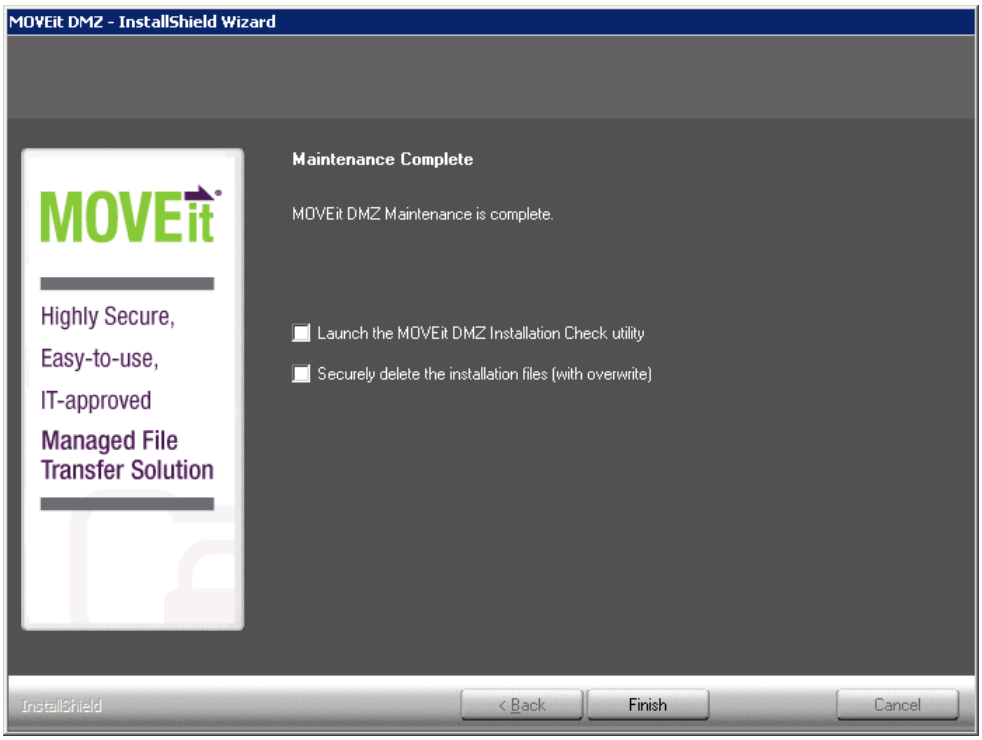
Note: When you run an upgrade/repair for MOVEit DMZ, the DMZ-wwwroot web.config is overwritten, removing any custom setting, for example SiteMinder mappings.



During the repair process you'll be asked whether you want the program to apply database updates. This is useful in a case where an upgrade fails before or during the database update, but after files are copied.



Click "Finish" to finalize the repair.



- **Launch the MOVEit DMZ Installation Check Utility**

  This option will run the MOVEit DMZ checker to verify settings.

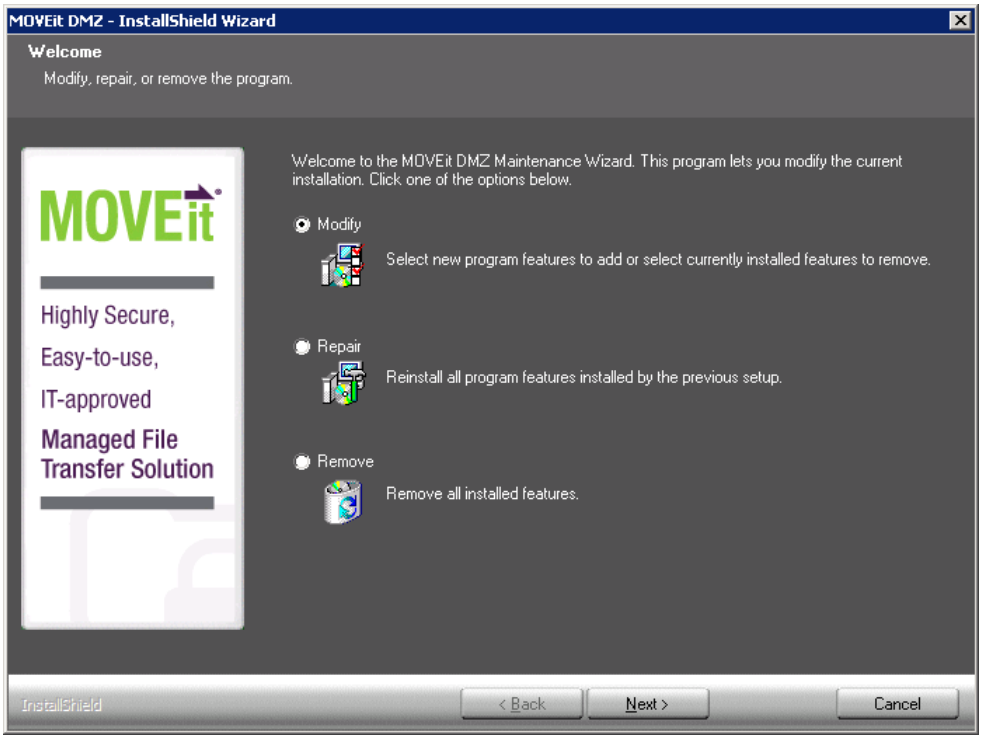
- **Securely delete the installation files (with overwrite)**

  This will securely delete the install files that contain configuration settings and passwords.

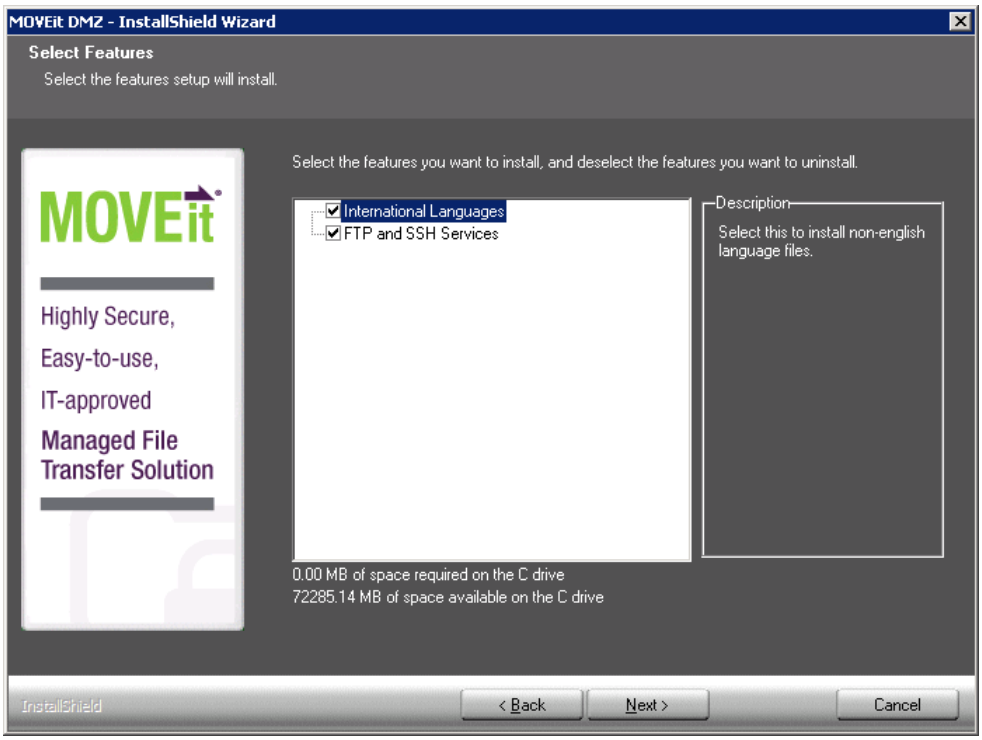
CHAPTER 6

Modify - Modify Dialog

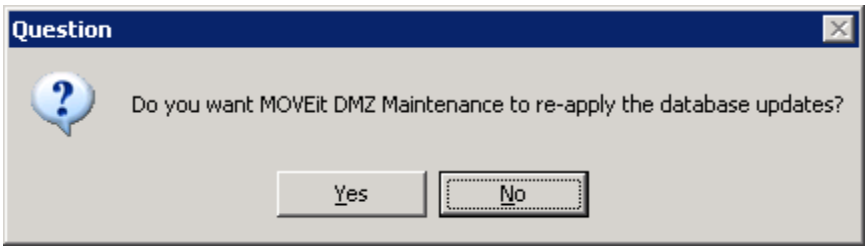
This option will install/remove MOVEit DMZ components.



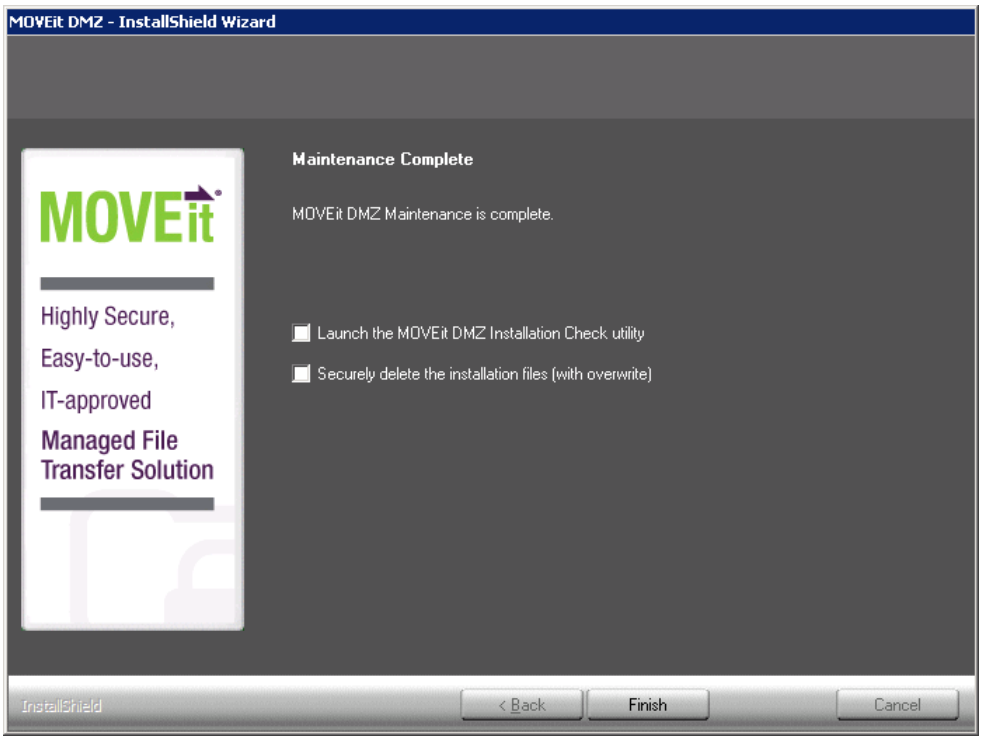
Select the features you would like to install and deselect the features that you would like to uninstall.



During the modify process you'll be asked whether you want the program to apply database updates. This is useful in a case where an upgrade fails before or during the database update, but after files are copied.



Click "Finish" to finalize the repair.



- **Launch the MOVEit DMZ Installation Check Utility**

  This option will run the MOVEit DMZ checker to verify settings.

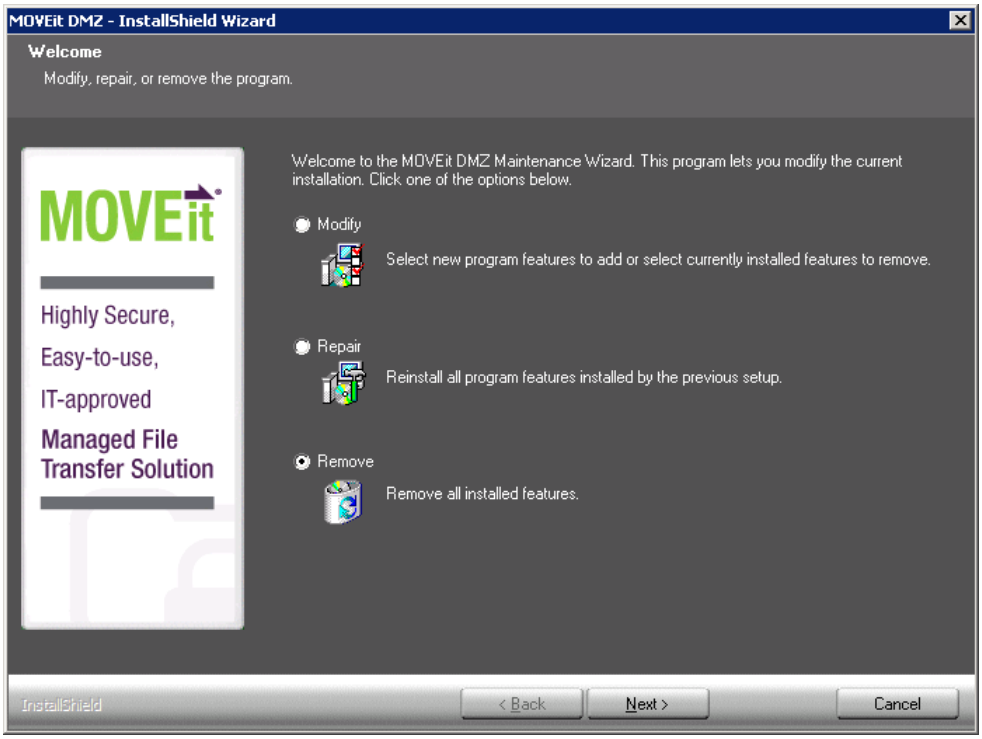
- **Securely delete the installation files (with overwrite)**

  This will securely delete the install files that contain configuration settings and passwords.

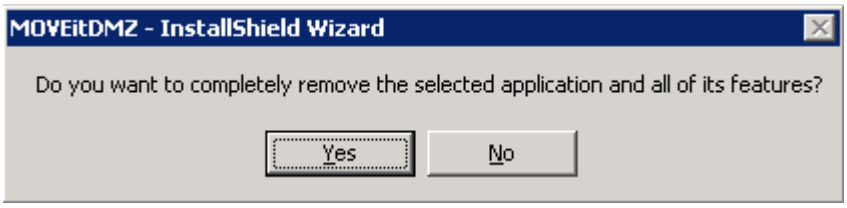
CHAPTER 7

Uninstall/Remove - Remove Dialog

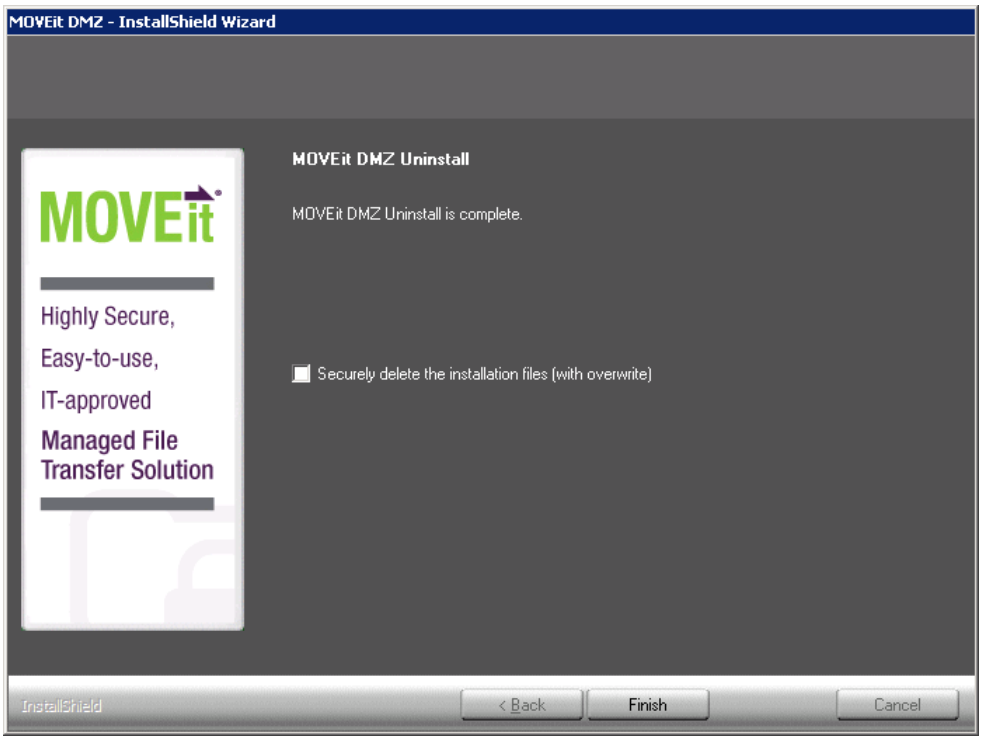
This option will completely remove MOVEit DMZ from the system.



You will be prompted for confirmation to remove MOVEit DMZ from the system.



Click "Finish" to finalize the remove.



- **Securely delete the installation files (with overwrite)**

  This will securely delete the install files that contain configuration settings and passwords.

CHAPTER 8

Unattended Install/Upgrade

The MOVEit DMZ installation program will install, upgrade, repair or uninstall MOVEit DMZ. An unattended or "silent mode" option to the install program, along with an input parameter file, allows the install, upgrade, repair or uninstall to be performed without user interaction. There are two uses for this facility:

1. Automatic testing software can create numerous installation scenarios by varying the input parameters and testing the output logs.
2. "Template" installations can be created if MOVEit DMZ needs to be installed in a large number of nearly identical configurations.

Before you perform an unattended installation, you should become very familiar with the standard MOVEit DMZ installation. It is recommended that you perform many MOVEit DMZ installations to become comfortable with all the installation options. Virtualization software makes it easy to perform repeated installations from a known starting point.

Just like the regular interactive MOVEit DMZ installation, the unattended installation will install, upgrade, or repair MOVEit DMZ, depending on the condition of the existing system. An unattended uninstall can also be performed, but requires a separate option to be used when executing the install package.

An unattended install cannot be used if you use the DMZ Web Farm feature.

In This Chapter

Requirements

Three files are required to be pre-loaded on the system in order to perform an unattended installation. It's recommended they be located in the C:\ root directory, although only the INI file is required to be there. The files are:

- **DMZ_xxxx.exe** - The self-extracting MOVEit DMZ Installation program.
- **MOVEitDMZ_Install.INI** - The parameter input file for the installation. You can create an INI file by performing a standard MOVEit DMZ installation and NOT deleting the file at the end. Once you have the INI file, you can modify it in a text editor to customize the input for use as an unattended install.
- **Setup.iss** - The "Silent Mode" Install control file.

Setup.iis

The Setup.iss file is used by the InstallShield installation program to simulate the responses by a user to the install dialogs in silent mode. The actual install parameters are loaded from a different file, so this is mostly a formality, but it is required. You can use this for the Setup.iss file:

```
[InstallShield Silent]
Version=v7.00
File=Response File
[File Transfer]
OverwrittenReadOnly=NoToAll
[{1366622F-31E2-4E10-8B8E-F1F6D61AD703}-DlgOrder]
Dlg0={1366622F-31E2-4E10-8B8E-F1F6D61AD703}-SdLicense2-0 Count=2
Dlg1={1366622F-31E2-4E10-8B8E-F1F6D61AD703}-SdStartCopy-0
[{1366622F-31E2-4E10-8B8E-F1F6D61AD703}-SdLicense2-0] Result=1
[{1366622F-31E2-4E10-8B8E-F1F6D61AD703}-SdStartCopy-0] Result=1
[Application]
Name=MOVEit DMZ
Version=5.1.9.2
Company=Ipswitch, Inc.
Lang=0009
```

MOVEitDMZ_Install.INI

MOVEitDMZ_Install.INI is the parameter file for the MOVEit DMZ installation. It is created from the dialog prompts during an initial installation and can be used to resume an installation if it is interrupted. For an unattended install, all the parameters are read from the INI file and the install jumps past the dialog prompts and proceeds directly to the file copy part. Here is a sample INI file, below. You probably want to run a normal install, answer the prompts, and save the file at the end of the installation. Look for the check box that says "securely delete the installation files", and uncheck the box.

```
[LICENSE]
LicenseKey=AAAAA-BBBBB-CCCCC-DDDDD
Express=0
[SITEPARMS]
PublicURL=https://win2003Sys1
EmailServer=mail.corp.com
EmailErrors=helpdesk@corp.com
EmailReturn=virtual@corp.com
[FOLDERS]
Application=C:\Program Files\MOVEit
Filesystem=C:\MOVEitDMZ
WebRoot=C:\MOVEitDMZ\wwwroot
ISAPI=C:\MOVEitDMZ\MOVEitISAPI
MySQL=C:\MySQL OS=C:\WINDOWS\
InstallLog=C:\MOVEitDMZ_Install.log
InstallConfig=C:\MOVEitDMZ_Install.INI
[CREDENTIALS]
MySQLAdministratorUsername=root
MySQLAdministratorPassword=P95Ux123
MySQLUserUsername=moveitdmz
MySQLUserPassword=F958m8P8
SysAdminUsername=sysadmin
SysAdminPassword=P95Ux123
RootKeyPassphrase=864584Zr417s
[WEBSITE]
CreateNewSite=1
NewSiteName=moveitdmz
OldSiteName=Default Web Site
CreateVDir=0
VDirName=moveitdmz
[SSLSERVERCERT]
CreateTestCert=1
ExistingCertIdent=win2003Sys1|00
```

Most of the parameters in the INI file are self explanatory. More information on these fields can be found in the dialog descriptions for the regular install process. The few that need more description in the context of the unattended install follow.

- **Express=0** is used in a normal install to skip many dialogs. In an unattended install, it is ignored.
- **CreateNewSite=1** instructs the installer to create a new IIS website for MOVEit DMZ. If it is set to 0, the installer will use an existing website for MOVEit DMZ.
- **NewSiteName=moveitdmz** is the website name created if CreateNewSite=1.
- **OldSiteName=Default Web Site** is the website name used if CreateNewSite=0.
- **CreateVDir=0** controls whether a full website is used for MOVEit DMZ or a virtual directory under a website. If the value is set to 1, the installer places MOVEit DMZ in a virtual director.
- **VDirName=moveitdmz** is the name of the virtual directory, relative to the 'OldSiteName' website in which the MOVEit DMZ is located. It is only used if CreateVDir=1. If you use a virtual directory, you should include the this virtual directory name in the PublicURL, above. The unattended install will not automatically modify the URL as does an interactive install.
- **CreateTestCert=1** tells the installer to create a test SSL certificate for the MOVEit DMZ website. If the value is set to 0, the installer will use an existing certificate and apply it to the website and FTP server.
- **ExistingCertIdent=win2003Sys1|00** is the CN= name of the SSL certificate, and the serial number of the certificate. If CreateTestCert=1, this is the information for the test certificate to be created by the installer. You want the CN= name part to match the DNS name in the PublicURL above. The serial number part is always '00' if the installer is creating the test certificate. If CreateTestCert=0, then the CN= part and the serial number part should describe the actual certificate to be used for the MOVEit DMZ website.
- **MSSQLAdministratorPW** is the password for the Microsoft SQL Server Administrator account. The setup program, when run manually, will not include this password in the INI file. You must add the following entry for this credential: MSSQLAdministratorPW=[password], for example, MSSQLAdministratorPW=P32Ux215

Running the Unattended Install

To launch the unattended install, run the installation package EXE from a command prompt or the Start | Run dialog:

```
c:\DMZ_xxxx.exe /s /f1"c:\setup.iss" /f2"c:\setup.log"
```

The installation package will run and create the files

- **Setup.log** which contains the result code returned by the installation process
- **MOVEitDMZ_Install.log** which contains all the steps completed by the installation package.

The MOVEitDMZ_Install.log will end with one of these messages:

- Silent Mode Installation is complete
- Silent Mode Abort
- Silent Mode Soft Abort
- Silent Mode maintenance installation is complete
- Silent Mode Upgrade is complete

In addition, the setup.log will contain the result code and version information:

```
[InstallShield Silent]
Version=v7.00
File=Log File
[ResponseResult]
ResultCode=0
[Application]
Name=MOVEit DMZ
Version=5.2.0.0
Company=Ipswitch, Inc.
Lang=0009
```

For a successful installation, the ResultCode will be 0. For a "Soft Abort", the ResultCode will be 1, and for an Abort, it will be 2. In addition, if the installation requires a reboot to complete, the MOVEitDMZ_Install.log will include a line like this:

- Reboot will be required to complete silent install
- Reboot will be required to complete silent maintenance install
- Reboot will be required to complete silent upgrade

If you start the unattended install from a command prompt, the installation package will be launched and the command prompt will return. You will need to check the MOVEitDMZ_Install.log for the correct completion line to know when the installation is done. It is not sufficient to check for the setup.log ResultCode value, because that file may be written before the installation ins complete. If you want to know that the installation has completed before checking any files, use this variation of the start command:

```
start /wait c:\DMZ_xxxx.exe /s /f1"c:\setup.iss" /f2"c:\setup.log"
```

Unattended Install Differences

Because the install skips all dialog prompts in silent mode, there are a number of actions the MOVEit DMZ installation can do that are skipped in the unattended install. Some parameters that would be calculated or pre-filled during the install dialogs, will only use the values from the MOVEitDMZ_Install.INI file. For example, the computer name is set in the PublicURL field during a regular install, but you must set that field in the INI. Also, the disk drive with the most space would be used for all base directories, but you must set the correct drive in the [FOLDERS] section of the INI file. Other steps skipped are:

- View installation configuration, including PASSWORDS
- View the installation log file
- Securely upload the installation files to your MOVEit DMZ
- Securely delete the installation files (with overwrite)
- Launch the MOVEit DMZ Configuration utility
- Launch the SecAux Security Program
- Launch the MOVEit DMZ Installation Check utility
- Launch MOVEit DMZ web session (as the system administrator)

MOVEit DMZ Unattended Upgrade or Repair

The MOVEit DMZ unattended install will automatically perform an Upgrade or a Repair if it finds an existing MOVEit DMZ already in place. An Upgrade will be performed if the existing MOVEit DMZ is an older version. A Repair will be performed if the existing MOVEit DMZ is the same version. In case of a Repair, the unattended install will always perform the database upgrade instead of prompting as the regular Repair install does.

MOVEit DMZ Unattended Uninstall

In order to perform an unattended uninstall, run the command this way:

```
c:\DMZ_xxxx.exe /removeonly /s /f1"c:\setup.iss" /f2"c:\setup.log"
```

Like the unattended install, the unattended uninstall will leave the ISS, INI and LOG files on disk when it completes.

CHAPTER 9

SecauxNET Utility

Running the SecAuxNet utility is optional. We recommenfd running the utility to further protext your operating system and the MOVEit host from security threats.

The SecAuxNET utility is used to prepare a Windows Server platform running the MOVEit DMZ application for deployment on an Internet-exposed network segment. Most of what SecAuxNET does is expressed in a Windows security template, which SecAuxNET generates and applies. The rest of SecAuxNET's activities involve applying some registry changes for the current user; these are not expressed in a Windows security template.

SecAuxNET applies several security settings that could interfere with the proper operations of a Domain Controller. For this reason, SecAuxNET will detect whether it is being run on a domain controller and will immediately exit with a warning message if it finds that it is.

SecAuxNET offers the installer/operator several different options to optimize and lock down the server, and uses answers to these options to generate the final template and perform other security actions.

In This Chapter

Welcome

The initial Welcome form provides a quick overview of what the utility does, and also allows the user to inform the utility as to whether the server is a member of an Active Directory domain, and whether MOVEit DMZ Web Farm will be or already is installed.

If the domain member checkbox is checked, indicating the server is a member of a domain, SecAuxNET will not disable the NetBIOS Helper service. This service is required in order for the server to authenticate Active Directory users who try to access the server via Remote Desktop Protocol. If the checkbox is not checked, the TCP/IP NetBIOS Helper service will be disabled along with the other non-essential services.

If the Web Farm checkbox is checked, the "Disable DCOM" option in the "Disable Unneeded Services and Applications" section will be unchecked by default, as DCOM is required for MOVEit DMZ Web Farm support. If the checkbox is not checked, the Disable DCOM option will be checked by default.

Command Line Arguments

-r : Tells SecAuxNET that the server will be part of a MOVEit DMZ web farm. This causes the utility to enable the web farm checkbox on the Welcome form, which automatically disables the "Disable DCOM" option. DCOM is required for MOVEit DMZ web farm support.

-l (logfile path) : Tells SecAuxNET to append logging information to the provided filepath. If the file does not exist, it will be created. Otherwise, it will be opened in APPEND mode and written to.

Optimize Windows and Internet Explorer

These options optimize certain Windows, Explorer, and Internet Explorer settings for both security and ease of use. All options are recommended, and are enabled by default.

Optimize Windows Operating System

This option sets recommended operating system settings for best performance and security when running the MOVEit DMZ application. The following registry changes are made when this option is enabled:

- **Optimize for background services**
  HKLM\SYSTEM\CurrentControlSet\Control\PriorityControl\Win32PrioritySeparation = 24
- **Enable logging during a crash**
  HKLM\SYSTEM\CurrentControlSet\Control\CrashControl\LogEvent = 1
- **Enable sending of an alert on crash**
  HKLM\SYSTEM\CurrentControlSet\Control\CrashControl\SendAlert = 1
- **Enable automatic reboot**
  HKLM\SYSTEM\CurrentControlSet\Control\CrashControl\AutoReboot = 1
- **Disable core dump on crash**
  HKLM\SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnabled = 0

Optimize Windows Explorer

This option sets recommended Windows Explorer settings for best performance, security, and ease of administration. The following registry changes are made when this option is enabled:

Note: These options are applied to the currently signed on user, and thus are not set by the security template, but rather are set by the SecAuxNET utility itself.

- **Enable alternate color for compressed files**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor = 1
- **Disable hiding of files (1 = disabled, 2 = enabled)**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden = 1
- **Disable hiding of file extensions**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt = 0
- **Enable showing of protected operating system files**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden = 1
- **Disable launching folder windows in a separate process**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess = 0
- **Disable webview in explorer**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView = 0

- **Disable full path in title bar**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CabinetState\FullPath = 0
- **Enable full path in address bar**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CabinetState\FullPathAddress = 1
- **Use one recycle bin setting for all drives**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\UseGlobalSettings = 1
- **Don't use recycle bin, just delete the file**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\NukeOnDelete = 1

Optimize Windows Internet Explorer

This option sets recommended Internet Explorer settings for best performance, security, and ease of administration. The following registry changes are made when this option is enabled:

Note: These options are applied to the currently signed on user, and thus are not set by the security template, but rather are set by the SecAuxNET utility itself.

- **Set the start page to localhost**
  HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page = "localhost"
- **Disable autocomplete on forms**
  HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\Use FormSuggest = "no"
- **Disable autocomplete of passwords**
  HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FormSuggest Passwords = "no"
- **Enable error display on all script errors**
  HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\Error Dlg Displayed On Every Error = "yes"
- **Enable script debugger**
  HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\Disable Script Debugger = "no"
- **Enable notification once done downloading**
  HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\Notify Download Complete = "yes"
- **Disable friendly http errors**
  HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\Friendly http errors = "no"
- **Enable printing of background and images**
  HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\Print_Background = "yes"
- **Disable Profile Assistant**
  HKCU\SOFTWARE\Microsoft\Internet Explorer\Security\P3Global\Enabled = 0
- **Check for new page on every visit**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\SyncMode5 = 3
- **Disable check for server certificate revocation**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\CertificateRevocation = 0

- **Disable caching of SSL-encrypted web pages**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\DisableCachingOfSSLPages = 1
- **Disable persistent cache**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Persistent = 0
- **Disable Fortezza protocol**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Fortezza = 0
- **Disable support for all secure protocols except SSL 3.0 and TLS 1.0**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols = 160
- **Warn if a bad certificate is received**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WarnonBadCertRecving = 1
- **Warn if zone crossing is detected**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WarnonZoneCrossing = 1
- **Warn if HTTP posts are redirected by the host**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WarnOnPostRedirect = 1

Disable Unneeded Services and Applications

These options disable services and applications that are unneeded by the MOVEit DMZ application and could pose a security threat, either by possibly allowing a server to be compromised, or by providing additional abilities to an attacker if the server is compromised. All of these options are recommended. The options to disable Outlook Express, FTP, and TELNET are left unchecked by default because they require the user to locate the executables for proper action to take place. The options should be enabled by the user for maximum security.

Disable Unneeded Services

This option marks the following services as Disabled, so they will not automatically start when Windows boots:

- **Dfs** - Distributed Filesystem
- **TrkWks** - Distributed Link Tracking Client
- **TrkSvr** - Distributed Link Tracking Server
- **RemoteRegistry** - Remote Registry Editing
- **LmHosts** - TCP/IP NetBIOS Helper Service

Note: If the Domain Member checkbox on the Welcome screen is checked, this service will NOT be disabled.

- **TapiSrv** - Telephony Service
- **TlntSvr** - Telnet Server
- **SharedAccess** - Internet Connection Sharing
- **cisvc** - Indexing Service
- **Fax** - Fax Service
- **Alerter** - Alerter Service
- **Browser** - Computer Browser
- **Messenger** - Messenger Service
- **Spooler** - Print Spooler
- **seclogon** - RunAs Services

Disable DHCP Client

Some administrators may want to disable unneeded services in order to lock down a system, but still require the DHCP client to set up their network interfaces. For this reason, disabling the DHCP client service is a separate option. Selecting this option will disable the DHCP Client service (DHCP).

This option should not be selected if the system relies on the DHCP Client service.

Note: This option will be off by default if the SecAuxNET program detects that all network interfaces on the server are using DHCP.

Disable DCOM

This option sets registry keys which disable DCOM-related services. The following registry changes are made when this option is enabled:

Note: DCOM is required for the MOVEit DMZ web farm support. If the server will be hosting a MOVEit DMZ web farm, this option should be disabled.

- **Disable DCOM**
  HKLM\SOFTWARE\Microsoft\OLE\EnableDCOM = "N"
- **Disable Remote Connect**
  HKLM\SOFTWARE\Microsoft\OLE\EnableRemoteConnect = "N"

Disable IIS WebDAV

This option sets a registry key which disables the WebDAV interface in the IIS service. The following registry change is made when this option is enabled:

- **Disable IIS WebDAV**
  HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\DisableWebDAV = 1

Disable Outlook Express, FTP Client, and Telnet Client

These options disable execute access to the Outlook Express, FTP, and Telnet client executable files to prevent their use by anyone who happens to get access to the system. Access is still allowed for administrators to update these files, to prevent service packs and other patches from failing with Permission Denied errors.

Clicking each checkbox will inform the user of the nature of the option, and then prompt the user for the location of the file. In most cases, the default location determined by the utility will be correct, and the user will simply have to click OK.

For each of the selected options, all permissions to the associated file are removed, and then full access except execute permission is given to the Local Administrators group.

Required Services

Any services not disabled by the SecAuxNET program should be left in their default state, as they may be required by either the MOVEit DMZ installation process, or the MOVEit DMZ application itself. The following list of services should be checked against the target server's service list to make sure all necessary services are in their proper states. Note that services marked as "Manual" may not be running.

Service Name	Startup Type
Application Experience Lookup Service	Automatic
Application Layer Gateway Service	Manual
Application Management	Manual
ASP.NET State Service	Manual
Background Intelligent Transfer Service	Automatic
COM+ Event System	Automatic
COM+ System Application	Manual
Cryptographic Services	Automatic
DCOM Server Process Launcher	Automatic
Distributed Transaction Coordinator	Automatic
DNS Client	Automatic

Error Reporting Service	Automatic
Event Log	Automatic
File Replication	Manual
Help and Support	Automatic
HTTP SSL	Manual
IPSEC Services	Automatic
IIS Admin Service	Automatic
Logical Disk Manager	Automatic
Logical Disk Manager Administrative Service	Manual
Microsoft Software Shadow Copy Provider	Manual
Net Logon	Manual
Network Connections	Manual
Network Provisioning Service	Manual
NT LM Security Support Provider	Manual
Performance Logs and Alerts	Automatic
Plug and Play	Automatic
Portable Media Serial Number Service	Manual
Protected Storage	Automatic
Remote Procedure Call (RPC)	Automatic
Remote Procedure Call (RPC) Locator	Manual
Removable Storage	Manual
Resultant Set of Policy Provider	Manual

Security Accounts Manager	Automatic
Server	Automatic
Smart Card	Manual
Special Administration Console Helper	Manual
System Event Notification	Automatic
Task Scheduler	Automatic
Uninterruptible Power Supply	Manual
Volume Shadow Copy	Manual
Windows Audio	Automatic
Windows Installer	Manual
Windows Management Instrumentation	Automatic
Windows Management Instrumentation Driver Extensions	Manual
Windows Time	Automatic
Windows User Mode Driver Framework	Manual
WinHTTP Web Proxy Auto-Discovery Service	Manual
WMI Performance Adapter	Manual
Workstation	Automatic
World Wide Web Publishing Service	Automatic

Apply Recommended Windows Security Settings

These options apply recommended security settings to the system. Some settings are implemented differently based on the version of Windows the system is running, so radio selectors are provided to allow the user to choose the correct operating system. In most cases, the utility will be able to auto-detect the Windows version, and will automatically select the proper option.

Apply basic Windows security settings

When this option is selected, the following security settings are applied:

- **System Access**
  - MinimumPasswordAge = 0
  - MaximumPasswordAge = 90
  - MinimumPasswordLength = 8
  - PasswordComplexity = 1
  - PasswordHistorySize = 7
  - LockoutBadCount = 3
  - ResetLockoutCount = 30
  - LockoutDuration = 30
  - ClearTextPassword = 0
  - RequireLogonToChangePassword = 0
  - ForceLogoffWhenHourExpire = 0
  - LSAAnonymousNameLookup = 0
  - EnableAdminAccount = 1
  - EnableGuestAccount = 0
- **System Log**
  - MaximumLogSize = 8192
  - AuditLogRetentionPeriod = 0
  - RestrictGuestAccess = 1
- **Security Log**
  - MaximumLogSize = 8192
  - AuditLogRetentionPeriod = 1
  - RetentionDays = 7
  - RestrictGuestAccess = 1

- **Application Log**
  - MaximumLogSize = 8192
  - AuditLogRetentionPeriod = 0
  - RestrictGuestAccess = 1
- **Event Audit**
  - AuditProcessTracking = 0

Enable FIPS compliance mode

When this option is selected, the FIPS compliance security policy option will be enabled for the system. When this mode is active, Windows will prevent all applications from using Microsoft-provided cryptographic algorithms and ciphers that are not FIPS compliant, usually meaning they are older and less secure. This includes protocols like SSL 2.0 and SSL 3.0, hash algorithms like MD5, and ciphers like DES, RC2, and RC4. Only FIPS compliant protocols, algorithms, and ciphers will be used. MOVEit DMZ is fully supported when running with FIPS compliance mode enabled, and its use is recommended for high security environments.

Configure 256-bit AES as primary SSL encryption algorithm

This option reconfigures the Microsoft SSL encryption stack to prefer 256-bit AES encryption over weaker forms when negotiating secure SSL connections with clients. By default, the slightly less secure, but faster, 128-bit AES algorithm is preferred, for performance reasons. In high security environments, this option is recommended to provide maximum security in transit. The 256-bit AES option is FIPS 140-2 validated.

Apply Recommended NTFS Permissions

These options apply recommended NTFS permissions to the various directories created and used by MOVEit DMZ and its MySQL database server. This helps lock the application directories down to prevent unauthorized access to MOVEit DMZ data, files, and application libraries. The auto-detected major folder paths for both MOVEit DMZ and MySQL are displayed here for verification.

Because some systems may have a pre-existing MySQL server already installed, which may be accessed by other applications, the option to lock down the MySQL folder is separate from the option to lock down the MOVEit DMZ folders. For most installations, however, it is recommended that both options be selected.

For each folder, permissions are applied to two different groups. First, the Local Administrators group usually receives full access to the folders, to allow administrators to view and edit MOVEit DMZ files and perform upgrades. Second, a MOVEit System group is given the necessary permissions to operate the MOVEit DMZ application. In some cases, these permissions are limited, while in others, the group may receive full access. The MOVEit System group is created automatically by the SecAuxNET utility, and populated using the security template generated. Accounts necessary for the operation of the MOVEit DMZ web application and other services are made members of this group, and include the Local System account, the IWAM and IUSR accounts, and the ASPNET account.

Note: The MOVEit System group is automatically created by the SecAuxNET utility if the Apply NTFS option is enabled. The group is NOT created by the security template that SecAuxNET generates.

When these options are selected, the following NTFS permissions are applied (subfolders not listed are set to inherit permissions from parent folders):

Folder	Administrator Permissions	MOVEit System Permissions
(DMZ NonWeb Path)	FULL	READ/LIST/EXECUTE
(DMZ NonWeb Path)\Certs	FULL	FULL
(DMZ NonWeb Path)\Files	FULL	FULL
(DMZ NonWeb Path)\Logs	FULL	FULL
(DMZ NonWeb Path)\Scheduler	FULL	FULL
(DMZ NonWeb Path)\Util	FULL	NONE
(DMZ Web Path)	FULL	READ/LIST/EXECUTE

(DMZ Web Path)\images\instlogos	FULL	FULL
(DMZ Web Path)\templates	FULL	FULL
(DMZ ISAPI Path)	FULL	READ/LIST/EXECUTE
(DMZ Programs Path)	FULL	READ/LIST/EXECUTE
(MySQL Path)	FULL	FULL

Rename Administrator Account

This option renames the default Administrator account on the system to the provided name. This enhances security on the system by preventing attackers from accessing the system through a well-known account name.

When this option is selected, a new name must be entered in the provided text box. The utility will not allow the user to proceed until they have done so.

Configure IIS

The Configure IIS options will affect the way that IIS processes the specified website (normally "moveitdmz").

The options on this page will be applied to the website identified in **Website to change**. This is nearly always "moveitdmz", which is the default. MOVEit supports being installed in an IIS virtual directory. If you are using a virtual directory for the website, you need to enter the name of that directory in **Virtual directory**.

Configure generic IIS error pages

Use this option to configure custom error pages for IIS and ASP.NET. You can configure IIS and ASP.NET to return custom error pages in the case of HTTP errors. The custom pages contain slightly less information than the default Microsoft error pages. Returning minimal system information is considered a good security practice.

To configure these error pages, select the **Configure generic IIS error pages** option. Click **Next** to save your changes and continue.

When the MOVEit server has an unhandled exception error in response to an HTTP request, MOVEit will send the custom error page.

Prevent "clickjacking" by adding X-Frame-Options: DENY HTTP

Use this option to prevent "clickjacking," which is an attack that tries to embed code or a script in a browser page in an attempt to trick the user into clicking on something that appears to perform another function. This option, which is enabled by default, adds the X-Frame-Options: DENY HTTP to the HTTP header of your MOVEit web site.

Prevent IP address disclosure in Location: header when no "Host"

Use this option to prevent the MOVEit server IP address from being shown in HTTP responses, when the client request does not contain an HTTP:Host header value. This option, which is enabled by default, configures IIS to not show the server IP address in the Location header field. If you specify a name in the **Use Hostname** field, it will show that value in the HTTP response.

Configure SMB (Server Message Block) Signing

Server Message Block (SMB) is a file system access protocol used by Windows. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent "man in the middle" attacks against SMB. SMB signing has some performance cost, but it results in more secure communications.

Use this dialog to configure SMB signing for the entire computer. SMB signing can be configured to be not required (less secure) or required (more secure). SMB signing is configured separately for the system when acting as a client to other systems, or when acting as a server to other systems. Therefore, if you do not require SMB signing, it does not necessarily mean that SMB communications will not be signed; it will depend on the settings of the other Windows computer involved in the conversation.

To configure SMB signing, select **Configure SMB (Server Message Block) signing**. You can then select any combination of the options **Require SMB signing as a client** and **Require SMB signing as a server** to configure whether SMB signing is required by servers and clients on this computer.

Note: Some specially-configured, older Windows computers may not be able to access remote file systems on the MOVEit DMZ computer, or vice versa, if SMB signing is required. This is unlikely to affect the average MOVEit DMZ customer, but if you change these settings, be sure to test any mounted file systems before returning the system to production.

Final Steps

Once all the security template options have been selected, the final section will be shown, providing the operator some final options for how to proceed with the generated security template. Clicking the Finish button will cause the SecAuxNET utility to proceed with its actions.

Final Options

The following final processing options are available in this section:

Backup Registry

When selected, this option will cause the SecAuxNET utility to create a backup copy of the HKEY_LOCAL_MACHINE and HKEY_USERS registry hives before executing its changes. The backup file will be placed in the MOVEit DMZ program files directory. Operators who wish to undo the registry changes made by SecAuxNET can use the regedit.exe windows utility to load this backup file.

Apply Security Template

When selected, this option will cause the SecAuxNET utility to apply the generated security template to the local system. The secedit.exe windows utility is used to generate a security database file in the MOVEit DMZ program files directory based on the generated security template file. The same utility is then used to apply the settings in the security database file to the system.

Final Processes

Upon clicking the Finish button, the SecAuxNET utility will attempt the following actions:

1. **Backup Registry** - If the Backup Registry option was selected, the registry backup will be done first. See above for details. This step may take several minutes.
2. **Apply Current User Registry Changes** - If the Optimize Windows Explorer and Optimize Internet Explorer options from the first options section are selected, these user-based options will be applied directly by the SecAuxNET utility. This is done because the security template mechanism is not able to apply changes to the HKEY_CURRENT_USER registry hive.
3. **Create "MOVEit System" Group** - If the Apply NTFS option is selected, SecAuxNET will create a local user group called "MOVEit System". This group will be populated with the necessary local accounts to run the MOVEit DMZ application and will be given appropriate rights to the MOVEit DMZ and MySQL folders.
4. **Generate Security Template File** - The template file content is generated now, based on the selected options from the previous sections.
5. **Save Security Template File** - The template file content is saved to the local filesystem as the file "MOVEit_SecAux_SecurityPolicy.inf" in the MOVEit DMZ program files folder.

6 **Apply Security Template** - If the Apply Security Template option was selected, the template will be processed into a database file and then applied to the system. See above for details. This step may take several minutes.

Complete

The SecAuxNET utility should now be finished. If there were no problems, the program will exit upon completion of its last processing step.

If the security template was not applied to the setting, the operator may apply it manually by following this procedure:

1 Open a command prompt and cd to the MOVEit DMZ program files folder (by default C:\Program Files\MOVEit).

2 Run the command "secedit /analyze /db MOVEit_SecAux_SecurityPolicy.sdb /cfg MOVEit_SecAux_SecurityPolicy.inf". This will generate the security database file based on the settings in the security template file. The database will be stored in the file "MOVEit_SecAux_SecurityPolicy.sdb".

3 Run the command "secedit /configure /db MOVEit_SecAux_SecurityPolicy.sdb". This will apply the security options in the database file to the local system.

Once the security template settings have been applied to the local system, either automatically by the SecAuxNET utility or manually by the operator, a system restart will be required to make sure all the settings take effect.

Rolling Back Changes

In order to roll back the changes applied by the SecAuxNET utility, follow these procedures.

Security Policy

Perform the following steps to roll back the security policy changes applied by the SecAuxNET utility.

1 Open the Security Configuration and Analysis MMC Snap-in:

1. Open a blank MMC console by clicking **Start > Run**, entering "mmc", and clicking **OK**.
2. Click the Console menu and select **Add/Remove Snap-in**.
3. On the Add/Remove Snap-in dialog, click **Add**.
4. On the Add Standalone Snap-in dialog, select the Security Configuration and Analysis snap-in and click **Add**.
5. On the Add Standalone Snap-in dialog, click **Close**, then on the Add/Remove Snap-in dialog, click **OK**.

2 If you have an existing security policy database file that you use for your systems, open that file and apply its settings now. Otherwise, to apply the standard security policy that newly installed Windows servers are configured with, follow these steps:

   1. Right-click the Security Configuration and Analysis node and select **Open database**.
   2. Open the MOVEit_SecAux_SecurityPolicy.sdb database file in the directory selected for MOVEit DMZ program files (by default C:\Program Files\MOVEit).
   3. Right-click the Security Configuration and Analysis node again and select **Import Template**.
   4. Select the "setup security.inf" file. If you do not see this file, try looking in C:\WINNT\Security\templates. Make sure the **Clear this database before importing** option is checked. Click **Open**.
   5. Right-click the Security Configuration and Analysis node again and select **Configure Computer Now**. Set a path for the log file which will be generated, and click **OK**.

3 Reboot the server to make sure changes are applied.

Registry

If the option is selected, SecAuxNET will create a backup of the HKEY_LOCAL_MACHINE node of the Windows registry. This backup is written to the file MOVEit_SecAux_RegBackup.reg in the directory selected for MOVEit DMZ program files (by default C:\Program Files\MOVEit).

To load the original registry settings, simply double-click the registry backup file and click OK to the confirmation prompt. Once the registry backup has been loaded, reboot the server to make sure the changes are applied.

CHAPTER 10

Installing a Local Version of MOVEit Documentation

The MOVEit documentation is now hosted on the Ipswitch web site, which allows for more frequent updates to the topics. The hosted version of the documentation will always be the most up-to-date version.

If you need to have the documentation installed locally, meaning on the MOVEit DMZ system, you can download the files and install locally as follows:

1. Log in to the MOVEit Support site.
2. Select the file named DMZ_LocalDoc8000.msi and download to the system on which you installed MOVEit.
3. Double-click DMZ_LocalDoc8000.msi to launch the installer and follow the on-screen prompts.

The documentation is installed on the local host. In MOVEit, in the navigation pane on the left, click **Online Manual** to display the documentation.