



Installation Guide

McAfee Security for Microsoft Exchange 8.6.0

COPYRIGHT

Copyright © 2017 McAfee, LLC

TRADEMARK ATTRIBUTIONS

McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

1	Installation and configuration	5
	Pre-installation	5
	System requirements	6
	Supported Microsoft Exchange Server roles	7
	Package contents	7
	Installation	8
	Install the software using setup wizard	8
	Install the McAfee Anti-spam add-on manually	11
	Perform a silent installation	11
	Upgrade a standalone deployment	13
	Post-installation	14
	Quick setup	14
	Cluster deployment	15
	Configure McAfee Security for Microsoft Exchange Access Control	16
	SiteList Editor	17
	Test your installation	20
2	Repair the installation	23
3	Uninstall the software	25
A	Frequently asked questions	27
	Index	29

1

Installation and configuration

Select the option to install and use your MSME software, which best suits your requirements.

Installation type		Description
Standalone	Wizard-based	When using the wizard-based setup file, select one of these options per your requirements: <ul style="list-style-type: none">• Typical — Configured for all standard features except the McAfee Anti-Spam add-on. You can install the McAfee Anti-spam add-on separately at a later stage.• Complete — Configured for all standard features with the McAfee Anti-Spam add-on that provides protection against Spam or Phish attacks.• Custom — Configure using the advanced options to customize your setup.
	Silent	Install the software without any user interaction or prompts. Modify and run the <code>Silent.bat</code> file that allows you to record selections for the installation process.
ePolicy Orchestrator-managed		Deploy MSME in ePolicy Orchestrator environment to allow centralized policy management and enforcement on your Microsoft Exchange Servers.



You can also deploy MSME to a Microsoft Exchange Server cluster. This deployment requires certain post-installation configuration tasks.

See also

[Cluster deployment on page 15](#)

Contents

- ▶ [Pre-installation](#)
- ▶ [Installation](#)
- ▶ [Post-installation](#)

Pre-installation



Use this information to prepare for the MSME installation.

Contents

- ▶ [System requirements](#)
- ▶ [Supported Microsoft Exchange Server roles](#)
- ▶ [Package contents](#)

System requirements

Make sure that your server meets these requirements.

Component	Requirement
Operating system	<ul style="list-style-type: none"> • Microsoft Windows 2008 Standard/Enterprise Server SP2 (64-bit) • Microsoft Windows 2008 Standard/Enterprise Server R2 (64-bit) • Microsoft Windows 2012 Standard/Enterprise Server (64-bit) • Microsoft Windows 2012 Standard/Enterprise Server R2 (64-bit) • Microsoft Windows Server 2016 (64-bit)
Microsoft Exchange Server	<ul style="list-style-type: none"> • Microsoft Exchange Server 2010 SP3 • Microsoft Exchange Server 2013 CU 12 and later • Microsoft Exchange Server 2016 CU 3 and later
Browser	<ul style="list-style-type: none"> • Microsoft Internet Explorer version 10.0 and 11.1016 • Mozilla Firefox 54.0.1 • Google Chrome 59.0.3071.115 <p> Make sure that you disable the pop-up blocker in the browser settings.</p>
Processor	<ul style="list-style-type: none"> • Intel x64 architecture-based processor that supports Intel Extended Memory 64 technology (Intel EM64T) • AMD x64 architecture-based processor with AMD 64-bit technology
Memory	<p> The memory requirement to install MSME is the same as Microsoft Exchange Server requirement. For more information, see the <i>Microsoft Exchange</i> website.</p> <p>Microsoft Exchange Server 2010</p> <ul style="list-style-type: none"> • Minimum — 4 GB RAM • Recommended — 4 GB RAM for a single role and 8 GB for multiple roles <p>Microsoft Exchange Server 2013</p> <ul style="list-style-type: none"> • Minimum — 8 GB RAM • Recommended — 8 GB RAM <p>Microsoft Exchange Server 2016</p> <ul style="list-style-type: none"> • Minimum — 8 GB RAM • Recommended — 8 GB RAM
Disk space	Minimum: 740 MB
Network	10/100/1000-Mbps Ethernet card
Screen resolution	1024 x 768
McAfee management software	McAfee ePolicy Orchestrator 5.1.x, 5.3.x, and 5.9.x
McAfee Agent	McAfee Agent 5.0.5 (build number 658)

Component	Requirement
Upgrade path	McAfee Security for Microsoft Exchange 8.0 Patch 2 McAfee Security for Microsoft Exchange 8.5 Patch 1
IIS components	For information about IIS components requirements, see KB77319



To view updated system requirements, see [KB76903](#).

Supported Microsoft Exchange Server roles

The MSME installation depends upon the role selected for the Microsoft Exchange Server installation.

These roles are supported for the various versions of Microsoft Exchange Servers:

- Microsoft Exchange Server 2010:
 - Edge Transport Server — Runs in the perimeter outside a domain and provides message hygiene and security. It is installed on a standalone server that is not a member of an Active Directory domain.
 - Hub Server — Handles all mail flow inside the organization, applies transport rules, and delivers messages to a recipient's mailbox in an Active Directory domain.
 - Mailbox Server — Holds the Exchange databases containing the user mailboxes.
 - An installation with a dual role of Mailbox with Hub.
- Microsoft Exchange Server 2013, 2013 SP1, and 2016 CU 2
 - MBX Server — Holds the dual role of Mailbox with Hub.
 - Edge Transport Server. (only for Microsoft Exchange Server 2013 SP1)

Package contents

The software package contains the files necessary to install and set up the software as required.

Unzip the `MSMEv86_x64.ZIP` archive, to find these directories.

Folder	Content
Standalone	<p>Contains the files required to perform a standalone installation of the product:</p> <ul style="list-style-type: none"> • <code>Setup_x64.exe</code> — Setup file to install the software using a wizard. • <code>Silent.bat</code> — Record file to install the software without any prompts or wizard.
ePO	<p>Contains installation and configuration files required for managing the product using ePolicy Orchestrator.</p> <ul style="list-style-type: none"> • <code>ePO_Extension_XX</code> — Contains the product extensions for all locales in their respective locale folders. For example, <code>ePO_Extension_EN</code>. • <code>MSME_Deployment_x64_xxxx.zip</code> — Deployment package to deploy the software on the managed clients. • <code>MSME_AS_Deployment_xxxx.zip</code> — Deployment package to deploy the McAfee Anti-spam component on to the managed clients. • <code>MSMEePOUpgrade.zip</code> — Contains the executable file required to migrates policies from MSME 8.0.2 or 8.5.1 to MSME 8.6 in an upgrade. • <code>MSME86REPORTS.zip</code> — Extension to add MSME reporting interface such as dashboards, queries. • <code>help_msme_<version_number>.zip</code> — The product help extension.
AntiSpam	<p>Contains <code>ASAddon_x64.exe</code> to install the McAfee Anti-Spam add-on component.</p>



MSME installer includes McAfee Agent 5.0.5 (build number 658). The agent collects and sends information between the ePolicy Orchestrator server and repositories, and manages installations across the network.

Installation

MSME is installed in a compatible environment with features depending on your requirement.

MSME can be installed on a standalone server or integrated with ePolicy Orchestrator.



Make sure that you have the Windows administrator credentials to install the product. This account must be a Domain administrator and these credentials are required to launch the product installer.

See also

Contents

- ▶ *Install the software using setup wizard*
- ▶ *Install the McAfee Anti-spam add-on manually*
- ▶ *Perform a silent installation*
- ▶ *Upgrade a standalone deployment*


Install the software using setup wizard

Install the software on a system where Microsoft Exchange Server 2010, 2013, or 2016 is installed.

In Microsoft Exchange Server 2010, MSME executes Transport Scanning for the Edge transport and Hub transport roles, and VirusScan API for the Mailbox role (based on the roles configured).

Task

- 1 As an administrator, log on to the system where Microsoft Exchange Server is installed.
- 2 Create a temporary directory on your local drive.
- 3 Download the archived software package and extract it to the temporary directory you created.
- 4 From the setup folder, double-click **setup_x64.exe** (this is the setup application for a 64-bit operating system).
- 5 Select a language from the drop-down list, then click **OK**.
- 6 In the **Preparing to Install** screen, the installation wizard is prepared and all required installation files are extracted. When the process is complete, the **Welcome** screen appears. Click **Next**.
- 7 The **Exchange Server Role Detection** screen lists the roles selected during the Microsoft Exchange Server installation. Click **Next**.
- 8 Select an installation type, then click **Next**.
 - **Typical** — Commonly used features are installed with Web-based Product Configuration. The McAfee Anti-Spam add-on is not installed.
 - **Complete** — (Recommended) Web based product configuration and McAfee Anti-Spam add-on are installed. If the node is cluster aware, the required cluster setup components and services are also installed.
 - **Custom** — (Recommended only for advanced users) Select which application features you want to install and where to install. If you select this type of installation, a dialog box displays the features you can install. To change the destination folder for the installation files, click **Change**.
- 9 Accept the terms in the license agreement, then click **Next**.
- 10 In the **Additional Configuration Settings** screen, complete these options, then click **Next**.
 - a Select **Import existing configuration** to import the MSME configuration from an existing installation in the same or a different system. This configuration setting is saved as a .cfg file. To import this configuration, click **Import**, browse to the .cfg file, then click **Open**.

 You must have already exported a configuration file from the product interface.
 - b Under **Select Quarantine mechanism**, select a location to store all quarantined items, then complete the options for the location you selected.
 - c If you select **Local Database**, click **Browse** to change the default location (optional). If you select **McAfee Quarantine Manager**, type the IP address of the McAfee Quarantine Manager server, the port number,

and the callback port number. Make sure that the McAfee Quarantine Manager server is up and is available for quarantining.

- **RPC** — Remote Procedure Call (RPC) is a communication mechanism that requires uninterrupted connection to communicate with McAfee Quarantine Manager server. If the network connection is not available, processes such as quarantine and release are interrupted.
- **HTTP** — A stateless communication mechanism to communicate with McAfee Quarantine Manager server. If there is a communication issue with McAfee Quarantine Manager server, the items are stored in the local database until the connection is restored. MSME tries to send the quarantined items to McAfee Quarantine Manager three times. If all three attempts fail, a product log entry is created and the item is stored in the local database.
- **HTTPs** — A secured HTTP communication mechanism where the data is transferred in encrypted format.



McAfee recommends that you use HTTP/HTTPs communication channel because stateless connections make sure that the software can communicate with McAfee Quarantine Manager seamlessly.

- d Under **Administrator Email address**, type the email address to which all notifications, configuration reports, and status reports must be sent.

11 Select a protection profile, then click **Next**.

- **Default** — This profile provides maximum performance with optimum protection.
- **Enhanced** — This profile enables default file filter rules and provides maximum protection. It also provides real-time protection using McAfee Global Threat Intelligence file and messaging reputation.
- **Use existing** — (Upgrade only) This option uses the existing protection profile.

12 Select **Create Desktop shortcuts** if you want the installation wizard to create shortcuts for the application on the desktop, then click **Next**.

13 In the **Ready to Install the Program** screen, verify the selected configuration, then click **Install**. The **Installing McAfee Security for Microsoft Exchange** screen appears that displays the features being copied, initialized, and installed.



MSME creates a user named **MSMEODuser** in the active directory. This user is required to perform on-demand scans.

14 When the installation is complete, the **Installation Wizard Completed** screen appears. Select the options as required, then click **Finish**.



You might be prompted to provide the domain administrator credentials.

- **Launch Product User Interface** — To launch the MSME standalone user interface after you exit the installation wizard.
- **Show the readme file** — To view the Release Notes of the product (**Readme.pdf**) for information on any last-minute additions or changes to the product, known issues, or resolved issues.
- **Update Now** — (Recommended) To update MSME with the latest DAT files, engine, and anti-spam updates.
- **Register at McAfee Business Community to stay up to date** — To receive information regarding the product, new releases, updates, and other relevant information.
- **Show Windows Installer logs** — To view the log file of the installation process.



We recommend that you restart your computer after the installation process is complete.

The MSME software is successfully installed on your system.

Install the McAfee Anti-spam add-on manually

If you've not installed McAfee Anti-spam as part of the complete or custom installation of MSME, install the add-on manually.

Task

- 1 As an administrator, log on to the system where Microsoft Exchange Server is installed.
- 2 Browse to the `\AntiSpam` folder in the software package, double-click `ASAddOn_x64_Eval.exe`.
- 3 Select a language from the drop-down list, then click **OK**.
- 4 In the **Welcome** screen, click **Next** to display the **End User License Agreement** screen.
- 5 Accept the terms in the license agreement, then click **Next**.
- 6 In the **Ready to Install the Program** screen, verify the selected configuration, then click **Install**. The **Installing McAfee Anti-Spam add-on for Microsoft Exchange** screen appears that displays the features being copied, initialized, and installed.
- 7 When the installation is complete, the installation wizard **Completed** screen appears. Select **Show Windows Installer logs** to view the log file of the installation process, if necessary, then click **Finish**.

The McAfee Anti-spam add-on is successfully installed on your system.

Perform a silent installation

You can automate the installation using the `Silent.bat` file that allows you to record the selections for the installation process.

To install the product with default settings, double-click the `Silent.bat` available in the download package.





Silent.bat internally is called from the MSME setup file. Make sure that the `setup_x64.exe` is available in the same directory because the installation can't succeed with `Silent.bat` alone.


To customize the installation, modify these parameters in the batch file before running it:

Parameter	Value	Description
ADMIN_EMAIL_ID	<admin>@<msme>.com	Specify the administrator's email address for notifications. For example, SET ADMIN_EMAIL_ID=administrator@msme.com MSME sends notifications to this email address, when you enable Send notification option for policies.
AUTO_UPDATE	1 or 0	Enable or disable automatic updates: <ul style="list-style-type: none"> • 1 = enabled • 0 = disabled When enabled, the DAT and engine update happens immediately after the software installation.



McAfee recommends that you enable the automatic update to make sure that the engine and DAT files are up to date.

Parameter	Value	Description
INSTALL_DIR	%SystemDrive%\MSME	Specify the installation path. For example, if you specify C:\MSME, a folder MSME is created in the C drive.
NEED_DESKTOP_SHORTCUT	1 or 0	Specify whether to create a desktop shortcut after successful installation: <ul style="list-style-type: none"> • 1 = yes • 0 = no The default value is 1.
DB_PATH_CHANGED	1 or 0	Specify whether to change the Postgres database path: <ul style="list-style-type: none"> • 1 = yes • 0 = no <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  You can modify the database path anytime after the installation. When you change the path, a new database is created to store the detected items. However, the detected items stored in the earlier database are not available in the new database. </div>
DATABASEDIR	<New Postgres DB Location>	Specify the new Postgres database location. For example, C:\TestDB.
QUARANTINE_MECHANISM	1 or 2	Specify the location for quarantined items: <ul style="list-style-type: none"> • 1 = Local database • 2 = McAfee Quarantine Manager <p>Local database — To quarantine detected items in the local system.</p> <p>McAfee Quarantine Manager server — To quarantine detected items in MQM server, a centralized storage server.</p> <p>If you select McAfee Quarantine Manager, make sure that you also define the MQMIPADDRESS, MQMPORTNUMBER, and MQM_COMMUNICATION_MECHANISM settings.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  You can modify the settings from the software interface any time after the installation. </div>
MQMIPADDRESS	IPv4 or IPv6 address	Specify the IP address of the MQM server. MSME supports both IPv4 and IPv6 format.

Parameter	Value	Description
MQM_COMMUNICATION_MECHANISM	0 or 1 or 2	Specify the communication channel to communicate with MQM server: <ul style="list-style-type: none"> • 0 = RPC • 1 = HTTP • 2 = HTTPs <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  McAfee recommends that you use HTTP/HTTPs communication channel because stateless connections make sure that the software can communicate with MQM server seamlessly. </div>
MQMPORTNUMBER	80 or 443 or 49500	Specify port numbers for communication channels: <ul style="list-style-type: none"> • 80 = HTTP protocol • 443 = HTTPs protocol • 49500 = RPC protocol
AGREE_TO_LICENSE	Yes or No	Agree to the license terms to install the software. For example, SET AGREE_TO_LICENSE = Yes.



The silent installation includes all standard features except the McAfee Anti-Spam add-on. You must install the McAfee Anti-Spam add-on separately. For details, see *Install the McAfee Anti-spam add-on manually*.

Upgrade a standalone deployment

MSME 8.6 supports upgrading your configuration settings from the previous version 8.0 Patch 2 or 8.5 Patch 1.

Before you begin

Place your Microsoft Exchange server in maintenance mode because the Exchange Database and Exchange Transport services restart during the installation process.

If you had installed the previously supported version of McAfee Anti-spam module separately earlier, make sure that you uninstall the McAfee Anti-spam module before upgrading the software. You can install the latest version of the McAfee Anti-spam after the upgrade.


MSME provides enhanced security by not supporting the HTML tags that have XSS vulnerability. McAfee recommends that you remove the HTML tags that have XSS vulnerability from the existing notification template before the upgrade. Otherwise, after the upgrade, if you try to modify the notification templates that contain unsupported tags, you will be prompted to remove the unsupported tags from the template or use the template without modification. For the list of unsupported HTML tags, see McAfee KnowledgeBase article [KB82214](#).


When upgrading to a new version, you need not uninstall the existing version. The installation program updates your installation to the new version.


Task

- 1 As an administrator, log on to the system where Microsoft Exchange Server is installed.
- 2 From the setup folder, double-click **setup_x64.exe** (this is the setup application for a 64-bit operating system).
- 3 In the **Preparing to Install** screen, the installation wizard is prepared and all required installation files are extracted. When the process is complete, the **Welcome** screen appears. Click **Next**.

- 4 The **Exchange Server Role Detection** screen lists the roles selected during the Microsoft Exchange Server installation. Click **Next**.
- 5 In the **Setup Type** screen, the **Custom** option is selected by default. Click **Next**.
- 6 The **Custom Setup** screen lists the features installed in the existing installation. Select the features you want to be updated with McAfee Security for Microsoft Exchange, then click **Next**.
- 7 Accept the terms in the license agreement, then click **Next**.
- 8 The **Additional Configuration Settings** screen displays the settings for quarantine mechanism and quarantine database applied in the existing installation. Change the settings, if necessary, then click **Next**. To migrate policies from an earlier version, select the option **Import existing configuration**, then browse and select the configuration file.
- 9 In the **Setup Protection Profile** screen, select **Default**, **Enhanced**, or **Use Existing**, as necessary, then click **Next**.

 If you selected the **Import existing configuration**, all options on this screen are grayed-out. The **Use Existing** option is selected by default.
- 10 Select **Create Desktop shortcuts** if you want the installation wizard to create shortcuts for the application on the desktop, then click **Next**.
- 11 In the **Ready to Install the Program** screen, verify the selected configuration, then click **Install**. The **Installing McAfee Security for Microsoft Exchange** screen appears that displays the features being copied, initialized, and installed.

 While upgrading, the software checks the existing DAT version in the system and upgrades only if the DAT version packaged with the software is greater than the DAT version available in the system.
- 12 When the installation is complete, the **Installation Wizard Completed** screen appears with the **Migrate Quarantine Data** option selected by default. Click **Finish**.

 If you had configured proxy settings in the previous version, you must configure the proxy settings again after the upgrade. We recommend that you restart your computer after the installation.

The McAfee Security for Microsoft Exchange software is successfully upgraded.

Post-installation

Once you've installed MSME, perform certain additional configuration to set it up for your environment.

Quick setup

Steps to quickly set up MSME and protect your Exchange server environment.

As an administrator, perform these tasks once you install MSME on your Exchange server.

Task

- 1 Update the software by performing a Engine/DAT update. For details, see the *Schedule a software update* section.
- 2 If you have installed MSME on an Edge Transport or Hub Transport server, make sure that MSME agents are loaded in the Exchange Power Shell (Exchange Management Shell), using this command:

```
Get-TransportAgent
```

The status for "Enabled" must be true to agents starting with "McAfee".

- 3 Make sure that you install the McAfee anti-spam add-on component to quarantine spam or phish email messages.
- 4 Update the administrator email address from **Settings & Diagnostics | Notifications | Settings** tab.
- 5 Schedule a status report task. For details, see the *Schedule a new status report* section.
- 6 Schedule a configuration report task. For details, see the *Schedule a new configuration report* section.
- 7 Schedule on-demand scans based on your requirement. For details, see the *On-Demand scan and its views* section.
- 8 Configure the on-access scan settings as per your requirement from **Settings & Diagnostics | On-Access Settings** page. For details, see the *On-Access settings* section.
- 9 Configure **DLP and Compliance** scanner settings and rules based on your company policy. For details, see the *Policy Manager* section for instructions on configuring policies, scanners, and filters.
- 10 For exceptions in a policy, create subpolicies based on your organization's requirement.
- 11 Send test email messages to verify the configuration.

Cluster deployment

You need additional configurations to install MSME in cluster deployments of Microsoft Exchange Server 2010, 2013 and 2016 CU 2.

Cluster replication utility for Microsoft Exchange 2010, 2013, and 2016 CU2

The **Cluster Replication Setup Utility** helps in the replication of the quarantine database, Policy configurations, engine, and DATs.

This utility is available only for an MSME installation that is recognized by a *Data Availability Group (DAG)*, in which case the MSME Replication Service is also available. Depending on the configuration settings, this utility replicates quarantined items from one server to the other, and makes them highly accessible.

The primary component in a Data Availability Group is called Active Manager. Microsoft Exchange Server 2010 relies on the Active Manager to manage switchovers and failovers between mailbox servers that are a part of a Data Availability Group. Active Manager runs on all Mailbox servers in a given Data Availability Group and can be installed in two roles:

- Primary Active Manager (PAM)
- Standby Active Manager (SAM)

For details regarding these roles, refer to the relevant Exchange 2010 documentation.

Configure the replication settings

Configure the replication settings for Quarantine database, Policy configurations, Engine, and DATs.

Task

- 1 From the **Start** menu, click **All Programs | McAfee | Security for Microsoft Exchange | Cluster Replication Setup**. A dialog box appears with various options to define for this service.



If the Mailbox role is installed in Microsoft Exchange Server 2010, 2013, and 2016, the service **Cluster Replication Setup** is automatically installed in all three types of setup: Typical, Complete, and Custom.

- 2 From **Server name**, retrieve the available servers for replication which are part of Data Availability Group and have MSME installed with Exchange Server in the mailbox role.
 - **Available server(s)** displays a list of servers that can be added for replicating the quarantine database, Policy configurations, Engine, and DATs.
 - **Replication server(s)** displays a list of servers that have been configured as replication servers for the quarantine database, Policy configurations, Engine, and DATs.
- 3 Select the server from **Available server(s)** and click >> to add it to the Replication servers list.
- 4 Select **Stop Replication service** to stop the MSME Cluster Replication service.
- 5 Select **Start Replication service for** to manage the MSME Cluster Replication service. Select appropriate options:
 - **Policy Configuration**
 - **Engine/DATs**
 - **Quarantine Database**
- 6 Click **Apply** to save and apply the cluster replication settings.
- 7 When prompted, select the option to restart the MSME service, which is required for the replication to work.

Configure McAfee Security for Microsoft Exchange Access Control

Allow or deny access to the MSME user interface for specific users or groups.

Task

- 1 From the **Start** menu, click **Programs | McAfee | Security for Microsoft Exchange | Access Control**. The **Permissions for Access** dialog box appears.

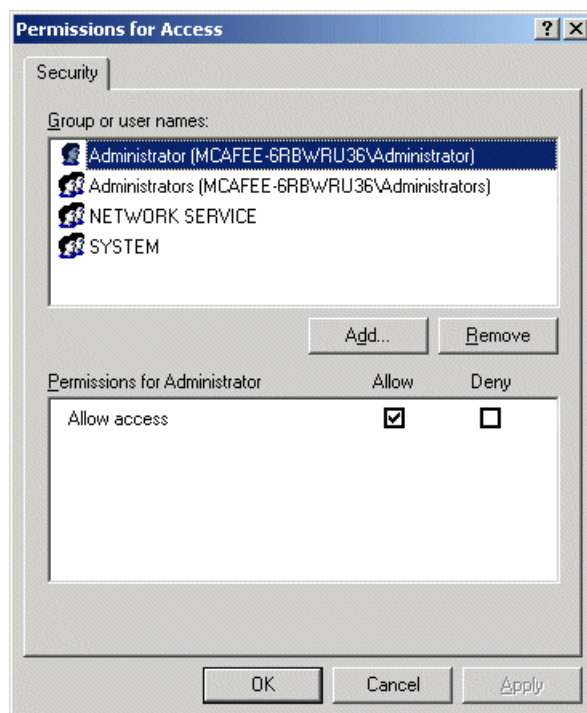


Figure 1-1 Permissions for Access

- 2 From **Group or user names**, select the user you want to allow or deny access to the MSME user interface.
- 3 Click **OK**.

SiteList Editor

SiteList specifies the location from where automatic updates (including DAT file and scanning engines) are downloaded.

Access SiteList Editor

- From the **Start** menu, click **Programs | McAfee | Security for Microsoft Exchange | SiteList Editor**.

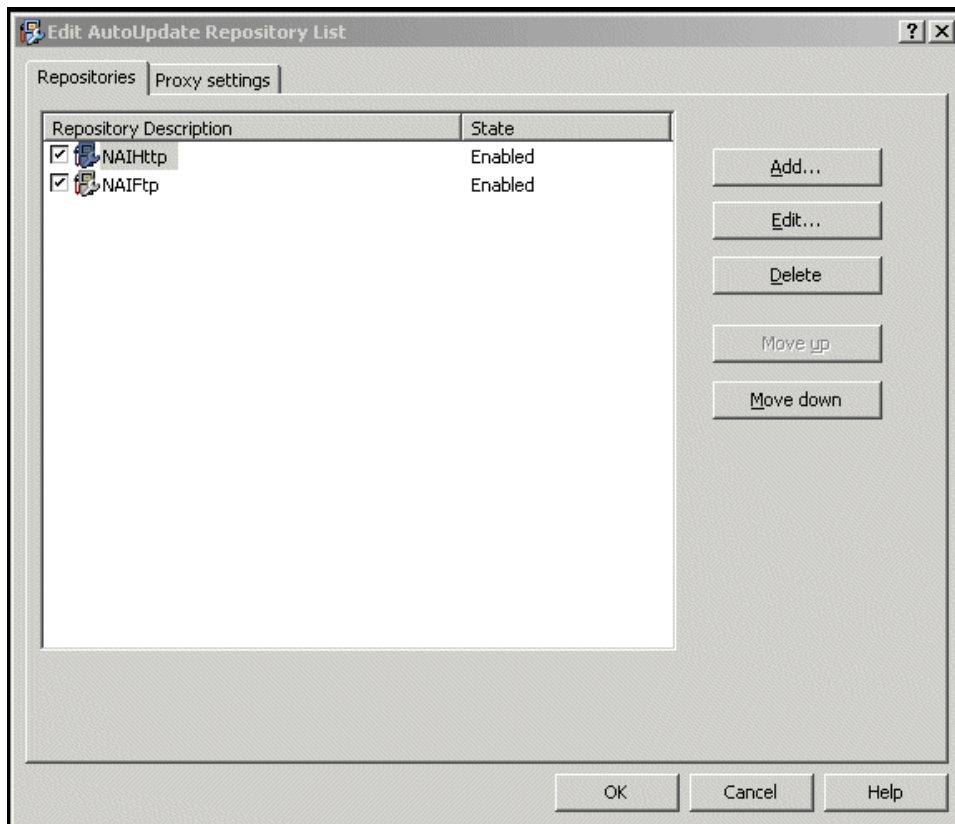


Figure 1-2 Edit AutoUpdate Repository List

You can use these tabs:

- **Repositories** — To configure repository settings from where MSME can download automatic updates. By default, MSME uses a sitelist that points to a McAfee site for automatic updates, but you can also create alternative sitelists that point to a different location. For example, you might have copied the automatic updates to a local repository and created a sitelist that points your MSME systems to that local repository.
- **Proxy settings** — To configure the proxy server settings, so that MSME can connect to the Internet using this server, to download automatic updates.



Settings applied in the SiteList Editor are saved in the `SiteList.xml` file under `C:\ProgramData\McAfee\Common Framework\` directory.

Configure sitelist repository settings

The **SiteList** specifies from where automatic updates are downloaded.

By default, McAfee Security for Microsoft Exchange uses a sitelist that points to a McAfee site for automatic updates, but you can use a sitelist that points to a different location. For example, you might have copied the automatic updates to a local repository and created a sitelist that points your McAfee Security for Microsoft Exchange systems to that local repository.

Task

- 1 Click **Start | Programs | McAfee | Security for Microsoft Exchange | SiteList Editor**. The **Edit AutoUpdate Repository List** dialog box appears.
- 2 From the **Repositories** tab, click **Add**. The **Repository Settings** dialog box appears.

Figure 1-3 Repository Settings

- 3 Select from the following options:
 - **Repository Description** — To give a brief description of the repository.
 - **Retrieve files from** — To specify from which type of repository to retrieve the files. The available options are **HTTP repository**, **FTP repository**, **UNC Path**, and **Local Path**.
 - **URL** — To specify the URL of the repository.
 - **Port** — To specify the port number of the repository.
 - **Use Authentication** — To enable user authentication to access the repository.
- 4 Specify a user name and password for authentication of the repository and confirm the password by typing it again.
- 5 Click **OK** to add the new repository to the **Repository Description** list.
- 6 Click **OK** to close the **Edit AutoUpdate Repository List** dialog box.

Configure sitelist proxy settings

Configure these settings if your organization uses a proxy server to connect to the Internet, for MSME to download the product updates.

If your organization uses proxy servers for connecting to the Internet, you can select the **Proxy settings** option.

Task

- 1 Click **Start | Programs | McAfee | Security for Microsoft Exchange | SiteList Editor**.

The **Edit AutoUpdate Repository List** dialog box appears.

- 2 Click the **Proxy settings** tab.

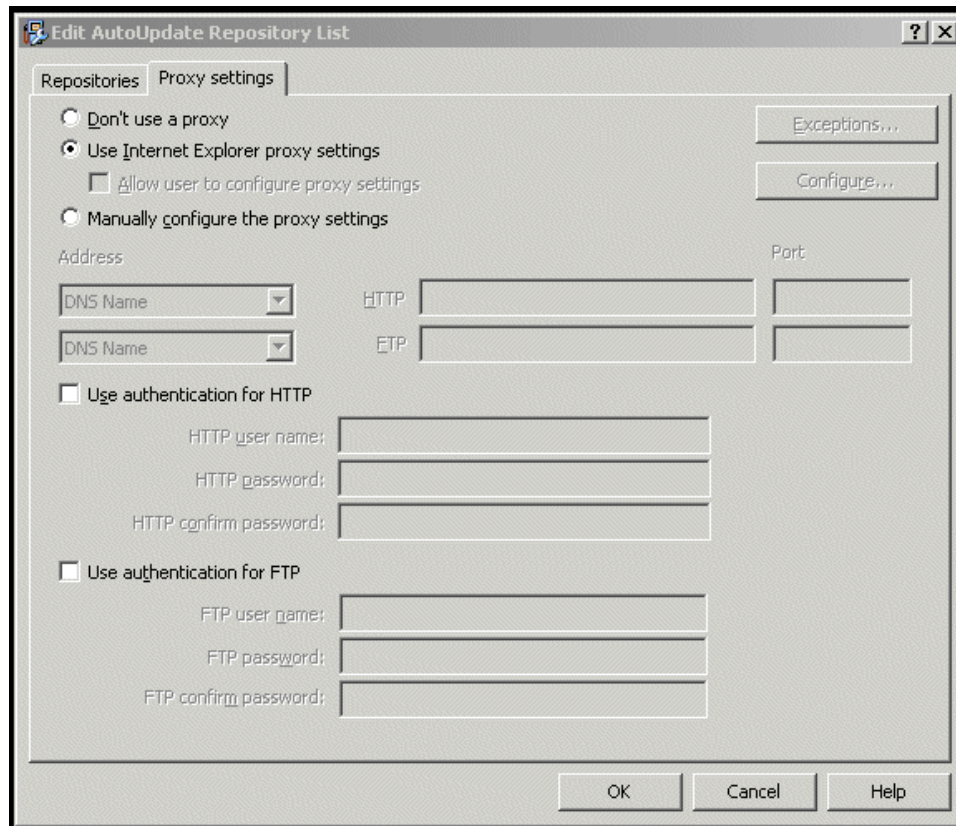


Figure 1-4 Proxy settings

- 3 Select the **Use Internet Explorer proxy settings** or **Manually configure the proxy settings** option as required.
- 4 Type the IP address and port number of the HTTP or FTP server.
- 5 You can use the following options:
 - **Use Authentication** — To enable user authentication to access the proxy server.
 - **Username** — To specify a user name for authentication to access the proxy server.
 - **Password** — To specify a password.
 - **Confirm Password** — To reconfirm the specified password.
 - **Exceptions** — To bypass a proxy server for specific domains. Click **Exceptions**, then select **Specify Exceptions** and type the domains that need to be bypassed.
- 6 Click **OK**.

Test your installation

When you have completed the installation of MSME, we recommend that you test it.

It makes sure that the software is installed properly and can detect viruses and spam within email messages.

Tasks

- [Test the anti-virus component on page 20](#)
Attach an EICAR anti-virus test file to an email message, then send the message through the Microsoft Exchange server where you've installed MSME.
- [Test the anti-spam component on page 21](#)
Run GTUBE (General Test mail for Unsolicited Bulk Email) to test the McAfee anti-spam software.
- [Test the installation using McAfee Virtual Technician on page 21](#)
McAfee Virtual Technician automatically checks for common deviations that might have occurred since you installed the product.

Installed components and services

MSME installs various components on your Microsoft Exchange server.

To access an MSME component, click **Start | Programs | McAfee | Security for Microsoft Exchange**, then click the component:

- **McAfee Anti-Spam for McAfee Security for Microsoft Exchange** — Detects spam and phishing content.
- **Access Control** — Allows or denies access to the MSME user interface for specific users or groups.
- **Product Configuration** — Launches MSME standalone version or through a web interface.
- **Sitelist Editor** — Specifies the location where automatic updates (including DATs and scanning engines) are downloaded from.
- **Cluster Replication Setup** — Replicates the quarantine database, policy configurations, and product updates (Microsoft Exchange Server 2010, 2013, and 2016 CU 2 only). This is dependent upon the replication setting across a **Data Availability Group (DAG)**, recognized by an MSME installation.

Services available

- **McAfee Agent Service, McAfee Agent Common Service, and McAfee Agent Backward Compatibility Service** — Prerequisite for installing and using McAfee ePO. For more details on this service, refer the McAfee ePO product documentation.
- **McAfee Security for Microsoft Exchange** — Protects your Microsoft Exchange Server (versions 2010, 2013, and 2016 CU 2) from viruses, unwanted content, potentially unwanted programs, and banned file types/ messages.
- **McAfee Anti-Spam rules updater** — Required to update the anti-spam rules.

Test the anti-virus component

Attach an EICAR anti-virus test file to an email message, then send the message through the Microsoft Exchange server where you've installed MSME.

Several anti-virus vendors throughout the world jointly created the EICAR standard anti-virus test file. It is a standard to verify anti-virus installations.



This file is not a virus. Make sure that you delete the file when you have finished testing your installation to avoid alarming users.

Task

- 1 Open a text editor, copy this code to notepad, then save the file with the name `EICAR.COM`:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

The file size is 68 bytes or 70 bytes.

- 2 Send an email message through the Microsoft Exchange server with the EICAR test file as an attachment.



When MSME examines the email message, it reports finding the EICAR test file. However, it cannot clean or repair the EICAR file because it is a test file.

- 3 MSME replaces the EICAR test file with an alert message.

Test the anti-spam component

Run GTUBE (General Test mail for Unsolicited Bulk Email) to test the McAfee anti-spam software.

The test email message must be sent from an external email account (a different domain).

Task

- 1 Create an email message.
- 2 Copy this code in the body text:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Make sure that you copy this text with no extra spaces or line breaks.

- 3 From an external email address, send this email message to a mailbox address on the server where you have installed MSME with McAfee Anti-Spam add-on component. McAfee Anti-Spam scans the message, recognizes it as a junk email message, and takes necessary actions.



The GTUBE test overrides blacklists and whitelists. For more information on the GTUBE test file, visit <http://spamassassin.apache.org/>.

Test the installation using McAfee Virtual Technician

McAfee Virtual Technician automatically checks for common deviations that might have occurred since you installed the product.

Run McAfee Virtual Technician to test whether MSME is installed correctly.

To download McAfee Virtual Technician, visit: <http://mvt.mcafee.com/mvt/index.asp>.

2

Repair the installation

Resolve installation errors in the program by fixing corrupt or missing files, shortcuts and registry entries.



You can also repair the MSME installation from **Control Panel | Programs and Features | Uninstall a program** console by clicking **Uninstall/Change**. Repairing an installation will revert to the default configuration settings.

Task

- 1 In the folder containing the installation files, double-click `setup_x64.exe`.
- 2 Click **Next**. The **Program Maintenance** screen appears.
- 3 From the **Program Maintenance** screen, select **Repair**, then click **Next**. The **Ready to Repair the program** screen appears.
- 4 Click **Install** to complete the repair. The **InstallShield Wizard Completed** dialog box appears.
- 5 Click **Finish** to exit.

3

Uninstall the software

Remove or uninstall MSME from the Exchange server.



You can also remove MSME from the **Control Panel | Programs and Features | Uninstall a program** console. In this method, the quarantine database is retained by default.

Task

- 1 In the folder containing the installation files, double-click `setup_x64.exe`.
The **Welcome** screen appears.
- 2 Click **Next**.
The **Program Maintenance** screen appears.
- 3 Select **Remove**, then click **Next**.
The **Preserve Settings** screen appears.
- 4 Select **Preserve quarantine database** to retain the quarantine database, then click **Next**.
The **Remove the program** screen appears.
- 5 Click **Remove** to uninstall MSME from your Exchange server.
The **InstallShield Wizard Completed** screen appears.
- 6 Click **Finish** to exit.

A

Frequently asked questions

Here are answers to frequently asked questions on MSME installation.

How do I perform a silent installation?

Execute the `Silent.bat` file in the download package. For information on customization, see the *Perform a silent installation*.

Can I Install McAfee Security for Microsoft Exchange 8.6 using the account that is not a domain administrator?

You can install. For more information, see McAfee KnowledgeBase article [KB82190](#).

What is the supported ePolicy Orchestrator version?

McAfee ePolicy Orchestrator 5.1.x, 5.3.x, and 5.9.x.

What is the supported McAfee Agent version?

McAfee Agent 5.0.5 build number 658.

On which port does the MSME configuration replication works?

This service doesn't work on ports, but it keeps monitoring the folders that are set by administrator using replication user interface.

Do I have to consider anything special while upgrading to MSME 8.6 from MSME 8.0 Patch 2 or 8.5 Patch 1 in the DAG environment?

No considerations. Follow the standalone installation steps.

Index

A

- access
 - SiteList Editor 17
- access control
 - configuring 16
- additional components 20
- anti-spam component 21
- anti-virus component 20

C

- configuration files 20
- configure
 - access control 16
 - sitelist proxy settings 19
 - sitelist repository settings 18
- contents, package 7

E

- EICAR test file 20
- exchange server
 - supported roles 7

F

- faqs
 - install 27

G

- GTUBE test file 21

I

- install
 - faqs 27
 - repairing 23
- installation
 - using wizard 8
- installed components 20

M

- McAfee Virtual Technician 21

P

- package contents 7
- pre-installation 5
- proxy settings
 - configuring sitelist 19

Q

- quick setup 14

R

- remove 25
- repair
 - installation 23
- repository settings
 - configuring sitelist 18
- requirements
 - system 6
- roles supported
 - exchange server 7

S

- services 20
- setup
 - quickly 14
- silent installation 11
- SiteList Editor
 - accessing 17
 - proxy settings 17
 - repository 17
- software
 - removing the 25
 - uninstalling the 25
 - upgrade 13
- system
 - requirements 6

T

- test the installation 21

U

- uninstall 25

