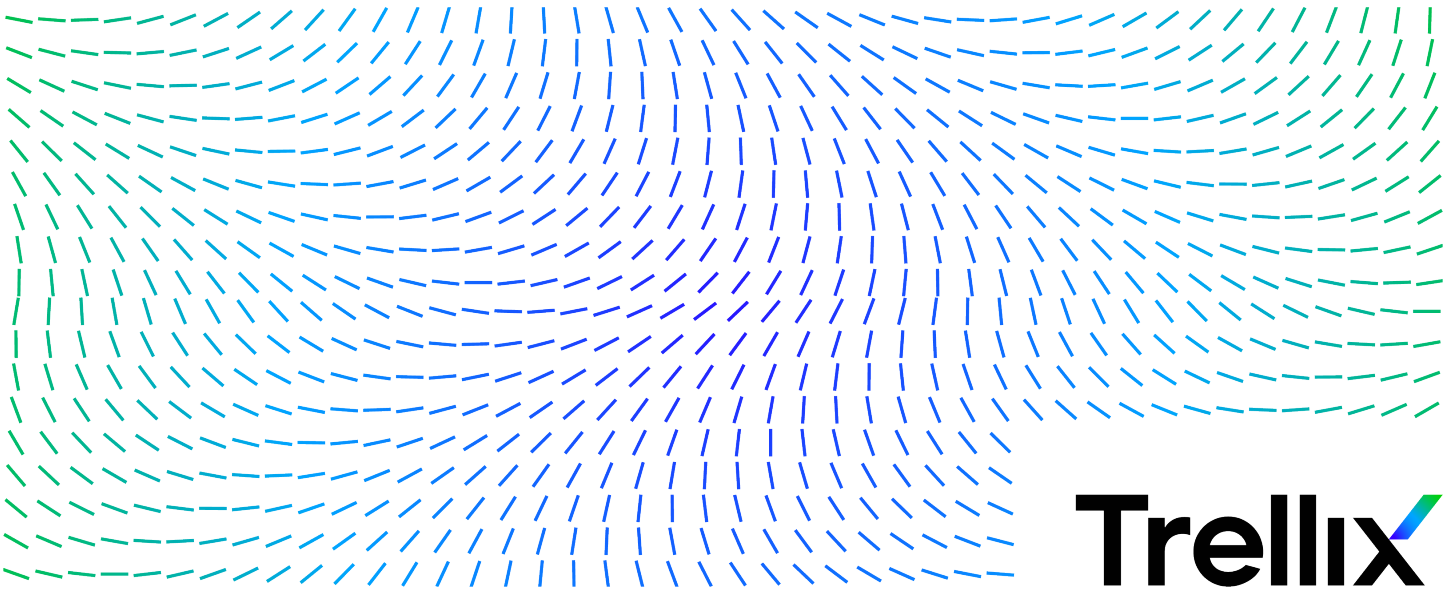
Trellix Security for Microsoft Exchange 8.8.1 Installation Guide



Contents

Installation Overview

Which type of installation do you need?

Install the TSME software, which best suits your environment.

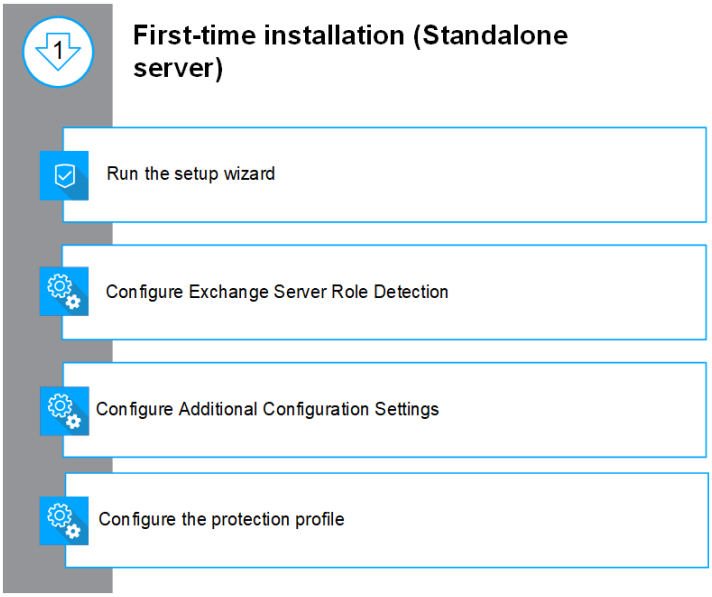
Installation type		Description
Standalone	**Wizard-based**	When using the wizard-based setup file, select one of these options as per your requirements: • **Typical** — Configure for all standard features. • **Custom** — Configure using the advanced options to customize your setup.
	Silent	Install the software without any user interaction or prompts. Modify and run the **Silent.bat** file that allows you to record selections for the installation process.
ePolicy Orchestrator-managed		Deploy TSME in ePolicy Orchestrator environment to allow centralized policy management and enforcement on your Microsoft Exchange Servers.

Note

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

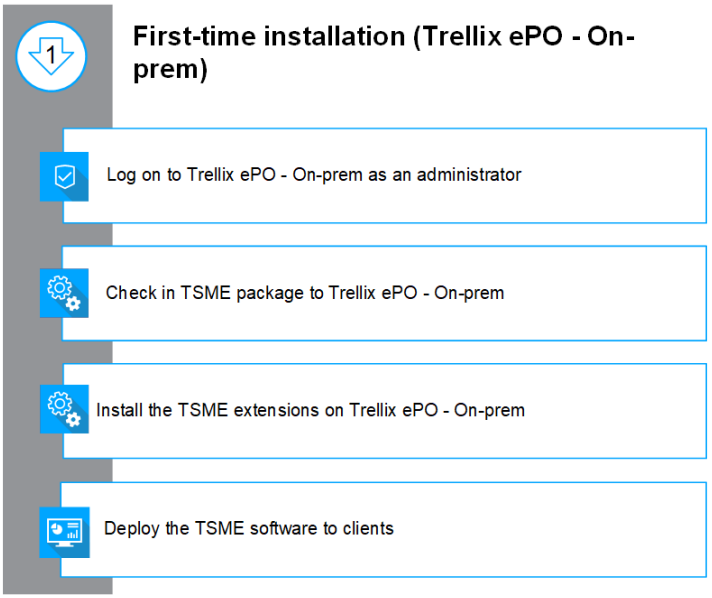
Installation workflow on standalone server

You can install the TSME software on a standalone server by following these workflow.



Installation workflow on Trellix ePO - On-prem

You can install TSME software on Trellix ePO - On-prem and deploy the software on client systems by following these steps.



System requirements

Hardware and software requirements

Make sure you meet these server requirements before installing the software.

Component	Requirement
Operating system	• Microsoft Windows 2012 Standard/Enterprise Server (64-bit) • Microsoft Windows 2012 Standard/Enterprise Server R2 (64-bit) • Microsoft Windows Server 2016 (64-bit) • Microsoft Windows Server 2019 (64-bit)
Browser	• Microsoft Internet Explorer version 11 • Mozilla Firefox 74.0 • Google Chrome 80 **Note:** Make sure that you disable the pop-up blocker in the browser settings.
Processor	• 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	**Note:** The memory requirement to install **TSME** is the same as Microsoft Exchange Server requirement. For more information, see the *Microsoft Exchange* website. Microsoft Exchange Server 2016 • Minimum — 8 GB RAM • Recommended — 16 GB RAM Microsoft Exchange Server 2019

Component	Requirement
	• Minimum — 8 GB RAM • Recommended — 16 GB RAM
Disk space	Minimum: Make sure you have 10 percent of free disk space, where **TSME** is getting installed.
Network	10/100/1000-Mbps Ethernet card
Screen resolution	1024 x 768
Trellix management software	**Trellix ePolicy Orchestrator - On-prem** 5.9.x and 5.10.x
Trellix Agent	**Trellix Agent** release build 5.7.2.162
Upgrade path	**Trellix Security for Microsoft Exchange** 8.6.x **Trellix Security for Microsoft Exchange** 8.7.x
IIS components	For information about IIS components requirements, see KB77319

Note

To view updated system requirements, see KB94547.

Supported Microsoft Exchange roles

The **TSME** 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 2013 CU23, 2016 CU20, and 2019 CU9
    - MBX Server — Holds the dual role of Mailbox with Hub.
    - Edge Transport Server.

Package contents

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

Unzip the **MSMEv88_x64.ZIP** archive, to find these directories.

Folder	Content
Standalone	Contains the files required to perform a standalone installation of the product: • **Setup_x64.exe** — Setup file to install the software using a wizard. • **Silent.bat** — Record file to install the software without any prompts or wizard.
ePO	Contains installation and configuration files required for managing the product using **ePolicy Orchestrator - On-prem**. • **MSME_*XXXX*** — Contains the product extensions for all locales in their respective locale folders. For example, **ePO_Extension_0409**. • **MSME_Deployment_x64_*xxxx*.zip** — Deployment package to deploy the software on the managed clients. • **MSMEePOUpgrade.zip** — Contains the executable file required to migrates policies from **TSME** 8.6.x to **TSME** 8.8 in an upgrade. • **MSME88REPORTS.zip** — Extension to add **TSME** reporting interface such as dashboards, queries.

Note

TSME installer includes **Trellix Agent** release build 5.7.2.162. The agent collects and sends information between the **ePolicy Orchestrator - On-prem** server and repositories, and manages installations across the network.

Installing the software on standalone servers

Install the software using setup wizard

Install the software on a system where Microsoft Exchange Server 2016 CU20 and 2019 CU9 is installed.

Task

1. **Log on to the system as an administrator, where Microsoft Exchange Server is installed.**
2. **Download the software package and extract it to the temporary directory you created.**
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. **Select an installation type, then click Next.**
    - **Typical** — Commonly used features are installed with Web-based Product Configuration.
    - **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**.
6. **Accept the terms in the license agreement, then click Next.**
7. **In the Additional Configuration Settings screen, complete these options, then click Next.**
    a. **Select Import existing configuration to import the TSME 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.**

    Note

    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. **Under Administrator Email address, type the email address to which all notifications, configuration reports, and status reports must be sent.**
8. **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 **Trellix Global Threat Intelligence** file and messaging reputation.
    - **Use existing** — (Upgrade only) This option uses the existing protection profile.
9. **Select Create Desktop shortcuts if you want the installation wizard to create shortcuts for the application on the desktop, then click Next.**

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

Note

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

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

Note

You might be prompted to provide the domain administrator credentials.

- **Launch Product User Interface** — To launch the **TSME** 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 **TSME** with the latest DAT files and engine updates.
- **Register at Trellix 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.

Note

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

Results

The **TSME** software is successfully installed on your system.

Install the software in silent mode

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.

Note

Silent.bat internally is called from the **TSME** 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 **TSME** sends notifications to this email address, when you enable **Send notification** option for policies.
AUTO_UPDATE	**1** or **0**	Enable or disable automatic updates: • 1 = enabled • 0 = disabled When enabled, the DAT and engine update happens immediately after the software installation. **Tip: Trellix** recommends that you enable the automatic update to make sure that the engine and DAT files are up to date.
INSTALL_DIR	***%SystemDrive%*\MSME**	Specify the installation path. For example, if you specify **C:\MSME**, a folder **TSME** is created in the C drive.
NEED_DESKTOP_SHORTCUT	**1** or **0**	Specify whether to create a desktop shortcut after successful installation: • 1 = yes • 0 = no The default value is 1.

Parameter	Value	Description
DB_PATH_CHANGED	`1` or `0`	Specify whether to change the Postgres database path: • 1 = yes • 0 = no **Note:** 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.
DATABASEDIR	*<New Postgres DB Location>*	Specify the new Postgres database location. For example, **C:\TestDB**.
QUARANTINE_MECHANISM	`1`	Specify the location for quarantined items: • 1 = **Local database** **Local database** — To quarantine detected items in the local system. **Note:** You can modify the settings from the software interface any time after the installation.
AGREE_TO_LICENSE	`Yes` or `No`	Agree to the license terms to install the software. For example, SET AGREE_TO_LICENSE = `Yes`.

TSME installation with case-sensitive installation path

The installation of **TSME** prevents, if the installation directory is configured to be case-sensitive.

To resolve this, ensure the installation directory are configured to be case-insensitive.

Upgrade the software on a standalone server

TSME 8.8 supports upgrading your configuration settings from the previous version 8.6.x or 8.7.x.

Before you begin

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

TSME provides enhanced security by not supporting the HTML tags that have XSS vulnerability. **Trellix** 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 **Trellix** 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. **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.**
3. **The Exchange Server Role Detection screen lists the roles selected during the Microsoft Exchange Server installation. Click Next.**
4. **In the Setup Type screen, the Custom option is selected by default. Click Next.**
5. **The Custom Setup screen lists the features installed in the existing installation. Select the features you want to be updated with Trellix Security for Microsoft Exchange, then click Next**
6. **Accept the terms in the license agreement, then click Next.**
7. **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.**
8. **In the Setup Protection Profile screen, select Default, Enhanced, or Use Existing, as necessary, then click Next.**

   Note

   If you selected the **Import existing configuration**, all options on this screen are grayed-out. The **Use Existing** option is selected by default.

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

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

    Note

    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.

11. **When the installation is complete, the Installation Wizard Completed screen appears with the Migrate Quarantine Data option selected by default. Click Finish.**

    Note

    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.

Results

The **Trellix Security for Microsoft Exchange** software is successfully upgraded.

Setting up your standalone Exchange environment

Post-installation

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

Quick setup

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

As an administrator, perform these tasks once you install TSME 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 TSME on an Edge Transport, make sure that TSME 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. **Update the administrator email address from Settings & Diagnostics → Notifications → Settings tab.**
4. **Schedule a status report task. For details, see the *Schedule a new status report* section.**
5. **Schedule a configuration report task. For details, see the *Schedule a new configuration report* section.**
6. **Schedule on-demand scans based on your requirement. For details, see the *On-Demand scan and its views* section.**
7. **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.**
8. **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.**
9. **For exceptions in a policy, create subpolicies based on your organization's requirement.**
10. **Send test email messages to verify the configuration.**

Cluster deployment

You need additional configurations to install TSME in cluster deployments of Microsoft Exchange Server 2016 CU20 and 2019 CU9.

Cluster replication utility for Microsoft Exchange 2016 CU20 and 2019 CU9

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 TSME installation that is recognized by a Data Availability Group (DAG), in which case the TSME 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.

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.**

   Note

   If the Mailbox role is installed in Microsoft Exchange Server 2016 CU20 and 2019 CU9, the service **Cluster Replication Setup** is automatically installed in all three types of setup: Typical and Custom.

2. **From Server name, retrieve the available servers for replication which are part of Data Availability Group and have TSME 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 TSME Cluster Replication service.**
5. **Select Start Replication service for to manage the TSME 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 TSME service, which is required for the replication to work.**

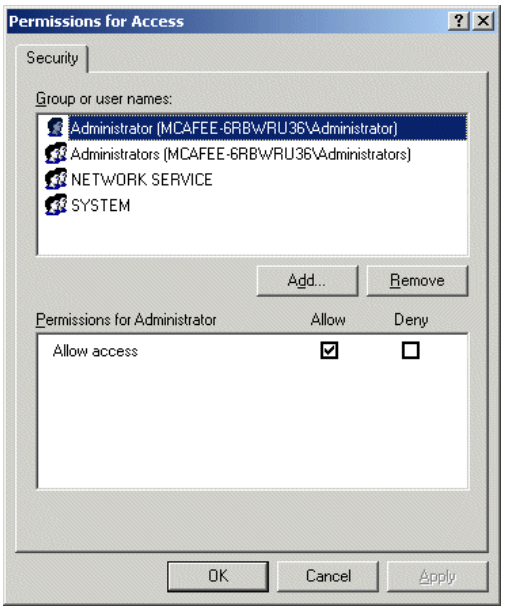
Configure Trellix Security for Microsoft Exchange Access Control

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

Task

1. **From the Start menu, click McAfee → Access Control. The Permissions for Access dialog box appears.**

Permissions for Access



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

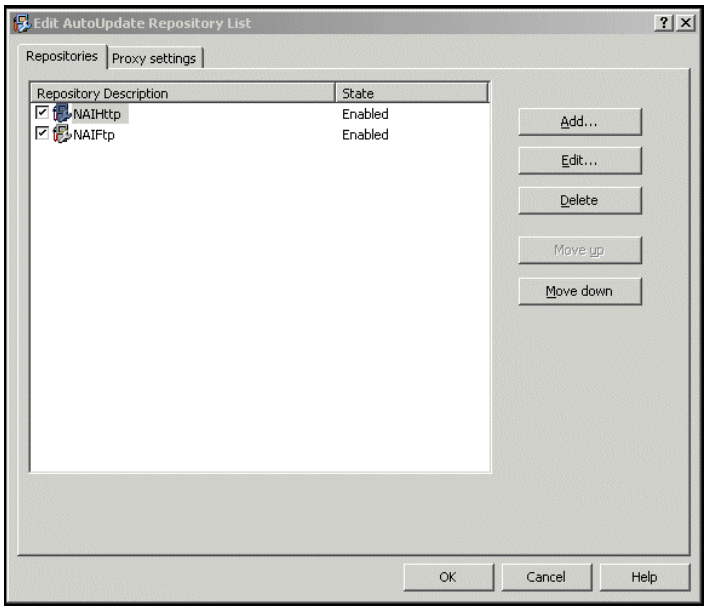
SiteList Editor

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

Access SiteList Editor

- From the **Start** menu, click **McAfee** → **SiteList Editor**.

Edit AutoUpdate Repository List



You can use these tabs:

- **Repositories** — To configure repository settings from where TSME can download automatic updates. By default, TSME uses a sitelist that points to a **Trellix** 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 TSME systems to that local repository.
- **Proxy settings** — To configure the proxy server settings, so that TSME can connect to the Internet using this server, to download automatic updates.

Note

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

Configure sitelist repository settings

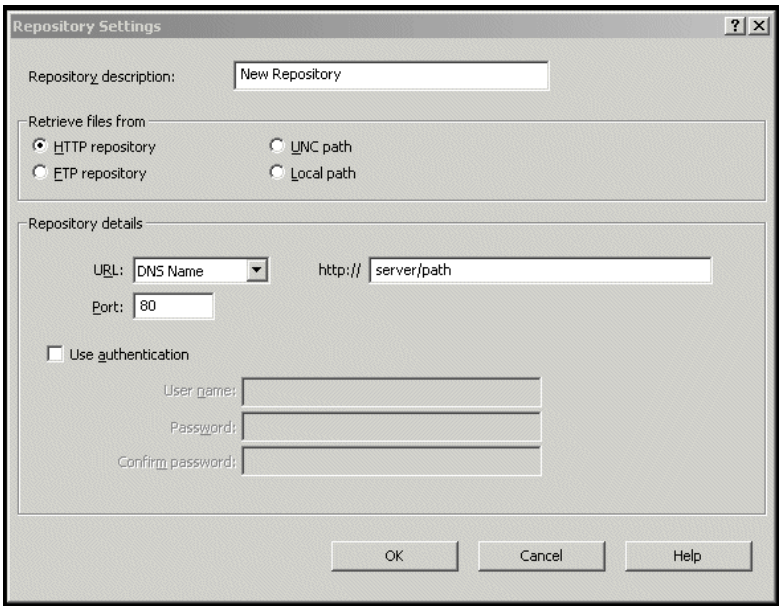
The **SiteList** specifies from where automatic updates are downloaded.

By default, **Trellix Security for Microsoft Exchange** uses a sitelist that points to a **Trellix** 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 **TSME** systems to that local repository.

Task

1. **Click Start → McAfee → SiteList Editor. The Edit AutoUpdate Repository List dialog box appears.**
2. **From the Repositories tab, click Add. The Repository Settings dialog box appears.**

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

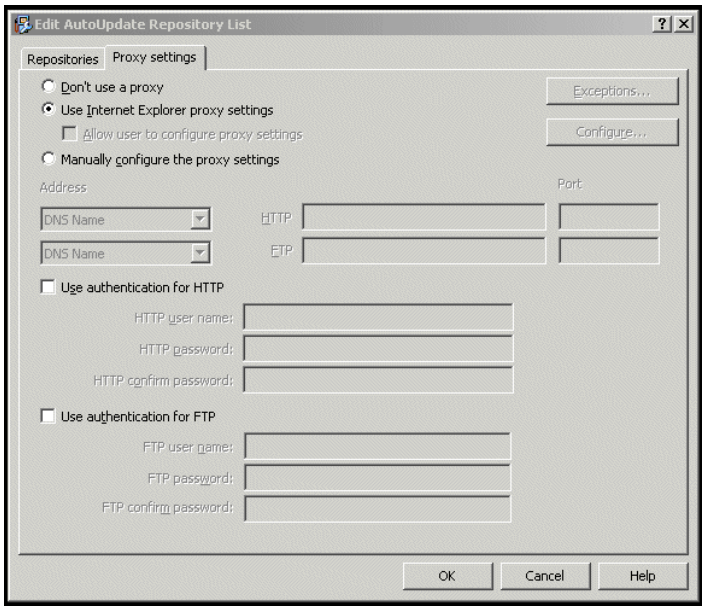
Configure these settings if your organization uses a proxy server to connect to the Internet, for TSME to download the product updates.

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

Task

1. **Click Start → McAfee → SiteList Editor.**
   The **Edit AutoUpdate Repository List** dialog box appears.
2. **Click the Proxy settings tab.**

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 TSME, we recommend that you test it.

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

Installed components and services

TSME installs various components on your Microsoft Exchange server.

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

- **Access Control** — Allows or denies access to the TSME user interface for specific users or groups.
- **Product Configuration** — Launches TSME 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 2016 CU20 and 2019 CU9 only). This is dependent upon the replication setting across a **Data Availability Group** (DAG), recognized by an TSME installation.

Services available

- **Trellix Agent Service, Trellix Agent Common Service, and Trellix Agent Backward Compatibility Service** — Prerequisite for installing and using **Trellix ePO - On-prem**. For more details on this service, refer the **Trellix ePO - On-prem** product documentation.
- **Trellix Security for Microsoft Exchange** — Protects your Microsoft Exchange Server (versions 2016 CU20 and 2019 CU9) from viruses, unwanted content, potentially unwanted programs, and banned file types/messages.

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 TSME.

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.

Note

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.**

   Note

   When TSME 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. **TSME replaces the EICAR test file with an alert message.**

Integrating TSME with Trellix ePO - On-prem

Integrate and manage **TSME** using **Trellix ePO - On-prem** management software.

Trellix ePO - On-prem 5.9.x and 5.10.x provides a scalable platform for centralized policy management and enforcement on your **Trellix** security products and systems on which they reside. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

For instructions about setting up and using **Trellix ePO - On-prem**, see the product guide for your version of the product.

Prerequisites for using the software with Trellix ePO - On-prem

Set up your environment before you integrate **TSME** with **Trellix ePO - On-prem**.

- Make sure that the system requirements are met.
- If a supported **Trellix Agent** is not installed on the client systems, install or upgrade your **Trellix Agent** release build 5.7.2.162. **Trellix Agent** is a component of **Trellix ePO - On-prem** that must be installed on each computer on the network and client computer. The agent collects and sends information between the **Trellix ePO - On-prem** server, repositories, and manages **TSME** installations across the network. See the **Trellix Agent** documentation for installation and deployment instructions.
- To use the TIE functionality:
    - **Trellix® Data Exchange Layer** 3.0 client software must be installed on client systems to allow communication between endpoints in a network. To install **Trellix Data Exchange Layer** client, *see **Trellix Data Exchange Layer** 3.0 Product Guide.*
    - The **Trellix ePO - On-prem** server that manages **TSME** must be connected to the **Trellix® Threat Intelligence Exchange (TIE)** server 2.0 or later. For information about configuring the **Threat Intelligence Exchange** server with **Trellix ePO - On-prem**, see the product guide of your version of **Trellix Data Exchange Layer** .

Check in the TSME package

Check in the **TSME** deployment package to the **Trellix ePO - On-prem** server.

Task

1. **Log on to Trellix ePO - On-prem server as an administrator.**
2. **Click Menu → Software → Master Repository.**
3. **On the Packages in Master Repository page, click Check in Package.**
4. **In the Package step, select Product or Update (.zip), click Browse and browse to the .zip file containing the TSME package (MSME_Deployment_x64_Lic.zip), then click Next.**
5. **In the Package Options step, select Current as the branch, then click Save.**

Install the TSME extension

Install the **TSME** extension on the **Trellix ePO - On-prem** server.

Note

When you already have a previous version of the software extension, this task adds the **TSME** 8.8 extension to the list. You can retain the previous extensions or remove them, as required.

Task

1. **Log on to the Trellix ePO - On-prem server as an administrator.**
2. **Click Menu → Software → Extensions, then click Install Extension.**
3. **Click Browse and browse to the .zip file containing the TSME extension (\MSMEv88_x64\ePO\ePO_Extension_EN\MSME___META_0409.zip for English), then click OK.**

Migrate policies from older versions

When you upgrade the software, migrate existing policies from older versions to **TSME** version 8.8.1.

Note

Ignore this task when you're performing a fresh installation.

Task

1. **Browse to the folder containing the MSME_ePOUpgrade.zip (\MSMEv88_x64\ePO), then extract it.**

   Note

   Make sure that all files in the .zip are extracted to the same folder.

2. **Go to the command prompt, navigate to the folder where the .zip file is extracted, and run the MSMEePOUpgrade.exe command.**
3. **Type the Trellix ePO - On-prem database password, then press Enter.**
4. **Type the Trellix ePO - On-prem SQL named instance if created during the server installation, otherwise leave it blank. Then press Enter.**
   The policy upgrade process starts. Wait for it to complete.

Results

On successful completion, a confirmation message appears. See **EPODebugTrace.txt** in the current directory for log details. Press **Enter** to exit.

Note

For more information on the policy upgrade tool, see **Trellix** Knowledge Base article KB76921 — *Using the TSME ePO Upgrade tool*.

What to do next

- Verify that the policies are upgraded: In the **Trellix ePO - On-prem** console, navigate to **Policy Catalog**, select the product as **Trellix Security for Microsoft Exchange 8.8.1**, then look for upgraded policies suffixed with **(Upgraded)**. For example, **My Default (Upgraded)**.
- Assign the custom policies to the required systems, otherwise the **Trellix** default policies are enforced.

Deploy the TSME software to clients

Deploy **TSME** to Microsoft Exchange systems.

Before you begin

Migrate existing policies from older versions to **TSME** 8.8.

TSME provides enhanced security by not supporting the HTML tags that have XSS vulnerability. **Trellix** 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 **Trellix** Knowledge Base article KB82214.

Note

When you already have a previous version of the software, this task upgrades the software on all managed Microsoft Exchange systems that you select.

Task

1. **Log on to the Trellix ePO - On-prem server as an administrator.**
2. **Click Menu → Systems → System Tree, then select the required group or systems.**

   Note

   When upgrading the software, make sure that you select all required systems.

3. **Click the Assigned Client Tasks tab, then click Actions → New Client Task Assignment. The Client Task Assignment Builder page appears.**
4. **Define these options, then click Create New Task.**
   a. **For Product, select Trellix Agent**
   b. **Task Type, select Product Deployment.**
5. **On the Client Task Catalog page, define these options:**
   a. **For Task Name, type a name for the task.**
   b. **Select Windows as a target platform.**
   c. **In Products and components, select Trellix Security for Microsoft Exchange (x64) - xxxxxxxx 8.8.1.xxxx, select Install as action, select the language, then click Save. The task is listed in the Task Name.**
6. **Select the task, then click Next.**

7. **Schedule the task to run immediately, then click Next to view a summary of the task.**
8. **Review the summary of the task, then click Save.**
9. **In the System Tree page, select the systems or groups where you assigned the task, then click Wake Up Agents.**
10. **In the Wake Up Trellix Agent screen, select Force complete policy and task update, then click OK.**

Results

On successful execution of this task, the **TSME** client software is deployed to the selected systems. For more information on deploying the software, see **Trellix** Knowledge Base article KB82484.

Remove the software

Remove the TSME client software and extensions to remove the software and its features.

To completely remove the TSME software and its features from your environment, remove them in this order:

1. Remove the TSME client software from the clients.
2. (If installed) Remove the TSME reporting extension.
3. Remove the TSME software extension from ePolicy Orchestrator.

Remove the client software

Create a client task to remove **TSME** client software from the managed Microsoft Exchange servers.

Task

1. **Log on to the ePolicy Orchestrator - On-prem server as an administrator.**
2. **Click Menu → Systems → System Tree, then select the required group or systems.**
3. **Click the Assigned Client Tasks tab, then click Actions → New Client Task Assignment. The Client Task Assignment Builder page appears.**
4. **Define these options, then click Create New Task.**
    a. **For Product, select Trellix Agent.**
    b. **For Task Type, select Product Deployment.**
5. **Type a name for the task, and any notes, then click Save. The task is listed in the Task Name.**
6. **On the Create New Task page, type a name for the task, and any notes:**
7. **Select Windows as a target platform.**
8. **In Products and components, select Trellix Security for Microsoft Exchange (x64) - xxxxxxxx 8.8.1.xxxx, select Remove as action, select the language, then click Save. The task is listed in the Task Name.**
9. **Select the task, then click Next.**
10. **Schedule the task to run immediately, then click Next to view a summary of the task.**
11. **Review the summary of the task, then click Save.**
12. **In the System Tree page, select the systems or groups where you assigned the task, then click Wake Up Agents.**
13. **In the Wake Up Trellix Agent screen, select Force complete policy and task update, then click OK.**

Remove the software extension

Remove the **TSME** extensions from the **ePolicy Orchestrator - On-prem** server.

Before you begin

If **TSME** reports extension is installed, remove it before removing the product extension.

Task

1. **Log on to the ePolicy Orchestrator - On-prem server as an administrator.**
2. **To remove the product extension, click Menu → Software → Extensions.**
3. **From the left pane, select Trellix Security for Microsoft Exchange.**
   The **TSME** extensions that are installed are displayed in the right pane.
4. **Click the Remove button next to the TSME extension, select Force removal, bypassing any checks or errors, then click OK.**
   Remove the reports extension **Trellix Security for Microsoft Exchange Reports 8.8** (**MSME88REPORTS.ZIP**) first. Then repeat this step to remove the product extension **Trellix Security for Microsoft Exchange 8.8** (**MSME___8800_0409.zip**).

TSME - Product maintenance

Repair the installation

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

Tip

You can also repair the TSME 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.**

Uninstall the software

Remove or uninstall TSME from the Exchange server.

Tip

You can also remove TSME 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 TSME from your Exchange server.**
   The **InstallShield Wizard Completed** screen appears.
6. **Click Finish to exit.**

Frequently asked questions

Here are answers to frequently asked questions on **TSME** 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 Trellix Security for Microsoft Exchange 8.8 using the account that is not a domain administrator?

You can install. For more information, see **Trellix** Knowledge Base article KB82190.

What is the supported ePolicy Orchestrator - On-prem version?

Trellix ePolicy Orchestrator - On-prem 5.9.x and 5.10.x.

What is the supported Trellix Agent version?

Trellix Agent release build 5.7.2.162.

On which port does the TSME 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 TSME 8.8 from TSME 8.6.x or 8.7.x in the DAG environment?

No considerations. Follow the standalone installation steps.

COPYRIGHT

Trellix