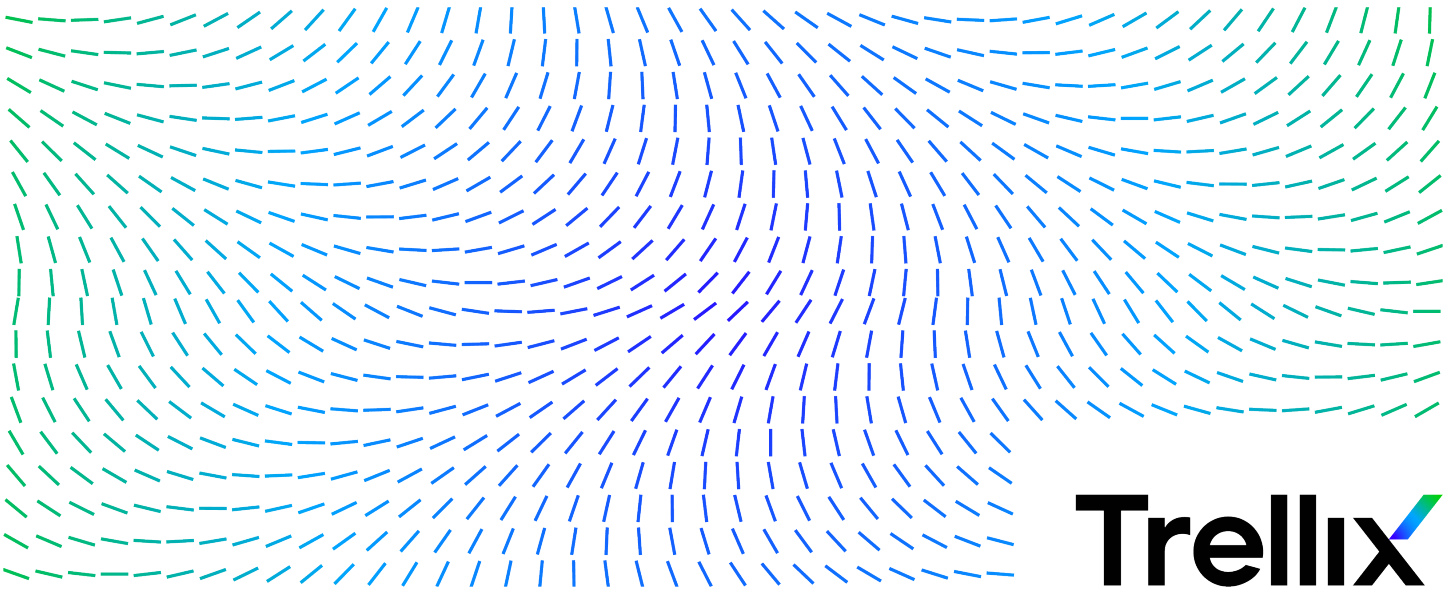
Trellix ePolicy Orchestrator - On-prem 5.10.0 Product Guide



Contents

Product overview

Overview

The **Trellix® ePolicy Orchestrator - On-prem** platform enables centralized policy management and enforcement for your endpoints and enterprise security products.

Trellix ePO - On-prem monitors and manages your network, detecting threats and protecting endpoints against these threats.

By using **Trellix ePO - On-prem**, you can perform many network and client tasks from a single console.

- Manage and enforce network and system security using policy assignments and client tasks.
- Monitor the health of your network.
- Collect data on events and alerts.
- Create reports using the query system builder, which displays configurable charts and tables of your network security data.
- Automate product deployments, patch installations, and security updates.

Key features

Trellix ePO - On-prem software provides flexible, automated management to identify and respond quickly to security issues and threats.

From the single view of **Trellix ePO - On-prem**, you can access managed clients, networks, data, and compliance solutions to protect your network.

Flexible security management

- Organize managed systems in groups to monitor, assign policies, and schedule tasks.
- Allow users access to specific groups of systems or give administrators full control.
- Open framework unifies security management for systems, applications, networks, data, and compliance solutions.
- Unify security management across endpoints, networks, data, and compliance solutions from **Trellix** and third-party solutions.
- Define how **Trellix ePO - On-prem** software directs alerts and security responses based on the type and criticality of security events in your environment.

Streamlined processes

- Guided Configuration, automated workflows, and predefined dashboards protect your network clients.
- Tag-based policies allow you to precisely assign predefined security profiles to systems based on their business role or at-risk status.
- Server Task Catalog and automated management capabilities streamline administrative processes and reduce overhead.
- Automated workflows between your security and information technology operations systems quickly remediate outstanding issues.

Large-scale deployments

- Architecture supports hundreds of thousands of devices on a single server, and complex and diverse environments.
- **Trellix ePO - On-prem** supports reporting across on-premises and cloud security information.

Unified view of your environment

- A single web interface aligns security processes for maximum visibility, while a single agent reduces the risk of endpoint conflicts.
- Drag-and-drop dashboards provide security intelligence across endpoints, data, mobile, and networks.
- Shorten response time through actionable dashboards with advanced queries and reports.
- **Rogue System Detection** identifies unknown assets on your network, and brings them under control.

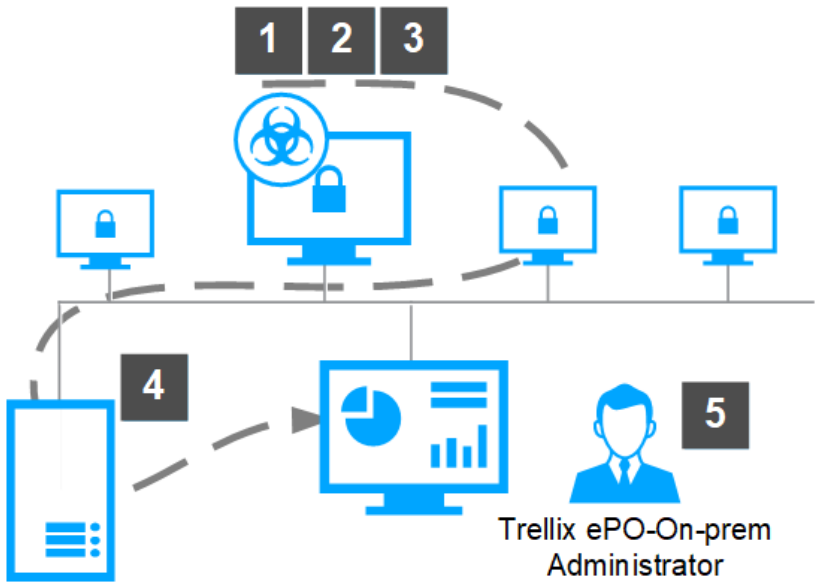
How it works

Trellix security software and **Trellix ePO - On-prem** work together to stop malware attacks on your systems and notify you when an attack occurs.

What happens during an attack

Trellix ePO - On-prem components and processes stop an attack, notify you when the attack occurs, and record the incident.

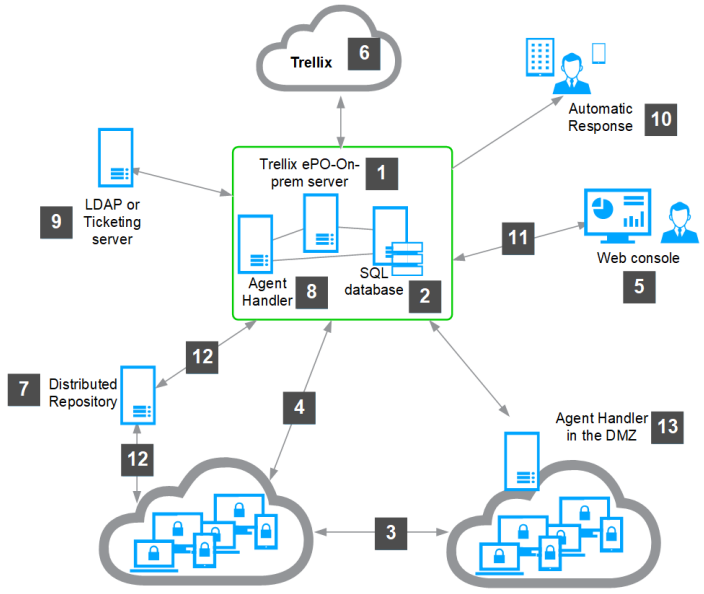
1. Malware attacks a computer in your **Trellix ePO - On-prem** managed network.
2. **Trellix** product software, for example **Trellix® Endpoint Security (ENS)**, cleans or deletes the malware file.
3. **Trellix Agent** notifies **Trellix ePO - On-prem** of the attack.
4. **Trellix ePO - On-prem** stores the attack information.
5. **Trellix ePO - On-prem** displays the notification of the attack on a **Number of Threat Events** dashboard and saves the history of the attack in the **Threat Event Log**.



Trellix ePO - On-prem components

The architecture helps you successfully manage and protect your environment, regardless of size.

1. **Trellix ePO - On-prem server**
    - Manages and deploys products, upgrades, and patches.
    - Connects to the **Trellix ePO - On-prem** update server to download the latest security content
    - Enforces policies on your endpoints
    - Collects events, product properties, and system properties from the managed endpoints and sends them back to **Trellix ePO - On-prem**
    - Reports on the security of your endpoint
2. **Microsoft SQL database** — Stores all data about your network-managed systems, **Trellix ePO - On-prem**, Agent Handlers, and repositories.
3. **Trellix Agent installed on clients** — Provides communication to the server for policy enforcement, product deployment and updates, and connections to send events, product, and system properties to the **Trellix ePO - On-prem** server.
4. **Agent-server secure communication (ASSC) connections** — Provides communications that occur at regular intervals between your endpoints and the server.
5. **Web console** — Allows administrators to log on to the **Trellix ePO - On-prem** console to perform security management tasks, such as running queries to report on security status or working with your managed software security policies.
6. **Trellix web server** — Hosts the latest security content so that your **Trellix ePO - On-prem** server can pull the content at scheduled intervals.
7. **Distributed repositories** — Hosts your security content locally throughout your network so that agents can receive updates more quickly.
8. **Agent Handlers** — Reduces the workload of the server by off-loading event processing and **Trellix Agent** connectivity duties.
9. **LDAP or Ticketing system** — Connects your **Trellix ePO - On-prem** server to your LDAP server or SNMP ticketing server.
10. **Automatic Responses** — Notifies administrators and task automation when an event occurs.
11. **Web Console connection** — Provides HTTPS connection between the **Trellix ePO - On-prem** server and the web browser using default port 8443.
12. **Distributed Repository connections** — Provides various connections to resources stored on Distributed Repositories in your network. For example, HTTP, FTP, or UDP connections.
13. **Agent Handler in DMZ** — Supports specific port connections to **Agent Handlers** installed in the DMZ allowing you to connect through a firewall.


Trellix
6
Automatic Response
10
Trellix ePO-On-prem server
1
LDAP or Ticketing server
9
Web console
5
11
Agent Handler
8
SQL database
2
12
7
Distributed Repository
4
Agent Handler in the DMZ
13
12
3

Using the ePolicy Orchestrator interface

Log on and log off

To access the **Trellix ePO - On-prem** software, enter your user name and password on the logon screen.

Before you begin

You must have an assigned user name and password before you can log on to **Trellix ePO - On-prem**.

When you connect to **Trellix ePO - On-prem**, the first screen you see is the **Trellix ePO - On-prem** logon screen.

Task

1. **Type your user name, password, and click Log On, or log on using your MVISION credentials.**
   Your **Trellix ePO - On-prem** software displays the default dashboard.
2. **To end your Trellix ePO - On-prem session, click Log Off.**

Results

Once you log off, your session is closed and cannot be opened by other users.

Edit Password page

Use this page to change the password that you use to log on to **Trellix ePO - On-prem**.

Trellix ePO - On-prem supports all printable characters in the ISO 8859-1 character set, except:

- Leading spaces, trailing spaces, or passwords consisting of only spaces.
- Double quotation marks (").
- Leading backslashes, trailing backslashes, or passwords consisting only of backslashes (\).

Option definitions

Option	Definition
Confirm password	Retype the password.
Password	Specifies the password you want to use for authentication. A maximum of 100 characters and a minimum of 1 character are allowed.

Navigating the interface

The **Trellix ePO - On-prem** interface uses menu-based navigation with a shortcut bar that you can customize to get where you want to go quickly.

Menu sections represent top-level features like Reporting, Systems, and Policy. As you add managed products to **Trellix ePO - On-prem**, the main menu options like Dashboards, System Tree, and Policy Catalog include new options to select.

Using the Trellix ePO - On-prem navigation menu

Open the **Trellix ePO - On-prem** menu to navigate the **Trellix ePO - On-prem** interface.

The menu uses categories that include features and functionality of **Trellix ePO - On-prem**. Each category contains a list of primary feature pages associated with a unique icon. Select a category in Menu to view and navigate to the primary pages that make up that feature.

Customizing the shortcut bar

Customize the shortcut bar for quick access to the features and functionality you use most often.

You can decide which icons are displayed on the shortcut bar by dragging any menu item on or off the shortcut bar.

When you place more icons on the shortcut bar than can be viewed, an overflow menu is created on the right side of the bar. Click the down-arrow to access the hidden menu items not displayed in the shortcut bar.

The icons displayed in the shortcut bar are stored as user preferences. Each user's customized shortcut bar is displayed regardless of which console they use to log on to the server.

A notification (bell) icon appears in the title bar, next to the user menu. Click the icon to view all notifications. Select a notification to navigate to the corresponding page.

A colored dot appears over the icon to indicate the level of importance.

- High—Red
- Medium—Yellow
- Low—Blue

Personal settings categories

Adjust personal settings to tailor your **Trellix ePO - On-prem** experience. Your customizations affect only your user sessions.

Category	Description
Password	Changes your **Trellix ePO - On-prem** logon password.

Category	Description
Queries and Reports Warning	Determines whether a warning message appears when you try to drag a query from one query group to another.
System Tree Warning	Determines whether a warning message appears when you try to drag systems or groups from one **System Tree** group to another.
Tables	Specifies how often auto-refreshed tables are refreshed during your session.
User Session	Controls the length of time that your user session remains open after you stop interacting with the user interface.

Option definitions

Option	Definition
Setting Categories	Lists the available settings that you can view and change. Selecting a category displays its current settings.
Search box	Highlights the category that matches the search text. Enter the first few characters of the category you want to find.
Edit	Allows you to change the current settings.

Server settings

Adjust server settings to fine-tune **Trellix ePO - On-prem** for the needs of your organization. Your customizations affect all your **Trellix ePO - On-prem** users.

For descriptions of the categories provided by managed products, see your managed product documentation.

Default server settings

Server settings category	Description
Active Directory Groups	Specifies the LDAP server to use for each domain.
Active Directory User Login	Specifies whether members of your mapped Active Directory (AD) groups can log on to your server using their AD credentials once the **Active Directory User Login** feature is fully configured.
Agent Contact Method	Specifies the priority of methods that **Trellix ePO - On-prem** uses when it tries to contact a **Trellix Agent**. To change the priority, select **Agent Contact Method** under **Setting Categories**, click **Edit**, then select the priority. Each contact method must have a different priority level. The methods to contact a **Trellix Agent** are: • **Fully Qualified Domain Name** • **NetBIOS name** • **IP Address**
Agent Deployment Credentials	Specifies whether users are allowed to cache agent deployment credentials.
Approvals	Allows you to choose whether a user needs approvals to make policy changes and client task changes.
Certificate Based Authentication	Specifies whether **Certificate Based Authentication** is enabled, and the settings and configurations required for the Certificate Authority (CA) certificate being used.
Dashboards	Specifies the default active dashboard that is assigned to new users' accounts at the time of account creation, and the default refresh rate (5 minutes) for dashboard monitors.

Server settings category	Description
Disaster Recovery	Enables and sets the keystore encryption passphrase for **Disaster Recovery**.
Email Server	• Specifies the email server that **Trellix ePO - On-prem** uses to send email messages. • Allows you to edit email server details.
Event Filtering	• Specifies which events the agent forwards. • Allows you to edit event filtering details that forwards to the server.
Event Notifications	• Specifies how often **Trellix ePO - On-prem** checks your notifications to see if any trigger **Automatic Responses**. • Allows you to edit event notifications details.
Extended Computer Properties	Specifies the maximum number of extended computer properties on the system details page.
Filter Criteria Setting	Allows you to enable/disable the display of query filter criteria in the exported PDF.
Global Updating	Specifies whether and how global updating is enabled.
License Key	Specifies the license key used to register this **Trellix ePO - On-prem** software.
Logon Message	Specifies whether a custom message is displayed when users log on to the **Trellix ePO - On-prem** console, and the message content.
Logon Protection	• Allows you to the invalid login attempts limit and restrict login by blocking source IP addresses or allowing only a few IP addresses.

Server settings category	Description
	• You can also monitor login attempts and manage IP addresses, manually or automatically.
Trellix ePO Server Public DNS	Specifies the **Trellix ePO - On-prem** Server Public DNS name.
Notifications	• Displays a warning dialog box when the policy\task deployment affects the endpoints more than the set limit. • Allows you to set the number of endpoints limit between 1-999,999,999.
Password Policy	Enables the password strength criteria with the minimum password requirements and limits the number of days before the password expires.
Policy and Task Retention	Specifies whether the policies and client task data is removed when you delete the product extension.
Ports	Specifies the ports used by the server when it communicates with agents and the database.
Printing and Exporting	Specifies how information is exported to other formats, and the template for PDF exports. It also specifies the default location where the exported files are stored.
Product Compatibility List	Specifies whether the **Product Compatibility List** is automatically downloaded and whether it displays any incompatible product extensions.
Product Improvement Program	Specifies whether **Trellix ePO - On-prem** can collect data proactively and periodically from the managed client systems.
Proxy Settings	Specifies the type of proxy settings configured for your **Trellix ePO - On-prem** server.

Server settings category	Description
Queries	• Specifies the maximum number of elements that can be displayed in the charts. Higher number of elements may affect query and chart performance. • Allows you to edit queries page.
Scheduler Tasks	Specifies the number of server tasks that run at the same time.
Security Keys	Specifies and manages the agent-server secure communication keys and repository keys.
Server Certificate	Specifies the server certificate that your **Trellix ePO - On-prem** server uses for HTTPS communication with browsers.
Server Information	Specifies Java, OpenSSL, and Apache server information, such as name, IP address, and version information.
Software Evaluation	Specifies the information required to enable check-in and deployment of evaluation software from the **Software Catalog**.
Source Sites	Specifies which source sites your server connects to for updates, and which sites are fallback sites.
System Details Settings	Specifies which queries and systems properties are displayed in the **System Details** page for your managed systems.
System Tree Sorting	Specifies whether and how **System Tree** sorting is enabled in your environment.
User Policies	Enables or disables database mirroring to improve performance for policy assignment rules.

Server settings category	Description
User Session	Specifies the amount of time a user can be inactive before the system logs them out.
Virtual MAC Vendors	Allows you to add virtual MAC vendor. You can also edit and delete existing vendors. For details, ***See Add Virtual MAC Vendor***.

Configure server settings

To familiarize yourself with configuring server settings, change the user session timeout interval from the default 30 minutes to 60 minutes.

By default when you are logged on to **Trellix ePO - On-prem**, if you don't use the interface for 30 minutes, the user session closes and you must log back on. Change the default setting to 60 minutes.

Task

1. **Select Menu → Configuration → Server Settings, select User Session from the Setting Categories, then click Edit.**
2. **Configure these settings, then click Save.**
    - **Default session timeout interval (minutes)** — Type `60` to replace the default.
    - **Maximum session timeout interval (minutes)** — Type `60` to replace the default.

Results

Now you aren't prompted to log on after only 30 minutes of inactivity.

Add Virtual MAC Vendor

This feature allows you to add the duplicated MAC address to the **Trellix ePO - On-prem** database and prevent it from matching the used MAC address to another system. Virtual machines are assigned a unique MAC (Media Access Control) address in a particular host system.

Task

1. **Click Menu → Configuration → Server Settings.**
2. **In the Server Settings page, click Virtual MAC Vendors in the Setting Categories pane.**
   You see a list of vendors and their respective ID.
3. **Click Edit.**
4. **In the Add New Virtual MAC Vendor area, enter a value in the Vendor ID field.**
   The Vendor ID must consist of six characters. It can be numeric (0–9), alphabetical (A to Z), or alphanumeric (combination of numbers and alphabets). A Vendor ID cannot have special characters.
5. **Enter the details in the Vendor Name/Note field.**

You can enter details such as the name of the organization, the reason to add the vendor, and you can also enter comments that you would like to add. This field does not accept these special characters:

- {
- }
- ;
- <
- >
- ?

6. **Click Add MAC Vendor to add more vendors.**
7. **Click Save.**

Results

Note

The vendor name and ID are added to the list of vendors.
You can also edit or delete existing Vendors.

Working with lists and tables

Use **Trellix ePO - On-prem** search and filter functions to sort lists of data.

Lists of data in **Trellix ePO - On-prem** can have hundreds or thousands of entries. Manually searching for specific entries in these lists can be hard without the **Quick Find** search filter.

Filter a list

Use filters to select specific rows in the lists of data in the **Trellix ePO - On-prem** interface.

Task

1. **From the bar at the top of a list, select the filter that you want to use to filter the list.**
   Only items that meet the filter criteria are displayed.
2. **Select the checkboxes next to the list items that you want to focus on, then select Show selected rows.**

Results

Only the selected rows are displayed.

Create a custom filter

Custom filters help you quickly sort through long lists of table entries, such as log items or server tasks, so you can focus on relevant information. The custom filters you create are added to the **Custom** filter drop-down at the top of your table, so you can reuse them later.

Task

1. **From the top of the table, select Custom → Add.**
2. **From the Available Properties list, click the properties you want to include in your filter.**
   The selected properties move the **Property** pane.

3. **For each property, select a comparison and a value.**
   The options you can select depend on the property you selected. Use the + or - signs to add or remove comparison and value pairs.
4. **Once all the properties that you selected are populated with valid and complete values, click Update Filter.**

Results

The new custom filter appears in the **Custom** drop-down list.

Search for specific list items

Use the **Quick Find** filter to find items in a large list.

Task

1. **Enter your search terms in the Quick Find field.**
2. **Click Apply.**

Results

Only items that contain the terms that you entered in the **Quick Find** field are displayed.

Tip

Click **Clear** to remove the filter and display all list items.

Example: Find detection queries

Here is an example of a valid search for a specific list of queries.

1. Select **Menu** → **Reporting** → **Queries & Reports**, then click **Query**. All queries that are available in **Trellix ePO - On-prem** appear in the list.
2. Limit the list to specific queries, for example, "detection." In the **Quick Find** field, type `detection`, then click **Apply**.

Note

Some lists contain items translated for your location. When communicating with users in other locales, remember that query names can differ.

Clicking table row checkboxes

The **Trellix ePO - On-prem** interface has special table row selection actions and shortcuts that allow you to select table row checkboxes using **click** or **Shift+click**.

Some output pages in the **Trellix ePO - On-prem** interface display a checkbox next to each list item in the table. These checkboxes allow you to select rows individually, as groups, or select all rows in the table.

Note

This table row selection action does not work in the **Audit Log** table.

This table lists the actions used to select table row checkboxes.

To select...	Action	Response
Individual rows	Click checkbox for individual rows.	Selects each individual row independently.
Group of rows	Click one checkbox, then hold **Shift** while you click the last checkbox in the group.	Selects all rows between and including the first and last rows that you clicked. **Caution:** Using **Shift+click** to select more than 1,500 rows in a table simultaneously might cause a spike in CPU utilization. This action might trigger an error message describing a script error.
All rows	Click the top checkbox in table headings.	Selects every row in the table.

Select the Columns to Display page

Use this page to choose the columns to display for the table on the selected page. Available columns of data depend on the table you are configuring.

Option definitions

Option	Definition
Available Columns	Available columns of data depend on the table you are configuring. Click the column titles or the icons next to them to move them to the **Selected Columns** list.

Option	Definition
Selected Columns	Shows the columns currently selected for display in the associated table. You can change or reorder the columns using the: • Delete icon (**x**) — Removes column from the selections. • Left arrow icon (**<**) — Moves column to the left. • Right arrow icon (**>**) — Moves column to the right.

Selecting items in tree lists

You can press **Ctrl+click** to select consecutive or non-consecutive items in tree lists.

Hierarchical tree lists, for example **System Tree** (Subgroups) and **Tag Group Tree** lists, let you select list items:

- Individually — Click an item.
- As a consecutive group — Press **Ctrl+click** and select the items sequentially.
- As a non-consecutive group — Press **Ctrl+click** and select each item individually.

Migrate to Trellix ePO - SaaS

Migrate to Trellix ePO - SaaS

Trellix ePO - SaaS is a multi-tenant, enterprise SaaS model of **Trellix ePO - On-prem**, accessible through an internet browser. You can migrate from your **Trellix ePO - On-prem** server to cloud using the **ePO - SaaS Migration** extension. This process allows you to manage your systems that are migrated to the cloud using **Trellix ePO - SaaS**.

Before you begin

Before you begin, make sure that these conditions are met.

- You have an active **Trellix ePO - SaaS** account.
- Your **Trellix ePO - On-prem** version is 5.3.1 or later.
- You have installed the **Trellix ePO - SaaS** Migration extension on your current **Trellix ePO - On-prem** server.
- The **Trellix ePO - On-prem** server has internet connectivity. If you're using a proxy server, make sure that you have configured the proxy server settings.
- The client systems can communicate with the **Trellix ePO - SaaS** server.
- The agent repository policies have proxy settings to connect to the **Trellix ePO - SaaS** server.
- You have configured the proxy and firewall settings to allow communication with the **Trellix ePO - SaaS** server. For more information, see KB90878.
- The **Trellix ePO - SaaS** tenant account that you're planning to link has an active subscription and administrator rights.
- You have identified inactive systems and excluded them from the migration process. Migration can't be complete if even one of the systems is not reachable.
- You have explored the available options in the **Settings** page and chose what is relevant to you.

Task

1. **Log on to Trellix ePO - On-prem and select Menu → ePO - SaaS → ePO - SaaS Migration.**
2. **Enter your Trellix ePO - SaaS credentials.**
3. **(If your email account is associated with multiple tenants...) Select a tenant account from the Select Tenant drop-down.**
   The **Select Tenant** drop-down appears only if the user account is configured for multiple tenants.
4. **Click Link to ePO - SaaS account.**
   You have successfully linked your **Trellix ePO - On-prem** to your **Trellix ePO - SaaS** account. The email ID used to log on is displayed in the left pane.
5. **Click Clone configuration to ePO - SaaS to copy the configurations.**

   You can see a list of systems that can be migrated, and a list of incompatible products that can't be migrated.

   Tip

   Plan to migrate your systems in multiple phases — A trial phase to migrate few systems, then one or more phases to migrate the remaining systems.

6. **Click Settings to customize the migration, then click Save.**

- **Migrate resources** — Select **Client Task**, **Policy**, **Tag**, and **Active Directory Configuration** to migrate them from your system to **Trellix ePO - SaaS**.
- **Delete Systems after Migration** — Select to delete the migrated systems on **Trellix ePO - On-prem** server after migrating to **Trellix ePO - SaaS**.
- **Auto Migrate newly added Systems** — Select to automatically migrate the newly added systems of a pre-migrated group.

The **Trellix ePO - On-prem** configurations such as policies, user-defined client tasks, and tags are copied to **Trellix ePO - SaaS**.

7. **Click Migrate active directory configurations to ePO - SaaS, then select active directories to initiate migration.**
   You can see the list of active directories configured under **Registered Servers**. You can select single or multiple active directories. If you don't want to migrate the active directories to **Trellix ePO - SaaS**, you can skip steps 7 to 10 by clicking **Skip This Step**.
8. **Select the type of system from the drop-down list, then search your system.**
   Type at least 3 characters to see the list of systems.
   - **All Systems**
   - **ePO - SaaS**
   - **On-Premises** (If you select an on-premises system, Active Directory migration will take some time because the system resources will migrate to **Trellix** in the next ASCI interval only.)
9. **Select the systems, click Save selected systems as AD connector then click Migrate AD configurations.**

   Note

   - The maximum number of systems you can select is 2.
   - The systems you select must have access to the domain to which you want to migrate them.
   - Active Directory connectors can be deployed on Windows systems only.

   Important

   The standard ASCI interval is 60 minutes. For Active Directory migration, set the ASCI interval short, preferably 5 minutes. For more information, see Configure the ASCI setting.

   The selected systems are migrated sequentially. Each Active Directory undergoes these 5 steps before successful migration.
   a. The selected systems (managed by **Trellix ePO - On-prem**) are migrated to **Trellix ePO - SaaS**.
   b. **Trellix Agent** and **DXL** on the selected systems upgrade to the latest version.
   c. The **DXL** connectivity of the selected systems is verified.
   d. The Active Directory connector package is deployed on the selected systems.
   e. Checks whether **Test Connection** for Active Directory passes.

   If one of the selected systems passes the **Test Connection** check, the Active Directory migration is considered successful.

10. **Click Migrate compatible systems to ePO - SaaS.**

11. **Select the groups that you want to migrate, then click Migrate Groups.**

    Note

    Choose a group of 10–25 systems as a pilot group to migrate from the current **Trellix ePO - On-prem** server to **Trellix ePO - SaaS**. This enables you to be aware of any issues that might occur before migrating all systems in System Tree.

    You can view the progress of migration in the **ePO - SaaS Migration** page.

    - All compatible systems in the selected group are tagged as **ePO - SaaS Migration**.
    - A deployment task **ePO - SaaS Migration** is created.
    - Three separate deployment packages for **Trellix ePO - SaaS** migration for Windows, Linux, and macOS are checked in to the Main Repository.

Results

Trellix ePO - SaaS starts to manage all migrated systems. Migration begins during the next agent-server communication, and systems start to communicate with **Trellix ePO - SaaS**.

What to do next

1. Log on to **Trellix ePO - SaaS** and verify if the selected systems appear in System Tree.
2. Verify if all policies appear as expected.
3. To see the list of systems in which the Active Directory Connector package is deployed and the details, go to **Menu** → **Configuration** → **Directory Service**.
4. Continue to migrate the remaining systems.

You can view information about your migrated systems using these queries that are included in the **Trellix ePO - SaaS** Migration extension.

- **Systems By migration status**
- **Table View of migrated systems**
- **Trend of Migrated systems**

Active Directory configuration migration actions and intervals

Active Directory configuration involves different actions. Each action has a timeout period. If the action is not complete within the timeout period, it is marked as failed.

Action	Timeout period	Interval between each stage
Client system migration from **Trellix ePO - On-prem** to **Trellix ePO - SaaS**.	90 min	30 sec
Trellix Agent upgrade	5 hrs	4 min

Action	Timeout period	Interval between each stage
DXL deployment/upgrade	30 min	30 sec
DXL connectivity	30 min	5 sec
Active Directory configuration deployment	60 min	5 min
Test Connection	30 times	1 min

Migrate to federal Trellix ePO - SaaS

Federal **Trellix ePO - SaaS** is a multi-tenant, enterprise SaaS model of **Trellix ePO - On-prem** hosted in federal cloud, accessible through an internet browser. You can migrate systems from the **Trellix ePO - On-prem** server to federal cloud using the **ePO - SaaS Migration** extension.

Before you begin

Before you begin, make sure that these conditions are met.

- You have an active federal **Trellix ePO - SaaS** account.
- Your **Trellix ePO - On-prem** version is 5.3.3 or later.
- You have installed the **Trellix ePO - SaaS** Migration extension 5.10.0.874 or later on your current **Trellix ePO - On-prem** server.
- The **Trellix ePO - On-prem** server has internet connectivity. If you're using a proxy server, make sure that you have configured the proxy server settings.
- The client systems can communicate with the **Trellix ePO - SaaS** server.
- The agent repository policies have proxy settings to connect to the federal **Trellix ePO - SaaS** server.
- You have configured the proxy and firewall settings to allow communication with the federal **Trellix ePO - SaaS** server. For more information, see KB90878.
- The federal **Trellix ePO - SaaS** tenant account that you're planning to link has an active subscription and administrator rights.
- You have identified inactive systems and excluded them from the migration process. Migration can't be complete if even one of the systems is not reachable.
- You have installed **Trellix Agent** 5.6.0.702.1 or later on the client systems.

Note

The most current supported version of **Trellix Agent** is 5.6.4.249. If you are migrating systems that have **Trellix Agent** versions higher than 5.6.4.249, the systems appear as noncompliant in Protection Workspace.

- You have excluded systems that have products other than **Trellix Agent** and **Trellix ENS** installed from the migration process. Federal **Trellix ePO - SaaS** currently supports **Trellix Agent** and **Trellix ENS** only.

Task

1. **Connect to the Trellix ePO - On-prem server database.**
2. **Run these SQL commands.**

```
Select * FROM OrionServerPropertiesMT WHERE [Key] IN ( 'iam.url' , 'iam.client.id' , 'MVision.url',
'tps.url','uam.url');

IF EXISTS (SELECT * FROM OrionServerPropertiesMT where [Key]='iam.url')
   UPDATE [OrionServerPropertiesMT] SET [Value] = 'https://api.iam.mcafee-gov.com/iam/v1.0/token'
where [Key]='iam.url'

IF EXISTS (SELECT * FROM OrionServerPropertiesMT where [Key]='iam.client.id')
                        UPDATE [OrionServerPropertiesMT] SET [Value] = 'efb532b4d8e914c2619d' where
[Key]='iam.client.id'

IF EXISTS (SELECT * FROM OrionServerPropertiesMT where [Key]='tps.url')
   UPDATE [OrionServerPropertiesMT] SET [Value] = 'https://tps.epo.mcafee-gov.com/govprod' where
[Key]='tps.url'

IF EXISTS (SELECT * FROM OrionServerPropertiesMT where [Key]='uam.url')
   UPDATE [OrionServerPropertiesMT] SET [Value] = 'https://api.uam.mcafee-gov.com/govprod/api/v1'
where [Key]='uam.url'

IF NOT EXISTS (SELECT * FROM OrionServerPropertiesMT where [Key]='MVision.url')
   INSERT INTO [OrionServerPropertiesMT] ([Key], [Value], [TenantId]) VALUES ('MVision.url', 'https://
ui.gov001.epo.mcafee-gov.com/', 1)
   ELSE
   UPDATE [OrionServerPropertiesMT] SET [Value] = 'https://ui.gov001.epo.mcafee-gov.com/' where
[Key]='MVision.url'

Select * FROM OrionServerPropertiesMT WHERE [Key] IN ( 'iam.url' , 'iam.client.id' , 'MVision.url',
'tps.url','uam.url');
```

3. **Reload the Trellix ePO - SaaS Migration extension by running the remote command — https://<epo server IP or fqdn>:8443/remote/core.reload-plugin?name=MVISIONClientMigration.**
4. **Log off and log on again to Trellix ePO - On-prem.**
5. **Migrate your systems from Trellix ePO - On-prem — Migrate to Trellix ePO - SaaS.**

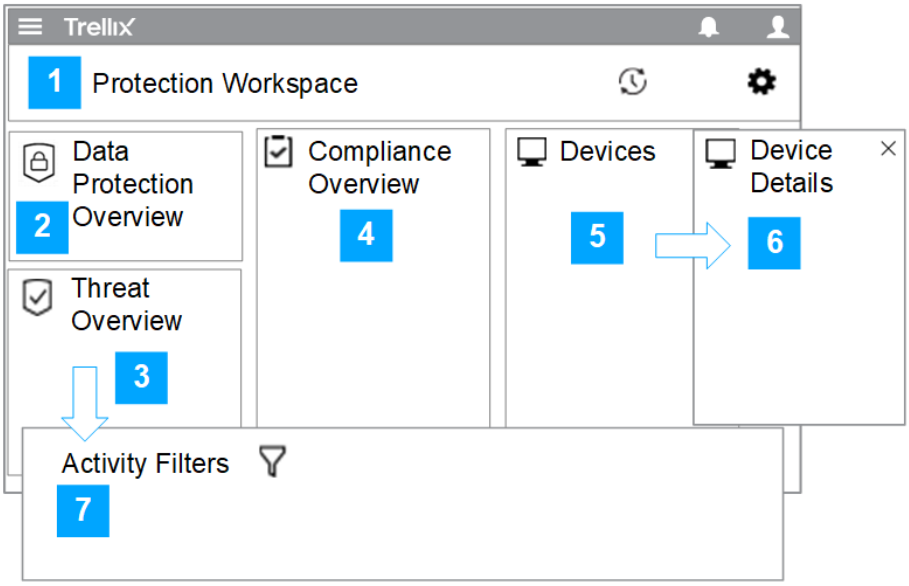
Tip

Plan to migrate your systems in multiple phases — A trial phase to migrate few systems, then one or more phases to migrate the remaining systems.

Protection Workspace

Protection Workspace Overview

Protection Workspace provides a visual representation of threat incidents in your environment and device compliance data on a single dashboard.



1. **Protection Workspace** — View the total number of devices tracked by the **Trellix ePO - On-prem** server, and the total number of devices that are tagged as escalated. View the number of devices that have communicated with **Trellix ePO - On-prem** at least once. Systems that have never communicated with **Trellix ePO - On-prem** are not included in the count.

   Important

   The systems that never communicated with **Trellix ePO - On-prem** appear in the System Tree and not in the Protection Workspace.

2. **Threat Overview** — View threat information across multiple categories. View the number of escalated devices to track devices that have encountered multiple threats and might require attention. Devices are escalated automatically if the number of threat events received in the last 24 hours is more than 5. Select any value to see a more detailed view of the categories.

3. **Compliance Overview** — View the status of security content and the individual products deployed in the environment. Devices are color-coded to indicate the security status (health) of the device. You can easily identify the systems that are up to date, or require an update or product deployment.
4. **Devices** — The **Devices** view changes depending on the device summary you select. View all escalated devices by **Escalations** (default view). Click the list icon to view the list of devices, folder icon for System Tree view and tag icon to view the devices by tags. Use the search feature to quickly find a device.
5. **Device Details** — Drill down to view the device details and the top 5 threats.
6. **Activity Filters** — Drill down to filter and view your threat activity. For example, you can filter by device, threat, or originating process.

Using Protection Workspace to identify and remediate threats

You can see all potential threats on managed devices and respond to them using Protection Workspace. You can identify threats and navigate seamlessly to any impacted device for remediation.

Protection Workspace helps you answer these questions:

- **What** threats are discovered by advanced threat protection technologies from products like **Trellix® Endpoint** and **Trellix® Endpoint Security (ENS) Adaptive Threat Protection (ATP)**?
- **Why** is a device escalated?
- **Where** did the threat come from?
- **When** was the threat discovered?

Minimum permissions needed to view Protection Workspace in the Trellix ePO - On-prem console

Non-admin users require some minimum permissions to view the Protection Workspace in the **Trellix ePO - On-prem** console.

Make sure that you have these user permissions in the **Permission Sets** page.

Category	Permission
Systems:	View "Systems Tree" tab
System Tree access:	Can search the following nodes and parts of the System Tree: My Organization Can access the following nodes and parts of the System Tree: My Organization
Threat Event log:	View events

Additionally, you need product and event-specific permissions to view threat and compliance data in Protection Workspace.

Identifying threats and the security status of your devices

The security status of your device is color coded to efficiently prioritize threats and take action.

- **Red** — A threat was discovered, or your software or device is running outdated versions and must be updated to be compliant.
- **Yellow** — There are threats to investigate or some devices are not up to date.
- **Green** — The current state of your environment is healthy, threats have been mitigated, and devices are compliant.
- **Light blue** — Information only. No action needed.
- **Gray** — No data available.

Threat event workflow

Protection Workspace provides a snapshot of your network's security status, allowing you to view key threats so you can investigate and determine a response.

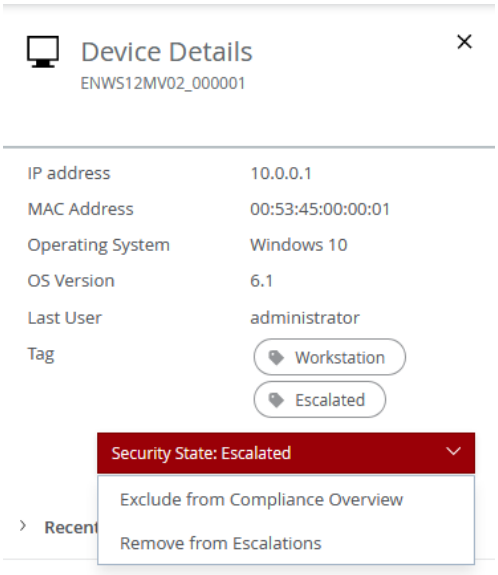
1. Protection Workspace displays key threat events and device compliance across **Trellix** products.
2. The security administrator quickly urgent events and escalated devices.
3. The security team investigates the escalated devices to determine a response.

Apply Protection Workspace tags to systems

Tag devices (systems) to escalate or exclude them from a compliance check.

Task

1. **In the Protection Workspace, select a device from the tag, tree, or list view.**
   The **Device Details** pane opens.
2. **From the Security State drop-down list, select a tag.**



3. **Click Confirm.**

Navigating Protection Workspace console

The Protection Workspace provides a visual representation of threat incidents in your environment and device compliance data, all from a single dashboard using several panes. You can quickly identify threats detected in the environment and seamlessly navigate to any impacted device to remediate the threat.

Protection Workspace

The Protection Workspace bar displays these details.

Item	Description
Devices	Total number of devices tracked by the **Trellix ePO - On-prem** server. Systems that have never communicated with **Trellix ePO - On-prem** are not included in the count.
Escalations	Total number of devices that are tagged as escalated. Select a device to view **Escalated Devices**. System is escalated if more than 5 threats are detected in 24 hours.
Update	Data on the back-end is automatically refreshed every 60 seconds, and the interface is automatically refreshed every 5 minutes. Click refresh to manually

Item	Description
	redisplay the Protection Workspace with the latest updates.
Settings	Use to adjust the **Security Content Color Thresholds** and **Check-In Failure Color Thresholds** to customize the security levels for your environment.

Threat Overview

The **Threat Overview** pane displays these details.

Item	Description
Escalated Devices	Total number of devices that received a threat over the past 7 days. System is escalated if 5 or more threats are detected in 24 hours.
Resolved Threats	Total number of threats that were resolved in the past 7 days. **Basic** — Detected by products like **Trellix® Endpoint Security (ENS) Threat Prevention**, and Microsoft Windows Defender. **Advanced** — Detected by products with advanced detection techniques like **Trellix® Endpoint** and **Trellix® Endpoint Security (ENS) Adaptive Threat Protection (ATP)**.
Unresolved Threats	Total daily count of unresolved threats. Arrow indicates the trend over the past 7 days.
Report Only Detections	Total and daily counts of report-only detections over the past 7 days. Arrow indicates the trend. Select the value to open the details for total or daily threat events.
Encryption Events	Total number of encryption events with critical and major severity over the past 7 days. Arrow indicates the trend. Select the value to open the details for total or daily threat events.

Activity Filters

From the **Threat Overview** pane, you can drill down to view the device details and the top 5 threats. Select a threat to open the **Threat Details** pane, and view details about the threat.

Threat Details

The **Threat Details** pane displays the details of the selected threat.

Item	Description
Threat Details	Displays these basic information about the selected threat event. • **Name** • **File Name** • **Analyzer Detection Method** • **Reporting Product Name** • **First seen in network** • **Last seen in network** • **Prevalence** • **Age**
Advanced Details	Displays the in-depth information about the selected threat event. • **Agent GUID** • **Event Generated Time** • **Event Category** • **Event ID** • **Threat Severity** • **Threat Type** • **Action Taken** • **Threat Target Host Name** • **Threat Source Process Name** • **Event Description**
Affected Devices	Displays the list of devices affected by the selected event.
Story Graph (Trace Summary)	Displays the trace summary for the selected event.

Compliance Overview

The **Compliance Overview** pane displays these details.

Item	Description
Security Content	Status of the security content in the environment. Here's how the compliance status is calculated for these items: **Trellix Endpoint Security (ENS)** AMCore — Number of systems with AMCore content compliant or noncompliant. • **Compliant** — The AMCore content creation date is less than 7 days old. • **Non-Compliant** — The AMCore content creation date is more than 7 days old. **Trellix Endpoint Security (ENS)** Exploit Prevention — Number of systems with Exploit Prevention content compliant or noncompliant. • **Compliant** — Enabled state in policy matches the enabled state on client system. • **Non-Compliant** — Enabled state in policy doesn't match the enabled state on client system. **Trellix** DAT — An endpoint is considered compliant if the **DAT Date** is within 7 days from today. For example, if today is July 19, endpoints with a DAT date of July 13 or later are compliant. Microsoft Windows Defender — An endpoint is considered compliant if the **Anti-Virus Signature Last Updated** date is within 7 days from today. For example, if today is July 19, endpoints with a DAT date of July 13 or later are compliant. For **Trellix** DAT and Microsoft Windows Defender, the endpoint reports the date, which can be viewed on the **Products** tab of the **System Information** page.
Software Status	Status of the individual products deployed in the environment. For example, **Trellix Endpoint Security (ENS)**, **Trellix Agent**, and **Trellix Endpoint**. The devices are color-coded to indicate the health of the security status (health) of the device.

Item	Description
Device Management	**Check-in Failure** indicates the number of devices that haven't checked in to the **Trellix ePO - On-prem** server for more than 15 days. **Managed Devices without Protection** indicates the number of devices that don't have these antimalware products installed: **Trellix Endpoint**. **Managed Devices** indicates the total number of managed devices over the past 7 days. View the number of devices that have communicated with **Trellix ePO - On-prem** at least once. Systems that have never communicated with **Trellix ePO - On-prem** are not included in the count. **Important:** The systems that never communicated with **Trellix ePO - On-prem** appear in the System Tree and not in the Protection Workspace.

Devices

The information that appears in the **Devices** pane changes depending on the category you select:

- **Devices**
- **Escalations** (default view)

You can view your devices by tags, by System Tree view, or as a list. Use the search feature to quickly find a device.

Important

The systems that never communicated with **Trellix ePO - On-prem** appear in the System Tree and not in Protection Workspace.

Device Details

From the **Devices** pane, you can drill down to view the device details and the top 5 threats. Select a threat under **Recent Threat Events** to open the **Threat Details** pane, and view details about a specific threat.

Dashboards and monitors

Dashboards help you keep constant watch on your environment.

Dashboards are collections of monitors. Monitors condense information about your environment into easily understood graphs and charts.

Usually, related monitors are grouped on a specific dashboard. For example, the **Threat Events** dashboard contains four monitors that display information about threats to your network.

Note

You must have the right permissions to view or modify dashboards and monitors.

Using dashboards and monitors

Customize your dashboards and monitors to get the information you need for your role and environment.

Dashboards are collections of monitors. Monitors condense information about your environment into easily understood graphs and charts. Usually, related monitors are grouped on a specific dashboard. For example, the **Threat Events** dashboard contains four monitors that display information about threats to your network.

If you have deleted all default dashboards, when you start **Trellix ePO - On-prem**, this text appears in the middle of the dashboards page: **No dashboards are configured. Create a new dashboard or import an existing dashboard.**

You can switch dashboards by selecting a different dashboard from the drop-down list. There are three different kinds of dashboards you can choose from.

- **Trellix Dashboards** — **Trellix** dashboards are not editable, and can be viewed by all users. You can duplicate a **Trellix Dashboard** as a starting point for your own customized dashboards.
- **Public Dashboards** — Public dashboards are user-created dashboards that are shared across users.
- **Private Dashboards** — These are the dashboards you have created for your own use. Private dashboards are not shared across users.

When you create a private or public dashboard, you can drag and drop the monitors you want from the **Monitor Gallery** to the new dashboard.

Manage dashboards

Create, edit, duplicate, delete, and assign permissions to dashboards.

Before you begin

You must have the correct permissions to modify a dashboard.

The default dashboards and predefined queries, shipped with **Trellix ePO - On-prem**, can't be modified or deleted. To change them, duplicate, rename, and modify the renamed dashboard or query.

Task

1. **Select Menu → Reporting → Dashboards, to navigate to the Dashboards page.**
2. **Select one of these actions.**

Action	Steps
Create a dashboard	To create a different view on your environment, create a new dashboard. 1. Click **Dashboard Actions → New**. 2. Type a name, select a dashboard visibility option, and click **OK**. A new blank dashboard is displayed. You can add monitors to the new dashboard as needed.
Edit and assign permissions to a dashboard	Dashboards are only visible to users with proper permission. Dashboards are assigned permissions identically to queries or reports. They can either be entirely private, entirely public, or shared with one or more permission sets. a. Select a dashboard, then click **Dashboard Actions → Edit**. b. Select a permission: • **Private** — Do not share this dashboard • **Public** — Share this dashboard with everyone **Note:** Users with Dashboards permissions can edit or delete public dashboards. If dashboards are used my multiple users, it might affect the user experience. • **Shared** — Share this dashboard with the following permission sets With this option, you must also choose one or more permission sets. c. Click **OK** to change the dashboard. It is possible to create a dashboard with more expansive permissions than one with more

Action	Steps
	queries contained on the dashboard. If you do this, users that have access to the underlying data can see the query when opening the dashboard. Users that do not have access to the underlying data receive a message saying they do not have permission to use that query. If the query is private to the dashboard creator, only the dashboard creator can modify the query or remove it from the dashboard.
Duplicate a dashboard	Sometimes the easiest way to create a new dashboard is to copy an existing one that's close to what you want. a. Click **Dashboard Actions** → **Duplicate**. b. **Trellix ePO - On-prem** names the duplicate by appending " **(copy)**" to the existing name. If you want to modify this name, do so now and click **OK**. The duplicated dashboard opens. The duplicate is an exact copy of the original dashboard including all permissions. Only the name is changed.
Delete a dashboard	a. Click **Dashboard Actions** → **Delete**. b. Click **OK** to delete the dashboard. The dashboard is deleted and you see the system default dashboard. Users who had this dashboard as their last viewed dashboard see the system default dashboard when they log on.

Export and import dashboards

Once you have fully defined your dashboard and monitors, the fastest way to migrate them to other **Trellix ePO - On-prem** servers is to export them and import them onto the other servers.

Before you begin

To import a dashboard, you must have access to a previously exported dashboard contained in an XML file.

A dashboard exported as an XML file can be imported to the same or a different system.

Task

1. **Select Menu → Reporting → Dashboards.**
2. **Select one of these actions.**

Action	Steps
Export dashboard	a. Click **Dashboard Actions → Export**. Your browser attempts to download an XML file according to your browser settings. b. Save the exported XML file to an appropriate location.
Import dashboard	a. Click **Dashboard Actions → Import**. The **Import Dashboard** dialog box appears. b. Click **Browse** and select the XML file containing an exported dashboard. Click **Open**. c. Click **Save**. The **Import Dashboard** confirmation dialog box appears. The name of the dashboard in the file is displayed, as well as how it will be named in the system. By default, this is the name of the dashboard as exported with **(imported)** appended. d. Click **OK**. If you do not want to import the dashboard, click **Close**. The imported dashboard is displayed. Regardless of their permissions at the time they were exported, imported dashboards are given private permissions. If you want them to have different permissions, change them after you import the dashboard.

Specify first-time dashboards

You can specify which dashboard a user sees when they first log on by mapping the dashboard to the user's permission set. Mapping dashboards to permission sets ensures that users assigned a particular role are automatically presented with the information they need.

Task

1. **Open the Edit Dashboards page.**
   a. **Select Menu → Configuration → Server Settings.**
   b. **From the Setting Categories list, select Dashboards.**
   c. **Click Edit.**
2. **Next to Default dashboard for specific permission sets, click the plus sign (+) and specify the default dashboard that appears for each permission set. Select a permission set and default dashboard from the menus.**
   The order of the pairs determines which default dashboard appears to users with more than one assigned permission set.
3. **Click Save.**

Results

The first time a user logs on, the dashboard you specified for their permission set appears. Subsequent logons return the user to the page they were on when they logged off.

Manage dashboard monitors

You can create, add, and remove monitors from dashboards.

Before you begin

You must have write permissions for the dashboard you are modifying.

If you do not have the necessary rights or product licenses to view a monitor, or if the underlying query for the monitor is no longer available, a message displays in place of the monitor.

Task

1. **Select Menu → Reporting → Dashboards. Select a dashboard from the Dashboard drop-down list.**
2. **Select one of these actions.**

Task	Steps
Add a monitor	a. Click **Add Monitor**. The **Monitor Gallery** appears at the top of the screen. b. Select a monitor category from the **Category** drop-down list. The available monitors in that category appear in the gallery. c. Drag a monitor onto the dashboard. As you move the cursor around the dashboard, the nearest available drop location is highlighted. Drop the monitor into your wanted location. The **New Monitor** dialog appears.

Task	Steps
	d. Configure the monitor as needed (each monitor has its own set of configuration options), then click **Close**. e. After you have added monitors to this dashboard, click **Save** to save the newly configured dashboard. f. When you have completed your changes, click **Close**. **Note:** If you add a **Custom URL Viewer** monitor that contains Adobe Flash content or ActiveX controls to a dashboard, it is possible the content might obscure **Trellix ePO - On-prem** menus, making portions of the menu inaccessible.
Edit a monitor	Most monitor types support different configuration options. For example, a query monitor allows the query, database, and refresh interval to be changed. a. Choose a monitor to manage, click the arrow in its top-left corner, and select **Edit Monitor**. The monitor's configuration dialog appears. b. When you have completed modifying the monitor's settings, click **OK**. If you decide to not make changes, click **Cancel**. c. If you decide to save the resulting changes to the dashboard, click **Save**, otherwise click **Discard**.
Remove a monitor	a. Choose a monitor to remove, select the arrow in its top-left corner, and select **Remove Monitor**. The monitor's configuration dialog appears. b. When you are finished modifying the dashboard, click **Close**, then **Save**.

Move and resize dashboard monitors

You can move and resize monitors to efficiently use screen space.

Before you begin

You must have write permissions for the dashboard you are modifying.
You can change the size of many dashboard monitors. If the monitor has small diagonal lines in its bottom-right corner, you can resize it. Monitors are moved and resized through drag and drop within the current dashboard.

Task

1. **Move or resize a monitor:**
    - To move a dashboard monitor:
        - Drag the monitor by its title bar to where you want it to appear. As you move the cursor, the background outline of the monitor shifts to the closest available location for the monitor.
        - When the background outline has shifted to the location you want, drop the monitor. If you attempt to drop the monitor in an invalid location, it returns to its prior location.
    - To resize a dashboard monitor:
        - Drag the resize icon in the bottom-right corner of the monitor toward an appropriate location. As you move the cursor, the background outline of the monitor changes shape to reflect the supported size closest to the current cursor location. Monitors might enforce a minimum or maximum size.
        - When the background outline has changed shape to a size you want, drop the monitor. If you attempt to resize the monitor to a shape not supported in the monitor's current location, it returns to its prior size.
2. **Click Save Changes. To revert to the prior configuration, click Discard Changes.**

Set default monitor refresh intervals

Use the **Dashboards** server setting to specify the default rate at which new monitors are refreshed.

Monitors are refreshed automatically. Each time a refresh occurs, the underlying query runs, and the results are displayed on the dashboard. Choose a default refresh interval for new monitors that is frequent enough to ensure accurate and timely information is displayed without consuming undue network resources. The default interval is five minutes.

Task

1. **Open the Edit Dashboards page.**
    a. **Select Menu → Configuration → Server Settings.**
    b. **From the Setting Categories list, select Dashboards.**
    c. **Click Edit.**
2. **Next to Default refresh interval for new monitors, enter a value between one minute and 60 hours.**
3. **Click Save.**

Results

Note
New monitors are refreshed according to the interval you specified. Existing monitors retain their original refresh interval. Users can always change the refresh interval of an individual monitor in the **Edit Monitor** window.

Generating queries and reports

Trellix ePO - On-prem comes with its own querying and reporting capabilities.

Included are the **Query Builder** and **Report Builder**, which create and run queries and reports that result in user-configured data in user-configured charts and tables. The data for these queries and reports can be obtained from **Trellix ePO - On-prem** database.

In addition to the querying and reporting systems, you can use these logs to gather information about activities on your **Trellix ePO - On-prem** server and your network:

- **Audit Log**
- **Server Task Log**
- **Threat Event Log**

Queries

Queries enable you to poll **Trellix ePO - On-prem** data. Information gathered by queries is returned in the form of charts and tables.

A query is used to get an answer right now. Query results are exported to several formats, any of which can be downloaded or sent as an attachment to an email message. Most queries are also used as dashboard monitors, enabling near real-time system monitoring. Queries can be combined into reports, giving a more broad and systematic look at your **Trellix ePO - On-prem** software system.

The default dashboards and predefined queries shipped with **Trellix ePO - On-prem** can't be changed or deleted. But you can duplicate them, then rename and change them as needed.

- Query results are actionable — Query results displayed in tables have actions available for selected items. Actions are available at the bottom of the results page.
- Queries as dashboard monitors — Most queries are used as a dashboard monitor (except those using a table to display the initial results). Dashboard monitors are refreshed automatically on a user-configured interval (five minutes by default).
- Exported results — Query results are exported to four formats. Exported results are historical data and are not refreshed like other monitors when used as dashboard monitors. Like query results and query-based monitors displayed in the console, you drill down into the HTML exports for more detailed information. Unlike query results in the console, you can't select an action when viewing exported data. You export to these file formats: .csv, .xml, .html, and .pdf.
- Combining queries in reports — Reports contain any number of queries, images, static text, and other items. They are run on demand or on a regular schedule, and produce PDF output for viewing outside **Trellix ePO - On-prem**.
- Sharing queries between servers — Any query can be imported and exported, allowing you to share queries between servers. In a multi-server environment, you only have to create a query once.
- Retrieving data from different sources — Queries retrieve data from any registered server, including databases external to **Trellix ePO - On-prem**.

Reports

Reports package query results into a PDF document, enabling offline analysis.

Generate reports to share information about your network environment, such as threat events and malware activity, with security administrators and other stakeholders.

Reports are configurable documents that display data from one or more queries, drawing data from one or more databases. The most recently run result for every report is stored in the system and is readily available for viewing.

You can restrict access to reports by using groups and permission sets in the same manner you restrict access to queries. Reports and queries can use the same groups, and because reports primarily consist of queries, this allows for consistent access control.

Query and report permissions

To run a query or report, you need permissions to not only that query or report, but the feature sets associated with their result types. A query's results pages only provide access to permitted actions given your permission sets.

Groups and permission sets control access to queries and reports. All queries and reports must belong to a group, and access to that query or report is controlled by the permission level of the group. Query and report groups have one of the following permission levels:

- **Private** — The group is only available to the user that created it.
- **Public** — The group is shared globally.
- **By permission set** — The group is only available to users assigned the selected permission sets.

Permission sets have four levels of access to queries or reports. These permissions include:

- **No permissions** — The **Query** or **Report** tab is not available to users with no permissions.
- **Use public queries** — Grants permission to use any queries or reports that have been placed in a **Public group**.
- **Use public queries; create and edit personal queries** — Grants permission to use any queries or reports that have been placed in a **Public group**, as well as the ability to use the **Query Builder** to create and edit queries or reports in **Private groups**.
- **Edit public queries; create and edit personal queries; make personal queries public** — Grants permission to use and edit any queries or reports placed in **Public groups**, create, and edit queries or reports in **Private groups**, as well as the ability to move queries or reports from **Private groups** to **Public** or **Shared groups**.

Introduction to queries

Queries allow you to poll **Trellix ePO - On-prem** data. Information gathered by queries is returned in the form of charts and tables.

A query can be used to get an answer right now. Query results can be exported to several formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can also be used as dashboard monitors, enabling

near real-time system monitoring. Queries can also be combined into reports, giving a more broad and systematic look at your **Trellix ePO - On-prem** software system.

The default dashboards and predefined queries shipped with **Trellix ePO - On-prem** cannot be changed or deleted. But you can duplicate them, then rename and change them as needed.

Query results are actionable

Query results displayed in tables have actions available for selected items. Actions are available at the bottom of the results page.

Queries as dashboard monitors

Most queries can be used as a dashboard monitor (except those using a table to display the initial results). Dashboard monitors are refreshed automatically on a user-configured interval (five minutes by default).

Exported results

Query results can be exported to four formats. Exported results are historical data and are not refreshed like other monitors when used as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.

Unlike query results in the console, you cannot select an action when viewing exported data.

You can export to these file formats:

- CSV — Use the data in a spreadsheet.
- XML — Use the data for scripts or applications.
- HTML — View the exported results in a browser.
- PDF — Save the exported results to read or print later.

Combining queries in reports

Reports can contain any number of queries, images, static text, and other items. They can be run on demand or on a regular schedule, and produce PDF output for viewing outside **Trellix ePO - On-prem**.

Sharing queries between servers

Any query can be imported and exported, allowing you to share queries between servers. In a multi-server environment, you only have to create a query once.

Retrieving data from different sources

Queries can retrieve data from any registered server, including databases external to **Trellix ePO - On-prem**.

Query Builder

Trellix ePO - On-prem provides an easy, four-step wizard that is used to create and edit custom queries. With the wizard, you can configure which data is retrieved and displayed, and how it is displayed.

Result types

The first selections you make in the Query Builder are the schema and result type from a feature group. This selection identifies from where and what type of data the query retrieves, and determines the available selections in the rest of the wizard.

Chart types

Trellix ePO - On-prem provides several charts and tables to display the data it retrieves. These charts and their drill-down tables are highly configurable.

Note

Tables do not include drill-down tables.

Chart type groups

Type	Chart or Table
Bar	• Bar Chart • Grouped Bar Chart • Stacked Bar Chart
Pie	• Boolean Pie Chart • Pie Chart
Bubble	• Bubble Chart
Summary	• Multi-group Summary Table • Single Group Summary Table
Line	• Multi-line Chart • Single-Line Chart
List	• Table

Table columns

Specify columns for the table. If you select **Table** as the primary display of the data, this configures that table. If you select a type of chart as the primary display of data, it configures the drill-down table.

Query results displayed in a table are actionable. For example, if the table is populated with systems, you can deploy or wake up agents on those systems directly from the table.

Filters

Specify criteria by selecting properties and operators to limit the data retrieved by the query.

Work with queries

Manage custom queries

You can create, duplicate, edit, and delete queries as needed.

Task

1. **Open the Queries & Reports page: select Menu → Reporting → Queries & Reports.**
2. **Select the Queries tab.**
3. **Select one of these actions.**

Task	Steps
Create custom query	a. Click **New Query**, and the **Query Builder** appears. b. On the **Result Type** page, select the **Feature Group** and **Result Type** for this query, then click **Next**. c. Select the information for the chart or table to display the primary results of the query, then click **Next**. If you select **Boolean Pie Chart**, configure the criteria to include in the query before proceeding. d. Select the columns to be included in the query, then click **Next**. If you selected **Table** on the **Chart** page, the columns you select here are the columns of that table. Otherwise, these columns make up the query details table. e. Select properties to narrow the search results, then click **Run**. The **Unsaved Query** page displays the results of the query, which is actionable. You can take any available action on items in any table or drill-down table.

Task	Steps
	Selected properties appear in the content pane with operators that can specify criteria used to narrow the data that is returned for that property. • If the query didn't return the expected results, click **Edit Query** to go back to the **Query Builder** and edit the details of this query. • If you don't want to save the query, click **Close**. • If you want to use this query again, click **Save** and continue to the next step. f. The **Save Query** page appears. Type a name for the query, add any notes, and select one of the following: • **New Group** — Type the new group name and select either: ▫ **Private group (My Groups)** ▫ **Public group (Shared Groups)** • **Existing Group** — Select the group from the list of **Shared Groups**. g. Click **Save**. The new query appears in the **Queries** list.
Duplicate query	a. From the list, select a query to copy, then click **Actions** → **Duplicate**. b. In the **Duplicate** dialog box, type a name for the duplicate and select a group to receive a copy of the query, then click **OK**. The duplicated query appears in the **Queries** list.
Edit query	a. From the list, select a query to edit, then click **Actions** → **Edit**. b. Edit the query settings and click **Save** when done. The changed query appears in the **Queries** list.

Task	Steps
Delete query	a. From the list, select a query to delete, then click **Actions** → **Delete**. b. When the confirmation dialog box appears, click **Yes**. The query no longer appears in the **Queries** list. If any reports or server tasks used the query, they now appear as invalid until you remove the reference to the deleted query.
Run query	a. From the list, select a query to run, then click **Actions** → **Run**. b. View the results of the report in the main page. c. Use the **Options** menu to export the results, if needed. d. Click **Close** to exit.
Schedule query	a. From the list, select a query to schedule, then click **Actions** → **Schedule**. b. Select the scheduling options c. Click **Save**.

Create a query group

Query groups allow you to save queries or reports without allowing other users access to them.

Creating a group allows you to categorize queries and reports by functionality and controlling access. The list of groups you see in the **Trellix ePO - On-prem** software is the combination of groups you have created and groups you have permission to see.

Note

You can also create private query groups while saving a custom query.

Task

1. **Select Menu → Reporting → Queries & Reports, then click Group Actions → New Group.**
2. **In the New Group page, enter a group name.**
3. **From Group Visibility, select one of the following:**
    - **Private group** — Adds the new group under **My Groups**.

- **Public group** — Adds the new group under **Shared Groups**. Any user with access to public queries and reports can view queries and reports in the group.
- **Shared by permission set** — Adds the new group under **Shared Groups**. Only users assigned the selected permission sets can access reports or queries in this group.

Note

Administrators have full access to all **Shared by permission set** and **Public group** queries.

4. **Click Save.**

Run a query on a schedule

A server task is used to run a query regularly. Queries can have sub-actions that allow you to perform various tasks, such as emailing the query results or working with tags.

Task

1. **Open the Server Task Builder.**
   a. **From the Queries and Reports page, select a query.**
   b. **Select Actions → Schedule.**
2. **On the Description page, name and describe the task, specify the schedule status, then click Next.**
3. **On the Actions page and from the Actions drop-down menu, select Run Query.**
4. **In the Query field, browse to the query that you want to run.**
5. **Select the language for displaying the results.**
6. **From the Sub-Actions list, select an action to take based on the results. Available sub-actions depend on the permissions of the user, and the products managed by your Trellix ePO - On-prem server.**

Note

You are not limited to selecting one action for the query results. Click the **+** button to add actions to take on the query results. Be careful to place the actions in the order you want them to be taken on the query results.

7. **Click Next.**
8. **Schedule the task, then click Next.**
9. **Verify the configuration of the task, then click Save.**

Results

The task is added to the list on the **Server Tasks** page. If the task is enabled (which it is by default), it runs at the next scheduled time. If the task is disabled, it only runs when you click **Run** next to the task on the **Server Tasks** page.

About reports

Reports package query results into a PDF document, enabling offline analysis.

Generate reports to share information about your network environment with security administrators and other stakeholders.

Reports are configurable documents that display data from one or more queries, drawing data from one or more databases. The most recently run result for every report is stored in the system and is readily available for viewing.

You can restrict access to reports by using groups and permission sets in the same way you restrict access to queries. Reports and queries can use the same groups, and because reports primarily consist of queries, this configuration allows for consistent access control.

Report anonymization permissions

You can restrict or allow users to access anonymized data in the reports for Content Security Reporting by setting appropriate permissions.

Restrict access to sensitive data by masking the field with a numeric value. However, you can share the key file that contains the actual values of the masked data by setting permissions for the users.

Permission sets provide you with two options including:

- No Permissions
- Allow Anonymized Key file download

Structure of a report

Reports contain a number of elements held within a basic format.

While reports are highly customizable, they have a basic structure that contains all varying elements.

Page size and orientation

Trellix ePO - On-prem currently supports six combinations of page size and orientation. These combinations include:

Page sizes:

- US Letter (8.5" x 11")
- US Legal (8.5" x 14")
- A4 (210 mm x 297 mm)

Orientation:

- Landscape
- Portrait

Headers and footers

Headers and footers also have the option of using a system default, or can be customized in a number of ways, including logos. Elements currently supported for headers and footers are:

- Logo

- Date/Time
- Page Number
- User Name
- Custom text

Page elements

Page elements provide the content of the report. They can be combined in any order, and can be duplicated as needed. Page elements provided with **Trellix ePO - On-prem** are:

- Images
- Static text
- Page breaks
- Query Tables
- Query Charts

Create a report

You can create reports and store them in **Trellix ePO - On-prem**.

Task

1. **Select Menu → Reporting → Queries & Reports, then select the Reports tab.**
2. **Click New Report.**
3. **Click Name, Description, and Group. Name the report, describe it, and select an appropriate group.**
4. **Click OK.**
5. **Use the items in the Toolbox and the links on top of the page to add, remove, rearrange elements, customize header and footer, and change the page layout.**
6. **Select Runtime Parameters.**
7. **In the Runtime Parameters window, set conditions applicable to the respective fields.**
8. **Click Save.**

Edit an existing report

You can modify an existing report's contents or the order of presentation.

If you are creating a report, you will arrive at this screen after clicking **New Report**.

Task

1. **Select Menu → Reporting → Queries & Reports, then select the Report tab.**
2. **Select a report from the list by selecting the checkbox next to its name.**
3. **Click Edit.**
   The **Report Layout** page appears.

What to do next

Any of the following tasks can now be performed on the report.

Add elements to a report

You can add new elements to an existing report.

Before you begin

You must have a report open on the **Report Layout** page.

Task

1. **Select an element from the Toolbox and drag and drop it over the Report Layout.**
   Report elements other than **Page Break** require configuration. The configuration page for the element appears.
2. **After configuring the element, click OK**

Configure image report elements

Upload new images and modify the images used within a report.

Before you begin

You must have a report open on the **Report Layout** page.

Task

1. **To configure an image already in a report, select the arrow at the top left corner of the image, then click Configure.**
   This displays the **Configure Image** page. If you are adding an image to the report, the **Configure Image** page appears immediately after you drag and drop the **Image** element onto the report.
2. **To use an existing image, select it from the gallery.**
3. **To use a new image, click Browse and select the image from your computer, then click OK.**
4. **To specify a specific image width, enter the width in the Image Width field.**
   By default, the image is displayed in its existing width without resizing unless that width is wider than the available width on the page. In that case, it is resized to the available width keeping aspect ratio intact.
5. **Select if you want the image aligned left, center, or right, then click OK.**

Configure text report elements

You can insert static text within a report to explain its contents.

Before you begin

You must have a report open on the **Report Layout** page.

Task

1. **To configure text already in a report, click the arrow at the top left corner of the text element. Click Configure.**
   This displays the **Configure Text** page. If you are adding new text to the report, the **Configure Text** page appears immediately after you drop the **Text** element onto the report.
2. **Edit the existing text in the Text edit box, or add new text.**
3. **Change the font size as appropriate.**
   The default is 12-pt type.
4. **Select the text alignment: left, center, or right.**

5. **Click OK.**

Results

The text you entered appears in the text element within the report layout.

Configure query table report elements

Some queries are better displayed as a table when inside a report.

Before you begin

You must have a report open on the **Report Layout** page.

Task

1. **To configure a table already in a report, click the arrow at the top left corner of the table. Click Configure.**
   This displays the **Configure Query Table** page. If you are adding query table to the report, the **Configure Query Table** page appears immediately after you drop the **Query Table** element onto the report.
2. **Select a query from the Query drop-down list.**
3. **Select the database from the Database drop-down list to run the query against.**
4. **Choose the font size used to display the table data.**
   The default is 8-pt type.
5. **Click OK.**

Configure query chart report elements

Some queries are better displayed as a chart when inside a report.

Before you begin

You must have a report open on the **Report Layout** page.

Task

1. **To configure a chart already in a report, click the arrow at the top left corner of the chart. Click Configure.**
   This displays the **Configure Query Chart** page. If you are adding a query chart to the report, the **Configure Query Chart** page appears immediately after you drop the **Query Table** element onto the report.
2. **Select a query from the Query drop-down list.**
3. **Select whether to display only the chart, only the legend, or a combination of the two.**
4. **If you have chosen to display both the chart and legend, select how the chart and legend are placed relative to each other.**
5. **Select the font size used to display the legend.**
   The default is 8-pt type.
6. **Select the chart image height in pixels.**
   The default is one-third the page height.
7. **Click OK.**

Customize a report

Customize a report layout to add, remove, or move the objects that you need.

Task

1. **Select Menu → Reporting → Queries & Reports. Select the Reports tab.**
2. **Select a report and click Actions → Edit, then perform the required actions.**

Action	Steps
Customize report headers and footers	Headers and footers provide information about the report. The 6 fixed locations in the header and footer contain different data fields: • Header fields: The header contains 3 fields. One left-aligned logo and 2 right-aligned fields, one above the other. These fields can contain one of the 4 values: ▫ Nothing ▫ Date/Time ▫ Page Number ▫ User name of the user running the report • Footer fields: The footer contains 3 fields. One left-aligned, one centered, and one right-aligned. These 3 fields can also contain the listed values and custom text. To customize the headers and footers, perform these steps: a. Click **Header and Footer**. b. By default, reports use the system setting for headers and footers. If you do not want this, deselect **Use Default Server Setting**. To change the system settings for headers and footers, select **Menu → Configuration → Server Settings**, then select **Printing and Exporting** and click **Edit**. c. To change the logo, click **Edit Logo**. i. If you want the logo to be text, select **Text** and enter the text in the edit box. ii. To upload a new logo, select **Image** then browse to and select the image on your computer and click **OK**.

Action	Steps
	iii. To use a previously uploaded logo, select it. iv. Click **Save**. d. Change the header and footer fields to match the wanted data, then click **OK**.
Remove elements from a report	You can remove elements from a report if no longer needed. a. Click the arrow in the top left corner of the element you want to delete, then click **Remove**. The element is removed from the report.
Reorder elements in a report	You can change the order in which elements appear in a report. a. To move an element, click the title bar of the element and drag it to a new position. The element positioning under the dragged element shifts as you move the cursor around the report. Red bars appear on either side of the report if the cursor is over an illegal position. b. When the element is positioned where you want it, drop the element.

3. **Click Save.**

Run a report on a schedule

Create a server task to run a report automatically.

If you want a report to be run without manual intervention, a server task is the best approach. This task creates a server task allowing for automatic, scheduled runs of a given report.

Task

1. **Open the Server Tasks page and click New Task.**
2. **Name the task, describe it, and assign a schedule status, then click Next.**
   If you want the task to be run automatically, set the **Schedule status** to **Enabled**.
3. **From the Actions drop-down list, select Run Report.**
4. **Select the report to run and the target language.**

5. **Optional and available only for Content Security Reporting: Select Anonymize to mask any sensitive information such as the IP address and User Name.**
6. **Optional and available only for Content Security Reporting: From the Sub-Actions drop-down list, select one of these:**
   - **Email File** — only the report is sent to the email recipient.
   - **Export file and key (for anonymized reports)** — the report and the key file are saved to the specified location.
   - **Export to File** — only the report is saved to the specified location.
   - **Send email with file and key (for anonymized reports)** — the report and the key file are sent to the email recipient.

   The report is saved with the given name and the key file is saved with the report name followed by a numeric value.

   For example: if the name of the report is `Samplereport`, the key file is saved as `Samplereport1`. You can overwrite an existing report or increment it by selecting from the drop-down list. If you select Increment, the next report generated will be saved as `Samplereport2` and the key file will be saved as `Samplereport3`.
7. **Click Next.**
8. **Choose a schedule type (frequency), dates, and time to run the report, then click Next.**
   The schedule information is used only if you enable **Schedule status**.
9. **Click Save to save the server task.**

Results

The new task now appears in the **Server Tasks** list.

Note

You can also schedule to run a report on the **Queries and Report** page.

1. On the **Queries and Reports** page, select a report.
2. Click **Schedule**.

View report output

View the last run version of every report.

Every time a report runs, the results are stored on the server and displayed in the report list.

Note

When a report runs, the prior results are erased and cannot be retrieved. If you are interested in comparing different runs of the same report, archive the output elsewhere.

Task

1. **Select Menu → Reporting → Queries & Reports.**
2. **Select the Reports tab.**

In the report list, you see a **Last Run Result** column. Each entry in this column is a link to retrieve the PDF that resulted from the last successful run of that report. Click a link from this column to retrieve a report.

Note

If the report contains anonymized data, you see two entries. One to download the report and the other link allows you to download the key file that contains the mapped values to the masked fields. However, you need to have the correct set of permissions to be able to download the key file.

Results

A PDF opens in your browser, and your browser behaves based on how you configured it for that file type.

Configure the template and location for exported reports

You can define the appearance and storage location for tables and dashboards you export as documents.

Using the **Printing and Exporting** server setting, you can configure:

- Headers and footers, including a custom logo, name, and page numbering.
- Page size and orientation for printing.
- Directory where exported tables and dashboards are stored.

Task

1. **Select Menu → Configuration → Server Settings, then select Printing and Exporting in the Settings list.**
2. **Click Edit. The Edit Printing and Exporting page appears.**
3. **In the Headers and footers for exported documents section, click Edit Logo to open the Edit Logo page.**
    a. **Select Text and type the text you want included in the document header, or do one of the following:**
        - Select **Image** and browse to the image file, such as your company logo.
        - Select the default **Trellix** logo.
    b. **Click OK to return to the Edit Printing and Exporting page.**
4. **From the drop-down lists, select any metadata that you want displayed in the header and footer.**
5. **Select a Page size and Page orientation.**
6. **Type a new location or accept the default location to save exported documents.**
7. **Click Save.**

Group reports together

Every report must be assigned to a group.

Reports are assigned to a group when initially created, but this assignment can be changed later. The most common reasons for grouping reports together are to collect similar reports together, or to manage permissions to certain reports.

Task

1. **Select Menu → Reporting → Queries & Reports, then select the Reports tab.**

2. **Select a report and click Actions → Edit.**
3. **Click Name, Description and Group.**
4. **Select a group from the Report Group drop-down list and click OK.**
5. **Click Save to save any changes to the report.**

Results

When you select the chosen group from the **Groups** list in the left pane of the report window, the report appears in the report list.

Audit log

Audit Log page

Find and view actions taken by all users.

Option definitions

Option	Definition
Purge	Removes entries from the **Audit Log** based on user-specified age. This action deletes all **Audit Log** entries older than the specified age.
Show/Hide Filter	Shows or hides the filter options.
Preset	The **Preset** drop-down list allows you to filter which **Audit Log** entries to display based on predefined criteria, including: • **Failed** — Displays only failed actions recorded in the **Audit Log**. • **Last Hour** — Displays all actions recorded in the last hour. • **Last day**— Displays all actions recorded in the last day. • **Last week** — Displays all actions recorded in the last week. • **Last month** — Displays all actions recorded in the last month. • **Last quarter** — Displays all actions recorded in the last quarter. • **Last year** — Displays all actions recorded in the last year.

Option	Definition
	• **No Filter** — Displays all actions recorded since the last time the **Audit Log** was purged.
Quick find	Enter a search term to filter the log entries by the search results. Click **Apply** to perform the search.
Clear	Deselects the **Quick find** text entry box.
Actions	Specifies the actions that you can perform on the **Audit Log**, including: • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this option to select the columns of data to be displayed on the **Audit Log** page. • **Export** — Opens the Export page. Use this option to specify the format and the package of the files to be exported. You can save or email the exported **Audit Log**.

Column header definitions

Use these column headers to filter the **Audit Log**.

Column header	Definition
Action	Specifies the action the user attempted to take.
Completion Time	Specifies the time (on the **Trellix ePO - On-prem** server) the action was completed.
Details	Specifies further information about the action, if available.
Priority	Specifies the importance of the action determined by **Trellix**.
Start Time	Specifies the time (on the **Trellix ePO - On-prem** server) that the action began.

Column header	Definition
Success	Specifies whether the action succeeded.
User Name	Specifies the **Trellix ePO - On-prem** user name of the account that attempted to take the action. The user name is unavailable for some actions, for example, failed logon attempts.

Audit Log Entry Details page

Use this page to view the details of any clicked entry in the **Audit Log**. Items on this page might be displayed in the language of the **Trellix ePO - On-prem** server.

Option definitions

Option	Definition
User Name	Specifies the **Trellix ePO - On-prem** user name of the account that attempted to take action. The user name is unavailable for some actions, for example, failed logons.
Priority	Specifies the importance of the action determined by **Trellix**. You can filter the **Audit Log** by the priority of actions.
Action	Specifies the action the user attempted to take.
Details	Specifies further information about the action, if available.
Success	Specifies whether the action succeeded.
Start Time	Specifies the time (on the **Trellix ePO - On-prem** server) the action began.
Completion Time	Specifies the time (on the **Trellix ePO - On-prem** server) the action was completed.

Threat Event Log

Threat Event Log page

Use this page to view threat events for all managed systems from the **Reporting** menu. Select a row to view details.

Option definitions

Option	Definition

Show Filter/Hide Filter	Shows or hides the following options used to filter which **Event Log** entries to display based on predefined criteria, including:
	• **Preset** — The preset drop-down list allows you to set the following time period to filter recorded actions.
	  ▫ **Last hour** — Displays all actions recorded in the last hour.
	  ▫ **Last day** — Displays all actions recorded in the last day.
	  ▫ **Last week** — Displays all actions recorded in the last week.
	  ▫ **Last month** — Displays all actions recorded in the last month.
	  ▫ **Last quarter** — Displays all actions recorded in the last quarter.
	  ▫ **Last year** — Displays all actions recorded in the last year.
	• **Quick find** — Enter a search term and click **Apply** to display only entries matching that search term.
	• **Clear** — Removes all filtering selections.
	• **Show selected rows** — Select this box to display only the rows you have selected.

Actions	Specifies the actions that you can perform on the selected events, including: • **Choose Columns** — Opens the Select the **Columns to Display** page. Use this to select which columns of data to display on the **Threat Event Log** page. • **Export Table** — Opens the Export page. From the **Export** page, you can specify the format of the

Option	Definition
	files to be exported, how they are packaged, and what to do with them. For example, files could be exported in .pdf format, packaged into a .zip file, and mailed to an administrator as an email attachment. • **Show Related Systems** — Takes you to a page where you can view and take action on the systems where selected events occurred. • **Show Source Systems** — Opens the **Source Systems** page, where you can view and take action on the systems where the threat event was generated. • **Show Targeted Systems** — Opens the **Target Systems** page with a list of systems targeted for the selected event.

Threat Event Log Details page

View the details of an event in the **Threat Event Log**.

Option definitions

Option	Definition
Event Received Time	Time the **Trellix ePO - On-prem** server received notification of the event using the default time zone.
Event Generated Time	Time of the event using the default time zone.
Preferred Event Time	Time of the event using the preferred local time zone.
Agent GUID	Unique identifier of the agent that forwarded the event.
Detecting Prod ID (deprecated0	ID of the detecting product.
Detecting Product Name	Name of the detecting managed product.

Option	Definition
Detecting Product Version	Version number of the detecting product.
Detecting Product Host Name	Name of the system hosting the detecting product.
Detecting Product IPv4 Address	IPv4 address of the system hosting the detecting product (if given in the event).
Detecting Product IP Address	IP address of the system hosting the detecting product (if given in the event).
Detecting Product MAC Address	MAC address of the system hosting the detecting product.
DAT Version	DAT version on the system that sent the event.
Engine Version	Version number of the detecting product's engine (if given in the event).
Threat Source Host Name	System name from which the threat originated (if given in the event).
Threat Source IPv4 Address	IPv4 address of the system from which the threat originated (if given in the event).
Threat Source IP	IP address of the system from which the threat originated (if given in the event).
Threat Source MAC Address	MAC address of the system from which the threat originated (if given in the event).
Threat Source User Name	User name from which the threat originated (if given in the event).
Threat Source Process Name	The process name from which the threat originated.
Threat Source URL	URL from which the threat originated (if given in the event).

Option	Definition
Threat Target Host Name	Name of the system that created the event.
Threat Target IPv4 Address	IPv4 address of the system that sent the event.
Threat Target IP Address	IP address of the system that sent the event.
Threat Target MAC Address	MAC address of the system that sent the event.
Threat Target User Name	The threat source user name or email address.
Threat Target Port Number	The threat target port for threat classes.
Threat Target Network Protocol	The threat target protocol for threat classes.
Threat Target Process Name	The target process name (if given in the event).
Threat Target File Path	Location of the threat on the detecting system.
Event Category	Category of the event. Possible categories depend on the product.
Event ID	Unique identifier of the event class.
Threat Severity	The severity of the detected threat as defined by each managed product.
Threat Name	Name of the threat.
Threat Type	Class of the threat.
Action Taken	The action taken by the product in response to the threat.
Threat Handled	Specifies whether the action taken was successful.

Option	Definition
Analyzer Detection Method	The name of the task or task type that was responsible for detecting the threat.
Actions menu	Specifies the actions that can be taken on this event, including: • **Show Related Systems** — View and take action on the systems where selected events occurred. • **Show Source Systems** — View systems that were the source of the selected event. • **Show Targeted Subsystem** — View systems targeted for the selected event.

Disaster Recovery

Disaster Recovery helps you quickly recover and reinstall your **Trellix ePO - On-prem** software.

To recover your **Trellix ePO - On-prem** environment, you must have a backup of the data that is unique to your environment and a mechanism for restoring **Trellix ePO - On-prem** using this backup. The data that makes your **Trellix ePO - On-prem** environment unique consists of two things: the **Trellix ePO - On-prem** database, and sections of the **Trellix ePO - On-prem** server file system. For example, the extensions that you checked in and the configuration files that control **Trellix ePO - On-prem**.

A **Trellix ePO - On-prem** database backup containing a valid Disaster Recovery Snapshot allows you to restore:

- **Trellix ePO - On-prem** to your current **Trellix ePO - On-prem** server, which allows you to recover from. For example, a failed **Trellix ePO - On-prem** software upgrade.
- **Trellix ePO - On-prem** to new server hardware with the original server name and IP address. For example, in the case of catastrophic hardware failure.
- **Trellix ePO - On-prem** server hardware with a new server name, which allows you to move your **Trellix ePO - On-prem** server from one domain to another.

For security, the files stored in the Snapshot are encrypted using the Keystore Encryption Passphrase. Keep a record of this passphrase; you need it to decrypt the Disaster Recovery Snapshot records and **Trellix** can't recover it.

Important considerations

For a successful disaster recovery, the database and the snapshot it contains must be in sync. For example, if you took a Disaster Recovery Snapshot a week ago, two days ago you checked in a new extension, and last night you backed up the **Trellix ePO - On-prem** database without taking a new snapshot, the database and snapshot are not in sync and it is unlikely you will be able to successfully restore from that database. The Server Snapshot dashboard monitor can be used to tell you if your snapshot is up to date.

To prepare for disaster recovery, save the files to the Snapshot in the database, and then perform a full backup of the **Trellix ePO - On-prem** database.

Working with Snapshots

Using a snapshot to restore your server

The **Disaster Recovery Snapshot Server** task allows you to save your files in an encrypted format and save the Snapshot to the database.

Disaster Recovery Snapshot contents

The files are saved in an encrypted format in the database when the **Disaster Recovery Snapshot Server** task runs.

The extensions are processed one at a time. Extensions can specify additional files to be stored in the snapshot: when each extension is processed, the snapshot task asks each extension what other files are required, and if any are defined it stores them in the snapshot.

Core **Trellix ePO - On-prem** configuration files	<ePO Install path>\Server\Keystore\ <ePO Install path>\Server\conf\
Installed extensions	<ePO Install path>\Server\extensions\installed\

The Disaster Recovery Snapshot records include the paths configured for your registered executables. The registered executable files are not stored in the Snapshot, and you must replace the executable files when you restore your **Trellix ePO - On-prem** environment. After you restore the **Trellix ePO - On-prem** environment, any registered executables with broken paths appear in red on the **Registered Executables** page.

Note

Test your registered executable paths after you restore your **Trellix ePO - On-prem** server. Some registered executable paths might not appear in red, but still fail because of dependency issues related to the registered executables.

Disaster Recovery Snapshot Server task

Use the **Disaster Recovery Snapshot Server** task to save the Snapshot to the database. The Snapshot is created when you install **Trellix ePO - On-prem**. The task can be scheduled to run at a specific time, by default it's configured to run every day at 2 a.m. You can also run the task manually from the **Trellix ePO - On-prem** dashboard and the WebAPI interface.

When **Trellix ePO - On-prem** is installed, the **Disaster Recovery Snapshot Server** task is enabled by default if the database is hosted on a full version of SQL Server. It's disabled by default if the database is hosted on an SQL Express instance, due to the hard-coded database size limit enforced by SQL Express.

Trellix ePO - On-prem only saves one Snapshot to the database at a time: each time the task runs, the current Snapshot information is removed, and the new Snapshot information takes its place.

How the Server Snapshot dashboard monitor works

The Server Snapshot monitor, found on your **Trellix ePO - On-prem** dashboard, allows you to manage and monitor your Disaster Recovery Snapshot.

If the Snapshot monitor does not appear in your dashboard, create a dashboard and add the Disaster Recovery monitor.

The Server Snapshot monitor allows you to:

- Manually start the Snapshot task by clicking **Take Snapshot**.
- View the Server Task Log entry for the last Snapshot task by clicking **See details of last run**. This page displays information and log messages about the most recent Snapshot saved.

- View the date and time the last Snapshot task ran.

The color and title of the Snapshot monitor tells you the status of your latest Snapshot.

- **Blue, Saving Snapshot to Database** — Snapshot process is in progress.
- **Green, Snapshot Saved to Database** — Snapshot process completed successfully and it is up to date.
- **Red, Snapshot Failed** — An error occurred during the Snapshot process.
- **Gray, No Snapshot Available** — No Snapshot has been saved.
- **Orange, Snapshot Out of Date** — Changes to the configuration have occurred and a recent Snapshot has not been saved. Changes that trigger a Snapshot out-of-date status include:
  - Any extension change; for example, updated, removed, deleted, upgraded, or downgraded.
  - The Keystore folder changed.
  - The conf folder changed.
  - The Disaster Recovery passphrase changed in Server Settings.

Save a snapshot from the Trellix ePO - On-prem Dashboard

Use the **Trellix ePO - On-prem** Dashboard to take **Disaster Recovery Snapshots** of your primary **Trellix ePO - On-prem** server and to monitor the **Snapshot** process as the **Dashboard** status changes.

Task

1. **Select Menu → Reporting → Dashboards, then select ePO Server Snapshot.**
2. **Click Take Snapshot to start saving the Snapshot to the database.**
   During the **Snapshot** process, the **Snapshot Monitor** title bar changes to indicate the status of the process.

   The time it takes for the Snapshot process to complete depends on several factors; for example, if the product extensions are checked in and the performance of the SQL Server.

3. **(Optional) After the Snapshot process is finished, click See details of current run to open the Server Task Log Details.**

Save a snapshot using Web API commands

Use Web API commands to save a snapshot for Disaster Recovery purposes.

Before you begin

All commands described in this task are typed in your web browser address bar to remotely access your **Trellix ePO - On-prem** server.
These are the variables in the remote command:

- <server_name> — The DNS server name or IP address of the remote server
- <port> — The assigned **Trellix ePO - On-prem** server port number, usually "8443", unless your server is configured to use a different port number

Review the following before you begin this task:

- You are prompted for the administrator user name and password before the output appears.

- The default name for the Snapshot task is **Disaster Recovery Snapshot Server**.
- These commands are case sensitive; make sure to review them carefully for proper capitalization and syntax.

Task

1. **The task ID is required to run the Snapshot server task; use this command if you don't know the task ID:**
   `https://<server_name>:<port>/remote/scheduler.listAllServerTasks?:output=terse`
   Find the ID next to the Disaster Recovery Snapshot Server task. For example, ID: 2:

   ```
   OK:
   ID Name                                                                    Next Run
   -- ------------------------------------------------------------------------ --------------------
   2  Disaster Recovery Snapshot Server                                       None
   ```

2. **Run the Snapshot server task using the following command.**
   `https://<server_name>:<port>/remote/scheduler.runServerTask?taskId=2`

   If the task is successful, output similar to the following appears:

   `OK`

   `102`

3. **(Optional) Confirm that the Web API server task Snapshot ran successfully.**
   a. **Use this command to find the Disaster Recovery Snapshot Server Task Log ID:**
      `https://<server_name>:<port>/remote/tasklog.listTaskHistory?taskName=Disaster%20Recovery%20Snapshot%20Server`
      This command displays all Disaster Recovery Snapshot Server tasks. Find the most recent task and note the ID number. For example, ID: 102:

      ```
      ID: 102
      Name: Disaster Recovery Snapshot Server
      Start Date: [date]
      End Date: [date]
      User Name: admin
      Status: Completed
      Source: scheduler
      Duration: Less than a minute
      ```

   b. **Use this command and the task ID number 102 to display all task log messages:**
      `https://<server_name>:<port>/remote/tasklog.listMessages?taskLogId=102`

Install Trellix ePO - On-prem software on a restore server

You can restore the **Trellix ePO - On-prem** software as a recovery installation where your Microsoft SQL Server already includes a **Trellix ePO - On-prem** configuration from a previous installation.

To re-create the **Trellix ePO - On-prem** server, reinstall the **Trellix ePO - On-prem** software on a server and link it to the restored SQL database.

Tip

Monitor the process because you might need to restart your system.

Task

1. **When you select the existing SQL Server, gather this information and complete these steps before beginning your installation. These steps ensure that your Trellix ePO - On-prem software can communicate with the database server:**
    - Verify that the SQL Browser Service is running.
    - Make sure that the TCP/IP Protocol is enabled in the SQL Server Configuration Manager.
    - Update the system that hosts your **Trellix ePO - On-prem** server and your SQL Server with the latest Microsoft security updates, then turn off Windows updates during the installation process.
    - Confirm the SQL backup file that you copied from the primary server was restored using the Microsoft SQL process.
    - Stop Agent Handler services on all systems, before restoring the **Trellix ePO - On-prem** software.
2. **If you have Agent Handlers configured, log on to the systems where the Agent Handlers are installed, then open the Windows Services panel. Stop the Trellix Event Parser and Trellix Apache services.**

    Note

    See your Microsoft software product documentation for more information about using the Windows Services panel.

3. **Using an account with local administrator permissions, log on to the Windows Server computer used as the restore Trellix ePO - On-prem server.**
4. **Downloaded from the Trellix website, extract the files to a temporary location, right-click Setup.exe, and select Run as Administrator.**

    Important

    The version you download must match the version being restored. If you try to run **Setup.exe** without first extracting the contents of the .zip file, the installation fails.

    The **Trellix ePolicy Orchestrator - InstallShield Wizard** starts.
5. **Click Restore ePO from an existing database snapshot and Next to begin the restore installation process.**
6. **In the Install additional software step, any remaining prerequisites are listed. To install them, click Next.**
7. **In the Destination Folder step, click:**
    - **Next** — Install your **Trellix ePO - On-prem** software in the default location (C:\Program Files (x86)**Trellix\ePolicy Orchestrator**).
    - **Change** — Specify a custom destination location for your **Trellix ePO - On-prem** software. When the **Change Current Destination Folder** window opens, browse to the destination and create folders if needed. When finished, click **OK**.
8. **In the Database Information step, select the Microsoft SQL Server name from the Database Server list. Specify which type of Database Server Credentials to use, then click Next.**

- **Windows authentication** — From the **Domain** menu, select the domain of the user account you're going to use to access the SQL Server. Type the **User name** and **Password** of your restored SQL database.
- **SQL authentication** — Type the **User name** and **Password** for your SQL Server. Make sure that credentials you provide represent an existing user on the SQL Server with appropriate rights. The **Domain** menu is grayed out when using SQL authentication.

Note

You might need to type the **SQL server TCP port** to use for communication between your **Trellix ePO - On-prem** server and database server. The **Trellix ePO - On-prem** installation tries to connect using the default ports, 1433 and 1434. If those ports fail, you are prompted to type an SQL Server TCP port.

9. **In the HTTP Port Information step, review the default port assignments. Click Next to verify that the ports are not already in use on this system.**
10. **In the Administrator Information step, type the Username and Password you used for your previously existing server administrator account.**
11. **Type the Server recovery passphrase you saved during the initial installation of the previously existing Trellix ePO - On-prem server, or changed in the Server Settings.**
    The Server recovery passphrase decrypts the sensitive files stored in the Disaster Recovery Snapshot.
12. **Accept the Trellix End User License Agreement and click OK.**
13. **From the Ready to install the Program dialog box, decide if you want to send anonymous usage information to Trellix, then click Install to begin installing the software.**
14. **When the installation is complete, click Finish to exit the InstallShield wizard.**
15. **If you restored Trellix ePO - On-prem to a server with a different IP address or DNS name than your previously existing server, configure a way to allow your managed systems to connect to your new Trellix ePO - On-prem server.**

Tip

Create a CNAME record in DNS that points requests from the old IP address, DNS name, or NetBIOS name of the previously existing **Trellix ePO - On-prem** server to the new information for the restore **Trellix ePO - On-prem** server.

16. **If you stopped the Agent Handlers in step 1, log on to the systems where the Agent Handlers are installed, then open the Windows Services panel. Start the Trellix Event Parser and Trellix Apache services.**

Results

Your **Trellix ePO - On-prem** software is now restored. If needed, double-click the **Launch ePolicy Orchestrator** icon on your desktop to start using your **Trellix ePO - On-prem** server, or browse to the server from a remote web console (`https://<server_name>:<port>`).

Change the server recovery passphrase

You can change the server recovery passphrase when you install **Trellix ePO - On-prem** and link it to a SQL database restored with Disaster Recovery Snapshot records.

Before you begin

You must have administrator rights to change the server recovery passphrase.

Change the server recovery passphrase from the Server Settings page. You can also change the existing passphrase without knowing the previously configured passphrase. Once the passphrase is changed, the next Snapshot will be encrypted using the new passphrase, but the new passphrase is not applied to any Snapshot currently stored in the database.

Important

If you change the passphrase, we recommend that you run another Snapshot task as soon as possible, so that your database contains a snapshot encrypted with a known passphrase.

Task

1. **Select Menu → Configuration → Server Settings, select Disaster Recovery, then click Edit.**
2. **From Server recovery passphrase, click Change passphrase, then type the new passphrase.**

Logon to Trellix ePO - On-prem using Identity Provider

Single Sign-On (SSO) allows you to securely authenticate multiple applications using one set of logon credentials. After configuring SSO for ePO identity provider (IdP), you can log on your existing enterprise IdP, then access your **Trellix ePO - On-prem** account directly without a second logon.

Before you begin, make sure the following conditions are met:

1. The **Trellix ePO - On-prem** version must be 5.10.0 Update 11 or later.
2. You have configured your Identity Provider application.

Download and install the Trellix ePO - On-prem Single Sign-On extension

You can download the **Trellix ePO - On-prem** Single Sign-On extension from the **Trellix** Software Download site using your **Trellix** Grant Number.

1. Search for **Trellix ePolicy Orchestrator - On-prem** and select version 5.10.0.
2. In **Available Downloads,** Select **Filters type** as **EXTENSION** and select **Trellix ePO - On-prem** Single Sign-On version 1.0.0.xxx, and download it to your local **Trellix ePO - On-prem** server.
3. Browse to and select the **ePOSingleSignOn_release_<version_number>.<build_number>.zip** extension file, then click **OK**.

Note

You can also download the extension from the Software Manager of your **Trellix ePO - On-prem** server.

Configuring Single Sign-On to log on to Trellix ePO - On-prem

To configure SSO for your **Trellix ePO - On-prem** server:

1. Configure the IdP application.
2. Input your Security Assertion Markup Language (SAML) configuration information in **Trellix ePO - On-prem**.
3. Update your IdP configuration with the information from **Trellix ePO - On-prem** server.

Configuring the IdP application

Configure a new IdP application in your SSO solution to get the ***IdP Entity Id (Issuer URL)***, ***IdP SSO URL***, and ***X 509 certificate*** to input in your SAML configuration information.

For instructions on how to configure your IdP application, see your identity provider's documentation.

Note

You might need to use placeholder information for the ACS URL and the Audience URI (Service Provider Entity ID) when you configure your third-party IdP. Enter the details when you ***Update your IdP application SAML settings with the information from Trellix ePO - On-prem server***.

Input your SAML configuration information in Trellix ePO - On-prem

Configure the settings in the **IDP SAML Settings** page under **Server Settings** to enable SSO using your IdP application.

1. Enter the information in the **IdP Settings** section.
    - **Import IDP Metadata xml file** — Download the metadata from your IdP, and then click **Import** to upload the metadata to **Trellix ePO - On-prem**.

      Note

      Some IdP's do not support the download of the metadata extension. You need to input data manually, after collecting the necessary details from your IdP application.

    - **SSO Identity provider name** — Enter the name of the Identity Provider.
    - **Service Provider (ePO) Entity Id** — Enter a unique identifier for the Service Provider application configured in IdP.
    - **Service Provider Assertion Consumer Service Url** — Url used to recognize the SAML request. For example: **https://<EPO_SERVER_URL>/core/orionNavigationExtLogin.do**.
    - **Identity Provider Entity Id** — Unique identity of the Identity Provider.
    - **Identity Provider SSO Url** — Single Sign-On Url of the Identity provider.
    - **Identity Provider X 509 Certificate** — Certificate from the Identity Provider used in the Single Sign-On process.
    - **Logout redirect URL** — The link where you navigate after logging out from **Trellix ePO - On-prem**. You can give the home page address of your identity provider.

    After entering the above details, Click **Save**. Once you log off from the ePO application, you will see the **Log On with IDP** option on the main screen.

Update your IdP configuration with the information from Trellix ePO - On-prem Server

After saving the IdP configuration in your **Trellix ePO - On-prem** server, go to your IdP application and edit the SAML settings with the information from **Trellix ePO - On-prem**.

1. **Audience URI (Service Provider Entity ID)** — Enter the Service Provider (ePO) Entity Id from **Trellix ePO - On-prem**.
2. **Single Sign On URL** — Enter the Service Provider Assertion Consumer Service URL from **Trellix ePO - On-prem**.

Assigning the user locale for the identity provider application

When logging in using an identity provider, the user locale is assigned in the following manner:

1. From the user_locale attribute — It is configured in the IdP application to inform the Service Provider application about the locale of a particular user. For example: Fr-fr or, FR_fr.
2. Using the drop-down option — It is present on the logon screen of the **Trellix ePO - On-prem** application.
3. Available as the default locale of the tenant.

Using the Logon with IdP feature

After a successful configuration, you can click the **Log On with IDP** option on the **Trellix ePO - On-prem** logon page (Service Provider initiated SSO), or click the configured application in the IdP console (Identity Provider initiated SSO), to test the logon option.

On successful authentication, you are navigated to a page that displays the following message — **SAML authentication is successful. Close your browser to end your session and contact your administrator for ePO permissions grant.**.

1. You need to request the **Trellix ePO - On-prem** administrator to grant the required permissions.
2. A new user is created in **Trellix ePO - On-prem** with a user name which is similar to the email address used in your IdP application, the authentication type is set to SAML authentication and no permission sets are assigned.
3. An administrator has to log on to the **Trellix ePO - On-prem** console and assign the required permissions to the newly created (IdP) user.

Note

Upon successful completion, the IdP user can now access **Trellix ePO - On-prem** via Single Sign-On.

Single Sign-On Error Messages

You might see some error messages after Single Sign-On to log on to **Trellix ePO - On-prem**.

This table lists error messages and their description for troubleshooting.

Error Messages	Description	Suggested Solution
SAML authentication is successful. Close your browser to end your session and contact your administrator for ePO permissions grant.	After successful SAML authentication, user will be redirected to intermediate ePO page and user will see this message. Same IdP user is created in **Trellix ePO - On-prem** with 'SAML authentication type' without any permissions.	User has to contact the ePO Administrator to get the required permissions. Once Administrator assign the permission, user can again log in into **Trellix ePO - On-prem** through identity provider credentials.
User already present in ePO with different Authentication Strategy. Close your browser to end your session and contact your administrator.	If IdP user is already present in **Trellix ePO - On-prem** with different authentication types like ePO, MVISION, or certificate based authentications, then single sign-on will not work. You	We can't have same user with different authentication type. You have to delete the existing user for single sign-on to work.

Error Messages	Description	Suggested Solution
	will then come across this error message.	
There is an internal error trying to log on to the server. Contact technical support (when trying to do Single Sign-On to **Trellix ePO - On-prem**).	This error occurs when: 1. If Identity Provider Entity Id in **Trellix ePO - On-prem** IdP settings is not matching with Entity Id (Issuer) in IdP application. 2. If Identity Provider X 509 Certificate in **Trellix ePO - On-prem** IdP settings is invalid or does not match with the certificate available in the configured IdP application.	See orion.log for more details about the error message. 1. Update the Identity Provider Entity Id in **Trellix ePO - On-prem** IdP properly. It must be same as of Entity Id (Issuer) in IdP application. 2. Make sure Identity Provider X 509 Certificate in **Trellix ePO - On-prem** IdP settings is same as of certificate available in configured IdP application.

Not all error messages appear in the product interface.

Check the orion.log file for information about a particular error message or contact Trellix Support.

Logon to Trellix ePO - On-prem using Trellix ePO - SaaS

You can now logon to your **Trellix ePO - On-prem** server using your **Trellix ePO - SaaS** account.

To Logon,

1. Configure your **Trellix ePO - On-prem** to logon with your **Trellix ePO - SaaS** account.
2. Logon with **Trellix ePO - SaaS** account.

Before you begin:

1. You must have installed the **Trellix Cloud Bridge** extension on your current **Trellix ePO - On-prem** server.
2. You must have linked an active **Trellix ePO - SaaS** account in **Trellix Cloud Bridge** server settings.
3. Make sure the ePO Logon URL is added while configuring **Trellix Cloud Bridge**. For more information, see Configure **Trellix Cloud Bridge**
4. The **Trellix ePO - On-prem** server has internet connectivity. If you are using a proxy server, make sure that you have configured the proxy server settings properly.
5. You must have configured the proxy and firewall settings to allow communication with the **Trellix ePO - SaaS** server. For more information, see KB90878 for adding firewall settings for **Trellix ePO - SaaS** and IAM.
6. Your **Trellix ePO - On-prem** server date and time must match with the time zone that you have set at the server level.

Configure your Trellix ePO - On-prem to logon with your Trellix ePO - SaaS account

Trellix ePO - SaaS is a multi-tenant, enterprise SaaS model of **Trellix ePO - On-prem**, accessible through an internet browser. You can now add SaaS users to on-premises **Trellix ePO - On-prem** server. Those added users can now log on to their on-premises **Trellix ePO - On-prem** console through IAM using their **Trellix ePO - SaaS** account. To enable **Log On with Trellix ePO - SaaS** feature, follow the below steps:

Task

1. **Log in to the Trellix ePO - On-prem server as an administrator.**
2. **Select Menu → Configuration → Server Settings, then select Trellix ePO - SaaS Cloud Bridge from Setting Categories.** Make sure, the **Trellix ePO - SaaS Cloud Bridge** Server Settings page display the following options:
    - **Status** — The status displays **This server is linked**.
    - **Linked Account** — Contains the email address of the linked **Trellix ePO - SaaS** account.
    - **Trellix ePO - SaaS Customer ID** — The Trellix ePO - SaaS Customer ID that is linked.
    - **ePO Logon URL**— The **Trellix ePO - On-prem** URL being used to access the ePO Server.
3. **Add the Trellix ePO - SaaS users who want to access Trellix ePO - On-prem via Log On with Trellix ePO - SaaS using the following steps —**
    - Select **Menu → User Management → User**, then click **New User** button.
    - In the User name field, type the email address of your **Trellix ePO - SaaS** account.
    - Under **Authentication type**, select **Trellix ePO - SaaS Authentication**.

- Under **Manually assigned permission sets**, assign a permission set for the user.
- Click **Save**.

4. **Upon successful creation of the user, log off from the Trellix ePO - On-prem console.**

Results

Now the **Trellix ePO - On-prem** log-on console displays **Log On with Trellix ePO - SaaS** button.

Logon with Trellix ePO - SaaS account

Once the **Log On with Trellix ePO - SaaS** option is displayed on the **Trellix ePO - On-prem** log-on console, do the following:

Task

1. **Select the option Log On with Trellix ePO - SaaS . You are navigated to the Trellix ePO - SaaS login page. Provide valid Trellix ePO - SaaS credentials to log on to the Trellix ePO - On-prem console.**
2. **If the linked Trellix account has Identity provider (IdP) configured in Trellix ePO - On-prem, you are navigated to the IdP logon page instead of Trellix ePO - On-prem logon page. On entering the IdP credentials, you are logged in successfully to the Trellix ePO - On-prem console.**

Note

If you want to use the **Log On with Trellix ePO - SaaS** feature, you must be present in all three systems that are, **Trellix ePO - On-prem**, Configured Identity Provider and **Trellix ePO - SaaS**.

Using the System Tree and Tags

You can organize, group, and tag your managed systems using the System Tree and Tags features. The System Tree is a hierarchical structure that organizes the systems in your network into groups and subgroups.

Adding systems

You can add systems to your System Tree using these methods:

- Manually add systems to an existing group
- Import systems from a text file
- Active Directory synchronization

Organizing systems

You can organize your System Tree using these methods:

- Manual organization from the console (drag and drop)
- Automatic synchronization with your Active Directory or NT domain server
- Criteria-based sorting, using criteria applied to systems manually or automatically

What the System Tree controls

Your System Tree dictates these items:

- How your policies for different products are inherited
- How your client tasks are inherited
- Which groups your systems go into

If you are creating your System Tree for the first time, these are the primary options available for organizing your systems dynamically:

- Using Active Directory (AD) synchronization
- Dynamically sorting your systems

Note

Although you can use AD synchronization with dynamic System Tree sorting, use only one method to avoid confusion and conflicts.

Organizing systems with the System Tree

Considerations when planning your System Tree

For smaller organizations, your **System Tree** might be simple and contain only a few groups. For larger organizations, we recommend that you must plan systems and group them depending on the unique needs of your network and business.

Grouping systems with similar properties or requirements enables you to manage policies for systems in one place, rather than setting policies for each system individually.

Consider the following criteria to classify the systems into groups:

Criteria to consider	Description
Geographic location	Organize your System Tree in a manner which balances protection and performance. Organize your System Tree to make the best use of network bandwidth. Consider how the server connects to all parts of your network, especially remote locations that use slower WAN or VPN connections, instead of faster LAN connections. You might want to configure updating and agent-server communication policies differently for remote sites to minimize network traffic over slower connections.
Network Location	Many large networks are divided by individuals or groups responsible for managing different parts of the network. Sometimes these borders do not coincide with topological or geographic borders. Who accesses and manages the segments of the System Tree affects how you structure it.
Functional borders	Some networks are divided by the roles of those using the network; for example, Sales and Engineering. Even if the network is not divided by functional borders, you might need to organize segments of the System Tree by functionality if different groups require different policies.
Business Unit	A business group might run specific software that requires special security policies.
Sub-business unit	Supplementary business units that isn't a separate business unit but require the dedicated security policies and management.
Function	The Servers group that has different server types based on function or role. For example, AD Domain

Criteria to consider	Description
	controllers, Mail servers, Sharepoint servers, and SQL servers.
Endpoint type	Classify the devices in your network and group them into laptops, servers, and desktops.
Operating Systems and software	Consider grouping systems with similar operating systems to manage products and policies more easily. If you have legacy systems, you can create a group for them and deploy and manage security products on these systems separately. Alternatively, you can assign a tag to systems based on the operating system type.

After you decide on the basic building blocks for groups in the **System Tree**, you must determine which building blocks to use and in which order based on these factors:

- **Policy assignment** — Do you have many custom product policies to assign to groups based on chassis or function? Do certain business units require their own custom product policy?
- **Network topology** — Do you have sensitive WANs in your organization that a content update might easily saturate? If you have only major locations, this is not a concern for your environment.
- **Client task assignment** — When you create a client task, such as an on-demand scan, do you need to do it at a ***group level***, like a business unit, or ***system type***, like a web server?
- **Content distribution** — Do you have an agent policy that specifies that certain groups must get their content from a specific repository?
- **Operational controls** — Do you need specific rights delegated to your **Trellix ePO - On-prem** administrators that allow them to administer specific locations in the tree?
- **Queries** — Do you need many options when filtering your queries to return results from a specific group in the System Tree?

After you choose the system groups for your tree structure, test the design for maintenance, performance, and protection with a few sample System tree models. There is no specific way to grouping systems, however the design you choose impacts the maintenance work in future.

Here are a few **System Tree** designs:

Example -1

Network location	Endpoint type	Operating system platform
Los Angeles	Desktop	
	Laptop	
	Server	Windows
		SQL
		Linux
San Francisco	Desktop	
	Laptop	
	Server	Windows
		SQL
		Linux

Example -2

Business Unit	Geographic location	Endpoint type	Operating system platform
Accounting	Los Angeles	Server	Windows
	Mumbai	Server	Macintosh
			Windows
	London	Server	Linux
			Windows

Business Unit	Geographic location	Endpoint type	Operating system platform
			SQL
Management	Los Angeles	Desktop	Windows
	Mumbai	Laptop	Macintosh
			Windows
	London	Server	Linux
			Windows
			SQL

Administrator access

When planning your **System Tree** organization, consider the access requirements of users who must manage the systems.

For example, you might have decentralized network administration in your organization, where different administrators have responsibilities over different parts of the network. For security reasons, you might not have an administrator account that can access every part of your network. In this scenario, you might not be able to set policies and deploy agents using a single administrator account. Instead, you might need to organize the **System Tree** into groups based on these divisions and create accounts and permission sets.

Consider these questions:

- Who is responsible for managing which systems?
- Who requires access to view information about the systems?
- Who should not have access to the systems and the information about them?

These questions impact both the **System Tree** organization, and the permission sets you create and apply to user accounts.

Environmental borders and their impact on system organization

How you organize the systems for management depends on the borders that exist in your network. These borders influence the organization of the System Tree differently than the organization of your network topology.

We recommend evaluating these borders in your network and organization, and whether they must be considered when defining the organization of your System Tree.

Topological borders

NT domains or Active Directory containers define your network. The better organized your network environment, the easier it is to create and maintain the System Tree with the synchronization features.

Geographic borders

Managing security is a constant balance between protection and performance. Organize your System Tree to make the best use of limited network bandwidth. Consider how the server connects to all parts of your network, especially remote locations that use slower WAN or VPN connections, instead of faster LAN connections. You might want to configure updating and agent-server communication policies differently for remote sites to minimize network traffic over slower connections.

Political borders

Many large networks are divided by individuals or groups responsible for managing different parts of the network. Sometimes these borders do not coincide with topological or geographic borders. Who accesses and manages the segments of the System Tree affects how you structure it.

Functional borders

Some networks are divided by the roles of those using the network; for example, Sales and Engineering. Even if the network is not divided by functional borders, you might need to organize segments of the System Tree by functionality if different groups require different policies.

A business group might run specific software that requires special security policies. For example, arranging your email Exchange Servers into a group and setting specific exclusions for on-access scanning.

Subnets and IP address ranges

Often, organizational units of a network use specific subnets or IP address ranges, so you can create a group for a geographic location and set IP address filters for it.

You can also use network location, such as IP address, as the primary grouping criterion, if your network isn't spread out geographically.

Tip

Best practice: Consider using sorting criteria based on IP address information to automate System Tree creation and maintenance. Set IP address subnet masks or IP address range criteria for applicable groups win the System Tree. These filters automatically populate locations with the appropriate systems.

Operating systems and software

Consider grouping systems with similar operating systems to manage products and policies more easily. If you have legacy systems, you can create a group for them and deploy and manage security products on these systems separately. Also, by giving these systems a corresponding tag, you can automatically sort them into a group.

Tags and systems with similar characteristics

You can use tags and tag groups to automate sorting into groups.

Tags identify systems with similar characteristics. If you can organize your groups by characteristics, you can create and assign tags based on that criteria. Then you use these tags as group sorting criteria to ensure that systems are automatically placed within the appropriate groups.

If possible, use tag-based sorting criteria to automatically populate groups with the appropriate systems. Plus, to help sort your systems, you can create tag groups nested up to four levels deep, with up to 1,000 tag subgroups in each level. For example, if you can organize your systems using geographic location, chassis type (server, workstation, or laptop), platform (Windows, Macintosh, Linux, or SQL), and user, you might have the tag groups in this table.

Location	Chassis type	Platform	Users
Los Angeles	Desktop	Windows	General
	Laptop	Macintosh	Sales
			Training
		Windows	Accounting
			Management
	Server	Linux	Corporate
		Windows	Corporate
		SQL	Corporate
San Francisco	Desktop	Windows	General
	Laptop	Macintosh	Sales
			Training
		Windows	Accounting
			Management

Location	Chassis type	Platform	Users
	Server	Linux	Corporate
		Windows	Corporate
		SQL	Corporate

System Tree groups

System Tree groups represent a collection of systems. Deciding which systems to group depends on the unique needs of your network and business.

You can group systems based on any criteria that supports your needs:

- Machine-type (for example, laptops, servers, or desktops)
- Geography (for example, North America or Europe)
- Department boundaries (for example, Finance or Marketing)

Groups have these characteristics:

- Administrators or users can create and use them with the appropriate permissions.
- You can include both systems and other groups (subgroups).

Grouping systems with similar properties or requirements into these units allows you to manage policies for systems in one place, rather than setting policies for each system individually.

As part of the planning process, consider the best way to organize systems into groups before building the **System Tree**.

The default **System Tree** structure includes these groups:

- **My Organization** — The root of your **System Tree**.
- **My Group** — The default subgroup added during the **Getting Started** initial software installation. This group name might have been changed during the initial software installation.
- **Lost and Found** — The catch-all subgroup for any systems that have not been or could not be added to other groups in your **System Tree**.

My Organization group

The **My Organization** group, the root of your **System Tree**, contains all systems added to or detected on your network (manually or automatically).

Until you create your own structure, all systems are added by default to **My Organization**. This group name might have been changed during the initial software installation.

The **My Organization** group has these characteristics:

- It can't be deleted.
- It can't be renamed.

My Group subgroup

My Group is a subgroup of the **My Organization** group and is added by default during the **Getting Started** initial software installation.

This group name might have been changed during the initial software installation.

When your network computers run the installation URL, they are grouped by default in **My Group**.

To rename the group, select **Menu** → **Systems** → **System Tree**, in the **System Tree** groups list click **My Group**, then click **System Tree Actions** → **Rename Group**.

Lost and Found subgroup

The **Lost and Found** group is a subgroup of the **My Organization** group.

Depending on the methods that you specify when creating and maintaining the **System Tree**, the server uses different characteristics to determine where to place systems. The **Lost and Found** group stores systems whose locations can't be determined.

The **Lost and Found** group has these characteristics:

- It can't be deleted.
- It can't be renamed.
- Its sorting criteria can't be changed from being a catch-all group, although you can provide sorting criteria for the subgroups that you create in it.
- It always appears last in the **System Tree** list and is not alphabetized among its peers.
- Users must be granted permissions to the **Lost and Found** group to see its contents.
- When a system is sorted into **Lost and Found**, it is placed in a subgroup named for the system's domain. If no such group exists, one is created.

Important

If you delete systems from the **System Tree**, make sure that you select **Remove Trellix Agent on next agent-server communication from all systems**. If the **Trellix Agent** is not removed, deleted systems reappear in the **Lost and Found** group because the **Trellix Agent** still communicates with **Trellix ePO - On-prem**.

Group inheritance

All child subgroups in the **System Tree** hierarchy inherit policies set at their parent groups. These inheritance rules simplify policy and task administration.

- Policies set at the **My Organization** level of the **System Tree** apply to all groups.
- Group policies apply to all subgroups or individual systems in that group.
- Inheritance is enabled by default for all groups and individual systems that you add to the **System Tree**. Default inheritance allows you to set policies and schedule client tasks in fewer places.
- To allow for customization, inheritance can be broken by applying a new policy at any location of the **System Tree**. You can lock policy assignments to preserve inheritance.

In this example, Windows users under the Server group for Los Angeles automatically inherit the Server group policies. Users under the Server group for San Francisco inherit a different set of policies.

System Tree				**Hierarchy**
My Organization				Top-level group
	Los Angeles			Child subgroup of My Organization
		Desktop		Child subgroup of Los Angeles
		Laptop		Child subgroup of Los Angeles
		Server		Child subgroup of Los Angeles
			Windows	Child subgroup of Server
			SQL	Child subgroup of Server
			Linux	Child subgroup of Server

System Tree				Hierarchy
	San Francisco			Child subgroup of My Organization
		Desktop		Child subgroup of San Francisco
		Laptop		Child subgroup of San Francisco
		Server		Child subgroup of San Francisco
	Lost and Found			Child subgroup of My Organization

Sorting your systems dynamically

You can dynamically sort your systems into your **Trellix ePO - On-prem System Tree** using a combination of system criteria and other elements.

Creating the basic groups

Sorting dynamically requires that you create some basic groups for your tree structure. For smaller organizations, your **System Tree** might not be complex and contain only a few groups. For larger organizations, we recommend that you create some groups similar to these sample designs:

- **GEO** — Geographic location
- **NET** — Network location
- **BU** — Business unit
- **SBU** — Subbusiness unit
- **FUNC** — Function of the system (web, SQL, app server)
- **CHS** — Chassis (server, workstation, laptop)

Selecting and ordering the basic groups

After you decide on the basic building blocks for groups in the **System Tree**, you must determine which building blocks to use and in which order based on these factors:

- **Policy assignment** — Do you have many custom product policies to assign to groups based on chassis or function? Do certain business units require their own custom product policy?

- **Network topology** — Do you have sensitive WANs in your organization that a content update might easily saturate? If you have only major locations, this is not a concern for your environment.
- **Client task assignment** — When you create a client task, such as an on-demand scan, do you need to do it at a ***group level***, like a business unit, or ***system type***, like a web server?
- **Content distribution** — Do you have an agent policy that specifies that certain groups must get their content from a specific repository?
- **Operational controls** — Do you need specific rights delegated to your **Trellix ePO - On-prem** administrators that allow them to administer specific locations in the tree?
- **Queries** — Do you need many options when filtering your queries to return results from a specific group in the System Tree?

After you choose the basics for your tree structure, create a few sample **System Tree** models and look at the pros and cons of each design. There is no right way or wrong way to build your **System Tree**, just pluses and minuses depending on what you choose.

Here are a few of the most commonly used **System Tree** designs:

- **GEO** -> **CHS** -> **FUNC**
- **NET** -> **CHS** -> **FUNC**
- **GEO** -> **BU** -> **FUNC**

Active Directory synchronization

If your network runs Active Directory, you can use Active Directory synchronization to create, populate, and maintain parts of the **System Tree**.

Once defined, the **System Tree** is updated with any new systems (and subcontainers) in your Active Directory.

Leverage Active Directory integration to perform these system management tasks:

- Synchronize with your Active Directory structure, by importing systems, and the **Active Directory** subcontainers (as **System Tree** groups), and keeping them up-to-date with Active Directory. At each synchronization, both systems and the structure are updated in the **System Tree** to reflect the systems and structure of Active Directory.
- Import systems as a flat list from the Active Directory container (and its subcontainers) into the synchronized group.
- Control what to do with potential duplicate systems.
- Tag newly imported or updated systems.
- Use the system description, which is imported from Active Directory with the systems.

Use this process to integrate the **System Tree** with your Active Directory systems structure:

1. Configure the synchronization settings on each group that is a mapping point in the **System Tree**. At the same location, configure whether to:
    - Deploy agents to discovered systems.
    - Delete systems from the **System Tree** when they are deleted from Active Directory.
    - Allow or disallow duplicate entries of systems that exist elsewhere in the **System Tree**.

2. Use the **Synchronize Now** action to import Active Directory systems (and possibly structure) into the **System Tree** according to the synchronization settings.
3. Use an NT Domain/Active Directory synchronization server task to regularly synchronize the systems (and possibly the Active Directory structure) with the **System Tree** according to the synchronization settings.

Types of Active Directory synchronization

There are two types of Active Directory synchronization (***systems only*** and ***systems and structure***). Which one you use depends on the level of integration you want with Active Directory.

With each type, you control the synchronization by selecting whether to:

- Deploy agents automatically to systems new to **Trellix ePO - On-prem**. You might not want to configure this setting on the initial synchronization if you are importing many systems and have limited bandwidth. The agent MSI is about 6 MB in size. However, you might want to deploy agents automatically to any new systems that are discovered in Active Directory during subsequent synchronization.
- Delete systems from **Trellix ePO - On-prem** (and remove their agents) when they are deleted from Active Directory.
- Prevent adding systems to the group if they exist elsewhere in the **System Tree**. This setting ensures that you don't have duplicate systems if you manually move or sort the system to another location.
- Exclude certain Active Directory containers from the synchronization. These containers and their systems are ignored during synchronization.

Systems and structure

When using this synchronization type, changes in the Active Directory structure are carried over into your **System Tree** structure at the next synchronization. When systems or containers are added, moved, or removed in Active Directory, they are added, moved, or removed in the corresponding locations of the **System Tree**.

When to use this synchronization type

Use this to ensure that the **System Tree** (or parts of it) look exactly like your Active Directory structure.

If the organization of Active Directory meets your security management needs and you want the **System Tree** to continue to look like the mapped Active Directory structure, use this synchronization type with subsequent synchronization.

Systems only

Use this synchronization type to import systems from an Active Directory container, including those in non-excluded subcontainers, as a flat list to a mapped **System Tree** group. You can then move these to appropriate locations in the **System Tree** by assigning sorting criteria to groups.

If you choose this synchronization type, make sure to select not to add systems again if they exist elsewhere in the **System Tree**. This synchronization type prevents duplicate entries for systems in the **System Tree**.

When to use this synchronization type

Use this synchronization type when:

- You use Active Directory as a regular source of systems for **Trellix ePO - On-prem**.
- The organizational needs for security management do not coincide with the organization of containers and systems in Active Directory.

NT domain synchronization

Use your NT domains as a source for populating your **System Tree**.

When you synchronize a group to an NT domain, all systems from the domain are put in the group as a flat list. You can manage these systems in the single group, or you can create subgroups for more granular organizational needs. Use a method, like automatic sorting, to populate these subgroups automatically.

If you move systems to other groups or subgroups of the **System Tree**, make sure you select to not add the systems when they exist elsewhere in the **System Tree**. This setting prevents duplicate entries for systems in the **System Tree**.

Unlike Active Directory synchronization, only the system names are synchronized with NT domain synchronization; the system description is not synchronized.

Criteria-based sorting

You can use IP address information to automatically sort managed systems into specific groups. You can also create sorting criteria based on tags, which are like labels assigned to systems. You can use either or both to ensure that systems are where you want them in the **System Tree**.

Systems must match only one criterion of a group's sorting criteria to be placed in the group.

After creating groups and setting your sorting criteria, perform a **Test Sort** action to confirm the criteria and sorting order.

Once you have added sorting criteria to your groups, you can run the **Sort Now** action. The action moves selected systems to the appropriate group automatically. Systems that do not match the sorting criteria of any group are moved to **Lost and Found**.

New systems that call into the server for the first time are added automatically to the correct group. However, if you define sorting criteria after the initial agent-server communication, you must run the **Sort Now** action on those systems to move them immediately to the appropriate group, or wait until the next agent-server communication.

Sorting status of systems

On any system or collection of systems, you can enable or disable **System Tree** sorting. If you do disable **System Tree** sorting on a system, it is excluded from sorting actions, except when the **Test Sort** action is performed. During a test sort, the sorting status of the system or collection is considered and can be moved or sorted from the **Test Sort** page.

System Tree sorting settings on the Trellix ePO - On-prem server

For sorting to take place, it must be enabled on the server and on the systems. By default, once sorting is enabled, systems are sorted at the first agent-server communication (or next, if applying changes to existing systems) and are not sorted again.

Test sorting systems

Use this feature to view where systems are placed during a sort action. The **Test Sort** page displays the systems and the paths to the location where they are sorted. Although this page does not display the sorting status of systems, if you select systems on the page (even ones with sorting disabled), clicking **Move Systems** places those systems in the location identified.

How settings affect sorting

You can choose three server settings that determine whether and when systems are sorted. Also, you can choose whether any system can be sorted by enabling or disabling **System Tree** sorting on selected systems in the **System Tree**.

Server settings

The server has three settings:

- **Disable System Tree sorting** — Prevents other **Trellix ePO - On-prem** users from configuring sorting criteria on groups by mistake and moving systems to undesirable locations in the **System Tree**.
- **Sort systems on each agent-server communication** — Sorts systems again at each agent-server communication. When you change sorting criteria on groups, systems move to the new group at their next agent-server communication.
- **Sort systems once** — Systems are sorted at the next agent-server communication and not sorted again as long as this setting is selected. You can still sort a system, however, by selecting it and clicking **Sort Now**.

System settings

You can disable or enable **System Tree** sorting on any system. If disabled on a system, that system isn't sorted, regardless of how the sorting action is taken. If enabled, systems can be sorted using the manual **Sort Now** action, and can be sorted at agent-server communication.

IP address sorting criteria

In many networks, subnets and IP address information reflect organizational distinctions, such as geographical location or job function. If IP address organization coincides with your needs, consider setting IP address sorting criteria for groups.

In this version of **Trellix ePO - On-prem**, this functionality has changed, and now allows for the setting of IP address sorting criteria randomly throughout the tree. As long as the parent has no assigned criteria, you no longer need to ensure that the sorting criteria of the child group's IP address is a subset of the parent's. Once configured, you can sort systems at agent-server communication, or only when a sort action is manually initiated.

⚠ Caution

IP address sorting criteria must not overlap between different groups. Each IP address range or subnet mask in a group's sorting criteria must cover a unique set of IP addresses. If criteria does overlap, the group where those systems end up depends on the order of the subgroups on the **System Tree Group Details** tab. You can check for IP address overlap using the **Check IP Integrity** action in the **Group Details** tab.

Tag-based sorting criteria

In addition to using IP address information to sort systems into the appropriate group, you can define sorting criteria based on the tags assigned to systems.

Tag-based criteria can be used with IP address-based criteria for sorting.

Group order and sorting

For additional flexibility with **System Tree** management, configure the order of a group's subgroups, and the order of their placement during sorting.

When multiple subgroups have matching criteria, changing this order can change where a system ends up in the **System Tree**. If you are using catch-all groups, they must be the last subgroup in the list.

Catch-all groups

Catch-all groups are groups whose sorting criteria is set to **All others** on the group's **Sorting Criteria** page.

Only subgroups at the last position of the sort order can be catch-all groups. These groups receive all systems that were sorted into the parent group, but were not sorted into any of the catch-all's peers.

How a system is added to the System Tree when sorted

When the **Trellix Agent** communicates with the server for the first time, the server uses an algorithm to place the system in the **System Tree**. When it cannot find an appropriate location for a system, it puts the system in the **Lost and Found** group.

On each agent-server communication, the server attempts to locate the system in the **System Tree** by **Trellix Agent** GUID. Only systems whose agents have already called into the server for the first time have a **Trellix Agent** GUID in the database. If a matching system is found, it is left in its existing location.

If a matching system is not found, the server uses an algorithm to sort the systems into the appropriate groups. Systems can be sorted into any criteria-based group in the **System Tree**, as long as each parent group in the path does not have non-matching criteria. Parent groups of a criteria-based subgroup must have no criteria or matching criteria.

The sorting order assigned to each subgroup (defined in the **Group Details** tab) determines the order that the server considers subgroups for sorting.

1. The server searches for a system without a **Trellix Agent** GUID (the **Trellix Agent** has never before called in) with a matching name in a group with the same name as the domain. If found, the system is placed in that group. This can happen after the first Active Directory or NT domain synchronization, or when you have manually added systems to the **System Tree**.
2. If a matching system is still not found, the server searches for a group of the same name as the domain where the system originates. If such a group is not found, one is created under the **Lost and Found** group, and the system is placed there.
3. Properties are updated for the system.
4. The server applies all criteria-based tags to the system if the server is configured to run sorting criteria at each agent-server communication.

5. What happens next depends on whether **System Tree** sorting is enabled on both the server and the system.
    - If **System Tree** sorting is disabled on either the server or the system, the system is left where it is.
    - If **System Tree** sorting is enabled on the server and system, the system is moved based on the sorting criteria in the System Tree groups.

    Note

    Systems that were added using Active Directory or NT Domain synchronization have **System Tree** sorting disabled by default. With **System Tree** sorting disabled, systems are not sorted on the first agent-server communication

6. The server considers the sorting criteria of all top-level groups according to the sorting order on the My Organization group's **Group Details** tab. The system is placed in the first group with matching criteria or a catch-all group it considers.
    - Once sorted into a group, each of its subgroups is considered for matching criteria according to their sorting order on the Group Details tab.
    - Sorting continues until there is no subgroup with matching criteria for the system, and is placed in the last group found with matching criteria.
7. If such a top-level group is not found, the subgroups of top-level groups (without sorting criteria) are considered according to their sorting.
8. If such a second-level criteria-based group is not found, the criteria-based third-level groups of the second-level unrestricted groups are considered.

    Note

    Subgroups of groups with criteria that doesn't match are not considered. A group must have matching criteria or have no criteria for its subgroups to be considered for a system.

9. This process continues down through the **System Tree** until a system is sorted into a group.

    Note

    If the server setting for **System Tree** sorting is configured to sort only on the first agent-server communication, a flag is set on the system. The flag means that the system can never be sorted again at agent-server communication unless the server setting is changed to enable sorting on every agent-server communication.

10. If the server cannot sort the system into any group, it is placed in the **Lost and Found** group within a subgroup that is named after its domain.

View system information details

You can view detailed information and status about a system in the System Tree.

Task

1. **Open the** System Tree **page.**
   a. Select **Menu** → **Systems** → **System Tree**.
   b. Click **Systems** tab and any system row.
2. **Click Customize to change the information displayed in the three system information monitors:**
   - Summary — Displays the results of the Trellix Agent Communication Summary, by default.
   - Properties — Displays information about the systems location in your network and the agent installed, by default.
   - Query monitor — Displays the system-specific results for the Threat Events in the Last 2 Weeks query, by default.
3. **Click one of these tabs, to view additional details about the selected system:**

Option	Description
System Properties	Displays details about the system. For example, operating system, memory installed, and connection information.
Products	Lists one of these product states: • Installed Product — The state of the installed product for which the **Trellix Agent** has communicated with the install event. • Uninstalled Product — The state of the uninstalled product for which the **Trellix Agent** has communicated with the uninstall event. • Deployment Task status of product — The state of the deployment task of a newer version of an existing product which is getting installed. **Note:** The status of the deployment task of the same version of the product or an older version of the same product is ignored.
Applied Policies	Displays the name of policies applied to this system and lists them alphabetically.
Applied Client Tasks	Displays the name of client tasks assigned to this system and lists them alphabetically.
Threat Events	Lists threat and other events, plus detailed information about those events,

Option	Description
Trellix Agent	List configuration information about the **Trellix Agent** installed on the system. **Note:** Click **More** to display additional **Trellix Agent** configuration and status information.

Creating and populating System Tree groups

To help you visualize your managed systems by geographic or machine-type values, create **System Tree** groups and populate the groups with systems.

Drag selected systems to any group in the **System Tree** to populate groups. Drag and drop to move groups and subgroups in the **System Tree**.

There is no single way to organize a **System Tree**. Because every network is different, your **System Tree** organization can be as unique as your network layout. You can use more than one method of organization.

Note

By default, the **System Tree** expands automatically when new systems are added by dragging and dropping. To disable this option, select **Settings** > **System Tree Settings** and uncheck the **Auto-Expand Tree Nodes** option.

For example, if you use Active Directory in your network, consider importing your Active Directory containers rather than your NT domains. If your Active Directory or NT domain organization does not make sense for security management, you can create your **System Tree** in a text file and import it. If you have a smaller network, you can create your **System Tree** by hand and add each system manually.

Add systems to an existing group manually

Add specific systems to a selected group.

Task

1. **Open the New Systems page.**
    a. **Select Menu → Systems → System Tree.**
    b. **Click New Systems.**
2. **Select whether to deploy the Trellix Agent to the new systems, and whether the systems are added to the selected group, or to a group according to sorting criteria.**

3. **Next to Target systems, type the NetBIOS name for each system in the text box, separated by commas, spaces, or line breaks. Alternatively, click Browse to select the systems.**

Option	Definition
Domain	Select the required domain from the drop-down list. The client systems in the selected domain are listed.
Show/Hide Filter	Shows or hides these options used to find and filter client systems: • **Show selected rows** — Displays only the rows you have selected.
Actions	Specifies the actions you can perform on the selected client systems, including: • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this option to select the columns to display. • **Export Table** — Opens the **Export** page. Use this option to specify the format and the package of files to be exported. You can save or email the list of client systems in the selected domain.

4. **Specify other options as needed.**
   If you selected **Push agents and add systems to the current group**, you can enable automatic **System Tree** sorting. Do this to apply the sorting criteria to these systems.
5. **Click OK.**

New Systems page

Use this page to add specific systems to the selected group.

Note

The options that appear depend on the **How to add systems** method you select.

Option definitions

Option	Definition
Abort after	Specifies the number of minutes after the start of the attempted agent deployment before the deployment quits.
Agent version	Specifies the version of the agent to send and install on the selected systems. Agent versions that are available depends on which agent installation packages are checked in to the **Main Repository**. To deploy agents to non-Windows systems: • The target systems must be configured to support SSH network protocol. For more information on these configurations and permission levels, see the product documentation provided with your target systems Operating System (OS).
Credentials for agent installation	Specifies the domain name, user name, and password associated with the user account when you want to install the agent on selected systems. Use this format **<domain>\<user>**; for example, **technical_group\jsmith**.
Push Agent using	Select the connection used for the deployment as either: • **All Agent Handlers**. • **Selected Agent Handler** — Select the server from the list.
File to import	Click **Browse** to upload the text file (.txt) with the systems to import.
How to add systems	Specifies how to add the new systems: • **Add systems to the current group, but do not deploy agents** — Adds specified systems to the current group, but agents are not deployed to them.

Option	Definition
	• **Create and download agent installation package** — Creates a custom **Trellix Agent** installation package in which you can embed credentials for the installation. • **Create url for client-side agent download** — Creates a custom agent installation URL that endpoint users can use to install the **Trellix Agent**. • **Deploy agents and add systems to current group** — Deploys agents to the specified systems and places them in the selected group of the **System Tree**. • **Deploy agents and place systems in the System Tree according to sorting criteria** — Deploys agents to the specified systems in the groups of the **System Tree** according to sorting criteria. • **Import systems from a text file into the selected group, but do not deploy agents** — Imports systems from a properly generated text file, but does not deploy agents to these systems.
Import from file	Select system import method: • **Systems and System Tree structure** • **Systems only**
Installation path	Specifies the path on the client system (default is **<system_drive>\epoagent**) where you want to install the agent. The location you specify must exist on client systems. Available only when you select an option that deploys the agent.
Number of attempts	Specifies the number of deployment attempts before it quits. Type **0** for continuous attempts.
Retry interval	Specifies the interval in minutes and seconds between deployment attempts.

Option	Definition
Suppress agent installation user interface	When selected, hides the installation of the agent from the user. Available only when you select an option that deploys the agent.
Systems that exist elsewhere in the System Tree	Select how the systems are organized in the System Tree after importing.
System Tree sorting	Disables **System Tree** sorting on all specified systems when they are added to the **System Tree**.
Target systems	Specifies the names of the system (up to 40 characters) as it appears in the **System Tree**. Each system name must be unique. The name can't contain these characters: `= ; , : [ ] * ? / |` Separate system names by commas, spaces, or line breaks. You can cut and paste a list of systems from a text file.

Create groups manually

Create **System Tree** subgroups.

Task

1. **Open the New Subgroups dialog box.**
   a. **Select Menu → Systems → System Tree.**
   b. **Select a group, then click New Subgroup.**

   Tip

   You can also create more than one subgroup at a time.

2. **Type a name then click OK.**
   The new group appears in the **System Tree**.
3. **Repeat as needed until you are ready to populate the groups with systems. Use one of these processes to add systems to your System Tree groups:**
   - Typing system names manually.

- Importing them from NT domains or **Active Directory** containers. You can regularly synchronize a domain or a container to a group for ease of maintenance.
- Setting up IP address-based or tag-based sorting criteria on the groups. When agents check in from systems with matching IP address information or matching tags, they are automatically placed in the appropriate group.

Export systems from the System Tree

Export a list of systems from the **System Tree** to a .txt file for later use. Export at the group or subgroup level while retaining the **System Tree** organization.

It can be useful to have a list of the systems in your **System Tree**. You can import this list into your **Trellix ePO - On-prem** server to quickly restore your previous structure and organization.

Note

This task does not remove systems from your **System Tree**. It creates a .txt file that contains the names and structure of systems.

Task

1. **Select Menu → Systems → System Tree.**
2. **Select the group or subgroup containing the systems you want to export, then from the Actions menu, select Export Systems.**
3. **Select whether to export:**
   - **All systems in this group** — Exports the systems in the specified **Source group**, but does not export systems listed in nested subgroups under this level.
   - **All systems in this group and subgroups** — Exports all systems at and below this level.
4. **Click OK.**
   The **Export** page opens. You can click the **systems** link to view the system list, or right-click the link to save a copy of the **ExportSystems.txt** file.

Create a text file of groups and systems

Create a text file of the NetBIOS names for your network systems that you want to import into a group. You can import a flat list of systems, or organize the systems into groups.

Define the groups and their systems by typing the group and system names in a text file. Then import that information into **Trellix ePO - On-prem**.

For large networks, use network utilities, such as the NETDOM.EXE utility available with the Microsoft Windows Resource Kit, to generate text files with complete lists of the systems on your network. Once you have the text file, edit it manually to create groups of systems, and import the whole structure into the **System Tree**.

Regardless of how you generate the text file, you must use the correct syntax before importing it.

Task

1. **List each system on its own line. To organize systems into groups, type the group name followed by a backslash (\), then list the system belonging to that group, each on a separate line.**

```
GroupA\system1
GroupA\system2
GroupA\GroupB\system3
GroupC\GroupD
```

2. **Verify the names of groups and systems, and the syntax of the text file, then save the text file to a temporary folder on your server.**

Import systems and groups from a text file

Import systems or groups of systems into the **System Tree** from a text file you have created and saved.

Task

1. **Open the New Systems page.**
   a. **Select Menu → Systems → System Tree.**
   b. **Click New Systems.**
2. **Select Import systems from a text file into the selected group, but do not push agents.**
3. **Select whether the import file contains:**
   - **Systems and System Tree Structure**
   - **Systems only (as a flat list)**
4. **Click Browse, then select the text file.**
5. **Select what to do with systems that already exist elsewhere in the System Tree.**
6. **Click OK.**

Results

The systems are imported to the selected group in the **System Tree**. If your text file organized the systems into groups, the server creates the groups and imports the systems.

Sort systems into criteria-based groups

Configure and implement sorting to group systems. For systems to sort into groups, sorting must be enabled, and sorting criteria and the sorting order of groups must be configured.

Add sorting criteria to System Tree groups

Sorting criteria for **System Tree** groups can be based on IP address information or tags.

Task

1. **Select Menu → Systems → System Tree, click the Group Details tab, then select the group in the System Tree.**
2. **Next to Sorting criteria click Edit. The sorting criteria page for the selected group appears.**

3. **Select Systems that match any of the criteria below (IP addresses or tags), then the criteria selections appear.**

   Note

   Although you can configure multiple sorting criteria for the group, a system only has to match a single criterion to be placed in this group.

4. **Configure the criteria. Options include:**
   - **IP addresses** — Use this text box to define an IP address range or subnet mask as sorting criteria. Any system whose address falls within it is sorted into this group.

     Note

     You can use either the IPv4 (**xxx.xxx.xxx.xxx**, where **x** is **0 – 255**; for example, **161.69.0.0** through **161.69.255.255**), or IPv6 address format. For example, **3FFE:85B:1F1F::A9:1234** is displayed as **[3FFE:085B:1F1F:0000:0000:0000:00A9:1234]**. Alternatively, specify the IP subnet mask and number of significant bits that you want to include in the current site or group. Use the format **xxx.xxx.xxx.xxx/yy**, where **x** is **0 – 255** and **y** is **0 – 32**. For example, the IP subnet mask of **161.69.0.0/16** equals the range **161.69.0.0** through **161.69.255.255**. The IP subnet mask of **161.69.255.0/18** equals the range **161.69.192.0** through **161.69.255.255**.

   - **Tags** — Click **Add Tags** and perform these steps in the **Add Tags** dialog box.
     - Click the tag name, or names, to add and sort the systems in this parent group.

       Note

       To select multiple tags, click **Ctrl +** the tag names.

     - Click **OK**.

     Note

     The tags selected appear in **Tags** on the **Sorting Criteria** page and next to **Sorting Criteria** on the **Group Details** page.

5. **Repeat as needed until sorting criteria is reconfigured for the group, then click Save.**

Enable System Tree sorting on the server

For systems to be sorted, **System Tree** sorting must be enabled on both the server and the systems.

In this task, if you sort only on the first agent-server communication, all enabled systems are sorted on their next agent-server communication and are never sorted again for as long as this option is selected. However, these systems can be sorted again manually by taking the **Sort Now** action, or by changing this setting to sort on each agent-server communication.

If you sort on each agent-server communication, all enabled systems are sorted at each agent-server communication as long as this option is selected.

Task

1. **Select Menu → Configuration → Server Settings, then select System Tree Sorting in the Setting Categories list and click Edit.**
2. **Select whether to sort systems only on the first agent-server communication or on each agent-server communication.**

Enable or disable System Tree sorting on systems

The sorting status of a system determines whether it can be sorted into a criteria-based group.

You can change the sorting status on systems in any table of systems (such as query results), and also automatically on the results of a scheduled query.

Task

1. **Select Menu → Systems → System Tree → Systems, then select the systems you want.**
2. **Select Actions → Directory Management → Change Sorting Status, then select whether to enable or disable System Tree sorting on selected systems.**
3. **In the Change Sorting Status dialog box, select:**
    - **Disable System Tree Sorting**
    - **Enable System Tree Sorting**

Note

Depending on the setting for **System Tree** sorting, these systems are sorted on the next agent-server communication. Otherwise, they can only be sorted with the **Sort Now** action.

Sort systems manually

Sort selected systems into groups with criteria-based sorting enabled.

Task

1. **Select Menu → Systems → System Tree → Systems, then select the group that contains the systems.**
2. **Select the systems then click Actions → Directory Management → Sort Now. The Sort Now dialog box appears.**

Note

If you want to preview the results of the sort before sorting, click **Test Sort** instead. (However, if you move systems from within the **Test Sort** page, all selected systems are sorted, even if they have **System Tree** sorting disabled.)

3. **Click OK to sort the systems.**

Import Active Directory containers

Import systems from **Active Directory** containers directly into your **System Tree** by mapping source containers to **System Tree** groups.

Mapping **Active Directory** containers to groups allows you to:

- Synchronize the **System Tree** structure to the **Active Directory** structure so that when containers are added or removed in **Active Directory**, the corresponding group in the **System Tree** is added or removed.
- Delete systems from the **System Tree** when they are deleted from **Active Directory**.
- Prevent duplicate entries of systems in the **System Tree** when they exist in other groups.

Task

1. **Select Menu → Systems → System Tree → Group Details, then select a group in the System Tree for mapping an Active Directory container to.**

   Note

   You cannot synchronize the **Lost and Found** group of the **System Tree**.

2. **Next to Synchronization type, click Edit. The Synchronization Settings page for the selected group appears.**
3. **Next to Synchronization type, select Active Directory. The Active Directory synchronization options appear.**
4. **Select the type of Active Directory synchronization you want to occur between this group and the Active Directory container (and its subcontainers):**
   - **Systems and container structure** — Select this option if you want this group to truly reflect the **Active Directory** structure. When synchronized, the **System Tree** structure under this group is changed to reflect the **Active Directory** container that it's mapped to. When containers are added or removed in **Active Directory**, they are added or removed in the **System Tree**. When systems are added, moved, or removed from **Active Directory**, they are added, moved, or removed from the **System Tree**.
   - **Systems only** — Select this option if you only want the systems from the **Active Directory** container (and non-excluded subcontainers) to populate this group, and this group only. No subgroups are created when mirroring **Active Directory**.
5. **Select whether to create a duplicate entry for systems that exist in another group of the System Tree.**

   If you are using **Active Directory** synchronization as a starting point for security management, and plan to use **System Tree** management functionality after mapping your systems, do not select this option.

6. **In the Active Directory domain section, you can:**
   - Type the fully qualified domain name of your **Active Directory** domain.
   - Select from a list of already registered LDAP servers.
7. **Next to Container, click Add and select a source container in the Select Active Directory Container dialog box, then click OK.**
8. **To exclude specific subcontainers, click Add next to Exceptions and select a subcontainer to exclude, then click OK.**

9. **Select whether to deploy the Trellix Agent automatically to new systems. If you do, configure the deployment settings.**

Tip

Best practice: Because of its size, do not deploy the **Trellix Agent** during the initial import if the container is large. Instead, import the container, then deploy the **Trellix Agent** to groups of systems at a time, rather than all at once.

10. **Select whether to delete systems from the System Tree when they are deleted from the Active Directory domain. Optionally choose whether to remove agents from the deleted systems.**
11. **To synchronize the group with Active Directory immediately, click Synchronize Now.**
Clicking **Synchronize Now** saves any changes to the synchronization settings before synchronizing the group. If you have an **Active Directory** synchronization notification rule enabled, an event is generated for each system that is added or removed. These events appear in the **Audit Log**, and are queryable. If you deployed agents to added systems, the deployment is initiated to each added system. When the synchronization completes, the **Last Synchronization** time is updated, displaying the time and date when the synchronization finished, not when any agent deployments completed.

Tip

Best practice: Schedule an NT Domain/**Active Directory** synchronization server task for the first synchronization. This server task is useful if you are deploying agents to new systems on the first synchronization, when bandwidth is a larger concern.

12. **When the synchronization is complete, view the results with the System Tree.**

Results

Tip

When the systems are imported, distribute agents to them if you did not select to do so automatically.

Best practice: Set up a recurring NT Domain/**Active Directory** synchronization server task to keep your **System Tree** current with any changes to your Active Directory containers.

Import NT domains into an existing group

Import systems from an NT domain into a group you created manually.

You can populate groups automatically by synchronizing entire NT domains with specified groups. This approach is an easy way to add all systems in your network to the **System Tree** at once as a flat list with no system description.

If the domain is large, you can create subgroups to assist with policy management or organization. To do this, first import the domain into a group of your **System Tree**, then manually create logical subgroups.

Tip

To manage the same policies across several domains, import each of the domains into a subgroup under the same group. The subgroups will inherit the policies set for the top-level group.

When using this method:

- Set up IP address or tag sorting criteria on subgroups to automatically sort the imported systems.
- Schedule a recurring NT Domain/Active Directory synchronization server task for easy maintenance.

Task

1. **Select Menu → Systems → System Tree → Group Details and select or create a group in the System Tree.**
2. **Next to Synchronization type, click Edit. The Synchronization Settings page for the selected group appears.**
3. **Next to Synchronization type, select NT Domain. The domain synchronization settings appear.**
4. **Next to Systems that exist elsewhere in the System Tree, select what to do with systems that exist in another group of the System Tree.**

   Tip

   Best practice: Don't select **Add systems to the synchronized group and leave them in their current System Tree location**, especially if you are using the NT domain synchronization only as a starting point for security management.

5. **Next to Domain, click Browse and select the NT domain to map to this group, then click OK. Alternatively, you can type the name of the domain directly in the text box.**
   When typing the domain name, do not use the fully-qualified domain name.
6. **Select whether to deploy the Trellix Agent automatically to new systems. If you do so, configure the deployment settings.**

   Tip

   Best practice: Because of its size, do not deploy the **Trellix Agent** during the initial import if the container is large. Instead, import the container, then deploy the **Trellix Agent** to groups of systems at a time, rather than all at once.

7. **Select whether to delete systems from the System Tree when they are deleted from the NT domain. You can optionally choose to remove agents from deleted systems.**
8. **To synchronize the group with the domain immediately, click Synchronize Now, then wait while the systems in the domain are added to the group.**
   Clicking **Synchronize Now** saves changes to the synchronization settings before synchronizing the group. If you have an NT domain synchronization notification rule enabled, an event is generated for each system added or removed. These events appear in the **Audit Log**, and are queryable. If you selected to deploy agents to added systems, the deployment is initiated to each added system. When the synchronization is complete, the **Last Synchronization** time is updated. The time and date are when the synchronization finished, not when any agent deployments completed.
9. **To synchronize the group with the domain manually, click Compare and Update.**
   a. **If you are going to remove any systems from the group with this page, select whether to remove their agents when the system is removed.**
   b. **Select the systems to add to and remove from the group as necessary, then click Update Group to add the selected systems. The Synchronize Setting page appears.**
10. **Click Save, then view the results in the System Tree if you clicked Synchronize Now or Update Group.**

Results

Once the systems are added to the **System Tree**, distribute agents to them if you did not select to deploy agents as part of the synchronization.

Consider setting up a recurring NT Domain/Active Directory synchronization server task to keep this group current with new systems in the NT domain.

Schedule System Tree synchronization

Schedule a server task that updates the **System Tree** with changes in the mapped domain or Active Directory container.

Depending on group synchronization settings, this task automates these actions:

- Adds new systems on the network to the specified group.
- Adds new corresponding groups when new Active Directory containers are created.
- Deletes corresponding groups when Active Directory containers are removed.
- Deploys agents to new systems.
- Removes systems that are no longer in the domain or container.
- Applies site or group policies and tasks to new systems.
- Prevents or allows duplicate entries of systems that still exist in the **System Tree** after you moved them to other locations.

The **Trellix Agent** can't be deployed to all operating systems in this manner. You might need to distribute the **Trellix Agent** manually to some systems.

Task

1. **Open the Server Task Builder.**
    a. **Select Menu → Automation → Server Tasks.**
    b. **Click New Task.**
2. **On the Description page, name the task and choose whether it is enabled once it is created, then click Next.**
3. **From the drop-down list, select Active Directory Synchronization/NT Domain.**
4. **Select whether to synchronize all groups or selected groups. If you are synchronizing only some groups, click Select Synchronized Groups and select specific ones.**
5. **Click Next to open the Schedule page.**
6. **Schedule the task, then click Next.**
7. **Review the task details, then click Save.**

Tip

In addition to running the task at the scheduled time, you can run this task immediately: on the **Server Tasks** page next to the task, click **Run**.

Update a synchronized group with an NT domain manually

Update a synchronized group with changes to the associated NT domain.

The update includes the following changes:

- Adds systems currently in the domain.
- Removes systems from your **System Tree** that are no longer in the domain.
- Removes agents from all systems that no longer belong to the specified domain.

Task

1. **Select Menu → Systems → System Tree → Group Details, then select the group that is mapped to the NT domain.**
2. **Next to Synchronization type, click Edit.**
3. **Select NT Domain, then click Compare and Update near the bottom of the page.**
4. **If you are removing systems from the group, select whether to remove the agents from systems that are removed.**
5. **Click Add All or Add to import systems from the network domain to the selected group.**

   Click **Remove All** or **Remove** to delete systems from the selected group.

6. **Click Update Group when finished.**

Move systems within the System Tree

Move systems from one group to another in the **System Tree**. You can move systems from any page that displays a table of systems, including the results of a query.

Tip

In addition to the steps below, you can also drag and drop systems from the **Systems** table to any group in the **System Tree**.

Even in a perfectly organized **System Tree** that's regularly synchronized, you might need to move systems manually between groups. For example, you might need to periodically move systems from the **Lost and Found** group.

Task

1. **Select Menu → Systems → System Tree → Systems, then select the systems.**
2. **Click Actions → Directory Management → Move Systems to open the Select New Group page.**
3. **Select whether to enable or disable System Tree sorting on the selected systems when they are moved.**
4. **Select the group to place the systems in, then click OK.**
   If you move systems between groups, the moved systems inherit the policies assigned to their new group.

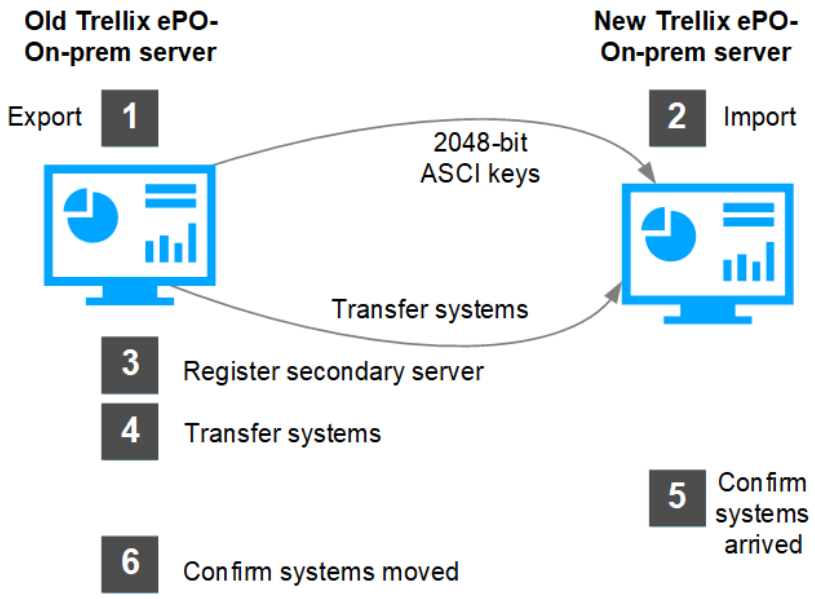
How Transfer Systems works

You can use the **Transfer Systems** command to move managed systems from one **Trellix ePO - On-prem** server to another. For example, from an old **Trellix ePO - On-prem** server to a new **Trellix ePO - On-prem** 5.x server.

You might need to transfer managed systems if you're upgrading the server hardware and operating system or the **Trellix ePO - On-prem** software version.

1. Export your security keys from the old server.
2. Import the security keys in the new server.
3. Register the new **Trellix ePO - On-prem** server to the old server.
4. Transfer your current systems to the new **Trellix ePO - On-prem** server.
5. Confirm that you can view the systems in the new server's System Tree.
6. Confirm that the systems no longer appear in the old server's System Tree.

This graphic shows the major processes to transfer systems from one **Trellix ePO - On-prem** server to another.



Transfer systems from one server to another

Use the **Transfer Systems** option to move systems from an old **Trellix ePO - On-prem** 4.x server to a new **Trellix ePO - On-prem** 5.x server.

You might see the following error when you register the servers and enable the **Transfer Systems** options with **Automatic Sitelist Import**:

ERROR: Master agent-server keys must be imported into the remote server before importing the sitelist. Go to Server Settings to export security keys from this server. Visiting this link now causes you to lose any unsaved changes to this registered server.

Both keys (1024 and 2048) must be imported for successful registration so the **Automatic Sitelist Import** can save without issue.

Export security keys from the old server

Export the 2048-bit and 1024-bit security keys.

Task

1. **On the older server, select Menu → Configuration → Server Settings.**
2. **Click Security Keys under the Setting Categories column, click Edit.**
   The **Edit Security Keys** page opens.
3. **Save the 2048-bit keys listed under the Agent-server secure communication keys list.**
   a. **Click the 2048-bit key and click Export.**
   b. **Click OK to confirm the export key confirmation message.**
   c. **Click Save.**
   d. **Type or browse to a path where you want to save the security key .zip file.**
   e. **Click Save again.**
4. **Save the 1024-bit keys listed under the Agent-server secure communication keys list.**
   a. **Click the 1024-bit key and click Export.**
   b. **Click OK to confirm the export key confirmation message.**
   c. **Click Save.**
   d. **Type or browse to a path where you want to save the security key .zip file.**
   e. **Click Save again.**

Import security keys to the new server

Import the 2048-bit and 1024-bit security keys from the old server on the new server.

Task

1. **On the new server, select Menu → Configuration → Server Settings.**
2. **Click Security Keys from the Setting Categories column, then click Edit.**
3. **Click Import.**
4. **Import the 2048-bit key.**
   a. **Click Browse, locate the exported 2048-bit security key .zip file.**
   b. **Click Open.**
   c. **Click Next.**
   d. **Confirm that you have selected the correct key on the Summary tab, and click Save.**
5. **Import the 1024-bit key.**
   a. **Click Browse, locate the exported 1024-bit security key .zip file.**
   b. **Click Open.**
   c. **Click Next.**
   d. **Confirm that you have selected the correct key on the Summary tab, and click Save.**

Register the new server to the old server

Register the new server. For example, register a **Trellix ePO - On-prem** 5.x server to a **Trellix ePO - On-prem** 4.x server.

Task

1. **From the old server, log on to the console.**
2. **Click Menu → Configuration → Registered Servers.**
3. **Click New Server.**
4. **Select Trellix ePO from the Server type drop-down list, type a name for this server in the Name section, and click Next.**
5. **Type the credentials to the new server and click Test Connection.**
6. **If the test is successful, select Enable for the Transfer systems entry.**
7. **Make sure that Automatic sitelist import is selected, and click Save.**

Results

- The **Manual sitelist import** option is also available and can be used if you want to do a manual import by selecting an existing **SiteList.xml** file.
- You can obtain the **SiteList.xml** file to use for this process in the following folder on the server where the agents are being transferred to: **<ePO_Installation_Directory>\DB\SiteList.xml**
- On a **Trellix ePO - On-prem** 4.6 server, you can select only version 4.6 or previous versions as the **Trellix ePO - On-prem** version. When you test the connection to the database of the registered server, you see the following warning: **Database connection successful! Warning Versions mismatch!** You can safely ignore the warning. The**Trellix ePO - On-prem** version selected (4.6) does not match the database (5.x) you have tested.

Transfer systems between servers

After you have imported the keys and registered the new server, you can use the old server to initiate the transfer process.

Task

1. **Log on to the old server.**
2. **Select Menu → Systems → System Tree.**
3. **Select the systems you want to transfer.**

   Note

   Ensure that the selected systems are communicating to the old server, before you transfer them.

4. **Click Actions → Agent → Transfer Systems.**
5. **Select the new server and click OK to transfer.**

   Note

   Two agent-server communication intervals must occur before the system appears in the **System Tree** of the new server. The length of time required depends on your configuration. The default agent-server communication interval is one hour.

Check the status of transferred computers

Verify that your systems now appear on the new server.

Task

1. **From the new server, select Menu → System Tree → Systems.**
   Your systems are listed in the **System Tree**.
2. **From the old server, select Menu → System Tree → Systems.**
   Your systems are not listed in the **System Tree**.

How the Automatic Responses feature interacts with the System Tree

Before you plan the implementation for **Automatic Responses**, understand how this feature works with the **System Tree**.

Note

This feature does not follow the inheritance model used when enforcing policies.

Automatic Responses use events that occur on systems in your environment and configured response rules. These rules are associated with the group that contains the affected systems and each parent above it. When an event occurs, it is delivered to the server. If the conditions of a rule are met, designated actions are taken.

This design allows you to configure independent rules at different levels of the **System Tree**.

These rules can have different:

- **Thresholds for sending a notification message**. For example, an administrator of a particular group wants to be notified if viruses are detected on 100 systems in 10 minutes. But an administrator does not want to be notified unless viruses are detected on 1,000 systems in the whole environment in the same amount of time.
- **Recipients for the notification message**. An administrator for a particular group might want to be notified only if a specified number of virus detection events occur in the group. Or, an administrator wants each group administrator to be notified if a specified number of virus detection events occur in the whole **System Tree**.

System Tree location does not filter server events.

System Tree page

The **System Tree** page provides a visual representation of your managed network.

Option definitions

Option	Definition
Common actions	• **New Systems** — Opens the **New Systems** page.

Option	Definition
	• **New Subgroups** — Creates a subgroup in the **System Tree**.
System Tree options	
System Tree *default groups*	• **My Organization** — The root of your **System Tree**. **Note:** This group can't be deleted or renamed. • **Lost and Found** — The catch-all for any systems that are not added to other groups in your **System Tree**. **Note:** This group can't be deleted or renamed.
System Tree Actions	• **New Subgroup** — Creates a subgroup in the **System Tree**. • **Rename Group** — Renames the selected group. • **Delete Group** — Deletes the selected group or groups. **Note:** If you don't select **Remove Trellix Agent from all systems** , the systems in the group reappear in the Lost and Found group because the **Trellix Agent** continues to communicate to **Trellix ePO - On-prem**. **Also, unless you select Remove agent installed products from all systems, the product software remains installed on the systems deleted from the System Tree.** • **Export Systems** — Exports a list of systems from the **System Tree** to a .txt file for later use. • **Sort Now** — Sorts selected systems into groups with criteria-based sorting enabled.

Systems tab

Option definitions

Category	Option	Definition
Computer options	**Custom**	Select custom filters and row selection to restrict the items displayed.
Filter options	**Quick find**	Type a term to filter the list results. Click **Apply** to start the search. Click **Clear** to delete text from the **Quick find** text entry box.
	Show selected rows	Displays only the rows you selected.
Actions	**Choose Columns**	Opens the **Choose Columns** page, allowing you to select the columns that are displayed on the **Systems** page.
	Export Table	Allows you to export this table.
	Tag	Allows you to modify the tags in the **Tags** column using: • **Apply tag** — Apply a tag manually to selected systems in the **System Tree**. • **Clear tag** — Remove a tag manually from the selected systems in the **Systems** page. • **Exclude tag** — Specifies system tags to exclude from the selected systems on the **Systems** page.

Category	Option	Definition
	Agent	Specifies the actions that can be taken on agents on the selected systems, including: • **Modify Policies on a Single System** — Opens the **Policy Assignment** page to edit the policy assignments of the selected system. This option is available only when one system is selected. • **Modify Tasks on a Single System** — Opens the **Client Tasks** page to create or edit client tasks assigned to this system. This option is available only when one system is selected. • **Set Description** — Opens the **Set Description** dialog box. This dialog box provides a description for the selected system. This description is included in the system details. • **Set Policy and Inheritance** — Applies a policy to the selected systems and resets or breaks the inheritance of the policy from the system group. • **Show Client Events** — Opens the **Client Event** page. This page lets you find events for the selected system. • **Show Threat Events** — Opens the **Threat Event Log** page. This page allows you to check for threat events for the selected system.

Category	Option	Definition
	Directory Management	Specifies the actions that you can use to manage systems in your directory, including: • **Change Sorting Status** — Allows you to enable or disable **System Tree** sorting. Enabled systems are sorted when selected and the **Sort Now** option is used. The systems can be sorted at each agent-server communication, depending on how **System Tree Sorting** is configured on the **Server Settings** page. • **Clear Agent GUID Sequence Error Count** — Deselects the **Sequence Error** count generated due to duplicate Global Unique IDs (GUID). • **Delete**— Deletes all selected systems from the **System Tree**. • **Export Systems** — Exports the list of systems (including their path to their location in the **System Tree**) to a text file. • **Move GUID to Duplicate List and Delete System** — Moves the GUID of the agent to the block list and deletes the system from the **System Tree**. • **Move Systems** — Opens the **Choose New Group for Selected Systems** page. This page lets you select one location to place all groups. • **Sort Now** — Sorts the system to a location in the **System Tree** based on the sorting criteria of groups.

Category	Option	Definition
		• **Test Sort** — Displays where the selected systems would appear if sorted, based on how sorting criteria is configured in the **System Tree**. • **View Assigned Policies** — Displays the policies applied to recent users.

Assigned Policies tab

Option definitions

Option	Definition
Filter options	• **Product** — Specifies which product's assigned policies are displayed. • **Enforcement Status** — Indicates whether the product's policy assignments for the selected group are enforced. If a policy is not enforced, any conflicting changes that have occurred on affected systems are not corrected at the policy enforcement interval.
Category	Specifies the policy categories for the product you selected.
Policy	Specifies the policy, in each category, that is assigned to the user.
Server	Specifies the server the policy is from.
Inherit From	Displays from where the policies were inherited.
Broken Inheritance	Displays "None" if the policy inheritance has not been broken.

Option	Definition
Actions column	Actions in this column affect the policy in the corresponding row. These actions include: • **Edit Assignment** — Opens the **Policy Assignment** page for this policy, where you can change settings that include: ▫ The parent policy source ▫ The assigned policy ▫ Whether policy inheritance is locked • **View Effective Policy** — Opens the **Policy Details** page for this policy.
Actions menu	Specifies the actions you can perform on the selected policies, including: • **Copy Assignments** — Displays the **Copy Policy Assignment** page, allowing you to choose which policy assignments for this system are copied. You are then directed to choose a system on which to paste the assignments. • **Export All Assignments** — Exports all displayed assignments to an XML file. • **Export Table** — Displays the **Export** page allowing you to choose the way the table is exported. • **Import Assignments** — Imports previously exported policy assignments. • **Paste Assignments** — Pastes recently copied assignments to the selected system.

Assigned Client Tasks tab

Option definitions

Option	Definition
Filter options	• **Preset** — Select the preset filter you want to use to filter the list.

Option	Definition
	Note: Only items that meet the filter criteria are displayed. • **Quick find** — Type a term to filter the list results. Click **Apply** to start the search. Click **Clear** to delete text from the **Quick find** text entry box.
Actions column	• **Delete** — Deletes the selected **Assigned Client Task**. • **Edit Assignment** — Starts the **Client Task Assignment Builder**, where you can change the selected **Client Task Assignment** and its schedule.
Actions menu	• **Choose Columns** — Opens the **Choose Columns** page, where you can select which columns are displayed in the **Assigned Client Tasks** pane. • **Export All System Tree Assignments** — Opens the **Export** page, where you can click the link to open the assignments XML file, or right-click the link to download and save the assignments file. • **Export Table** — Opens the **Export** page, where you can export a file with the details of client tasks listed in the **Assigned Client Tasks** pane. Exporting client task details is useful, for example, to create a file to report on the client task assignments in your environment. To create a complete report on all client tasks, all tasks must be assigned at the **My Organization** level. **Note:** This action does not export the actual client task assignments. Exporting the table is a reporting function. The exported content is at the group level. • **Import Assignments** — Opens the **Client Task Assignment Importer** page, where you can browse to a saved assignments XML file and import the file to client tasks and client task assignments.

Option	Definition
	Note: Importing conflicting items overwrite the existing identically named task object and assumes their assignments. • **New Client Task Assignment** — Starts the **Client Task Assignment Builder**, where you can assign and manage client task objects to run on managed systems in your environment.

Group Details tab

Option definitions

Category	Option	Definition
Filter options	**Group**	Displays the name of the selected group. Click **Edit** to change the group name.
	Sorting criteria	Displays the sorting criteria or sorting criteria type assigned to the selected group. Click **Edit** to change the sorting criteria.
	Notes	Allows you to edit the displayed notes.
System Tree options	**Check IP Integrity**	Opens the **IP Integrity Check** dialog box and displays the output of the IP address integrity check.
	Choose Columns	Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the **Group Details** tab.

Category	Option	Definition
	Delete Group	Deletes the selected group.
	Export Table	Opens the **Export** page to specify the format and the package of files to be exported. You can save or email the exported file.
	Export Tree Structure	Opens the **Download File** page to download exported data.
	Import Tree Structure	Opens the **Import Tree Structure** page to input or browse to the file to import. Allows you to select a text file (.txt) that can be imported to define your **System Tree** structure. **Tip:** Consider using this feature when you want to import a previously exported file containing your tree structure. For example, if you are restoring your server. This action overwrites your existing **System Tree** structure.
	Move Group	Moves the selected group to a user-specified location of the **System Tree**.
	New Subgroup	Creates a subgroup of the selected group.
	Rename Group	Renames the selected group.

Agent Deployment tab

Option definitions

Option	Definition
Filter options	• **Preset** — Select the preset filter you want to use to filter the list. Only items that meet the filter criteria are displayed. • **Show selected rows** — Displays only the rows you selected.
Create Agent Deployment URL	The custom URL used to download the **Trellix Agent** installer. Copy the URL and share it with managed system users for manual installation. **Create Agent Deployment URL** page • **URL name** — Specifies a name for the customized **Trellix Agent** smart installer URL. • **Agent Version** — Specifies the version of the **Trellix Agent** to send and install on the selected systems. The **Trellix Agent** versions that are available depend on which **Trellix Agent** installation packages are checked in to the **Main Repository**. • **Assign to Agent Handler** — Select Agent Handler assignment. ▫ **All Agent Handlers** — Downloads the **Trellix Agent** configuration files from the primary Agent Handler or the Trellix ePO server and lists all Agent Handlers in the **Sitelist.xml** for download. ▫ **Selected Agent Handler** — Downloads the **Trellix Agent** configuration and installation files from the selected Agent Handler. ▫ **Secondary Agent Handler** — Downloads the **Trellix Agent** configuration and installation files from the specified Agent Handler if the primary Agent Handler fails.
Actions	• **Choose Columns** — Opens the **Choose Columns** page allowing you to select the columns that are displayed on the **Agent Deployment** tab.

Option	Definition
	• **Create Agent Deployment URL** — Opens the **Agent Deployment URL** page allowing you to create a URL for **Agent Deployment**. • **Delete Agent Deployment URL** — Deletes the selected **Agent Deployment URL**. • **Enable/Disable Agent Deployment URL** — Enables or disables the client system users from deploying the agent using the URL. • **Export Table** — Displays the **Export** page allowing you to choose the way the table is exported. • **View Agent Deployment URL** — Displays the **Agent Deployment URL**.

Systems: Information page

View information about the systems in your **System Tree**.

The content displayed on this page is divided into two groups:

- **System information monitors** — These customizable monitors display important information about the selected system at a glance. The default monitors are described in the option definitions table.
- **System information tabs** — System information is organized into tabs, each displaying a specific set of data. As new products are checked in to your server, more tabs are added to this page. Properties reported in the default tabs are defined in the option definitions table.

Option definitions

Category	Option	Definition
System information monitors	**Summary**	By default, the summary monitor displays the results of the **Trellix Agent Communication Summary** query.
	Properties	By default, the properties monitor displays information about the systems location in your network and the agent installed. You can customize this monitor to display the specific

Category	Option	Definition
		system properties that are most important to you.
	Query monitor	By default, the query monitor displays the system-specific results for the **Threat Events in the Last 2 Weeks** query. **Note:** Queries configured without first configuring **Computer Properties** are not valid.
System Properties tab	**Agent GUID**	Displays the GUID assigned to the **Trellix Agent** installed on this system.
	Communication Type	Displays the protocol used when communicating with this system. Communication types include HTTP and HTTPS.
	CPU Serial Number	Serial number of the CPU.
	CPU Speed	Speed in Hz of the CPU.
	CPU Type	Type of CPU.
	Custom 1 through 4	These fields are the four entries per system in the **Trellix ePO - On-prem** database that you can use for your own purposes.
	Default Language	The default language of the operating system.
	Description	Displays the user-configured description (with **Edit**

Category	Option	Definition
		Description) of the system in **Trellix ePO - On-prem**.
	DNS Name	Displays the full Domain Name System for this system.
	Domain Name	Displays the domain on the network that contains this system.
	Excluded Tags	Lists any tags that this system has been excluded from. Excluding a system from a tag prevents that system from receiving actions assigned to all systems of a particular tag.
	Free Disk Space (GB)	The amount of free space on the local disk of the system.
	Free Memory (MB)	The amount of free memory on this system.
	Free System Drive Space (MB)	The amount of free drive space available on this system. This value might differ from the amount of free disk space in instances where one system hosts multiple virtual machines.
	Installed Products	Displays the managed products installed on this system.
	IP Address	Displays the network IP address of this system.
	Is 64 Bit OS	Displays whether the operating system on this system is 64-bit.

Category	Option	Definition
	Is Laptop	Displays whether this system is a laptop.
	Last Communication	Displays the date and time when the **Trellix Agent** on this system last communicated with **Trellix ePO - On-prem**.
	Last Update	Displays the date and time the last time this system called into the server.
	Last Sequence Error	Displays the last time a sequence error occurred on this system.
	MAC Address	Displays the MAC address of the system.
	Managed State	Displays whether the system is managed or unmanaged.
	Management Type	Displays the method for managing this system. For example, the most common management type is the **Trellix Agent**.
	Number of CPUs	Displays the number of central processing units in this system.
	Operating System	Displays the name of the operating system that the system is running.
	OS Build Number	Displays the build number of the operating system running on the system.

Category	Option	Definition
	OS OEM Identifier	Displays the operating system original equipment manufacturer (OEM) identifier. Each manufacturer is assigned a unique OEM identifier. As a result, you can use this information to determine the manufacturer of the system.
	OS Platform	Displays the operating system platform for the system. For example, the operating system platform for your system might be server or desktop.
	OS Service Pack Version	Displays the Service Pack version of the operating system running on the system.
	OS Type	Displays the type of operating system running on the system. For example, Windows 2003.
	OS Version	Displays the version of the operating system running on this system.
	Product Coverage Reports	Displays the version of product coverage reports, when applicable.
	Sequence Errors	Displays how many sequence errors have occurred on this system.
	Server Key	Displays the server key that the system uses to authenticate

Category	Option	Definition
		with your **Trellix ePO - On-prem** server.
	Subnet Address	Displays the IP address of the subnet where this system is located.
	Subnet Mask	Displays the subnet mask address of the subnet where this system is located.
	System Description	Reports the computer name for this system.
	System Location	Displays the **System Tree** group where this system is located.
	System Name	Displays the NETBIOS name of the system.
	System Location	Displays the path to the group in the **System Tree** that contains this system.
	System Tree Sorting	Displays whether this system is enabled for **System Tree** sorting.
	Tags	Displays all tags currently applied to this system.
	Time Zone	Displays the time zone of this system. For example, Pacific Standard Time.
	To Be Transferred	Displays whether this system is set to be transferred to another server.

Category	Option	Definition
	Total Disk Space	Displays the total disk space available on this system.
	Total Physical Memory	Displays the total physical memory installed on this system.
	Used Disk Space	Displays the amount of disk space currently in use on this system.
	User Name	Displays the user name logged on to this system at the time of the last update.
	Vdi	Displays whether the **Trellix Agent** is installed on a non-persistent virtual image.
Products tab	**Product**	Lists one of these product states: • Installed Product — The state of the installed product for which the **Trellix Agent** has communicated with the install event. • Uninstalled Product — The state of the uninstalled product for which the **Trellix Agent** has communicated with the uninstall event. • Deployment Task status of product — The state of the deployment task of a newer version of an existing product which is getting installed.

Category	Option	Definition
		Note: The status of the deployment task of the same version of the product or an older version of the same product is ignored.
	Version	Specifies the version number of each deployed product.
	Dat Version	Specifies the version number of the DAT deployed to the system.
	Action Type	Specifies only the latest action state. For example, Install or Uninstall. **Note:** If you click an uninstalled product, this message appears: **Product has been uninstalled and no product properties available for this system.**
	Reported Date	Specifies the reported date and time, by the **Trellix Agent**, for the selected product's last action type. Format: MM/DD/YY HH:MM:SS AM/PM Time Zone.
	Status	Specifies the status of the selected product's latest action type. For example, Successful, Pending, or Failure.
Applied Policies tab	**Policy Name**	Displays the name of policies applied to this system. Policies are listed alphabetically.

Category	Option	Definition
	Policy Assignment Origin	• **Tree assignment** — Indicates that the policy is assigned to the system based on **System Tree** location. • **Rule System-based** — Indicates that the policy is assigned to the system based on policy assignment rules.
	Edit Status	• **Editable** — Indicates that you can edit the policy. • **ReadOnly** — Indicates either that you don't have permissions to edit the policy, or that the policy is a **Trellix Default** policy, which can't be edited. • **Shared To Others** — Indicates that the policy has been copied to other systems. These polices can be edited. • **Shared From Other** — Indicates that the policy has been copied from other systems. These policies can't be edited.
	Policy Settings Up-To-Date	Identifies whether the policy that is applied to the system has been edited in **Trellix ePO - On-prem** since the last agent-server communication.
Applied Client Tasks tab	**Task Name**	Displays the name of client tasks assigned to this system. Tasks are listed alphabetically.
	Task Assigned	• **True** — Indicates that the task was assigned to the system based on a tag.

Category	Option	Definition
		• **False** — Indicates that the task was assigned to the system based on **System Tree** assignment.
	Task Settings Up-To-Date	Identifies whether the task that is applied to the system has been edited in **Trellix ePO - On-prem** since the last agent-server communication.
Threat Events tab **Tip:** Click an event to see more information about the event.	**Quick find**	Filters the threat events list by the term entered. Click **Apply** to apply the filter. Click **Clear** to remove the filter.
	Event Generated Time	Displays the time when the event took place.
	Event ID	Displays the identifier for the class of event.
	Event Description	Displays a brief description of the event.
	Event Category	Displays the category of the event.
	Action Taken	Displays the action that was taken in response to the event.
Trellix Agent tab	**Agent-to-Server Communication Interval**	Displays the interval for configuring the agent on this system to communicate with the server.

Category	Option	Definition
	Agent-to-Server Communication Port	Displays which port the agent on this system uses when communicating with the server.
	Cluster Node	Displays whether the system is a node in your clustered server environment.
	Policy Enforcement Interval	Displays the interval for configuring the agent on this system to enforce new and updated security policies.
Actions	**Tag**	Specifies the actions you can take on system tags on systems in your network, including: • **Apply Tag** — Specifies a tag and applies it to the selected systems. • **Clear Tag** — Removes a specified tag from the selected systems. • **Exclude Tag** — Specifies a tag that cannot be applied to selected systems.
	Agent	Specifies the actions that can be taken on agents on the selected systems. • **Modify Policies on a Single System** — Takes you to the **Policy Assignment** page, where you can edit an assigned policy, or assign a different policy to the selected system. • **Modify Tasks on a Single System** — Takes you to the **Client Tasks** page, where you

Category	Option	Definition
		can change or create client tasks to be carried out on the selected system. • **Set Description** — Opens the **Set Description** dialog box, where you can supply a description for the selected system. This description is included in the system details. • **Set Policy & Inheritance** — Opens the **Assign Policy** page for all selected systems. Use this page to set or change policies and inheritance assigned to the selected systems. • **Show Client Events** — Opens the **Audit Log** page and displays only entries triggered by the selected client system. • **Show Threat Events** — Opens the **Threat Event Log** page and displays **Threat Events** for only the selected systems.
	Directory Management	Specifies the actions that you can use to manage systems in your directory. • **Change Sorting Status** — Specifies whether **System Tree** sorting is enabled on selected systems. • **Clear Agent GUID Sequence Error Count** — Removes the **Sequence Error** count generated due to duplicate Global Unique IDs (GUID). • **Delete** — Deletes the selected systems from the **System Tree**. Optionally, you can remove the

Category	Option	Definition
		agent on the system at the same time. • **Move GUID to Duplicate List and Delete System** — Moves the GUID of the agent to the **Duplicate List** and deletes the system from the **System Tree**. • **Move Systems** — Moves all selected systems to a specified group in the **System Tree**. If you are using **System Tree** sorting in your environment, and you don't want the systems moved again at the next agent-server communication, disable **System Tree** sorting on the systems. • **Sort Now** — Sorts the selected systems into groups based on sorting criteria. Systems with **System Tree** sorting disabled are not sorted. • **Test Sort** — Takes you to the **Test Sort** page, where you view where the selected systems end up when sorted. From this page, you can move all systems to the sorting target groups, regardless of whether the system has **System Tree** sorting enabled. • **View Assigned Policies** — Opens the **Policy Assignment** page, where you can review and act on policies assigned to the selected system.

System Information page

View further details of any system.

Option definitions

Option	Definition
CPU Serial Number	Serial number of the CPU.
CPU Speed	Speed in Hz of the CPU.
CPU Type	Type of CPU.
Custom 1 through 4	These options are the four entries per system in the **Trellix ePO - On-prem** database which you can use for your own purposes.
Default Language	The default language of the operating system.
Description	Specifies the user-configured description (with **Edit Description**) of the system in **ePolicy Orchestrator - On-prem**.
DNS Name	Specifies the DNS name of the system.
Domain Name	Specifies the domain on the network that contains the system.
Free Disk Space	The amount of free space in MB (megabyte) on the local disk of the system.
Free Memory	The amount of free memory in bytes on the system.
IP Address	Specifies the network IP address of the system.
IPX Address	Specifies the Novell Internet Packet Exchange (IPX) address of the system.
Last Communication	Specifies the date and time when this system last called into the **Trellix ePO - On-prem** server.
MAC address	Specifies the MAC address of the system.

Option	Definition
Number Of CPUs	Specifies the number of system CPUs.
OS Build Number	Specifies the operating system build number.
OS OEM Identifier	Specifies the operating system original equipment manufacturer (OEM) identifier number.
OS Platform	Specifies the operating system platform type that the system is running, for example, server or professional.
OS Service Pack Version	Specifies the operating system Service Pack installed.
OS Type	Specifies the operating system type, for example, Windows 7 or Windows 2008 R2.
OS Version	Specifies the operating system version number.
Subnet Address	Specifies the IP address subnet address assigned to the system.
Subnet Mask	Specifies the IP address subnet mask assigned to the system.
System Description	Specifies the NETBIOS name of the system.
System Name	Specifies the name of the system.
Time Zone	Specifies the time zone assigned to the system.
Total Disk Space	Specifies the total disk space on the system.
Total Physical Memory	Specifies the total amount of physical memory on this system.

Option	Definition
User Name	Specifies the user name logged on to the system at the time of the last update.

Tags

Create tags in Trellix ePO - SaaS

You can create tags and group them according to their relevance to tasks for a particular domain or systems with a specific configuration.

Task

1. **Select Menu → Systems → Tag Catalog → New Tag.**
2. **On the New Tag pane, enter a name.**
3. **Click + in the Criteria row or click Add below the Criteria row to open the Properties Catalog pane.**
4. **Select the system properties that you want to include.**
5. **Specify value for the selected system property.**
6. **Expand Evaluation to select whether systems are evaluated against the tag's criteria only when the Run Tag Criteria action is taken, or also at each agent-server communication.**

   Note

   These options are unavailable if criteria is not configured. When systems are evaluated against a tag's criteria, the tag is applied to systems that match the criteria.

7. **Expand Restrictions and select Restrict usage to the below Permission Sets to restrict a tag to specific Permission Sets. Select the Permission Sets so that only those users belonging to these selected Permission Sets have access to this tag.**
   By default, **Do not restrict by Permission Sets** is selected.
   After you save the tag, you can see this on the **Restrictions (Permission Sets)** column on the **Tags** pane.
8. **Expand Usage to see the Policy Assignment rules, Client Task Assignments and Server Tasks that the tag is associated with.**
9. **Verify the details you have specified, then click Save.**
   The page displays the number of systems when evaluated against its criteria.

Results

The tag is added under the selected tag group in the **Tag Group Tree** pane on the **Tag Catalog** page.

Manage tags

Once tags are created, you can edit, delete, and move the tags.

Task

1. **Select Menu → Systems → Tag Catalog.**
2. **From the Tags list, select a tag or multiple tags, then perform one of these tasks:**
   a. **Edit tag —** Click the tag that you want to edit, then on the **Tag Details** pane, you can edit these settings:
      i. Select and configure the criteria.

      Note

      To apply the tag automatically, you must configure criteria for the tag.

      ii. Select whether systems are evaluated against the tag's criteria only when the **Run Tag Criteria** action is taken, or also at each agent-server communication.

      Note

      These options are unavailable if criteria was not configured. When systems are evaluated against a tag's criteria, the tag is applied to systems that match the criteria and are not excluded from the tag.

      iii. Select **Restrict usage to the below Permission Sets** to restrict a tag to specific Permission Sets. Select the Permission Sets so that only those users belonging to these selected Permission Sets have access to this tag.
      iv. Verify the information about this page, then click **Save**.

      Note

      This page displays the number of systems that receive this tag when evaluated against its criteria.

   The tag is updated on the **Tag Catalog** page under the selected tag group in the **Tag Tree**.
   b. **Delete tag —** Click **Actions → Delete**, then from the **Delete** dialog-box, click **OK** to delete the tag.
   c. **Move tag to another Tag Group —** Click **Actions → Move Tags**, then from the **Move Tags** dialog-box select the destination tag subgroup for the tag, then click **OK** to move the tag.

   Note

   You can also drag and drop the tags into the tag groups in the **Tag Group Tree**.

Create, delete, and change tag subgroups

Tag subgroups allow you to nest tag groups up to four levels deep, with up to 1,000 tag subgroups under a single parent group. These tag groups allow you to use criteria-based sorting to automatically add systems to the correct groups.

Task

1. **Select Menu → Systems → Tag Catalog.**

2. **Perform one of these tasks for a tag subgroup:**
    a. **Create a tag subgroup** — Use these steps:
        i. In the **Tag Tree**, select the tag group (or parent tag group) where you want to create the tag subgroup.

        Note

        My Tags is the default top-level tag group added during **Trellix ePO - On-prem** installation.

        ii. Click **New Subgroup** to see the **New Subgroup** dialog box.
        iii. In the **Name** field, enter a descriptive name for the new tag subgroup.
        iv. Click **OK** to create the tag subgroup.
    b. **Rename a tag subgroup** — Use these steps:
        i. In the **Tag Tree**, select the tag subgroup that you want to rename.
        ii. Click **Tag Tree Actions** → **Rename Group** to open the **Rename Subgroup** dialog box.
        iii. In the **Name** field, enter the new name for the tag subgroup.
        iv. Click **OK** and the tag subgroup is renamed.
    c. **Delete a tag subgroup** — Use these steps:
        i. In the **Tag Tree**, select the tag subgroup that you want to delete.
        ii. Click **Actions** → **Delete**. An **Action: Delete** confirmation dialog box appears.
        iii. If you still want to delete the tag subgroup, click **OK** and the tag subgroup is removed.

Exclude systems from automatic tagging

Prevent systems from having specific tags applied.

Tip

You can also use a query to collect systems, then exclude the tags from those systems from the query results.

Task

1. **Select Menu → Systems → System Tree → Systems, then select the group that contains the systems in the System Tree.**
2. **Select one or more systems in the Systems table, then click Actions → Tag → Exclude Tag.**
3. **In the Exclude Tag dialog box, select the tag group, select the tag to exclude, then click OK.**

    Tip

    To limit the list to specific tags, type the tag name in the text box under **Tags**.

4. **Verify that the systems have been excluded from the tag:**
    a. **Select Menu → Systems → Tag Catalog, then select the tag or tag group from the list of tags.**
    b. **Next to Systems with tag, click the link for the number of systems excluded from the criteria-based tag application. The Systems Excluded from the Tag page appears.**
    c. **Verify that the systems are in the list.**

Apply tags using queries

You can use queries to extract the specific list of systems and apply tags on systems, based on selected tags. In addition, you can remove and exclude tags from the listed systems. For example, you can apply the **Server** tag, then remove the **Workstation** tag.

Before you begin

Create tags

Task

1. **Open the Server Task Builder.**
    a. **Select Menu → Automation → Server Tasks.**
    b. **Click New Task.**
2. **On the Description page, name and describe the task, then click Next.**
3. **Select Enabled in the Schedule status to run the task at the next scheduled occurrence.**
   If you select **Disabled**, the task runs when you click **Run**.
4. **From the Actions drop-down list, select Run Query.**
5. **In the Query field, select one of these queries from the Trellix Groups tab, then click OK.**
    - **Inactive Agents**
    - **Duplicate Systems Names**
    - **Systems with High Sequence Errors**
    - **Systems with no Recent Sequence Errors**
    - **Unmanaged Systems**
6. **Select the language for displaying the results.**
7. **From the Sub-Actions list, select one of these subactions to take on the query result.**
    - **Apply Tag** — Applies a selected tag to the systems returned by the query.
    - **Clear Tag** — Removes a selected tag on the systems returned by the query. Select **Clear All** to remove all tags from the systems in the query results.
    - **Exclude Tag** — Excludes systems from the query results if they have the selected tag applied to them.
8. **From the Select Tag window, select a tag group from the Tag Group Tree and optionally filter the list of tags by specifying Tags.**

    Note

    Click the **+** button to add more actions. Be careful to place the actions in the order that you want them to occur.

9. **Click Next.**
10. **Schedule the task, then click Next.**
11. **Verify the configuration of the task, then click Save.**

Results

The task is added to the list on the **Server Tasks** page.

Apply tags manually

You can select systems and apply the tags manually.

Task

1. **Select Menu → Systems → System Tree → Systems, then select the group that contains the required systems.**
2. **Select the systems, then click Actions → Tag → Apply Tag.**
3. **In the Apply Tag dialog box, select the tag group, select the tag to apply, then click OK.**
   Only those tags to which you have permission are listed in the **Apply Tag** dialog box.
4. **Verify that the tags have been applied:**
   a. **Select Menu → Systems → Tag Catalog, then select a tag or tag group from the list of tags.**
   b. **Next to Systems with tag in the details pane, click the link for the number of systems tagged manually. The Systems with Tag Applied Manually page is displayed.**
   c. **Verify that the systems are in the list.**

Clear tags from systems

Remove tags from selected systems.

Task

1. **Select Menu → Systems → System Tree → Systems, then select the group that contains the systems you want.**
2. **Select the systems, then click Actions → Tag → Clear Tag.**
3. **In the Clear Tag dialog box, perform one of these steps, then click OK.**
   - Remove a specific tag — Select the tag group, then select the tag.

     Tip

     To limit the list to specific tags, type the tag name in the text box under **Tags**.

   - Remove all tags — Select **Clear All**.

   Note

   All tags are cleared except Deployment Tags.

4. **Verify that the tags have been removed:**
   a. **Select Menu → Systems → Tag Catalog, then select a tag or tag group in the list of tags.**
   b. **Next to Systems with tag in the details pane, click the link for the number of systems tagged manually. The Systems with Tag Applied Manually page appears.**
   c. **Verify that the systems are not included in the list.**

Apply tags automatically

A tag can be automatically assigned to the systems if they meet the criteria you have defined.

Before you begin

Create tags

Task

1. **Select Menu → Systems → Tag Catalog.**
2. **Select the tag or tag group from the Tags list.**
3. **Click Run Tag Criteria from the Actions column.**
4. **On the Run Tag Criteria window, select whether to reset manually tagged and excluded systems.**
   Resetting manually tagged and excluded systems removes the tag from systems that don't match the criteria, and applies the tag to systems that match criteria but were excluded from receiving the tag.
5. **Click OK.**
   The number of systems to which the tag is applied is displayed at the bottom of the page.

Results

The tag is applied to all systems that match the criteria.

Apply tags on a schedule

You can schedule a server task that runs and applies the tags on systems.

Before you begin

Create tags

Task

1. **Open the Server Task Builder.**
   a. **Select Menu → Automation → Server Tasks.**
   b. **Click New Task.**
2. **Specify Name and Notes for the task.**
3. **Select Enabled in the Schedule Status to run the task at the scheduled time.**
4. **Select Run Tag Criteria from the drop-down list, then select a tag from the Tag drop-down list.**
5. **Select whether to reset manually tagged and excluded systems, which will,**
   - Removes the tag on systems that don’t match the criteria
   - Applies the tag to systems that match the criteria but were excluded from receiving the tag
6. **Click Next.**
   The **Schedule** page is displayed.
7. **Schedule the task, then click Next.**
8. **Click Save.**

Results

The server task is added to the list on the **Server Tasks** page.

User accounts and permission sets

User accounts

User accounts allow you to control how people access and use **Trellix ePO - On-prem**.

You can create user accounts manually, then assign each account an appropriate permission set. You can also configure your **Trellix ePO - On-prem** server to allow users to log on using Windows authentication, but this requires configuration and set up of multiple settings and components.

While user accounts and permission sets are closely related, they are created and configured using separate steps.

Authentication versus authorization

Authentication is the process of determining if a user is permitted to log on to **Trellix ePO - On-prem** by verifying the user's identity and matching the credentials supplied by the user to something the system trusts. For example, by providing the correct user name and password for an **Trellix ePO - On-prem** user account, an Active Directory account, or a certificate.

Authorization is the process of determining what actions an authenticated user is permitted to perform in **Trellix ePO - On-prem**. For example, adding new users or creating policies. Permissions and permission sets control what a user is authorized to perform in **Trellix ePO - On-prem**.

Managing users

Before a user can access **Trellix ePO - On-prem**, a user account must be created and assigned a permission set. **Trellix ePO - On-prem** allows you to manually configure the user account. You can also configure **Trellix ePO - On-prem** so that when a member of an Active Directory group tries to log on for the first time, a **Trellix ePO - On-prem** account for that user is automatically created with a permission set assigned to it.

User Authentication Types

Trellix ePO - On-prem supports three types of authentication.

ePO authentication — The user name and password are stored in **Trellix ePO - On-prem** and **Trellix ePO - On-prem** authenticates the user.

Windows authentication — The Windows domain and user name details are stored in **Trellix ePO - On-prem**, and the user is authenticated by a Windows domain controller. By default **Trellix ePO - On-prem** authenticates against the domain that the **Trellix ePO - On-prem** server is a member of. Windows users who can't authenticate by the parent domain can enable the Windows Authentication feature and specify the details of the untrusted domains.

Certificate-based authentication — Enable certificate-based authentication to allow your users to access **Trellix ePO - On-prem** with a valid client certificate instead of a user name and password.

Edit user accounts

You can manage user access by adding, updating, or deleting user accounts on the **User Management** page.

Task

1. **Select User Management → Users.**
2. **Select one of these actions.**
    - Create user:
        - Click **New User**, then type a user name.
        - Select whether to enable or disable the logon status of this account. If this account is for someone who is not yet a part of the organization, you might want to disable it.
        - Select whether the new account uses **ePO authentication**, **Windows authentication**, or **Certificate-Based Authentication** and provide the required credentials or browse and select the certificate.

          Note

          Using **Trellix ePO authentication** allows the administrator to provide a one-time password where the user is prompted to change the password when they log on the first time.

        - Optionally, provide the user's full name, phone number, description, and any notes in the **Notes** text box.
        - Choose to make the user an administrator, or select the appropriate permission sets for the user.
    - Edit user:
        - From the **Users** list, select the user you want to edit, then click **Actions → Edit**, and the **Edit User** page appears.
        - Edit the account as needed.
3. **Click Save.**

Creating Trellix ePO - On-prem users with Active Directory

Trellix ePO - On-prem can simplify the process of managing users by automatically creating Windows authentication users based on their Active Directory group membership.

If **Active Directory User Login** is enabled when an unknown user tries to log on, **Trellix ePO - On-prem** checks to see any permission sets mapped to Active Directory groups for which the user is a member. If there are, **Trellix ePO - On-prem** creates a Windows authentication user and assigns the mapped permission sets to it.

To enable this feature, you must do the following:

- **Active Directory User Login** must be enabled
- At least one permission set must be mapped to the user's Active Directory group
- A registered LDAP server must be configured for the domain, so that **Trellix ePO - On-prem** can determine the user's group membership

Active Directory User Login

You can enable the **Active Directory User Login** server setting from the **Server Settings** page, which allows user records to generate automatically when the following conditions are met:

- Users provide valid credentials, using the **<domain\name>** format. For example, a user with Windows credentials **jsmith1**, who is a member of the Windows domain named **eng**, supplies these credentials: **eng\jsmith1**, with the appropriate password.
- An Active Directory server that contains information about this user has been registered with **Trellix ePO - On-prem**.
- The user is a member of at least one Domain Local or Domain Global group that maps to a **Trellix ePO - On-prem** permission set.

Support for Universal Groups

Trellix ePO - On-prem partially supports Active Directory Universal Groups.

It restricts its communication to one domain when retrieving group information.

It supports these features when retrieving group memberships for a Universal Group:

- Direct membership lookup in a Universal Group
- Indirect membership lookup through a nested Universal Group
- Indirect membership lookup through Global or Domain Local Groups, if that group resides in the same domain as the Global Catalog being used to perform the lookup

Finally, it does not support indirect membership when that group resides on a different domain from the Global Catalog being used to perform the lookup.

Register an LDAP server

You must register LDAP servers with your **Trellix ePO - On-prem** server to permit dynamically assigned permission sets for Windows users. Dynamically assigned permission sets are permission sets assigned to users based on their Active Directory group memberships.

Note

Users trusted via one-way external trusts are not supported.

The user account used to register the LDAP server with **Trellix ePO - On-prem** is trusted through a bidirectional transitive trust. Otherwise, it must physically exist on the domain that the LDAP server belongs to.

Map a permission set to the Active Directory group

Assign at least one permission set to an Active Directory group other than a user's Primary Group. Dynamically assigning permission sets to a user's Primary Group is not supported, and results in application of only those permissions manually assigned to the individual user. The default Primary Group is **Domain Users**.

Users attempting to log on to a **Trellix ePO - On-prem** server with Windows authentication need a permission set assigned to one of their Active Directory groups.

Consider these items when determining how permission sets are assigned:

- Permission sets can be assigned to multiple Active Directory groups.
- Permission sets can be dynamically assigned only to an entire Active Directory group. They can't be assigned to just some users in a group.

If you want to assign special permissions to an individual user, create an Active Directory group that contains only that user.

Advanced Windows authentication

Users can authenticate with Windows credentials from the domain that the **Trellix ePO - On-prem** server uses. They can also authenticate by using any domain that has a two-way trust relationship with the **Trellix ePO - On-prem** server's domain. If you have users in domains that don't meet that criteria, enable and configure advanced Windows authentication.

Enable Windows authentication in the Trellix ePO - On-prem server

Before more advanced Windows authentication can be used, the server must be prepared.

To activate the **Windows Authentication** page in the server settings, stop the **Trellix ePO - On-prem** service.

Task

1. **From the server console, select Start → Settings → Control Panel → Administrative Tools.**
2. **Select Services.**
3. **In the Services window, right-click Trellix ePolicy Orchestrator Applications Server and select Stop.**
4. **Rename Winauth.dll to Winauth.dll.bak.**
   In a default installation, this file is found in **C:\Program Files\McAfee\ePolicy Orchestrator\Server\bin**.
5. **Restart the server.**

Results

When you next open the **Server Settings** page, a **Windows Authentication** option appears.

Configure advanced Windows authentication

There are many ways to use existing Windows account credentials in **Trellix ePO - On-prem**.

Before you begin

You must have first prepared your server for Windows authentication.

How you configure these settings depends on several issues:

- Do you want to use multiple domain controllers?
- Do you have users spread across multiple domains?
- Do you want to use a WINS server to look up which domain your users are authenticating against?

Task

1. **Select Menu → Configuration → Server Settings, then select Windows Authentication from the Settings Categories list.**

2. **Click Edit.**
3. **Specify whether you want to use one or more domains, one or more domain controllers, or a WINS server.**
   Domains must be provided in DNS format (for example, **internaldomain.com**). Domain controllers and WINS servers must have fully qualified domain names (for example, **dc.internaldomain.com**).

   Note

   You can specify multiple domains or domain controllers, but only one WINS server. Click **+** to add more domains or domain controllers to the list.

4. **Click Save when you are finished adding servers.**

Results

If you specify domains or domain controllers, the **Trellix ePO - On-prem** server tries to authenticate users with servers in the order they are listed. It starts at the first server in the list and continues down the list until the user authenticates successfully.

Windows authentication and authorization strategies

You can take several approaches when planning how to register your LDAP servers. Taking the time in advance to plan your server registration strategy helps you get it right the first time and reduce problems with user authentication.

Ideally, authentication and authorization is a process you do once, and only change if your overall network topology changes. Once servers are registered and Windows authentication is configured, you do not have to modify these settings often.

User account network topology

The effort required to fully configure Windows authentication and authorization depends on your network topology, and the distribution of user accounts across your network.

- If the credentials for users are contained in a small set of domains or servers in a single domain tree, register the root of the tree.
- If your user accounts are more spread out, register a number of servers or domains. Determine the minimum number of domain (or server) subtrees you need and register the roots of those trees. Try to register them in the order of usage. Placing the most commonly used domains at the top of the list improves average authentication performance.

Permission structure

For users to be able to log on to a **Trellix ePO - On-prem** server using Windows authentication, attach a permission set to the Active Directory group on the domain their account belongs to. When determining how permission sets are assigned, consider the following capabilities:

- Permission sets can be assigned to multiple Active Directory groups.
- Permission sets can be dynamically assigned only to an entire Active Directory group. They cannot be assigned to just some users in a group.

If you want to assign special permissions to an individual user, you can do so by creating an Active Directory group that contains only that user.

Locking out user accounts to protect your server

The option to **Lock Out User Accounts**, part of the **Logon Protection** feature, protects your **Trellix ePO - On-prem** server by locking out user accounts after a specified number of failed attempts.

This feature is disabled by default and must be manually enabled by an administrator.

From **Server Settings**, select **Logon Protection**, then **Edit**. You can edit these settings:

- Email notifications for failed logon attempts
- Number of incorrect attempts before an account is locked
- Length of time until the lockout counter resets
- Length of time the account is locked
- IP address restrictions after failed logon attempts

From **User Management** → **User**, you can reset your account before the specified wait period ends.

Restricting or allowing IP addresses to protect your server

The option to **Restrict IP Addresses**, part of the **Logon Protection** feature, protects your **Trellix ePO - On-prem** server from invalid logon attempts by blocking source IP addresses or allowing only certain IP addresses. You can also monitor logon attempts and manage IP addresses, manually or automatically.

This feature is disabled by default and must be manually enabled by an administrator.

If **Trellix ePO - On-prem** detects a malicious logon attempt from an IP address, that IP address is added to the IP Address Management table and blocked. Access to **Trellix ePO - On-prem** is blocked until you unblock or delete the address from the table. The **Actions** option allows you to unblock an IP address by adding it, so logon from the address is allowed.

Managing IP addresses

You must enable automatic IP address restriction to manually add IP addresses.

From **Server Settings**, select **Logon Protection**, then **Edit**. You can manage IP addresses in two ways:

- **Automatically** — When enabled, automatically blocks IP addresses after failed logon attempts (more than 10 tries within 60 seconds), and adds the address to the IP Address Management table.
- **Manually** — Allows you to add an IP address or range of addresses to the IP Address Management table. You can permanently block or allow access, regardless of logon attempts.

Note

When adding a range of IP addresses, you might accidentally block your own IP address. If this occurs, access the **Trellix ePO - On-prem** console directly from the hosted server and add or unblock the IP address so that it's included in the **Allow List**. The server always has access because the localhost is never blocked.

Monitoring logon attempts

The Audit Log tracks the history of changes to or enforcement of any IP address. For example, you can see if an IP address is blocked, if logon attempts are made from a blocked IP address, and the start and completion time of an attempt.

From Automatic Responses, select **Logon Protection**, then **Edit**. You can configure email notifications when the following occurs:

- Too many failed logons occur from an IP address.
- A blocked IP address attempts to log on.
- A system blocks an IP address.

Managing password policy

The **Password Policy** feature allows you to define the strength of a password. For example, an administrator can restrict the number of previously used passwords and limit the number of days before the password expires.

Note

This feature is disabled by default.

From **Server Settings**, select **Password Policy**, then **Edit**. Define password criteria by editing these settings:

- **Password Strength Criteria** — Define the strength of a password and restrict the number of previously used passwords.
  - **Minimum Password Length** — configure the password length (7–30 characters).
  - **Restrict usage of previously used passwords** — configure the limit on password reuse (3-24 previous passwords).

  When you enable password strength criteria, it automatically requires that passwords contain the following:
  - One uppercase (A–Z)
  - One lowercase (a–z)
  - One numeric (0–9)
  - One special character (#?!@$%^&*-)

  Note

  The password requirements can't be customized. If an existing password doesn't match the criteria, you are prompted to change it during the next logon.

- **Password Expiration Criteria** — Enter the number of days before a password expires (30–365 days).

Disable user account

Disable a user account without permanently deleting it, retaining objects and policies that the user created. Use this feature when a user leaves an organization or if a user account is no longer in use.

This feature is only available to administrators.

If the user account is deleted, all policies and objects the user created are also deleted.

Task

1. **Select Menu → User Management → Users, then select the user account you want to disable.**
2. **From the Actions menu, select Disable. You can also disable a user account from the Edit User page.**
3. **Click Save.**
   A user must re-enter their credentials to access the **Trellix ePO - On-prem** console any time the IP address changes.

Reset administrator password

Reset the global administrator password if you have forgotten your credentials, or are locked out and no other administrator accounts are available.

Before you begin

- You must be able to log on to your server directly and access **Trellix ePO - On-prem** using the localhost address.
- You must have the current database credentials for **Trellix ePO - On-prem**.

Task

1. **From your server, open a browser to https://localhost:8443/core/restore-admin.**

   Note

   If you have customized the port of ePO console, you must update the same port number in the restore link.

   The **Trellix ePO - On-prem** logon page opens.
2. **Click Restore Administrator Access.**
3. **Under Database credentials, enter the current user name and password for the database.**
4. **Under Administrator credentials, enter the new password for the administrator account.**
5. **Click Submit to update the administrator account password.**

Results

After resetting the password, the global administrator user name is displayed in the confirmation message.

Create a custom logon message

Create and display a custom logon message to be displayed on the **Log On** page.

Your message can be written in plain text, or formatted using HTML. If you create an HTML formatted message, you are responsible for all formatting and escaping.

Custom logon messages with HTML are now escaped by default to prevent Cross-site Scripting (XSS) issues. To include HTML markups and prevent formatting issues, go to the <ePO_install_location>\Server\conf\orion folder, open the orion.properties file, add `secure.login.custom.message=false`, and save the file and restart **Trellix ePO - On-prem** services.

Task

1. **Select Menu → Configuration → Server Settings, select Login Message from the Settling Categories, then click Edit.**
2. **Select Display custom login message, then type your message and click Save.**

Restrict a user session to a single IP address

Restricting logons to a single IP address can prevent attacks that take advantage of persistent session information.

By default, user sessions are maintained across IP addresses. Maintaining user sessions enables users to change locations without having to log on repeatedly.

If your network requires more security, you can restrict user sessions to a single IP address. Doing so forces users to resubmit their credentials every time their IP address changes, such as when they take their laptop to a different location.

Task

1. **Select Menu → Configuration → Server Settings, select User Session from the Settings Categories, then click Edit.**
2. **Select Restrict session to a single IP address.**
3. **Click Save.**

Results

Any time a user changes IP addresses, they must re-enter their credentials to access the **Trellix ePO - On-prem** console.

The Audit Log

The **Audit Log** records all **Trellix ePO - On-prem** user actions. Visit the **Audit Log** to track user actions. For example, you can see who created a product deployment.

Since the **Audit Log** is a growing list of information, to improve performance, periodically purge the old information.

Note

Audit Log information appears in the language of the **Trellix ePO - On-prem** server locale.

Audit Log entries can be queried against. You can create queries with the **Query Builder** that target this data, or you can use the default queries that target this data. For example, the **Failed Logon Attempts** query retrieves a table of all failed logon attempts.

View user actions

The **Audit Log** displays past user actions. Use the **Audit Log** to track access to your **Trellix ePO - On-prem** server, and what changes users make.

Task

1. **Open the Audit Log: select Menu → Reporting → Audit Log.**
2. **Sort and filter the table to focus on relevant entries.**
    - To change which columns are displayed, from the **Actions** menu, click **Choose Columns.**
    - To order table entries, click a column title.
    - To show or hide entries, select a filter option.
3. **To view additional details, click an entry.**

Remove outdated actions from the Audit Log

Periodically remove outdated actions from the **Audit Log** to improve database performance.

Important

Items removed from the **Audit Log** are deleted permanently.

Task

1. **Open the Audit Log: select Menu → Reporting → Audit Log.**
2. **Click Purge.**
3. **In the Purge dialog box, enter a number, then select a time unit.**
4. **Click OK.**

Results

Any items of the specified age or older are deleted, including items not in the current view. The number of removed items is displayed in the lower right corner of the page.

Tip

Create a server task to automatically remove outdated items.

Authenticating with certificates

Enable certificate-based authentication to allow your users to access **Trellix ePO - On-prem** with a valid client certificate instead of a user name and password.

Client certificate authentication is a type of public-key authentication. It differs from public-key authentication because you grant trust to a trusted third party, known as a certification authority (or CA). Certificates are digital documents that combine identity information and public keys. The CA digitally signs the certificates and verifies that the information is accurate.

When a user tries to access **Trellix ePO - On-prem** using certificate-based authentication, **Trellix ePO - On-prem** checks the client certificate to make sure that it was signed. After the client certificate is verified, the user is granted access.

Certificates have predefined expiration dates, which force the review of user permissions.

For users configured with valid certificates, certificate-based authentication replaces password authentication. All other users continue to use passwords to access **Trellix ePO - On-prem**.

Before your organization can use certificate-based authentication, install the CA certificate on **Trellix ePO - On-prem** and a signed client certificate on your endpoints.

Configure Trellix ePO - On-prem for certificate-based authentication

Before users access **Trellix ePO - On-prem** with certificate-based authentication, enable the authentication method and upload a signed CA certificate.

Before you begin

You must have a signed certificate in P7B, PKCS12, DER, or PEM format.

Task

1. **Open the Edit Certificate-based Authentication page.**
    a. **Select Menu → Configuration → Server Settings.**
    b. **From the Setting Categories list, select Certificate-based Authentication, and click Edit.**
2. **Select Enable certificate-based Authentication.**
3. **Next to CA certificate for client certificate, click Browse, navigate to and select the certificate file, then click OK.**
   When a file is applied, the prompt changes to **Replace current CA certificate**.

   Note

   Replace the certificate when it expires, or if your organization's security requirements change. For example, your organization might require SHA-256 certificates for authentication.

4. **(Optional) If you provided a PKCS12 certificate, enter a password.**
5. **Configure any advanced or optional settings as needed.**
    - If you have a certificate revocation list (CRL), click **Browse**, navigate to and select the CRL file, then click **OK**.

      Note

      The CRL file must be in PEM format.

    - (Optional) As an alternative or additional method of checking a certificate's authenticity, configure the Online Certificate Status Protocol (OCSP).
        - Click **Enable OCSP checking**.
        - Type the URL to the OCSP server.

- (Optional) Select **Enable CRL Distribution Point checks when the Trellix ePO server receives no response from the OSCP**. If the connection to the default OCSP URL fails, **Trellix ePO - On-prem** tries to connect to the certification authority CRL mentioned in the certificate under **CRL Distribution Point Check** instead.
- (Optional) Select **Make the default OCSP URL the primary OCSP URL**. If that connection fails, **Trellix ePO - On-prem** falls back to the other OCSP responder, if mentioned in the certificate under **Authority Information Access**.

- To require certificate-based authentication for all remote users, click **Remote users use the certificate to sign in**.
- To make the user name the same as the subject Distinguished Name (DN) specified in the certificate, click **Default certificate user name is the subject DN**.
- Configure **Active Directory Integration**.

Important

For these settings to work, you must have Active Directory user logon enabled and the user group added to a permission set.

- To automatically assign Active Directory users to a permission set, select **Automatically assign permission for user logon with an Active Directory certificate**.
- To automatically create an **Trellix ePO - On-prem** user account for anyone who accesses **Trellix ePO - On-prem** with the valid AD certificate, select **Automatically create users for Active Directory certificate owners**.

6. **Click Save.**
7. **Restart Trellix ePO - On-prem to activate certificate authentication.**

Disable certificate-based authentication

If certificates are no longer used in your network environment, remove certificate-based authentication as an authentication option.

Task

1. **Open the Edit Certificate-based Authentication page.**
   a. **Select Menu → Configuration → Server Settings.**
   b. **From the Setting Categories list, select Certificate-based Authentication, and click Edit.**
2. **Deselect Enable Certificate Based Authentication, then click Save.**

Results

Once you disable certificate-based authentication, your users can no longer access **Trellix ePO - On-prem** with a certificate, and must log on with their user name and password instead. Your previous configuration settings are reset.

Restart the server to complete the configuration change.

Configure user accounts for certificate-based authentication

Users must have certificate-based authentication configured before they can authenticate with a client certificate.

The client certificates used for certificate-based authentication are typically acquired with a smart card or similar device. Software bundled with the smart card hardware can extract the certificate file. This extracted certificate file is usually the file uploaded in this procedure.

Task

1. **Open the Edit User page.**
    a. **Select Menu → User Management → Users.**
    b. **From the Users list, select a user, then click Actions → Edit.**
2. **Next to Authentication type, select Change authentication or credentials → Certificate-Based Authentication.**
3. **Use one of these methods to provide credentials.**
    - Copy the DN field from the certificate file and paste it into the **Personal Certificate Subject DN Field** edit box.
    - Upload the signed certificate file: click **Browse** to navigate to and select the certificate file, then click **OK**.

    Note

    This certificate file was uploaded in the procedure, *Configure MFS certificate-based authentication*.

    User certificates can be in PEM or DER format. The actual certificate format does not matter as long as the format is X.509 or PKCS12 compliant.
4. **Click Save to save changes to the user's configuration.**

Results

The certificate information is verified. A warning appears if the certificate is invalid. If the certificate is vaild, the **Trellix ePO - On-prem** logon page appears. The user can choose a language and click **Log On** without entering a user name and password.

Update the certificate revocation list

To prevent access to **Trellix ePO - On-prem** by specific users that were configured for certificate-based authentication, add the user's client certificate to the certificate revocation list (CRL) installed on your **Trellix ePO - On-prem** server.

Before you begin

You must already have a CRL file in ZIP or PEM format.

The CRL file is a list of revoked **Trellix ePO - On-prem** users and their digital certificate status. The list includes the revoked certificates, the reasons for revocation, dates of certificate issue, and the issuing entity. When a user tries to access the **Trellix ePO - On-prem** server, the CRL file is checked and it allows or denies access for that user.

Task

1. **Select Menu → Configuration → Server Settings.**
2. **Select Certificate-based Authentication, then click Edit.**
3. **To update the CRL file, next to Certificate revocation list file, click Choose File, navigate to the CRL file, then click OK.**
4. **Click Save to save all changes.**
5. **Restart Trellix ePO - On-prem to activate certificate authentication.**

Results

Trellix ePO - On-prem checks the updated CRL file to confirm that the client certificate has not been revoked every time a user tries to access the **Trellix ePO - On-prem**.

You can also use the cURL command line to update the CRL file.

Note

To run cURL commands from the command line, install the cURL and grant remote access to the **Trellix ePO - On-prem** server.

At the cURL command-line type:

```
curl -k --cert <admin_cert>.pem --key <admin_key>.pem https://<localhost>:<port>/remote/console.cert.updatecrl.do -F crlFile=@<crls>.zip
```

In this command:

- `<admin_cert>` — Administrator client certificate .PEM file name
- `<admin_key>` — Administrator client private key .PEM file
- `<localhost>:<port>` — **Trellix ePO - On-prem** server name and communication port number
- `<crls>` — CRL .PEM or .zip file name

Troubleshooting certificate-based authentication

A few problems cause most authentication issues using certificates.

If a user cannot log on with their certificate, try one of these options to resolve the problem:

- Verify that the user has not been disabled.
- Verify that the certificate has not expired or been revoked.
- Verify that the certificate is signed with the correct certificate authority.
- Verify that the DN field is correct on the user configuration page.
- Verify that the browser is providing the correct certificate.
- Check the **Audit Log** for authentication messages.

Permission sets

How users, groups, and permission sets fit together

Trellix ePO - On-prem controls access to items using interactions between users, groups, and permission sets.

A user account grants log on access to the **Trellix ePO - On-prem** console and when mapped with a permission set, it defines what the user is allowed to access. Administrators can create accounts for individual users and assign permissions, or they can create a permission set that maps to users or groups in your Active Directory/NT server.

Trellix ePO - On-prem users fall into two general categories. Either they are administrators, having full rights throughout the system, or they are regular users. Regular users can be assigned any number of permission sets to define their access levels in **Trellix ePO - On-prem**.

Administrators

Administrators have read and write permissions and rights to all operations. When you install the server, an administrator account is created automatically. By default, the user name for this account is **admin**. If the default value is changed during installation, this account is named accordingly.

You can create additional administrator accounts for people who require administrator rights.

Permissions exclusive to administrators include:

- Create, edit, and delete source and fallback sites.
- Change server settings.
- Add and delete user accounts.
- Add, delete, and assign permission sets.
- Import events into **Trellix ePO - On-prem** databases and limit events that are stored there.

Users

Users can be assigned any number of permission sets to define their access levels in **Trellix ePO - On-prem**.

User accounts can be created and managed in several ways. You can:

- Create user accounts manually, then assign each account an appropriate permission set.
- Configure your **Trellix ePO - On-prem** server to allow users to log on using Windows authentication.

Allowing users to log on using their Windows credentials is an advanced feature that requires configuration and setup of multiple settings and components.

Groups

Queries and reports are assigned to groups. Each group can be private (to that user only), globally public (or "shared"), or shared to one or more permission sets.

Permission sets

A particular access profile is defined in a permission set. This profile usually involves a combination of access levels to various parts of **Trellix ePO - On-prem**. For example, one permission set might grant the ability to read the **Audit Log**, use public and shared dashboards, and create and edit public reports or queries.

Permission sets can be assigned to individual users, or if you are using Active Directory, to all users from specific Active Directory servers.

Default permission sets

Trellix ePO - On-prem provides these four default permission sets that provide permissions to its functionality.

- Executive Reviewer — Provides view permissions to dashboards, events, contacts, and can view information that relates to the whole System Tree.
- Global Reviewer — Provides view access globally across functionality, products, and the System Tree, except for extensions, multi-server roll up data, registered servers, and software.
- Global Admin — Provides view and change permissions across **Trellix ePO - On-prem** features. Users that are assigned this permission set each need at least one more permission set that grants access needed products and groups of the System Tree.
- Group Reviewer — Provides view permissions across **Trellix ePO - On-prem** features. Users that are assigned this permission set each need at least one more permission set that grants access needed products and groups of the System Tree.

A user group administrator or the global administrator can edit the canned permission sets as required.

When you upgrade a product extension:

- An edited canned permission set for the product is retained with the default canned permission set.
- A deleted permission set for the product is added again.

Add or edit permission set

Control user access by creating and changing permission sets from the **Permission Sets** page.

You can also copy and delete permission sets from the **Permission Sets** page.

Task

1. **Open the Permission Sets page: select Menu → User Management → Permission Sets.**
2. **Select one of these actions.**
    - Add a permission set:
        - Click **New Permission Set**.
        - Type a unique name for the new permission set.
        - To immediately assign specific users to this permission set, select their user names in the **Users** section.
        - To map any Active Directory groups to this permission set, select the server from the **Server Name** list, then click **Add**.
        - If you added any Active Directory servers that you want to remove, select them in the Active Directory list box, then click **Remove**.

      The XML file contains only roles with a defined level of permissions. If, for example, a **Permission Set** has no permissions for queries and reports, no entry appears in the file.
    - Edit a permission set:
        - Select a permission set to change.
        - Type a unique name for the new permission set.
        - To immediately assign specific users to this permission set, select their user names in the **Users** section.
        - To map any Active Directory groups to this permission set, select the server from the **Server Name** list, then click **Add**.
        - If you added any Active Directory servers that you want to remove, select them in the Active Directory list box, then click **Remove**.

Import or export permission set

Once you have fully defined your permission sets, the fastest way to migrate them is to export them, then import them to the other servers.

Task

1. **Open the Permission Sets page: select Menu → User Management → Permission Sets.**
2. **Select one of these actions.**

    - Export permission sets:
        - Click **Export All**.

      The **Trellix ePO - On-prem** server sends an XML file to your browser. Open or Save this file. The XML file contains only roles with a definTed level of permissions. If, for example, a **Permission Set** has no permissions for queries and reports, no entry appears in the file.
    - Import permission sets:
        - Click **Import**.
        - Click **Browse** to navigate to and select the XML file with the permission sets that you want to import.
        - Choose whether to keep permission sets with the same name as an imported permission set by selecting the appropriate option. Click **OK**. If **Trellix ePO - On-prem** cannot locate a valid permission set in the indicated file, an error message is displayed and the import process is stopped.

      The permission sets are added to the server and displayed in the **Permission Sets** list.

Software Catalog

What's in the Software Catalog

The Software Catalog removes the need to access the **Trellix Product Download** website to retrieve new **Trellix** software and software updates.

You can use the Software Catalog to download:

- **Licensed software** — Software your organization has purchased from **Trellix**. The **Status** column provides a list of licensed software that is not currently installed on your server. The number displayed next to each category in the **Status** list indicates where updates are available. Select the number to view specific details about the updates. For example, the available version, checked in version, or component type.
- **Evaluation software** — Software for which your organization does not currently possess a license. You can install evaluation software on your server, but functionality might be restricted until you acquire a product license.
- **Software updates** — Released software that has new updates. You can use the Software Catalog to check in new packages and extensions. Available software updates are listed in the **Updates Available** category.
- **Product documentation** — New and updated product documentation you can retrieve from the Software Catalog. Product Guides and Release Notes can also be downloaded from the Software Catalog.

Note

DATs and Engines are not available from the Software Catalog.

About software component dependencies

Many of the software products you can install for use with your **Trellix ePO - On-prem** server have predefined dependencies on other components. Dependencies for product extensions are installed automatically. For all other product components, you must review the dependencies list in the component details page, and install them first.

Software Catalog interface

Use the Software Catalog to view and manipulate your new and existing software.

Option			Definition
Category			Search for or select products to view or manipulate in the selected product tables.

Option			Definition
Software Catalog	List of products and their status		Select a product in this list and details appear in the component rows.
	Status column		Displays if a product is up to date or has an update available.
	Actions column	**Check In All**	Checks in all ***new*** versions and components of the selected product that are not already checked in. **Note: Check In All** doesn't update components that have updates available. If one fails, the remaining fail to download and check in to **Trellix ePO - On-prem**.
		Update All	Updates all ***existing*** versions and components of the selected product to the latest version.

Option			Definition
			Note: Update **All** doesn't download and check in components that have never been checked in. If one fails, the remaining fail to download and check in to **Trellix ePO - On-prem**.
		Remove All	Removes all versions and components of the selected product.
	Component rows		Displays all components of the selected product and, depending on the component, allows you to check in, update, remove, or download the individual component.

Check in, update, and remove software using the Software Catalog

From the Software Catalog, you can check in, update, and remove managed product components from your server.

Both licensed and evaluation software can be accessed in the Software Catalog.

Note

Software availability, and whether it is **Licensed** or **Evaluation**, depends on your license key. For more information, contact your administrator.

Task

1. **Click Menu → Software → Software Catalog.**

2. **In the Software Catalog page Category list, select one of the following categories, or use the search box to find your software:**
    - **Updates Available** — Lists any available updates to licensed software components already installed or checked in to the Trellix ePO server.
    - **Evaluation** — Displays the **Evaluation** software installed or checked in to this server.
    - **Product categories** — Displays the licensed **Trellix** software installed or checked in to this server.
3. **When you have located the correct software, select an action that applies to all the components in the software, or individual components.**
    - For all the components in the software, click:
        - **Check In All** to check in all components of the ***new*** product on this server.
        - **Update All** to update all components of the ***existing*** product on this server.
        - **Remove All** to remove all components of the ***existing*** product on this server.
    - For individual components in the software, click:
        - **Download** to download software or product documentation to a location on your network.
        - **Check In (branch)** to check in a ***new*** product package on this server.
        - **Check In** to check in a ***new*** product extension on this server.
        - **Update** to update an ***existing*** package or extension that is already installed or checked in to this server.
        - **Remove** to uninstall a package or extension that is installed or checked in to this server.
4. **Under Check In, review and accept the product details and End User License Agreement (EULA), select the Client Package Branch, then click Check In to complete the operation.**

Software Catalog page

The **Software Catalog** informs you about the availability of new and updated **Trellix** software products that your organization uses, and trial versions of other **Trellix** products. You can also use the Software Catalog to check in, update, remove, and download software.

Option definitions

Category	Option	Definition
Component details	Name	Specifies the name of the selected component.
	Type	Specifies the type of component. Most **Trellix** managed products contain multiple components. Component types include: • **Extension** — This is the part of the software that gets

Category	Option	Definition
		installed on your **Trellix ePO - On-prem** server. For example, the **VirusScan Enterprise** extension is checked in to your server, whereas the **VirusScan Enterprise** package is checked in to your repository to be deployed to your managed systems. • **Package** — This is the part of the software that gets checked in to your repository for distribution to your managed systems. • **Other** — Other types include MSI installers (standalone), documentation, and any other type of content that is not directly checked in to your server. All content in this category must be downloaded and checked in manually.
	Status	Lists the status of the product: **Up to date**, **Update available**, or **Not checked in**. A number appears next to the status when a product has an update. For example, if there are five components in a product that have an update, the number appears next to the status.
	Available Version	Specifies the version of this product.
	Checked in Version	Specifies the version of the component, if checked in.

Category	Option	Definition
	Check-in Date	Specifies the date when the component was checked in.
	Installed Name	Specifies the name of the installed software.
	Branch	Specifies details about which branch of the repository this component is checked in to, if applicable.
	Actions	• **Check In All** — Checks in all product components listed in the product details pane. **Note:** Some available product components, such as MSI installers, can't be installed using this action. You must download and manually install these types of components. • **Update All** — Updates all packages or extensions listed in the product details pane to the newest version available from the **Trellix** download site. • **Remove All** — Removes all packages and extensions listed in the product details pane. If a product, package, or extension was checked in manually (such as those using an MSI installer), you must remove it manually.
	Package Type	Specifies the package type.

Category	Option	Definition
	Distribution Type	Specifies whether the product is licensed or evaluation. You might have the evaluation version checked in, even though your organization is licensed to use the full version.
	Released	Specifies the date when this component was released for distribution by **Trellix**.
	File Size	Specifies the size of this component.
	Language	Lists the language of this component.
Common actions	***Search***	Use the search box to locate a specific product. For example, type `VSE` to find available **VirusScan Enterprise** licensed software, evaluation software, software updates, and documentation.
	Branch	The **Branch** drop-down list allows you to filter branches to be displayed. Choose from these options: • **All Branches** • **Current Branch** • **Previous Branch** • **Evaluation Branch**
	Hide older versions if not checked in	Provides the option to hide older versions of software that isn't checked in.

Category	Option	Definition
	Language filter	Lists the languages available and allows you to limit the download to the selected language.
	Refresh	Updates the list of products contained in the **Products Category** pane. Your server must have Internet access to accomplish this task, because it connects to the **Trellix** download server to verify which products are available. The information retrieved depends on whether your server is in **Licensed** or **Evaluation** mode, and which products your license key entitles you to use.
Category	**Evaluation**	Software for which your organization does not currently possess a license. You can install evaluation software on your server, but functionality might be restricted until you acquire a product license.
	Updates Available	Lists licensed software already checked in to this server or its repository for which an update is available.
	Software	**Trellix** products are grouped by category based on the specific security solutions they provide.
Product details	**Status**	Lists the status of the selected software version.

Category	Option	Definition
Note: Available actions depend on which list item is highlighted in the **Category** pane, and which product is highlighted in the adjacent pane. For example, when **Evaluation** is highlighted in the **Category** pane, the adjacent table displays evaluation versions of products.	**Check In All**	Checks in all product components listed in the product details pane. **Note:** Some available product components, such as MSI installers, can't be installed using this action. You must download and manually install these types of components.
	Update All	Updates all packages or extensions listed in the product details pane of the selected version.
	Remove All	Removes all packages and extensions listed in the product details pane. If a product, package, or extension was checked in manually (such as those using an MSI installer), you must remove it manually.
	Check In	Checks in the package or extension on this **Trellix ePO - On-prem** server.

Category	Option	Definition
		Note: Many **Trellix** products consist of the product extension and product package. Product extensions are checked in to your **Trellix ePO - On-prem** server, and product packages are checked in to your **main Repository**, then deployed to managed systems. For more information about this process, see the product documentation for the specific product you are working with.
	Remove	Removes the product or extension from this server.
	Update	Updates all packages or extensions listed in the product details pane of the selected version.
	Download	Downloads the selected item to the location you specify. This content is not checked in. It is saved and you must take the appropriate action manually.

Bundle Details (Software Catalog)

View details about the bundle selected in the Software Catalog.

Option definitions

Option	Definition
Bundle	Specifies the name of the selected bundle.

Option	Definition
Details	Specifies details about this product bundle.
Additional Check In Details	Specifies details about which branch of the repository this bundle is checked in to, if applicable.
File Size	Specifies the size of this bundle.
Components	Specifies the components included in this bundle.

Extensions page

You can install, remove, and manage extension files in **Trellix ePO - On-prem**. Extension files for products or components are in .zip file format and must be installed before **Trellix ePO - On-prem** can manage that product or component.

Note

See the product documentation for the location and name of its extension file.

Option definitions

Option	Definition
Extensions	The **Extensions** pane lists products by category. Select a product in the **Extensions** pane to view the extensions that are installed. **Extensions** categories include: • **Trellix** — Lists the **Trellix** product and component extensions installed on your server. • **Third Party** — Lists all third-party product and component extensions installed on your server. • **Unsigned** — Lists all unsigned product and component extensions installed on your server.
Install Extension	Allows you to browse to and install an extension (.zip) file. If the extension file you want to install depends on any other files, ensure that those files are installed first.

Option	Definition
	Note: You can only have one task updating the **Main Repository** at once. If you try to install an extension at the same time as a **Main Repository** update is running, the following error appears: **Unable to install extension com.mcafee.core.cdm.CommandException: Cannot check in the selected package while a pull task is running.** Wait until the **Main Repository** update is done and try to install your extension again.
Remove	Uninstalls the selected product or component extension.

Fields shown in the extension table include:

- **Details** — Lists details of extension installation.
- **Installed by** — Specifies the user who installed the currently selected extension.
- **Modules** — Specifies the modules that controlled bt this extension and whether they are running. This information is valuable for troubleshooting.
- **Name** — Specifies the name of the currently selected extension.
- **Remove** — Removes the selected extension from the Extensions list.
- **Requires** — Specifies any extensions on which the currently selected extension is dependent.
- **Status** — Identifies whether the extension was installed successfully. If it was not installed successfully, any errors are identified.
- **Version** — Specifies the version of the currently selected extension. Multiple versions of the same extension can be installed.

Checking product compatibility

You can configure a **Product Compatibility Check** to automatically download a **Product Compatibility List** from **Trellix**.

This list identifies products that are no longer compatible in your **Trellix ePO - On-prem** environment.

Trellix ePO - On-prem performs this check any time the installation and startup of an extension might leave your server in an undesirable state. The check occurs:

- During an upgrade from a previous version of **Trellix ePO - On-prem**
- When an extension is installed from the **Extensions** menu

- Before a new extension is retrieved from the **Software Catalog**
- When a new compatibility list is received from **Trellix**
- When the **Data Migration Tool** runs

See the ***Trellix ePolicy Orchestrator - On-prem*** *Installation Guide* for details.

Product Compatibility Check

The **Product Compatibility Check** uses an XML file, the **Product Compatibility List**, to determine which product extensions aren't compatible with a version of **Trellix ePO - On-prem**.

An initial list is included in the **Trellix ePO - On-prem** software package from the **Trellix** website. When you run setup during installation or upgrade, **Trellix ePO - On-prem** automatically retrieves the most current list of compatible extensions from a trusted **Trellix** source. If the Internet source is unavailable or if the list can't be verified, **Trellix ePO - On-prem** uses the latest version it has available.

The **Trellix ePO - On-prem** server updates the **Product Compatibility List** in the background once per day.

Remediation

When you view the list of incompatible extensions through the installer or the **Upgrade Compatibility Utility**, you are notified if a known replacement extension is available.

Sometimes during an upgrade:

- An extension blocks the upgrade and must be removed or replaced before the upgrade can continue.
- An extension is disabled, but you must update it after the **Trellix ePO - On-prem** upgrade is complete.

Disabling automatic updates

You might want to disable automatic updates of the **Product Compatibility List**. The download occurs:

- As part of a background task.
- When the **Software Catalog** content is refreshed (helpful when your **Trellix ePO - On-prem** server does not have inbound Internet access).
- When you re-enable the download setting for the **Product Compatibility List** (also re-enables **Software Catalog** automatic updates of the **Product Compatibility List**).

Using a manually downloaded Product Compatibility List

If your **Trellix ePO - On-prem** server does not have Internet access, you can use a manually downloaded **Product Compatibility List**.

You can manually download the list:

- When you install **Trellix ePO - On-prem**.
- When using **Server Settings** → **Product Compatibility List** to manually upload a **Product Compatibility List**. This list takes effect immediately after upload.

Tip

Best practice: Disable automatic updating of the list to prevent overwriting the manually downloaded **Product Compatibility List**.

Open **https://epo.trellix.com/ProductCompatibilityList.xml** to manually download the list.

Blocked or disabled extensions

If an extension is blocked in the **Product Compatibility List**, it prevents the **Trellix ePO - On-prem** software upgrade. If an extension is disabled, it doesn't block the upgrade, but the extension isn't initialized after the upgrade until a known replacement extension is installed.

Command-line options for installing the Product Compatibility List

You can use these command-line options with the `setup.exe` command to configure **Product Compatibility List** downloads.

Command	Description
`setup.exe DISABLEPRODCOMPATUPDATE=1`	Disables automatic downloading of the **Product Compatibility List** from the **Trellix** website.
`setup.exe PRODCOMPATXML=<full_filename_including_path>`	Specifies an alternate **Product Compatibility List** file.

Both command-line options can be used together in a command string.

Reconfigure Product Compatibility List download

You can download the **Product Compatibility List** from the Internet, or use a manually downloaded list to identifying products that are no longer compatible in your **Trellix ePO - On-prem** environment.

Any manually downloaded **Product Compatibility List** must be a valid XML file provided by **Trellix**. If you make any changes to the **Product Compatibility List** XML file, the file is no longer valid.

Task

1. **Select Menu → Configuration → Server Settings, select Product Compatibility List from the Setting Categories, then click Edit.**
   A list of disabled incompatible extensions appears.
2. **Click Disabled to stop automatic and regular downloads of the Product Compatibility List from Trellix.**
3. **Click Browse and navigate to the Upload Product Compatibility List, then click Save.**

Results

Automatic downloading of the **Product Compatibility List** is disabled. Your **Trellix** server uses the same list until you upload a new list, or connect your server to the Internet and enable automatic downloading.

Manual package and update management

Bring products under management

A product's extension must be installed before **Trellix ePO - On-prem** can manage the product.

Before you begin

Make sure that the extension file is in an accessible location on the network.

Task

1. **From the Trellix ePO - On-prem console, select Menu → Software → Extensions → Install Extension.**
2. **Browse to and select the extension file, then click OK.**

   You can only have one task updating the Main Repository at once. If you try to install an extension at the same time as a Main Repository update is running, the following error appears:

   Unable to install extension com.mcafee.core.cdm.CommandException: Cannot check in the selected package while a pull task is running.

   Wait until the Main Repository update is done and try to install your extension again.

3. **Verify that the product name appears in the Extensions list.**

Check in packages manually

Check in the deployment packages to the **Main Repository** so that the ePolicy Orchestrator software can deploy them.

Task

1. **Open the Check In Package wizard.**
   a. **Select Menu → Software → Main Repository.**
   b. **Click Check In Package.**
2. **Select the package type, then browse to and select the package file.**
3. **Click Next.**
4. **Confirm or configure the following:**
   - **Package info** — Confirm this is the correct package.
   - **Branch** — Select the branch. If there are requirements in your environment to test new packages before deploying them throughout the production environment, use the **Evaluation** branch whenever checking in packages. Once you finish testing the packages, you can move them to the **Current** branch by selecting **Menu → Software → Main Repository**.
   - **Options** — Select whether to:
     - **Move the existing package to the Previous branch** — When selected, moves packages in the Main Repository from the **Current** branch to the **Previous** branch when a newer package of the same type is checked in. Available only when you select **Current** in **Branch**.

- **Package signing** — Specifies if the package is a **Trellix** or a third-party package.

5. **Click Save to begin checking in the package, then wait while the package is checked in.**

Results

The new package appears in the **Packages in Main Repository** list.

Delete DAT or engine packages from the Main Repository

Delete DAT or engine packages from the **Main Repository**. As you check in new update packages regularly, they replace the older versions or move them to the **Previous** branch, if you are using the **Previous** branch.

Task

1. **Click Menu → Software → Main Repository.**
2. **Select one of more packages to delete, and from the Actions menu, click Delete Package.**
3. **Click OK.**

Move DAT and engine packages between branches

Move packages manually between the **Evaluation**, **Current**, and **Previous** branches after they are checked in to the **Main Repository**.

Task

1. **Select Menu → Software → Main Repository.**
2. **Select a package to move, and from the Actions menu, click Change Branch.**
3. **Select whether to move or copy the package to another branch.**
4. **Select which branch receives the package.**
5. **Click OK.**

Check in Engine, DAT, and Extra.DAT update packages manually

Check in update packages to the **Main Repository** to deploy them using the **Trellix ePO - On-prem** software. Some packages can only be checked in manually.

Task

1. **Open the Check In Package wizard.**
    a. **Select Menu → Software → Main Repository.**
    b. **Click Check In Package.**
2. **Select the package type, browse to and select a package file, then click Next.**
3. **Select a branch:**
    - **Current** — Use the packages without testing them first.
    - **Evaluation** — Use the packages in a lab environment first.

Note

Once you finish testing the packages, you can move them to the **Current** branch by selecting **Menu → Software → Main Repository**.

- **Previous** — Use the previous version to receive the package.

4. **Next to Options, select Move the existing package to the Previous branch to archive the existing package.**
5. **Click Save to begin checking in the package. Wait while the package is checked in.**

Results

The new package appears in the **Packages in Main Repository** list.

Main Repository page

View the settings for the **Main Repository** and the packages it contains.

Option definitions

Option	Definition
Actions	
Choose Columns	Controls which columns are displayed in the table.
Export Table	Exports the list of packages in the **Main Repository** to a user-configured file format. The file can be saved or emailed.

Distributed Repositories page

Create, view, and manage distributed repositories.

Option definitions

Category	Option	Definition
Common actions	**New Repository**	Starts the **Distributed Repository Builder**. Use this builder to add a new distributed repository to the server.

Category	Option	Definition
	Replicate Now	Starts the **Replicate Now** wizard. Use this builder to configure and start a replication task.
Filter options	**Show/Hide Filter**	Shows or hides the **Preset** drop-down list.
	Preset	The **Preset** drop-down list allows you to filter the type of distributed repository to be displayed, including: • **All Types** — Displays all distributed repository types. • **SuperAgent** — Displays only SuperAgent distributed repositories. • **HTTP** — Displays only HTTP distributed repositories. • **FTP** — Displays only FTP distributed repositories. • **UNC** — Displays only UNC distributed repositories.
Distributed Repositories list Actions	**Delete**	Deletes the distributed repository.
	Edit Settings	Opens the **Distributed Repository Builder**, where you can change any of the repository settings.
	View Packages	Grants access only to view the packages and repositories in the **Distributed Repository** pages.
Actions	**Change Credentials**	Starts the **Change Credentials** page to change, download, and

Category	Option	Definition
		replicate credentials for your distributed repositories.
	Choose Columns	Opens the **Select the Columns to Display** page. Use this to select which columns of data to display on the **Distributed Repository** page.
	Export Repositories	Saves the **SiteMgr.xml** file to a user-selected location.
	Export Table	Exports the current table to a user-configured file format. The file can be saved or emailed.
	Import Repositories	Imports a previously exported **SiteMgr.xml** file. Use this setting to select repositories to import to this server.
	Schedule Replication	Starts the **Server Task Builder**. Use this to configure and schedule a **Repository Replication** server task.

Import Repositories page

Use this page to select and import distributed repositories from the **SiteMgr.xml** file.

Option definitions

Option	Definition
Select the SiteMgr.XML file to import	After you choose the file, select the checkboxes next to each repository you want, and click **OK**. Do not import any distributed repositories that are in conflict. This conflict might be because the distributed repository exists on this server.

Option	Definition
	All distributed repositories are selected by default.

Best practice: Automating DAT file testing

Use the built-in functionality of **Trellix ePO - On-prem** to automatically validate DAT file compatibility and content files that are downloaded from the **Trellix** public site.

Trellix Labs rigorously tests the content, such as DAT and engine files, before they are released on the public update servers. Because every organization is unique, you can perform your own compatibility validation to ensure the compatibility of DATs and content in your unique environment.

The compatibility validation processes vary by organization. The process in this section is meant to automate much of the compatibility validation process and reduce the need for administrator intervention.

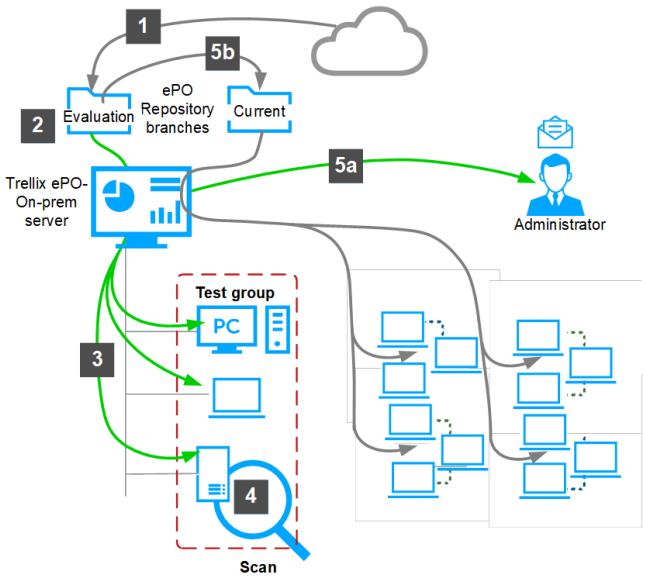
Tip

Best practice: To confirm that only compatible DAT files are distributed in your environment, you might chose move the content manually from the **Evaluation** branch into the **Current** branch of the repository.

1. A server task pulls DAT updates from the **Trellix** public site to the Evaluation branch of the Main Repository.
2. A **Trellix Agent** policy applies the DAT files from the Evaluation repository branch restricted to a group of systems in a Test group.
3. A **Trellix Agent** update client task installs the DAT on the Test group systems.
4. An on-demand scan task runs frequently on the Test group.
5. Depending on the on-demand scan output, one of these scenarios occurs:
    a. If the DAT is not compatible with the test group, an **Automatic Response** email is sent to the appropriate administrators. The email tells the administrators to stop distribution of the DAT files from the Current repository.
    b. Otherwise, after a specified time, a server task copies the files from the **Evaluation** branch to the **Current** branch of the repository. Then those files are automatically sent to the rest of the managed systems.

DAT file validation overview

Automatic DAT file testing steps



Pull and copy DAT updates from Trellix

To create an automated DAT file testing process requires configuring tasks to pull the DATs from **Trellix** and copy them to the **Current** branch of the repository.

The **Trellix ePO - On-prem** platform provides three repository branches in your Main and Distributed Repositories:

- **Current** branch — By default, the main repository branch for the latest packages and updates.
- **Evaluation** branch — Used to test new DAT and engine updates before deploying to your whole organization.
- **Previous** branch — Used to save and store prior DAT and engine files before adding the new ones to the **Current** branch.

You must create two server tasks to automate the DAT file testing.

- One task pulls the DAT files hourly to the Evaluation branch to ensure that the latest DAT is in the **Evaluation** branch shortly after **Trellix** releases it to the public.

  Tip

  Best practice: Run the task hourly to get an extra DAT file in case the initial file, released at 11:00 a.m., was replaced later in the day.

- One server task waits until a few hours after the test group of systems is scanned. Then, unless the administrator stops the server task, it automatically copies the DAT files from the **Evaluation** branch to the **Current** branch.

Best practices: Configure task to pull DAT to Evaluation branch

To automate your DAT file testing process, you must create a task to automatically pull DAT files from the **Trellix** public site into the **Evaluation** repository branch.

You might want to configure this task to distribute only DAT files, if your organization tests the engine for a longer time, than the few hours in this example, or restricts their automatic release.

Task

1. **Select Menu → Automation → Server Tasks, then click Actions → New Task to display the Server Task Builder wizard.**
2. **In the Description tab, type a server task name, for example,** DAT pull hourly to Evaluation repository**, and a description to appear on the Server Task page.**
3. **In Schedule status, click Enable, then click Next.**
4. **In the Actions tab, configure these settings:**
    - From the **Actions** list, select **Repository Pull**.
    - From the **Source site list**, select the **Trellix** public site you want to use, **TrellixFtpMigrated** or **TrellixHttp**.
    - From the **Branch** list, select **Evaluation.**
    - Deselect **Move existing package to Previous branch**, if needed.
    - From **Package types**, click **Select packages**.
5. **From the Available Source Site Packages dialog box, select DAT and Engine, then click OK.**
   We recommend that, at minimum, you pull the DAT and engine files from the **Trellix** public website.

   If you have multiple distributed repositories, you can chain a replication task to the same pull task to replicate your **Evaluation** branch to your distributed repositories.
6. **In the Schedule tab, configure these settings:**
    - For the **Schedule type**, click **Hourly**.
    - For the **Start date**, select today's date.
    - For the **End date**, click **No end date**.
    - From **Schedule**, configure the task to run every hour at 10 minutes past the hour.
7. **Click Next, confirm that all settings are correct in the Summary tab, then click Save.**

Results

To confirm that the automatic DAT file pull is working, go to **Menu → Software → Main Repository** and use the Check-In date information to confirm that the Evaluation branch DAT file was updated within the last two hours.

Best practices: Configure server task to copy files from Evaluation to Current branch

To automate your DAT file testing process, create a task to automatically copy DAT files from the **Evaluation** branch of the repository to the **Current** branch.

Before you begin

You must have created the server task to automatically copy the DAT and content files to the **Evaluation** branch of the repository.

Task

1. **Select Menu → Automation → Server Tasks, then click Actions → New Task.**
2. **In the Server Task Builder Descriptions tab, type a task name and notes, then in Schedule status, click Enabled, then click Next.**
3. **In the Actions tab, configure these settings, then click Next:**
    - For **Actions** list, select **Change the Branch for a Package**, select **All packages of type 'DAT' in branch 'Evaluation'** as the package to change, **Copy** as the action, then click **Current** as the target branch.
    - Click **+** to create another action, and from the second **Actions** list, select **Change the Branch for a Package**, select **All packages of type 'Engine' in branch 'Evaluation'** as the package to change, **Copy** as the action, and **Current** as the target branch.
4. **In the Schedule tab, change these settings:**
    - For **Schedule type**, click **Daily**.
    - For **Start date**, select today's date.
    - For **End date**, click **No end date**.
    - Change the **Schedule** settings to configure the task to run at 4:00 or 5:00 p.m.

      Note

      Historically, **Trellix** releases DAT files only once a day, at about 3:00 p.m. Eastern Time (19:00 UTC or GMT). In the rare case that a second DAT file is released later in the day, it requires an administrator to disable the copy task to your **Current** Branch.

    - Click **Next**, confirm that all settings are correct in the **Summary** tab, then click **Save**.

Results

To confirm that the DAT file copy from the Evaluation branch to the Current branch is working, go to **Menu → Software → Main Repository** and use the Check-In date information to confirm that the **Evaluation** branch DAT file was copied to the **Current** branch at the time configured in the schedule.

Best practice: Create a test group of systems

To safely test DAT and content files, create a test group of systems used to run the files in your **Evaluation** repository.

Make sure that the test group of systems you use meet the following criteria:

- Use a representative sampling of system server builds, workstation builds, and operating systems and Service Packs in your environment for validation.
- Use 20–30 systems for validation for organizations with less than 10,000 nodes. For larger organizations, include at least 50 types of systems.

Note

You can use VMware images that replicate your operating system builds. Make sure that these systems are in a "clean" state to ensure that no malware has been introduced.

- Use Tags to apply policies and tasks to individual systems that are scattered throughout your **System Tree**. Tagging these systems has the same effect as creating an isolated test group, but allows you to keep your systems in their current groups.

Task

1. **To create a System Tree group, select Menu → Systems Section → System Tree.**
2. **From the System Tree group list, select where you want to add your new group, then click System Tree Actions → New Subgroups, and in the New Subgroups dialog box, type a name, for example** DAT Validation**, then click OK.**
3. **To add systems to your test group, you can drag systems from other groups to your newly created subgroup, add new systems, or add virtual machine systems.**

Results

You created a test group as an isolated group of systems. This test group allows you to test new DAT and engine updates before you deploy the updates to all other systems in your organization.

Best practice: Configure an agent policy for the test group

Create a **Trellix Agent** policy with an update task that automatically copies DAT and content files to the systems in your test group.

Task

1. **In the System Tree, select Menu → Systems Section → System Tree, then click the test group that you created.**
2. **To duplicate the existing policy, click the Assigned Policies tab, select Trellix Agent from the Product list, then in the Category list in the General policy row, click My Default.**
3. **On the My Default page, click Duplicate, and in the Duplicate Existing Policy dialog box, type the name, for example** Update from Evaluation**, add any notes, then click OK.**
   This step adds a policy, **Update from Evaluation**, to the Policy Catalog.
4. **Click the Updates tab to change the repository used by this policy.**
5. **In the Repository branch to use for each update type, click the DAT and Engine list down-arrows, then change the listed repositories to Evaluation.**
6. **Click Save.**

Results

Now you have created a **Trellix Agent** policy to use with an update task that automatically copies the DAT and content files to the systems in your test group from the **Evaluation** repository.

Best practice: Configure an on-demand scan of the test group

Create an on-demand scan task that starts after you update the DAT files to your test group, to scan for any problems that occur in your test group.

Before you begin

You must have created the test group in your **System Tree**.

Note

This configuration assumes that you are not using user systems as your test systems. If you are using actual user systems, you might need to change some of these scan configurations.

Task

1. To create a new on-demand scan task, select Menu → Policy → Client Task Catalog, then from the Client Task Catalog page in the Client Task Types list, expand VirusScan Enterprise and click On Demand Scan.
2. In the Client Task Catalog page, click New Task, and in the New Task dialog box, confirm that On Demand Scan is selected and click OK.
3. On the Client Task Catalog: New Task page, type a name, for example, Evaluation test group ODS task, and add a detailed description.
4. Click the Scan Locations tab, then configure these settings:
    a. For the Locations to scan, configure:
        - Memory for rootkits
        - Running Processes
        - All local disks
        - Windows folder
    b. For the Scan options, select Include subfolders and Scan boot sectors.
5. Click the Scan Items tab, then configure these settings:
    a. For File types to scan, select All files.
    b. For Options, select Detect unwanted programs.
    c. For Heuristics, select Find unknown program threats and Find unknown macro threats.
6. In the Actions tab:
    a. For When a threat is found, configure Clean files, then Delete files.
    b. For When an unwanted program is found, configure Clean files, then Delete files.
7. Click the Performance tab and configure System utilization as Low and Artemis as Very Low.

    Important

    Do not change any settings on the **Reports** tab.

8. In the Task tab:
    a. For Platforms where this task will run, select Run this task on servers and Run this task on workstations.
    b. For User account to use when running task, set your credentials and select the test group domain.
9. Click Save.

Results

Now the on-demand scan task is configured to scan for any problems that might occur in your test group. Next configure a client task to schedule when to launch the task.

Best practice: Schedule an on-demand scan of the test group

Schedule your on-demand scan task to run five minutes after each **Trellix Agent** policy update from the **Evaluation** repository to the test group.

Before you begin

You must have created a test group of systems and an on-demand scan of the test group.

Task

1. **Select Menu → Policy → Client Task Catalog.**
2. **On the Client Task Catalog page, select VirusScan Enterprise and On Demand Scan in Client Task Types.**
3. **Find the on-demand scan you created, click Assign in the Actions column, select the test group of systems that you created to assign the task, then click OK.**
4. **In the Client task Assignment Builder, configure these settings, then click Next:**
    a. **For Product list, select VirusScan Enterprise.**
    b. **For Task Type list, select On Demand Scan.**
    c. **For Task Name list, select the ODS task you created.**
5. **In the Schedule tab, configure these settings:**
    a. **For Schedule status, select Enabled.**
    b. **For Schedule type, select Daily from the list.**
    c. **For Effective period, select today's date as the Start date, then select No end date.**
    d. **For Start time, configure these settings:**
        - Select **9:05 AM** from the time lists.
        - Click **Run at that time, and then repeat until**, then select **2:00 PM** from the time lists.
        - For **During repeat, start task every**, select **5 minute(s)** from the lists.
    e. **For Task runs according to, click Local time on managed systems.**
    f. **For Options, deselect everything.**
6. **Click Next, check the Summary page, then click Save.**

Results

Your on-demand scan task is now scheduled to run every 5 minutes, from 9:05 a.m. until 2:00 p.m., after each agent policy update, from the **Evaluation** repository to the test group.

Best practice: Configure an Automatic Response for malware detection

If malware is found by the on-demand scan in the test group, you want to block the files from being copied automatically to the **Current** repository. Set up an automatic notification to the administrator.

Before you begin

You must have already created an on-demand scan task to scan for any problems that might occur in your test group.

Task

1. **To display the Response Builder, select Menu → Automation → Automatic Responses, click New Response, then configure these settings in the Descriptions tab, then click Next.**
    a. **Type a name, for example** `Malware found in test group`**, and a detailed description**
    b. **For Language, select a language from the list.**
    c. **For Event Group, select ePO Notification Events from the list.**
    d. **From Event type, select Threat from the list.**
    e. **For Status, select Enabled.**
2. **Configure these settings in the Filter tab, then click Next.**
    a. **For Available Properties list, select Threat Category.**
    Optionally, you can add additional categories, such as an access protection rule being triggered.
    b. **In the Required Criteria column and the Defined at row, click ... to select the test group of systems that you created in the Select System Tree Group dialog box, then click OK.**
    c. **In the Threat Category row, select Belongs to from the Comparison list and Malware from the Value list. Click + to add another category.**
    d. **Select Belongs to from the Comparison list and Access Protection from the Value list.**
3. **Configure these settings in the Aggregation tab, then click Next.**
    a. **For Aggregation, click Trigger this response for every event.**
    b. **Do not configure any Grouping or Throttling settings.**
4. **Configure these settings in the Actions tab:**
    a. **Select Send Email from the Actions list.**
    b. **For Recipients, type the email address of the administrator to be notified.**
    c. **For Importance, select High from the list.**
    d. **For Subject, type an email header, for example** `Malware found in the Test Group!`
    e. **For Body, type a message, for example** `Research this NOW and stop the server task that pulls content into the Current branch!`
    f. **Following the message body, insert these variables to add to the message, and click Insert:**
        - **OS Platform**
        - **Threat Action Taken**
        - **Threat Severity**
        - **Threat Type**
5. **Click Next, confirm that the configuration is correct in the Summary tab, then click Save.**

Results

Now you have an **Automatic Response** configured that sends an email to an administrator any time malware is detected in the test group running the Evaluation DAT file.

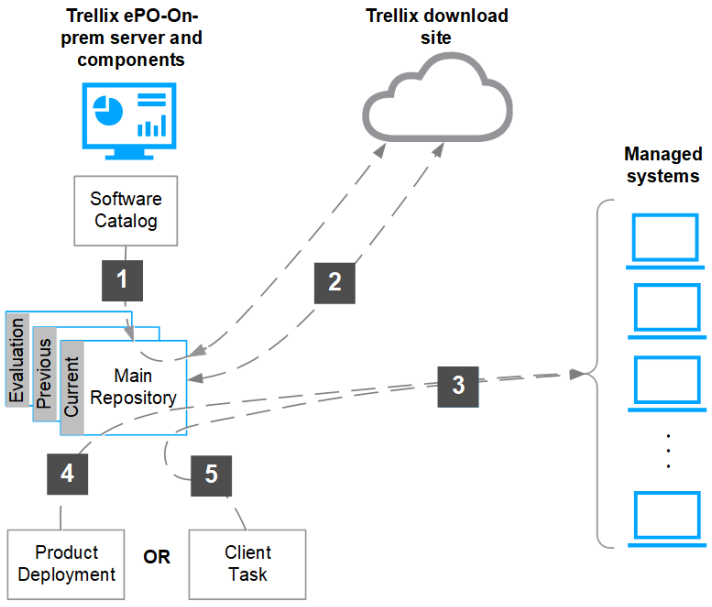
Deploying products

Product deployment steps

You can deploy product software to your managed systems using automatic or manual configuration methods. The method you choose depends on the level of detail you want to configure to complete the process.

The following diagram shows the processes you can use to add and update software on the **Main Repository**, then deploy that software to your managed systems.

1. Use the **Software Catalog** to automatically review and update **Trellix** software and software components.
2. From the **Main Repository**, you can manually check in deployment packages then use **Product Deployment** or client tasks to deploy them to your managed systems.
3. The **Product Deployment** feature offers a simplified workflow and increased functionality to deploy products to your **Trellix ePO - On-prem** managed systems.
4. Create client tasks to manually assign and schedule product deployments to groups or individual managed system.
5. Product deployment is the output process that keeps your security software as current as possible to protect your managed systems.



Choosing a product deployment method

Deciding which product deployment method to use depends on what you have already configured.

Product Deployment projects offer a simplified workflow and increased functionality for deploying products to your **Trellix ePO - On-prem** managed systems. However, you can't use a **Product Deployment** project to act on or manage client task objects and tasks created in a version of the software before 5.0.

To maintain and use client tasks and objects created outside of a **Product Deployment** project, use the client task object library and assignment interfaces. You can maintain existing tasks and object while using the **Product Deployment** project interface to create new deployments.

Benefits of product deployment projects

Product deployment projects simplify the process of deploying security products to your managed system by reducing the time and overhead to schedule and maintain deployments throughout your network.

Product deployment projects streamline the deployment process by consolidating many of the steps to create and manage product deployment tasks individually. They also add the ability to:

- **Run a deployment continuously** — You can configure your deployment project so that when new systems matching your criteria are added, products are deployed automatically.
- **Stop a running deployment** — If you must stop a deployment once it's started, you can. Then you can resume that deployment when you're ready.
- **Uninstall a previously deployed product** — If a deployment project has been completed, and you want to uninstall the associated product from the systems assigned to your project, select **Uninstall** from the **Action** list.

The following table compares the two processes for deploying products — individual client task objects and product deployment projects.

Product deployment methods compared

Client task objects	Function comparison	Product deployment project
Name and description	Same	Name and description
Collection of product software to deploy	Same	Collection of product software to deploy
Use tags to select target systems	Enhanced in Product Deployment project	Select when the deployment occurs: • **Continuous** — Continuous deployments use **System Tree** groups or tags which allow you to move systems to those groups or assign systems tags and cause the deployment to apply to those systems.

Client task objects	Function comparison	Product deployment project
		• **Fixed** — Fixed deployments use a fixed, or defined, set of systems. System selection is done using your **System Tree** or **Managed Systems Query** output tables.
Deployment schedule	Similar	Simplified deployment schedule allows you to either run the deployment immediately or run it once at a scheduled time.
Not specified	New in Product Deployment project	Monitor the current deployment status, for example deployments scheduled but not started, in progress, stopped, paused, or completed.
Not specified	New in Product Deployment project	(Fixed deployments only) View a historical snapshot of data about the number of systems receiving the deployment.
Not specified	New in Product Deployment project	View the status of individual system deployments, for example systems installed, pending, and failed.
Not specified	New in Product Deployment project	Modify an existing deployment assignment using: • **Create New** for modifying an existing deployment • **Edit** • **Duplicate** • **Delete** • **Stop** and **Pause Deployment** • **Continue** and **Resume Deployment**

Client task objects	Function comparison	Product deployment project
		• Uninstall

Viewing Product Deployment audit logs

Audit logs from your deployment projects contain records of all product deployments made from the console using the **Product Deployment** feature.

Audit log entries are displayed in a sortable table within the **Deployment** details area of the **Product Deployment** page. Audit log entries are also available on the **Menu** → **Reporting** → **Audit Log** page, which contains log entries from all auditable user actions. You can use these logs to track, create, edit, duplicate, delete, and uninstall product deployments. Click a log entry to display entry details.

View product deployment

During the initial product deployment, **Trellix ePO - On-prem** automatically creates a product deployment process. You can use this product deployment process as a base to create other product deployments.

Before you begin

You must run the **Getting Started** dashboard process to create a product deployment or create a product deployment manually.

Task

1. **Find the initially created product deployment: select Menu → Product Deployment.**
   The initially created product deployment uses the name of the **System Tree** group you configured in the **Getting Started** dashboard process and appears in the **Deployment summary** list with the name **Initial Deployment My Group**.
2. **To view the product deployment details, select the name of the product deployment assigned to the initial product deployment URL that you created. The page changes to display details of the product deployment configuration.**

Caution

Don't change this default product deployment. This deployment is running daily to update your managed systems if any products or the **Trellix Agent** are updated.

Results

Now you know the location and configuration of the initially created product deployment. You can duplicate this product deployment, for example, to deploy the **Trellix Agent** to platforms using different operating systems.

You can also change the initially created client task named, for example **Initial Deployment My Group**. To find the client task, select **Menu** → **Client Task Catalog**; it is listed in the **Client task Types** under **Product Deployment**.

Product Deployment page

View the configuration and status of currently configured deployment or uninstallation projects. You can edit, delete, duplicate, start, stop, and uninstall deployment projects using this page.

Deployment summary option definitions

Option	Definition
Type	The list of deployment type filters include: • **All** — Displays all deployments. • **Continuous** — Displays only **Continuous** deployments. • **Fixed** — Displays only **Fixed** deployments. **Note:** Deployments are sorted by start date, displaying the newest first.
Status	The list of deployment status filters include: • **All** — Displays all deployments. • **Finished** — Displays the completed deployments. • **In Progress** — Displays only **Fixed** deployments that have begun. • **Pending** — Displays when the server is waiting for the next agent communication. The default is 60 minutes. **Note:** Items are often pending while waiting for the next agent communication to the server. • **Running** — Displays only **Continuous** deployments that have begun. • **Stopped** — Displays only the deployments selected as stopped.
Configured deployment list	Displays the status of the deployment as: • **Finished** — For fixed deployments, displays **Completion** and 100%.

Option	Definition
Note: The information displayed for each list item depends on the deployment type.	• **In Progress** — Displays **Completion** and percentage complete. • **Pending** — For continuous deployments, displays the icon ∞. For **Fixed** deployments, displays **Completion** and percentage 0%. • **Running** — For continuous deployments, displays the icon ∞. • **Uninstallation** — Displays **Uninstalling...** until completion.
	Displays the deployment type: • **Continuous Deployment** — Assigns client tasks using the **System Tree** groups or tags. This setting allows the number of systems inheriting the task to change dynamically. • **Fixed Deployment** — Uses a defined, set of systems. You can select systems for deployment using the **System Tree** or **Managed Systems Queries**.
	Displays the system selection method used and varies depending on the type of deployment. • **Group** — For continuous deployments, displays the number of **System Tree** groups selected for product deployment updates. **Note:** You can hover over the number to see the list of **System Tree** groups. • **Tags** — For continuous deployments, displays the number of tags selected for product deployment updates. **Note:** You can hover over the number to see the list of tags.

Option	Definition
	• **Systems** — For fixed deployments, displays the number of systems selected for product deployment updates.

Deployment details option definitions

Option	Definition
Actions	The list of deployment actions include: • **Delete** — Displays a caution about the consequences of this selection. **Note:** The consequences of the delete action depend on the status of the deployment. If you click **Delete** and the deployment status is: ▫ **Pending** — Remove the deployment from the list of Deployments and cancels and deselects all settings and assignments associated with the deployment. ▫ **In Progress** or **Stopped** — Warns you that you must "Uninstall" before deleting the packages from clients that have already received deployment. If deployment is stopped, delete only removes the deployment from the list of deployments, cancels and deselects all settings, and cancels and deselects assignments associated with the deployment. ▫ **Finished** — Removes the deployment from the list of **Deployments** and cancels and deselects all settings and assignments associated with the deployment. ▫ **Running** — Warns you that you must "Uninstall" before deleting the packages from clients that have already received deployment. If deployment is stopped, delete only removes the deployment from the list of deployments, cancels and

Option	Definition
	deselects all settings, and cancels and deselects assignments associated with the deployment. • **Duplicate** — Opens the **Duplicate Deployment** page with the selected deployment information displayed and available to edit. Rename the new deployment and save it to create a duplicate deployment. **Note:** Adds (copy) to the original deployment name. Rename the deployment and save it to create a duplicate. • **Edit** — Opens the **New Deployment** page with the selected deployment information displayed and available to edit. • **Mark Finished** — Stops the deployment and displays a dialog box you can use to change settings and assignments. **Caution:** This is a permanent stop. It deletes the client, task, and the system list and cannot be undone. The deployment remains in the list as a reference and can be deleted in the future. • **Resume** — The selected stopped deployment resumes deployment. • **Stop** — The selected deployment changes: ▫ Client tasks assigned to all pending system tasks change to disabled. ▫ Status changes to stopped. • **Uninstall** — Uninstalls all packages that have been deployed.
Deployment details **Note:** The information displayed depends on the deployment type.	

Option	Definition
Calendar	Displays a calendar image with the next scheduled date of a pending deployment.
Progress	Toggles between these options: • **Current** — Displays a bar chart with a task status: ▫ **Successful** — Displays the number of successful products deployed or uninstalled. ▫ **Failed** — Displays the number of failed products deployed or uninstalled. ▫ **Pending** — Displays the number of pending products deployed or uninstalled. • **Duration** — For **Fixed** deployments only, displays a histogram. Each column displays: ▫ **Successful** — Displays the number of successful products deployed or uninstalled. ▫ **Failed** — Displays the number of failed products deployed or uninstalled. ▫ **Pending** — Displays the number of pending products deployed or uninstalled. **Note:** The displayed columns show the days or weeks that the deployment has been running. If the deployment is longer than the 18 days that can be displayed, the columns indicate weeks. **Tip:** You can hover over a color in a column of the histogram to display a tooltip with the number of systems indicated.
Details	Display depends on the type of deployment. • **Start Date** — Displays date deployment started or is going to start. • **Type** — Displays **Continuous** or **Fixed** Deployment. • **Status** — Displays: ▫ **Running** — For **Continuous** Deployments ▫ **In Progress** — For **Fixed Deployments**

Option	Definition
	▫ **Pending** ▫ **Finished** • **Group** — (**Continuous**) Displays the **System Tree** groups used to select systems for deployment. • **Systems** — (**Fixed**) Display the number of systems assigned for the deployment. • **Tag** — (**Continuous**) Displays the tags used to select systems for deployment. • **Packages** — Displays the software packages associated with the deployment. The action associated with the package is added to the package name. For example, " - Install" or " - Uninstall." **Note:** If the associated deployment package has been deleted, moved or expired, the package name appears grayed out with an exclamation point. You must fix the associated package or you can't save the deployment. • **View Task Details** — Opens the **Edit Deployment** page with the selected deployment's information visible and editable.

System table option definitions

Option	Definition
Filter	Filters the systems, **System Tree** groups, or tags to display in the table, depending on the type of deployment selected. • **All** — Displays the systems or tags in the table, depending on the type of deployment. • **Install Successful** — Displays the successfully deployed systems or tags in the table, depending on the type of deployment. • **Pending** — Displays the pending deployed systems or tags in the table, depending on the type of deployment.

Option	Definition
	• **Failed** — Displays the systems, **System Tree** groups, or tags that failed to deploy in the table, depending on the type of deployment. If the selected deployment is an uninstallation, the list items include: • **All** — Displays the systems or tags in the table, depending on the type of deployment. • **Packages Removed** — Displays the systems with the deployment removed. • **Install Successful** — Displays the successfully deployed systems or tags in the table, depending on the type of deployment. • **Pending** — Displays the pending deployed systems or tags in the table, depending on the type of deployment. • **Failed** — Displays the systems, **System Tree** groups, or tags in the table, that failed to deploy in the table, depending on the type of deployment.
System Actions	Displays the filtered list of systems in a dialog box with more details.
System Name	Display the system names filtered in the table, depending on the type of deployment selected.
Status	The system deployment status indicator is separated into segments. Each segment indicates its status using these colors: • Gray — Pending • Red — Error • Green — Finished When all segments are green, the deployment is complete.
Tags	Displays the system tags selected for product deployment updates.

Deploy products using a deployment project

A deployment project allows you to easily select products to deploy to your target systems, and schedule the deployment.

Note

Expired products appear in the Packages list. You can uninstall them from target systems in Actions.

Task

1. **Select Menu → Software → Product Deployment.**
2. Select **New Deployment** to start a new project.
3. Type a name and description for this deployment. This name appears on the **Product Deployment** page after you save the deployment.
4. **To specify which software to deploy or uninstall, select a product from the Package list. Click + or - to add or remove packages.**

   Important

   Your software must be checked in to the **Main Repository** before it can be deployed. The **Language** and **Branch** fields are populated automatically, as determined by the location and language specified in the **Main Repository**.

5. **From the Actions list, select Install or Uninstall.**
6. **In the Command line text field, specify any command-line installation options. For information about command-line options, see the product documentation for the software you're deploying.**
7. Under **Select the systems**, click **Select Individual Systems** or **Select by Tag or Group**.
   - **Select Individual Systems** — Results in a fixed deployment
   - **Select by Tag or Group** — Results in a continuous deployment

   The **System Selection** dialog box allows you to select systems in your **System Tree** using these tabs:
   - **System Tree** — Select **System Tree** groups or subgroups and their associated systems.
   - **Tags** — Select tag groups or tag subgroups and their associated systems.
   - **Selected Systems** — Displays the total selections you made in each tab, creating the target systems for your deployment.

   For example, if your **System Tree** contains Group A, which includes both servers and workstations, you can target the entire group. You can also target only the servers or only the workstations (if they are tagged correctly), or a subset of either system type in Group A.

   The **Total** field displays the number of systems, groups, or tags selected for the deployment.
8. **To automatically update your products, select from these Auto Update options.**
   - **Automatically deploy latest version of the products**
   - **Allow end users to postpone this deployment (Windows only)**
   - **Maximum number of postponements allowed**
   - **Option to postpone expires after**

- **Display this text**

Note

During a new deployment, the **Trellix Agent** checks for new updates, hotfixes, and content packages of all installed products on the client. See the **Trellix Agent** documentation for details.

9. **Under Select a start time select a schedule for your deployment:**
    - **Run Immediately** — Starts the deployment task during the next ASCI.
    - **Once** or **Daily** — Opens the scheduler so you can configure the start date, time, and randomization.
10. Click **Save** at the top of the page. The **Product Deployment** page opens with your new project added to the list of deployments.

Results

After you create a deployment project, a client task is automatically created with the deployment settings.

Monitor and edit deployment projects

Use the **Product Deployment** page to create, track, and change deployment projects.

Task

1. **Select Menu → Software → Product Deployment.**
2. **Filter the list of deployment projects using the following:**
    - **Type** — Filters the deployments that appear by **All**, **Continuous**, or **Fixed**.
    - **Status** — Filters the deployments that appear by **All**, **Finished**, **In Progress**, **Pending**, **Running**, or **Stopped**.
3. **From the list on the left side of the page, click a deployment to display its details on the right side of the page.**

Note

If a package in this deployment expires, the deployment is invalid. If you mouse-over the deployment, you see this message: "Package(s) in this deployment have been moved, deleted, or expired."

4. **Use the progress section of the details display to view:**
    - Calendar displaying the start date for pending continuous and fixed deployments.
    - Histogram displaying systems and the time to completion for fixed deployments.
    - Status bar displaying system deployment and uninstallation progress.

Note

Under the status bar, Task Status lists Successful, Failed, and Pending for the number of target systems in parentheses.

5. **Click Action and one of these actions to modify a deployment:**
    - **Edit**
    - **Delete**
    - **Duplicate**
    - **Mark Finished**
    - **Resume**
    - **Stop**
    - **Uninstall**
6. **In the details section, click View Task Details to view and modify the settings for the deployment.**
7. **In the Systems table, select an option in the Filter list to change which systems appear.**

Note

The options in the list depend on the status of the deployment.

- For the **Uninstall** action, the filters include **All**, **Packages Removed**, **Pending**, and **Failed.**
- For all other actions, the filters include **All**, **Install Successful**, **Pending**, and **Failed**.

8. **In the Systems table you can:**
    - Check the status of each row of target systems in the **Status** column. A three-section status bar indicates the progress of the deployment.
    - Check the tags associated with the target systems in the **Tags** column.
    - Click **System Actions** to perform system-specific actions on the systems you select.

Global updating

Global updating automates replication to your distributed repositories and keeps your managed systems current.

Replication and update tasks are not required. Checking contents into your Main Repository initiates a global update. The entire process finishes within an hour in most environments.

You can also specify which packages and updates initiate a global update. When you specify that certain content initiates a global update, make sure to create a replication task to distribute content that was not selected.

Tip

Best practice: When using global updating, schedule a regular pull task (to update the Main Repository) at a time when network traffic is minimal. Although global updating is much faster than other methods, it increases network traffic during the update.

Global updating process

1. Contents are checked in to the Main Repository.

2. The server performs an incremental replication to all distributed repositories.
3. The server issues a **SuperAgent** wake-up call to all **SuperAgent** in the environment.
4. The **SuperAgent** broadcasts a global update message to all agents within the **SuperAgent** subnet.
5. Upon receipt of the broadcast, the agent is supplied with a minimum catalog version needed for updating.
6. The agent searches the distributed repositories for a site that has this minimum catalog version.
7. Once a suitable repository is found, the agent runs the update task.

If the agent does not receive the broadcast, the minimum catalog version is supplied at the next agent-server communication.

Note

If the agent receives notification from a **SuperAgent**, the agent is supplied with the list of updated packages. If the agent finds the new catalog version at the next agent-server communication, it is not supplied with the list of packages to update, and updates all packages available.

Requirements

These requirements must be met to implement global updating:

- A **SuperAgent** must use the same agent-server secure communication (ASSC) key as the agents that receive its wake-up call.
- A **SuperAgent** is installed on each broadcast segment. Managed systems cannot receive a **SuperAgent** wake-up call if there is no **SuperAgent** on the same broadcast segment. Global updating uses the **SuperAgent** wake-up call to alert agents that new updates are available.
- Distributed repositories are set up and configured throughout your environment. We recommend **SuperAgent** repositories, but they are not required. Global updating functions with all types of distributed repositories.
- If using **SuperAgent** repositories, managed systems must be able to access the repository where its updates come from. Although a **SuperAgent** is required on each broadcast segment for systems to receive the wake-up call, **SuperAgent** repositories are not required on each broadcast segment.

Deploy update packages automatically with global updating

You can enable global updating on the server to automatically deploy user-specified update packages to managed systems.

Task

1. **Click Menu → Configuration → Server Settings, select Global Updating, then click Edit at the bottom of the page.**
2. **On the Edit Global Updating page next to Status, select Enabled.**
3. **Edit the Randomization interval, if wanted.**
   Each client update occurs at a randomly selected time within the randomization interval, which helps distribute network load. The default is **20 minutes**.
   For example, if you update 1000 clients using the default randomization interval of 20 minutes, roughly 50 clients update each minute during the interval. This randomization lowers the load on your network and on your server. Without the randomization, all 1000 clients would try to update simultaneously.
4. **Next to Package types, select which packages initiate an update.**

Global updating initiates an update only if new packages for the components specified here are checked in to the **Main Repository** or moved to another branch. Select these components carefully.

- **Signatures and engines** — Select **Host Intrusion Prevention Content**, if needed.

Note

Selecting a package type determines what initiates a global update (not what is updated during the global update process). Agents receive a list of updated packages during the global update process. The agents use this list to install only updates that are needed. For example, agents only update packages that have changed since the last update and not all packages if they have not changed.

5. **When finished, click Save.**
   Once enabled, global updating initiates an update the next time you check in any of the selected packages or move them to another branch.

Note

Make sure to run a **Pull Now** task and schedule a recurring **Repository Pull** server task, when you are ready for the automatic updating to begin.

ePO Support Center

The ePO Support Center extension provides access to information about your servers and installed products.

The Support Center helps you with the following tasks:

- Viewing live data about your **Trellix ePO - On-prem** Server Health.
- Receiving Support Notifications (SNS).
- Searching across content portals and knowledgebases.
- Accessing product-specific best practices and how-to information.

Note

For FAQs and installation information, see KB91510. Support Center requires ePO 5.9.0 or later.

ePO Server Health

ePO Server Health provides useful details about your ePO server and database. The health timeline shows regularly scheduled status updates.

ePO Server Details

ePO Server Details provides an overview of your ePO server, ePO version, and database.

- Server Details
- ePO Details
- SQL Server Details
- ePO Database Details
- ePO Event Database Details

Server Health Timeline

Server Health Timeline provides a visual display of regularly scheduled health checks over time. By default, these checks run hourly and you can modify the schedule using the **Server Task** page. You can also run a manual health check.

The color coded icons represent each of the checks. The icons describe the type of check and are color coded to indicate the status. Typically, green means the check was successful, yellow that there was a warning, and red that the check failed. You can hover over an icon to view quick details. Click the icon to view more details.

You can view the details of the default and manual health checks in the **Audit Log** page.

Health Check Details

Health Check Details provides a summary of the selected row in the timeline. It also includes detailed information about each of the specific checks.

Health check details

Option	Definition	Indicators
ePO Database Connection Check	Verifies connectivity between the ePO server and the ePO database server.	Can ePO connect to the database? • Successful — Yes • Failed — No
ePO Server machine CPU Check	Verifies the CPU load of the ePO server.	ePO server CPU load is... • Successful — Less than 70% • Warning — More than 70% • Failed — More than 90%
ePO Server Machine Memory Check	Verifies the memory load of the ePO server.	Free memory is... • Successful — More than 30% • Warning — Less than 30% • Failed — Less than 10%
ePO Database CPU Check	Verifies the CPU load of the ePO database server.	ePO database server CPU load is... • Successful — Less than 70% • Warning — More than 70% • Failed — More than 90%
ePO Database Index Fragmentation Check	Verifies the index fragmentation state of the ePO database.	Index fragmentation is... • Successful — Less than 70% • Warning — More than 70%
ePO Database Memory Check	Verifies the memory load of the ePO database server.	Free memory is... • Successful — More than 30% • Warning — Less than 30% • Failed — Less than 10%
ePO Database Size Check	Verifies the free space available on the ePO database server.	Free space is... • Successful — More than 30% • Warning — Less than 30%

Option	Definition	Indicators
		• Failed — Less than 10%
ePO Application Server JVM Thread Check	Verifies the thread status of the ePO Application Server JVM.	Threads timed waiting count and blocked count are... • Successful — Less than 100 and 0 • Warning — More than 100 and 0 • Failed — More than 100 and more than 0
ePO Application Server JVM CPU Check	Verifies the CPU load of the ePO Application Server JVM.	ePO Application Server JVM CPU load is... • Successful — Less than 70% • Warning — More than 70% • Failed — More than 90%
ePO Application Server JVM Memory Check	Verifies the memory load of the ePO Application Server JVM.	Free memory is... • Successful — More than 30% • Warning — Less than 30% • Failed — Less than 10%
Data Channel Waiting Queue Check	Verifies the waiting queue load for data channel messages.	Waiting count is... • Successful — Less than 5 • Warning — More than 5
Event Parser Failing Check	Verifies the ePO Event Parser failing count.	Failing count is... • Successful — Equal to 0 • Failed — More than 0
Event Parser Waiting Check	Verifies the waiting queue load of the ePO Event Parser.	Waiting count is... • Successful — Less than 50 • Warning — More than 50

Option	Definition	Indicators
Failing Server Tasks Check	Verifies whether server tasks have been failing in the last 7 days.	Tasks are failing? • Successful — No • Failed — Yes
Waiting Server Tasks Check	Verifies whether server tasks have been in a waiting state from more than an hour at the time of the check.	Tasks are in a waiting state for more than an hour? • Successful — No • Warning — Yes

Manual server health checks

Apart from the scheduled default server health checks that run every hour, you can trigger the health checks manually at any point in time.

Manual Health Check Details

These are the manual health checks that are not run by default and the detailed information about each of the specific checks.

Manual Health check details

Option	Definition	Indicators
ePO Database Collation Check	Verifies the database collation match between the ePO database server and the ePO database.	Does the database collation match between the ePO database server and the ePO database? • Successful — Yes • Failed — No

Note

You can't run the scheduled Default Health Check group manually; but you can run the health check for a group or an individual check manually. However, you can run the default server health checks at any time on the **Server Tasks** page.

Support Notifications

Support Notifications provides a view of the most recent information posted by the Support Notifications Service (SNS). You can use this feed to view the most up-to-date information on product upgrades, product releases, end-of-life notices, and critical incidents.

The **Support Notifications** page is a continuously updated news feed that displays notifications received in the last 30 days. The page displays the newest notifications first and updates every hour. When a notification is added to the page for the first time, it is tagged as **New**. Clicking a link opens the notice in a new browser tab.

In the upper-right corner, you can see when the Support Notification page was updated. By default, the page refreshes hourly. Click the refresh icon to manually refresh the Support Notification page.

Create Support Notification tags

Tags allow you to filter the support notifications based on various criteria such as criticality, software updates, release notifications and so on. You can provide a name of your choice and color code the tags for easy identification. Tagging the notifications helps you to categorize and prioritize the notifications.

Task

1. **Select Menu → Support Center → Support Notifications.**
2. **Click Tags and then click Create new tag.**
3. **Enter a name for the new tag, choose a tag color from the palette and then click Save.**

Results

You have created a new tag and now you can apply this tag to the support notifications.

Apply Support Notification tags

You can create and apply tags based on various criteria to categorize the support notifications. You can apply multiple tags to a single notification.

Task

1. **Select Menu → Support Center → Support Notifications.**
2. **Select the notifications that you want to tag, then click Tags.**
3. **You can select from the existing list of tags or create a new tag and then click Apply tags.**
   You can see the tag under the notification.

Results

The selected notifications are tagged and can be easily filtered based on the tag.

Remove a support notification tag

You can remove a tag that is applied to a support notification if the tag is not applicable to that notification anymore.

Task

1. **Select Menu → Support Center → Support Notifications.**
   You can view the tags applied to a notification below the notification itself.
2. **Click the cross mark on the tag to remove the tag from the notification.**

Results

The tag is removed from the notification.

Delete a support notification tag

Tags are created to categorize and filter notifications. After the notifications are viewed and addressed, you may choose to delete the tags that are of no use anymore.

Task

1. **Select Menu → Support Center → Support Notifications.**
2. **Click Tags and then select the tag that you want to delete and click Delete Tags. You can select multiple tags and delete at once.**

Results

The selected tags are deleted permanently.

Edit a support notification tag

You can edit an existing tag using the Edit tag option. You can change the name of the tag or change the color assigned to the tag or do both.

Task

1. **Select Menu → Support Center → Support Notifications.**
2. **Click Tags and select the tag that you want to edit. Then, click Edit Tag.**
3. **Make the required changes to the name or the color or both. Then, click Save.**

Results

The changes are applied to the tag.

Filter tagged support notifications

You can filter notifications based on the tags applied. The page displays only the tagged notifications.

Task

1. **Select Menu → Support Center → Support Notifications.**
2. **Click Tags and then select the tag that you want to filter and click Filter Tagged.**

Results

The tagged support notifications are filtered and displayed .

Search Support

The **Search Support** feature allows you to search for content on the support services site from within the ePO Console.

Enter a search term in the field to view a list of related articles.

Product Information

Product Information includes a selection of useful topics about your products. The page organizes content by product and topic. Each topic includes high-level information and links to relevant best practices on the documentation portal.

The **Product Information** page includes content for 10 **Trellix** products.

Reference Configuration

Reference Configuration includes **Trellix**-recommended deployment scenarios to make sure that you follow step-by-step deployment sequence for the products installed on your environment.

The **Reference Configuration** page includes a link that directs you to a list of products. After you select a product and its version, the Reference Configuration tool displays the recommended deployment sequence to install and upgrade the product.

For more information, see KB88274.

Enforcing policies

A policy is a collection of settings that you create and configure, then enforce.

Trellix ePO - On-prem organizes its policies by product, then by categories in each product. For example, **Trellix Agent** includes categories for **General**, **Repository**, and **Troubleshooting**.

To see policies in a specific policy category, select **Menu** → **Policy** → **Policy Catalog**, then select a product and category from the drop-down lists. **The Policy Catalog page displays only policies for products that the user has permissions to.**

Each category includes two default policies, **McAfee Default** and **My Default**. You can't delete, edit, export, or rename these policies, but you can copy them and edit the copy.

For example, you might want to change the default response time that managed systems communicate back to the **Trellix ePO - On-prem** server.

About policies

A policy is a collection of settings that you create and configure, then enforce.

Trellix ePO - On-prem organizes its policies by product, then by categories for each product. For example, the **Trellix Agent** product includes categories for **General**, **Repository**, and **Troubleshooting**.

To see policies in a specific policy category, select **Menu** → **Policy** → **Policy Catalog**, then select a product from the Products pane and the corresponding categories appear on the right pane. Expand the category to see the list of policies. **On the Policy Catalog page, users can see only policies for products they have permissions to.**

Each category includes two default policies,

- **McAfee/Trellix Default** — You can't delete, edit, export, or rename this policy, but you can copy it and then edit the copy.
- **My Default** — You can perform all the actions on this policy.

For example, you can increase the **Trellix ePO - On-prem** response time from the default value of every 60 minutes. To add time, change the agent-server communication interval (ASCI) for workstations in the **Trellix Agent** policy to every 240–360 minutes.

To change the workstation ASCI setting, duplicate the **Trellix Agent**, **Trellix Default** policy, in the **General** category, and change the ASCI setting. Then you must assign the new policy to a **System Tree** group or tag that includes all those workstations.

When policies are applied and enforced

Policies are applied to systems according to the amount of time defined in 2 settings. ASCI defines how often the agent communicates with the server. Policy enforcement interval defines when policy settings are enforced.

Applying policies

After you configure policy settings, the new settings are applied to specified managed systems at the next agent-server communication. By default, the agent-server communication occurs every 60 minutes. You can adjust this interval on the **General** tab of the **Trellix Agent** policy pages. **Or, depending on how you implement agent-server communication, you might change the ASCI using the agent wake-up client task.**

If you want to change the settings of a default policy, you need to duplicate the policy and rename it. Make the required changes and reassign the policy to the managed systems. The next time an agent-server communication occurs, the new policy is applied to these systems.

Enforcing policies

The timing of policy enforcement depends on the configuration of the policies. Enforcement can happen:

- **Instantly** Example: On-Access Scan policy occurs when you start any application.
- **At agent-server communication or policy enforcement intervals** Example: Product Deployment policy runs to confirm that the installed software versions on the managed systems match the versions on the Main Repository. If a new version is available, it is downloaded to all systems.
- **At configured Client Task intervals**: Example: On-demand scan policy, by default, runs every day at midnight to scan all your managed systems for threats.

After policy settings are applied on the managed system, the **Trellix Agent** continues to enforce policy settings according to the policy enforcement interval (default is 60 minutes). You can adjust this interval on the **General** tab as well.

When you want an on-demand scan to run every day at midnight, you configure the settings so that:

1. The Policy Based on-demand scan Client Task runs at 12 a.m.
2. The client task starts the full on-demand scan on the managed systems.
3. Using the configured settings in the policy, the scan runs and if any threats are found they are cleaned, quarantined, or deleted as required.

How policies are assigned to systems

Policies are assigned to systems by inheritance or assignment.

Inheritance — When a system or group of systems takes its policy settings and client tasks from its parent group. Enabled by default.

Assignment — When an administrator assigns a policy to a system or group of systems. You can define a policy once for a specific need, then apply it to multiple locations.

When you copy and paste policy assignments, only true assignments are pasted. If the source location inherited a policy that you selected to copy, it is the inheritance characteristic that was pasted to the target. The target then inherits the policy (for that particular policy category) from its parent.

Note

The inherited policy might be a different policy than the source policy.

Assignment locking

You can lock the assignment of a policy on any group or system. Assignment locking prevents other users from inadvertently replacing a policy. Assignment locking is inherited with the policy settings.

Assignment locking is valuable when you want to assign a certain policy at the top of the **System Tree** and make sure that no other users remove it.

Assignment locking does not prevent the policy owner from changing policy settings. So, if you intend to lock a policy assignment, make sure that you are the owner of the policy.

Policy ownership

The user that creates a policy is the assigned owner of that policy. You must have the correct permissions to edit a policy you don't own.

You can't use a policy owned by a different user, but you can duplicate the policy, then use the duplicate. Duplicating policies prevents unexpected policy changes from affecting your network. If you assign a policy that you don't own, and the owner modifies the policy, all systems that were assigned the policy receive the modifications.

You can specify multiple users as owners of a single policy.

Policy assignment rules

Policy assignments rules reduce the overhead of managing numerous policies and help maintain more generic policies across your System Tree.

This level of granularity in policy assignments limits the instances of broken inheritance in the System Tree. Policy assignments can be based on user-specific or system-specific criteria:

- **User-based policies** — Policies that include at least one user-specific criteria. For example, you can create a policy assignment rule that is enforced for all users in your engineering group. You can then create another policy assignment rule for members of your IT department. This rule allows the members of the IT department to log on to any computer in the engineering network with the access rights to troubleshoot problems on a specific system in that network. User-based policies can also include system-based criteria.
- **System-based policies** — Policies that include only system-based criteria. For example, you can create a policy assignment rule that is enforced for all servers on your network based on the tags you have applied, or all systems in a specific location in your System Tree. System-based policies cannot include user-based criteria.

Policy assignment rule priority

Policy assignment rules can be prioritized to simplify how you manage and maintain your policy assignments. When you set priority to a rule, it is enforced before other assignments with a lower priority.

In some cases, the outcome can be that rule settings are overridden. For example, consider a system that is included in two policy assignment rules, rules A and B. Rule A has priority level 1, and allows included systems unrestricted access to Internet content. Rule B has priority level 2, and heavily restricts the same system's access to Internet content. In this scenario, rule A is enforced because it has higher priority. As a result, the system has unrestricted access to Internet content.

Policy assignment rule priority on multi-slot policies

Multi-slot policies allow administrators to send more than 1 policy of a particular policy type to the client system. For example, an administrator can assign more than 1 Firewall rules policy which are merged and enforced on the client system.

Priority of rules is not considered for multi-slot policies. When a single rule containing multi-slot policies of the same product category is applied, all settings of the multi-slot policies are combined. Similarly, if multiple rules containing multi-slot policy settings are applied, all settings from each multi-slot policy are combined. As a result, the applied policy is a combination of the settings of each individual rule.

>

When multi-slot policies are aggregated, they are aggregated only with multi-slot policies of the same type. Multi-slot policies assigned using policy assignment rules override policies assigned in the **System Tree**. Also, user-based policies take priority over system-based policies. Consider the following scenario where:

Scenario: Using multi-slot policies to control Internet access

Your **System Tree** includes a group named "Engineering" that consists of systems tagged with "IsServer" or "IsLaptop." Policy A is assigned to all systems in this group. Assigning policy B to any location in the **System Tree** above the Engineering group using a policy assignment rule overrides the settings of policy A, and allow systems tagged with "IsLaptop" to access the Internet. Assigning policy C to any group in the **System Tree** above the Engineering group allows users in the Admin user group to access the Internet from all systems, including those in the Engineering group tagged with "IsServer."

Policy type	Assignment type	Policy name	Policy settings
Generic policy	Policy assigned in the **System Tree**	A	Prevents Internet access from all systems to which the policy is assigned.
System-based	Policy assignment rule	B	Allows Internet access from systems with the tag "IsLaptop."
System-based	Policy assignment rule	C	Allows unrestricted Internet access to all users in the Admin user group from all systems.

Policy type	Assignment type	Policy name	Policy settings
User-based	Policy assignment rule	C	Allows unrestricted Internet access to all users in the Admin user group from all systems.

Excluding Active Directory objects from aggregated policies

Rules that consist of multi-slot policies are applied to assigned systems without regard to priority. Because of this, you might need to prevent policy setting aggregation. You can do this by excluding a user (or other Active Directory objects such as a group or organizational unit) when creating the rule.

For more information on the multi-slot policies that can be used in policy assignment rules, see the product documentation for the managed product you are using.

User-based policy assignment

With user-based policy assignment rules, you can create user-specific policy assignments.

These assignments are enforced at the target system when a user logs on.

On a managed system, the agent keeps a record of the users who log on to the network. The policy assignments you create for each user are pushed down to the system they log on to, and are cached during each agent-server communication. The **Trellix ePO - On-prem** server applies the policies that you assigned to each user.

Note

To use user-based policy assignments, you must register and configure a registered LDAP server for use with your **Trellix ePO - On-prem** server.

System-based policy assignment

With system-based assignments, you can assign policies based on **System Tree** location or tags.

System-based policies are assigned based on selection criteria you define with the **Policy Assignment Builder**.

All policy assignment rules require that **System Tree** location is specified. Tag-based policiy assignments are useful when you want all systems of a particular type to have the same security policy, regardless of their **System Tree** location.

Scenario: Creating new SuperAgents using tags

You have decided to create a set of SuperAgents in your environment, but you don't have time to manually identify the systems in your **System Tree** to host these **SuperAgents**. Instead, you can use the **Tag Builder** to tag all systems that meet a specific set

of criteria with a new tag: "isSuperAgent." Once you build the tag, you can create a **Policy Assignment Rule** that applies your SuperAgent policy settings to every system tagged with "isSuperAgent."

Once the tag is created, you can assign the new policy. As each system with the new tag calls in at its regular interval, it is assigned a new policy based on your isSuperAgent **Policy Assignment Rule**.

Policy Assignment Rules page

Create, view, and manage policy assignment rules.

Option definitions

Option	Definition
Common actions	**New Assignment Rule** — Opens the **Policy Assignment Builder** wizard. Use this setting to create a policy assignment rule.
Filter actions	• **Show/Hide Filter Options** — Click to show or hide the filter options. • **Filter List By Product** — Filters the list of policy rules displayed by the product selected.

Actions	• **Edit Priority** — Allows you to change the priority of policy assignment rules. Setting the priority of rules affects the order in which they are applied. When a domain element (for example, a user) is assigned to more than one policy, the policy with the highest priority is applied before others. As a result, the first assignment might nullify settings in assignments with lower priorities. Use this page to edit the priority of Policy Assignment Rules that are enforced in your environment.
	  ▫ **Move to Top** — Moves the selected **Policy Assignment Rule** to the top of the Priority list.
	  ▫ **Assignments** — Displays the number of policies assigned in this **Policy Assignment Rule**.
	  ▫ **Name** — Displays the name of this **Policy Assignment Rule**. Drill down to view its summary.
	  ▫ **Priority** — Specifies the priority for this **Policy Assignment Rule**. Click and hold the drag-and-

Option	Definition
	drop handle to move the **Policy Assignment Rule** to a new priority level. The priority of rules affects the order in which they are applied. When a domain element (such as a user) is assigned to more than one policy, the policy with the highest priority is applied before others. As a result, the first assignment might nullify settings in assignments with lower priorities. • **Export** — Downloads or displays policy assignment rules in .xml format. • **Import** — Opens the **Import Policy Assignment Rules** dialog box. Use this setting to import previously exported policy assignment rules files.

Create and manage policies

Configure security policies

Custom policies that you can create from the **Policy Catalog** are not assigned to any groups or systems. You can create policies before or after a product is deployed.

Task

1. **Open the New Policy dialog box.**
    a. **Select Menu → Policy → Policy Catalog.**
    b. **Select the product in the left pane to display the corresponding categories in the right pane.**
    c. **Click New Policy.**
2. **Select a category from the drop-down list.**
3. **Select the policy you want to duplicate from the Create a policy based on this existing policy drop-down list.**
4. **Type a name for the new policy.**
5. **Enter a note that might be useful to track the changes for this policy, then click OK.**
6. **Click the name of the new policy to open the Policy Details pane .**
7. **Click the edit icon to edit the policy settings as needed.**
   For the detailed documentation about the policy settings, refer the corresponding product guide.
8. **Click Save.**

Results

The policy is added to the list on the **Policy Catalog** page.

Enforcing product policies

Policy enforcement is enabled by default, and is inherited in the **System Tree**, but you can manually enable or disable enforcement on specified systems.

You can manage policy enforcement from these locations:

- **Assigned Policies** tab of the **System Tree** — Choose whether to enforce policies for products or components on the selected group.
- **Policy Catalog** page — View policy assignments and enforcement. You can also lock policy enforcement to prevent changes below the locked node.

Important consideration: If policy enforcement is turned off, systems in the specified group don't receive updated site lists during an agent-server communication. As a result, managed systems in the group might not function as expected.

For example, you might configure managed systems to communicate with Agent Handler A. If policy enforcement is turned off, the managed systems do not receive the new site list with this information and the systems report to a different Agent Handler listed in an expired site list.

Enforce policies for a product in a System Tree group

The systems in a group, by default, inherit policies for a product from their parent group. Now, you can enforce changes to this default policy assignment on a product by using policy enforcement feature. You can also choose to lock policy inheritance to prevent any user from making changes to this assignment inadvertently.

Task

1. **Select Menu → Systems → System Tree, click Assigned Policies tab, then select a group in the System Tree.**
2. **Select the product you want, then click the link next to Enforcement Status.**
3. **To change the enforcement status, select Break inheritance and assign the policy and settings below.**
4. **Next to Enforcement status, select Enforcing or Not enforcing.**
5. **Choose whether to lock policy inheritance to prevent breaking enforcement for groups and systems that inherit this policy.**
6. **Click Save.**

Results

Now, you have enforced new policy settings on the selected product and locked the inheritance.

Enforce policies for a product on a system

The systems in a group, by default, inherit policies from their parent group. Now, you can enforce changes to this default policy assignment on a single managed system by using policy enforcement feature.

Task

1. **Select Menu → Systems → System Tree, click Systems tab, then select the group under System Tree where the system belongs.**
   The list of systems belonging to this group appears in the details pane.

2. **Select a system, then click Actions → Agent → Edit Policies on a Single System to open the Policy Assignment page.**
3. **Select a product, then click Enforcing next to Enforcement status.**
4. **Select Break inheritance and assign the policy and settings below.**
5. **Next to Enforcement status, select Enforcing or Not enforcing.**
6. **Click Save.**

Results

Now, the policy changes are enforced to the target system.

Managing policy history

When you change a policy, a **Policy History** entry is created where you can describe the change for future reference.

Policy History entries appear in three places: **Policy History**, **Server Task Log Details**, and **Audit Log Details**.

Only policies you create in the **Policy Catalog** have **Policy History** entries. Make sure that you leave a comment when you revise a policy. Consistent commenting provides a record of your changes.

If you have policy users configured to create and edit policies, the Status column options depend on user permissions. For example:

- **Trellix ePO - On-prem** administrators have full control of all policy history functions.
- Policy administrators can approve or reject changes submitted by policy users.
- Policy users can monitor the status of their policies. Status includes **Pending Review**, **Approved**, or **Declined**.

Manage policy history

You can view and compare policy history entries. You can also revert to a previous version of a policy if you feel the changes are not required anymore.

Before you begin

You must have appropriate permissions to revert to a previous policy version.

Task

1. **To view the Policy History, select Menu → Policy → Policy History.**

   Note

   No **Policy History** entries appear for **Trellix Default** policies. You might need to use the page filter to select a created or duplicated **Trellix Default** policy.

2. **Use the Product, Category, and Name filters to select Policy History entries.**
3. **To manage a policy or Policy History entry, click Actions, then select an action.**
   - **Choose Columns** — Opens a dialog box that allows you to select which columns to display.
   - **Compare Policy** — Opens the **Policy Comparison** page where you can compare two selected policies.

- **Export Table** — Opens the **Export** page where you can specify the package and format of **Policy History** entry files to export, then email the file.
- **Revert Policy** — Reverts the policy to the selected version. You can select only one target policy. When you revert a policy, you are prompted to add a comment to the **Policy History** entry.

Edit policy history permission sets

Configure the permission sets for your products so that users can revert policies to previous versions using the **Policy History** page.

Before you begin

You must have appropriate permissions to change permission sets.

Task

1. **Select Menu → User Management → Permission Sets.**
2. **In the right pane, click Edit in the Permission row for the product associated with the policy.**
3. **Click View and change policy and task settings, then click Save.**

Results

Now, you have provided the required permissions to revert existing policies for the selected product to their previous versions.

Compare policies

Compare and identify differences between similar policies.

Many of the values and variables included on the **Policy Comparison** page are specific to each product. For option definitions not included in the table, see the documentation for the product that provides the policy you want to compare.

Task

1. **Select Menu → Policy → Policy Comparison, then select a product, category, and Show settings from the lists.**

   Tip

   Best practice: To reduce the amount of data that is displayed, change the **Show** setting to **Policy Differences** or **Policy Matches**.

   These settings populate the policies to compare in the **Policy 1** and **Policy 2** lists.
2. **From the Policy 1 and Policy 2 column lists, select the policies to compare in the Compare policies row**
   The top two rows of the table display the number of settings that are different and identical.
3. **Click Print to open a printer friendly view of the comparison.**

Compare Policies page

You can compare like policies using this page. Many of the values and variables included on this page are specific to each product. For option definitions not included in the table, see the documentation for the product that provides the policy you want to compare.

Option definitions

Option	Definition
Show	Specify which details you want to compare: • **Show All Settings** • **Show Only Differences**
Product	Select from a list of installed products to compare policies.
Category	Specify a product-specific category to refine the list of available policies for comparison. **Note:** Not all products have multiple categories.
Settings	Specify settings and details about the policies being compared: • **Compare policies** — Use these menus to select which policies are compared. • **Settings that are different** — Specifies the number of differences between the compared policies. • **Settings that are identical** — Specifies the number of exact matches between the compared policies.
Policy Object Details	Specify details about the policies being compared, including: • **Assignment** — Specifies how many times this policy is assigned in your **System Tree**. **Note:** Assignments occur at the group level.

Option	Definition
	• **Owner** — Specifies the creator of this policy object.
Print	Use this option to open a printer friendly view of this comparison.

Change the owners of a policy

By default, ownership is assigned to the user who creates the policy. **If you have the required permissions, you can change the ownership of a policy.**

Task

1. **Select Menu → Policy → Policy Catalog, then select the product and category.**
   Expand the category to see all the policies for that category.
2. **Click the policy you want, then click the owner of the policy on the Policy Details pane.**
3. **Select the owners of the policy from the list, then click Save.**

Move and share policies between Trellix ePO - On-prem servers

In environments with multiple **Trellix ePO - On-prem** servers, you can move and share policies to avoid re-creating them on each server.

You can move and share policies only with equal or earlier major versions of **Trellix ePO - On-prem**. For example, you can share a policy created on a version 5.3 server with a 5.1 server; you can't share a policy from a 5.1 server to a 5.3 server.

Register servers for policy sharing

Register servers to share a policy.

Task

1. **Select Menu → Configuration → Registered Servers, then click New Server. The Registered Server Builder opens to the Description page.**
2. **From the Server type menu, select ePO, specify a name and any notes, then click Next. The Details page appears.**
3. **Specify any details for your server and click Enable in the Policy sharing field, then click Save.**

Designate policies for sharing

You can designate a policy for sharing among multiple **Trellix ePO - On-prem** servers.

Task

1. **Select Menu → Policy → Policy Catalog, then click Product menu and select the product whose policy you want to share.**
2. **In the Actions column for the policy to be shared, click Share.**

Results

Shared policies are automatically pushed to **Trellix ePO - On-prem** servers with policy sharing enabled. When you click **Share** in step 2, the policy is immediately pushed to all registered **Trellix ePO - On-prem** servers that have policy sharing enabled. Changes to shared policies are similarly pushed.

Schedule server tasks to share policies

The **Share Policies** server task ensures that any changes you make to shared policies are pushed to sharing-enabled **Trellix ePO - On-prem** servers.

If you set a long server task interval, or disable the **Share Policies** server task, we recommend manually running the task whenever you edit shared policies.

Task

1. **Open the Server Task Builder.**
    a. **Select Menu → Automation → Server Tasks.**
    b. **Click New Task.**
2. **On the Description page, specify the name of the task and any notes, then click Next.**
   New server tasks are enabled by default. If you do not want this task to be enabled, in the **Schedule status** field, select **Disabled**.
3. **From the Actions drop-down menu, select Share Policies, then click Next.**
4. **Specify the schedule for this task, then click Next.**
5. **Review the summary details, then click Save.**

Create and manage policy assignment rules

Create policy assignment rules

Creating policy assignment rules allows you to enforce policies for users or systems based on configured rule criteria.

Task

1. **Open the Policy Assignment Builder.**
    a. **Select Menu → Policy → Policy Assignment Rules.**
    b. **Click New Assignment Rule.**
2. **Specify the details for this policy assignment rule, including:**
    - A unique name and description.
    - The rule type you specify determines which criteria is available on the **Selection Criteria** page.

Note

By default, the priority for new policy assignment rules is assigned sequentially based on the number of existing rules. After creating the rule, you can edit the priority by clicking **Edit Priority** on the **Policy Assignment Rules** page.

3. **Click Next.**
4. **Click Add Policy to select the policies that you want to enforce with this policy assignment rule.**
5. **Click Next.**
6. **Specify the criteria you want to use in this rule. Your criteria selection determines which systems or users are assigned this policy.**
7. **Review the summary and click Save.**

Manage policy assignment rules

Perform common management tasks when working with policy assignment rules.

Task

1. **Select Menu → Policy → Policy Assignment Rules.**
2. **Perform one of these actions:**
    - **Edit a policy assignment rule** — Perform these steps:
        - Click the selected assignment. The **Policy Assignment Builder** opens.
        - Work through each page to change this policy assignment rule, then click **Save**.
    - **Delete a policy assignment rule** — Click **Delete** in the selected assignment row.
    - **Edit the priority of a policy assignment rule** — Perform these steps:
        - Select **Actions → Edit Priority** and the **Edit Priority** page opens.
        - Grab the handle and drag the row up or down in the list to change the priority, then click **Save**.
    - **View the summary of a policy assignment rule** — Click **>** in the selected assignment row. The row expands to display the summary information.

Policy approval management

You can assign different permission sets to different policy users, so that they can create and modify specific product policies. Some users can approve or deny changes from policies and policy assignments submitted by other users.

Policies can be managed by users with different permissions. As an administrator, you can create users with hierarchical levels of policy permissions. For example, you can create these policy users:

- Policy administrator — Approves policies and policy assignments created and modified by other users.
- Policy and Policy Assignment user — Duplicates and creates policies and modifies the policy assignment, that they submit to the policy administrator for approval before they are used.

Overview of creating policy users

1. In **Permission Sets**, create different permission sets for the policy administrator and policy user.
2. In **User Management**, create policy administrator and policy user, then manually assign them the different permission sets.

Policy user capabilities

- Duplicate, modify, or create policies and policy assignments and submit them to the policy administrator for approval.
- Monitor the approval status by the policy administrator.

Policy administrator capabilities

- All functions of the policy user.
- Approve or reject changes.

Comparing capabilities of a policy user vs. policy administrator

Capabilities	Policy user	Policy administrator
Duplicate, modify, or create policies and policy assignments and submit them for approval	×	×
Monitor the approval status	×	×
Approve or reject policies		×

Create policy and policy assignment permission sets

As an administrator, you can create permission sets for different policy user levels. The **Permission Sets** allow some policy users not only to create and modify policies and policy assignments, but also to approve or reject policies/ policy assignments created by other users.

Before you begin

You must have administrator rights to change **Permission Sets**.

To manage policy or policy assignment creation, you can create permission sets for users who can create and modify specific product policies. For example, you can create permission sets that allow one user to change policies and policy assignments and another user to approve or reject those changes.

- Policy User permission set — The policy user can create and modify specific product policies and policy assignments, but the policy changes must be approved before the policy or policy assignment is saved.
- Policy Administrator permission set — The policy administrator can create and modify specific product policies and policy assignments, and approve or reject the changes created by policy users and other administrators.

Task

1. **Select Menu → User Management → Permission Sets, then click New Permission Sets.**
2. **To create the policy administrator permission set, type the name, for example,** `policyAdminPS`**, then click Save.**
3. **Select the new permission set, scroll down to the Approval Management row, then click Edit.**
4. **Select Approver Permission for Policy Approval or Policy Assignment Approval setting , then click Save.**
   This option allows the policy administrator to approve or reject policy and policy assignment changes for other users who don't have administrator approval.
5. **Scroll down to a row, for example, the Endpoint Security Common, and click Edit.**

6. **Select View and change policy and task settings and click Save.**
   This option allows the policy administrator to make changes to **Endpoint Security Common** policies.
7. **Configure the edit permissions for different parameters as needed.**
8. **To create the policy user permission set, click Actions → Duplicate.**
   a. **Type a name for the policy user permission set, for example, policyUserPS and click OK.**
   b. **From the Permission Sets list, click the policyUserPS permission set.**
   c. **Scroll down to the Approval Management row and click Edit.**
   d. **Select No Permission for Policy Approval or Policy Assignment Approval setting , then click Save.**
      This setting forces the users assigned with this permission set to request approval from the administrator before they can save a new or changed policy or policy assignment.

Results

You have created two permission sets; one to assign to a policy user and one to assign to a policy administrator.

Create policy users

You can create different policy user levels with different permission sets that allow users to create and modify policies and policy assignments, and an administrator user to approve or reject policy changes.

Before you begin

You must have administrator rights to create users.

Task

1. **Open the User Management page: select Menu → User Management → Users.**
2. **Click New User.**
3. **Type a user name. For example, policyUser or policyAdmin.**
4. **Select Enable for the logon status of this account.**
5. **Select the authentication method for the new user.**
   - **Trellix ePO - On-prem** authentication
   - Windows authentication
   - Certificate-based authentication

   Note

   The **Trellix ePO - On-prem** authentication password is for one-time use only and must be changed during the next logon.

6. **Provide the required credentials or browse to select the certificate.**
7. **(Optional) Provide the user's full name, email address, phone number, and a description.**
8. **Select the policy user permission set you created, then click Save.**
   The new user or administrator appears in the **Users** list of the **User Management** page.

Results

You have two policy users: a policy user who can change policies and policy assignments and a policy administrator who can approve or reject those changes.

Configure approval settings for Policy and Policy Assignment Changes

You can choose whether policy users and administrators need approval to make policy and policy assignment changes. This prevents users from making inadvertent changes to any product policies or policy assignments.

Before you begin

You must have administrator rights.

Task

1. **Select Menu → Configuration → Server Settings.**
2. **Click Approvals on the Setting Categories pane.**
3. **Click Edit.**
    a. **Select Users needs approval for policy changes if policy users have to seek approval to make changes.**
    b. **Select Users needs approval for policy assignment changes if policy users have to seek approval to make changes.**
    c. **Select Administrator/ Approver needed approval for policy and policy assignment changes if the administrators and approvers also need to seek approval to make changes.**

Note

The **Administrator/ Approver needed approval for policy and policy assignment changes** option gets highlighted only when you select either option a or b. If you change these settings when a policy or policy assignment is submitted for review, it is rejected automatically.

When you select the option for administrator approval, the **Show Approvers** option pops up. When you click **Show Approvers**, the users who have the authority to approve policies and policy assignments is shown in the respective tables.

Submit policy and policy assignment changes for review

All users, including administrators and policy approvers, can create and change policies and policy assignment; but they might need to submit the policy and policy assignment for review by the administrator, or users with approval permissions, or a policy administrator.

Submit policy changes for review

Server Settings and user permission sets must be configured to allow users to submit policies for approval.

1. Create and maintain policies.

Note

Policy users only have access to policies and settings configured by the administrator in their assigned permission set.

2. To save the policy and send it to the administrator, click **Submit for Review**.
3. Check the policy approval status using one of these methods:
    - Select **Menu** → **Policy** → **Policy History**
    - Select **Pending Approvals** → **Policy Details** → **History**
4. Use the **Product**, **Category**, and **Name** filters to select **Policy History** entries to check.

The **Status** column displays one of these entries:

- **Review in progress** — Has not been reviewed
- **Rejected** — Has been rejected and not saved
- **Approved** — Has been approved and saved

Submit policy assignment changes for review

Server Settings and user permission sets must be configured to allow users to submit policy assignments for approval.

1. Select **Menu** → **System** → **System Tree** → **Assigned Policies** → **Select Product** → **Category** → **Edit Assignment**.
2. In the Edit Assignment page, do the following:
    a. If the policy is inherited, next to **Inherited from**, select **Break inheritance and assign the policy and settings below**.
    b. Select the policy from the **Assigned policy** drop-down list.

    Note

    From this location, you can also edit the selected policy's settings, or create a policy.

    c. Choose whether to lock policy inheritance. Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.
    d. Click **Save**.

    Note

    Policy assignment users will have access to System tree and policy assignments configured by the administrator in their assigned permission set.

3. To save the policy assignment and send it to the administrator, click **Submit for Review**.

Note

You must enter comments (mandatory) in the Comments text box.

4. Check the policy assignment approval status using the following method:

- Select **Menu** → **Policy** → **Policy Catalog** → **Pending Approvals** → **Pending Policy Assignment Approvals**.

5. Select the Policy Assignment entry to check the status.

The **Policy assignment details** column displays one of these entries:

- **Cancel Review** — To cancel the review
- **Approve** — To approve and save
- **Reject** — To reject and save

Note

The notification icon notifies if an action has been taken on the policy or policy assignment submitted for review.

Cancel policy and policy assignment review

If you are the user making changes and submitting a policy or policy assignment for review, you can withdraw the policy or policy assignment from review.

Before you begin

You must be the user who submitted the policy or policy assignment changes for review.

Task

1. **Select Menu → Policy → Policy Catalog.**
2. **Select Pending Approvals from the Products pane.**
3. **Select the policy or policy assignment for which you want to cancel review.**
4. **Click Cancel Review on the Policy Details pane.**
   For Policy Assignment Details the **Cancel Review** button is present in the **Policy assignment details** pane.
5. **Click Cancel on the pop-up dialog box that appears to confirm cancellation of review.**

Results

The policy and policy assignment changes that were submitted for review are cancelled. They are now removed from the **Pending Approvals** list.

Review policy and policy assignment changes

As a policy administrator, you need to periodically approve or reject policies and policy assignments submitted by non-admin users. You receive notifications when a non-admin user submits a policy or policy assignment for approval.

Before you begin

The **Server Settings** and user permission sets must be configured to allow users to submit policies and policy assignments for approval.

Task

1. **To change the status of the policy or policy assignment submitted for review, select Menu → Policy → Policy Catalog.**
2. **Select Pending Approvals from the Products pane and select the policy or policy assignment you want to review.**

3. **View all proposed changes on the Policy Details or, Policy Assignment Details pane.**
4. **Click Approve or Reject.**
   A pop-up dialog box appears to confirm your decision. You can enter comments in the **Comments** text box.

Results

If you approve the changes, the policy or policy assignment is saved; otherwise the changes are not saved.

Configure email notifications using Automatic Response

You can set up an automatic response to receive email notifications when a policy is submitted for approval, or when a policy submitted for approval is approved or rejected.

Before you begin

Your email server must be configured and registered.

Task

1. **Select Menu → Automation → Automatic Responses.**
2. **Click New Response.**
3. **Enter a name for the new response and provide a description about this automatic response.**
4. **Select ePO Approval Events in the Event group drop-down list.**
5. **Select Policy Approval in the Event type drop-down list.**
6. **Click Next to set filters to define when to trigger an email notification.**
7. **Click Next to set aggregation.**
8. **Click Next and select Send emails in the Actions drop-down list.**

   Note

   You receive a warning message stating that the email server is not configured if you have not registered and configured your email server.

9. **Enter details for the email to be triggered as an automatic response and click Next.**
10. **Verify the settings of the automatic response on the Summary tab and click Save.**

Results

Now, you receive an automatic email notification when a policy is submitted for approval and if the policy is approved or rejected.

Assign policies to managed systems

Assign policies to a group or to specific systems in the System Tree. You can assign policies before or after a product is deployed.

We recommend assigning policies at the highest level possible so that the groups and subgroups below inherit the policy.

Assign a policy to a System Tree group

Assign a policy to a specific group of the **System Tree**.

Task

1. **Select Menu → Systems → System Tree, click Assigned Policies tab, then select a product.**
   Each assigned policy per category appears in the details pane.
2. **Locate the policy category you want, then click Edit Assignment.**
3. **If the policy is inherited, next to Inherited from, select Break inheritance and assign the policy and settings below.**
4. **Select the policy from the Assigned policy drop-down list.**

   Note

   From this location, you can also edit the selected policy's settings, or create a policy.

5. **Choose whether to lock policy inheritance.**
   Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.
6. **A pop-up dialog box appears to confirm your decision. You can enter comments (mandatory) in the Comments text box.**
   The comment box is applicable when you select approval for policy assignment changes.
7. **Click Save.**
   The **Submit for Review** button is displayed if Policy Assignment Approval option is enabled in Server Settings.
   The **Edit Assignment** option is grayed out and displays **Pending Approval** if a policy assignment is under review.

Assign a policy to a managed system

Assign a policy to a specific managed system.

Task

1. **Select Menu → Systems → System Tree, click Systems tab, then select a group under System Tree.**
   All systems within this group (but not its subgroups) appear in the details pane.
2. **Select a system, then click Actions → Agent → Modify Policies on a Single System.**
   The **Policy Assignment** page for that system appears.
3. **Select a product.**
   The categories of selected product are listed with the system's assigned policy.
4. **Locate the policy category you want, then click Edit Assignments.**
5. **If the policy is inherited, next to Inherited from, select Break inheritance and assign the policy and settings below.**
6. **Select the policy from the Assigned policy drop-down list.**

   Note

   From this location, you can also edit settings of the selected policy, or create a policy.

7. **Choose whether to lock policy inheritance.**

Locking policy inheritance prevents any system that inherits this policy, from having another one assigned in its place.

8. **A pop-up dialog box appears to confirm your decision. You can enter comments (mandatory) in the Comments text box.**
   The comment box is applicable when you select approval for policy assignment changes.
9. **Click Save.**
   The **Submit for Review** button is displayed if Policy Assignment Approval option is enabled in Server Settings.
   The **Edit Assignment** option is grayed out and displays **Pending Approval** if a policy assignment is under review.

Policy Assignment page

Use this page to view and change the assignment of configuration policies to the selected system. The page header lists the name of the system where the information is being displayed.

Option definitions

Option	Definition
Product	Specifies the product whose policies you want to list.
Enforcement Status	Displays the enforcement status for the currently selected group or system whose policies you want to change. Clicking the status value opens the **Enforcement** page for that group or system.
Policy Assignment Table	Displays the policies for this server from the selected product. Columns that can be displayed are: • **Category** — Specifies the policy categories for the product you selected. • **Policy** — Specifies the policy, in each category, that is assigned to the user. • **Server** — Specifies the server the policy is from. • **Inherit From** — Displays from where the policies were inherited. • **Broken Inheritance** — Displays "None" if the policy inheritance has not been broken. • **Actions** — Click **Edit Assignment(s)** to open the **Policy Assignments** page. Use this setting to select a new policy to assign and configure inheritance.
Actions	Specifies actions you can take on the displayed policy assignments. Options are:

Option	Definition
	• **Choose Columns** — Select to choose which columns you want displayed in the policy assignment table. • **Copy Assignments** — Displays the **Copy Policy Assignment** page, allowing you to choose which policy assignments for this system are copied. You are then directed to choose a system on which to paste the assignments. • **Export All Assignments** — Exports all displayed assignments to an XML file. • **Export Table** — Displays the **Export** page allowing you to choose the way the table is exported. • **Import Assignments** — Imports previously exported policy assignments. • **Paste Assignments** — Pastes recently copied assignments to the selected system.

Assign a policy to systems in a System Tree group

Assign a policy to multiple managed systems within a group.

Task

1. **Select Menu → Systems → System Tree, click Systems tab, then select a group in the System Tree.**
   All systems in this group (but not its subgroups) appear in the details pane.
2. **Select the systems you want, then click Actions → Agent → Set Policy & Inheritance.**
   The **Assign Policy** page appears.
3. **Select the Product, Category, and Policy from the drop-down lists.**
4. **Select whether to Reset inheritance or Break inheritance, then click Save.**

Copy and paste policy assignments

Copy policy assignments from a group

You can use **Copy Assignments** to copy policy assignments from a group in the **System Tree**.

Task

1. **Select Menu → Systems → System Tree, click Assigned Policies tab, then select a group in the System Tree.**
2. **Click Actions → Copy Assignments.**
3. **Select the products or features where you want to copy policy assignments, then click OK.**

Copy policy assignments from a system

You can use **Copy Assignments** to copy policy assignments from a specific system.

Task

1. **Select Menu → Systems → System Tree, click Systems tab, then select a group in the System Tree.**
   The systems belonging to the selected group appear in the details pane.
2. **Select a system, then click Actions → Agent → Modify Policies on a Single System.**
3. **Click Actions → Copy Assignments, select the products or features where you want to copy policy assignments, then click OK.**

Paste policy assignments to a group

You can paste policy assignments to a group after you copy them from a group or system.

Task

1. **Select Menu → Systems → System Tree, click Assigned Policies tab, then select the group you want in the System Tree.**
2. **In the details pane, click Actions and select Paste Assignments.**
   If the group already has policies assigned for some categories, the **Override Policy Assignments** page appears.

   Note

   When pasting policy assignments, the **Enforce Policies and Tasks** policy appears in the list. This policy controls the enforcement status of other policies.

3. **Select the policy categories you want to replace with the copied policies, then click OK.**

Paste policy assignments to a specific system

Paste policy assignments to a specific system after copy the policy assignments from a group or system.

Task

1. **Select Menu → Systems → System Tree, click Systems tab, then select a group in the System Tree.**
   All systems belonging to the selected group appear in the details pane.
2. **Select the system where you want to paste policy assignments, then click Actions → Agent → Modify Policies on a Single System.**
3. **In the details pane, click Actions → Paste Assignment.**
   If the system already has policies assigned for some categories, the **Override Policy Assignments** page appears.

   Note

   When pasting policy assignments, the **Enforce Policies and Tasks** policy appears in the list. This policy controls the enforcement status of other policies.

4. **Confirm the replacement of assignments.**

View policy information

View groups and systems where a policy is assigned

View the **Policy Catalog** Assignment page to see the group, or system that inherits the policy.

Note

The parent **Policy Catalog** page lists the number of policy assignments. It does not list the group or system that inherits the policy.

For example, if you view the **Trellix Agent** product in the Product Catalog you can view the default assignments for each policy. For the **Trellix** Default policy, the General category is assigned to the Global Root node and Group node type.

Task

1. **Select Menu → Policy → Policy Catalog, then select a product and category.**
   All created policies for the selected category appear in the details pane.
2. **Under Assignments for the row of the policy, click the link.**
   The link indicates the number of groups or systems the policy is assigned to (for example, **6 assignments**).

Results

On the **Assignments** page, each group or system where the policy is assigned appears with its node name and node type.

View policy settings

View details for a policy assigned to a product category or system.

The policy assigned to a System Tree group or system can tell you, for example, the policy enforcement interval, the priority event forwarding interval, or if peer-to-peer communication is enabled.

Task

1. **Select Menu → Policy → Policy Catalog, then select a product and category.**
   All created policies for the selected category appear in the details pane.
2. **Click the policy name link.**
   The policy pages and their settings appear.

Note

You can also view this information when accessing the assigned policies of a specific group. To access this information, select **Menu → Systems → System Tree**, click **Assigned Policies** tab, then click the link for the selected policy in the **Policy** column.

View policy ownership

View the owners of a policy.

Task

1. **Select Menu → Policy → Policy Catalog, then select a product and category.**
   All created policies for the selected category appear in the details pane.
2. **The owners of the policy are displayed under Owner.**

View assignments where policy enforcement is disabled

View assignments where policy enforcement, per policy category, is disabled.

Normally you want policy enforcement enabled. Use this task to find any policies that are not being enforced and change their configuration.

Task

1. **Select Menu → Policy → Policy Assignments**
   The **Assigned Policies** tab opens on the **System Tree** page.
2. **Click the link next to Enforcement status, which indicates the number of assignments where enforcement is disabled, if any.**
   The **Enforcement for <policy name>** page appears.
3. **Select Enforcing for the Enforcement Status to enforce a policy for the selected product.**

View policies assigned to a group

View the policies assigned to a **System Tree** group, sorted by product.

For example, if you have different policies assigned to servers and workstation groups, use this task to confirm the policies are set correctly.

Task

1. **Select Menu → Systems → System Tree, click Assigned Policies tab, then select a group in the System Tree.**
   All assigned policies, organized by product, appear in the details pane.
2. **Click any policy link to view its settings.**

View policies assigned to a specific system

View a list of all policies assigned to a system from one central location, the **System Tree**.

For example, if you have different policies assigned to specific systems, use this task to confirm the policies are set correctly.

Task

1. **Select Menu → Systems → System Tree, click the Systems tab, then select a group in the System Tree.**
   All systems belonging to the group appear in the details pane.
2. **Click the name of a system to drill into the System Information page, then click the Applied Policies tab.**

View policy inheritance for a group

View the policy inheritance of a specific group.

For example, if you have policy inheritance configured for different groups, use this task to confirm the policy inheritance is set correctly.

Task

1. **Select Menu → Systems → System Tree.**
2. **Click Assigned Policies tab.**
   All assigned policies, organized by product, appear in the details pane.

Results

The policy row, under **Inherit from**, displays the name of the group from which the policy is inherited.

View and reset broken inheritance

Identify the groups and systems where policy inheritance is broken.

For example, if you have policies with broken inheritance configured for some groups, use this task to confirm the policies are set correctly.

Task

1. **Select Menu → Systems → System Tree, then click Assigned Policies tab.**
   All assigned policies, organized by product, appear in the details pane. The policy row, under **Broken Inheritance**, displays the number of groups and systems where this policy's inheritance is broken.

   Note

   This number is the number of groups or systems where the policy inheritance is broken, not the number of systems that do not inherit the policy. For example, if only one group does not inherit the policy, **1 doesn't inherit** appears, regardless of the number of systems within the group.

2. **Click the link indicating the number of child groups or systems that have broken inheritance.**
   The **View broken inheritance** page displays a list of the names of these groups and systems.

   #### Option definitions

Option	Definition
Assigned Policy	Specifies the name of the policy that is assigned.
Node Name	Specifies the **System Tree** path to the group or system that is not inheriting the policy.

Option	Definition
Node Type	Specifies whether the node is a group or system.
Policy Owner	Specifies the name of the policy owner. Only policy owners and global administrators can edit a policy setting.
Reset Inheritance	Forces the system or group to inherit the policy again.

3. **To reset the inheritance of any of these, select the checkbox next to the name, then click Actions and select Reset Inheritance.**

Create policy management queries

Retrieve the policies assigned to a managed system, or policies broken in the system hierarchy.

You can create either of the following **Policy Management** queries:

- **Applied Policies** — Retrieves policies assigned to a specified managed system.
- **Broken Inheritance** — Retrieves information on policies that are broken in the system hierarchy.

Task

1. **Select Menu → Reporting → Queries & Reports, then click New Query.**
   The **Query Builder** opens.
2. **On the Result Type page, select Policy Management from the Feature Group list.**
3. **Select a Result Type, then click Next to display the Chart page:**
   - **Applied Client Tasks**
   - **Applied Policies**
   - **Client Tasks Assignment Broken Inheritance**
   - **Policies Assignment Broken Inheritance**
4. **Select the type of chart or table to display the primary results of the query, then click Next.**
   The **Columns** page appears.

   Note

   If you select **Boolean Pie Chart**, configure the criteria that you want to include in the query.

5. **Select the columns to be included in the query, then click Next.**
   The **Filter** page appears.

6. **Select properties to narrow the search results, then click Run.**
   The **Unsaved Query** page displays the results of the query, which is actionable.

   Note

   Selected properties appear in the content pane with operators that can specify criteria, which narrows the data that is returned for that property.

7. **On the Unsaved Query page, take any available action on items in any table or drill-down table.**
   - If the query didn't return the expected results, click **Edit Query** to go back to the **Query Builder** and edit the details of this query.
   - If you don't want to save the query, click **Close**.
   - To use this query again, click **Save** and continue to the next step.
8. **In the Save Query page, enter a name for the query, add any notes, and select one of the following:**
   - **New Group** — Enter the new group name and select either:
     - **Private group (My Groups)**
     - **Public group (Shared Groups)**
   - **Existing Group** — Select the group from the list of **Shared Groups**.
9. **Click Save.**

Server and client tasks

Use server and client tasks to automate **Trellix ePO - On-prem** and managed system processes.

Trellix ePO - On-prem includes preconfigured server tasks and actions. Most of the additional software products you manage with **Trellix ePO - On-prem** also add preconfigured server and client tasks.

Server tasks

Server tasks are configurable actions that run on **Trellix ePO - On-prem** at scheduled times or intervals. Leverage server tasks to automate repetitive tasks.

Trellix ePO - On-prem includes preconfigured server tasks and actions. Most of the additional software products you manage with **Trellix ePO - On-prem** also add preconfigured server tasks.

View server tasks

The **Server Task Log** provides the status of your server tasks and displays any error that might have occurred.

Task

1. **Open Server Task Log: select Menu → Automation → Server Task Log**
2. **Sort and filter the table to focus on relevant entries.**
    - To change which columns are displayed, from the **Actions** menu, click **Choose Columns.**
    - To order table entries, click a column title.
    - To show or hide entries, select a filter option.
3. **To view additional details, click an entry.**

Server task status

The status of each server task appears in the **Status** column of the **Server Task Log**.

Status	Definition
Waiting	The server task is waiting for another task to finish.
In Progress	The server task has started, but not finished.
Paused	A user paused the server task.
Stopped	A user stopped the server task.

Status	Definition
Failed	The server task started, but did not finish successfully.
Completed	The server task finished successfully.
Pending Termination	A user requested that the server task end.
Ended	A user closed the server task manually before it finished.

Create a server task

Create server tasks to schedule various actions to run on a specified schedule.

If you want **Trellix ePO - On-prem** to run certain actions without manual intervention, a server task is the best approach.

Task

1. **Open the Server Task Builder.**
    a. **Select Menu → Automation → Server Tasks.**
    b. **Click New Task.**
2. **Give the task an appropriate name, and decide whether the task has a Schedule status, then click Next.**

    Tip

    If you want the task to run automatically, set **Schedule status** to **Enabled**.

3. **Select and configure the action for the task, then click Next.**
4. **Choose the schedule type (the frequency), start date, end date, and schedule time to run the task, then click Next.**

    Note

    The schedule information is used only if you enable **Schedule status**.

5. **Click Save to save the server task.**

Results

The new task appears in the **Server Tasks** list.

Remove outdated server tasks from the Server Task Log: best practice

Periodically remove old server task entries from the **Server Task Log** to improve database performance.

Important

Items removed from the **Server Task Log** are deleted permanently.

Task

1. **Open the Server Task Log: select Menu → Automation → Server Task Log.**
2. **Click Purge.**
3. **In the Purge dialog box, enter a number, then select a time unit.**
4. **Click OK.**

Results

Any items of the specified age or older are deleted, including items not in the current view. The number of removed items is displayed in the lower right corner of the page.

Tip

Create a server task to automatically remove outdated items.

Remove outdated log items automatically

Use a server task to automatically remove old entries from a table or log, such as closed issues or outdated user action entries.

Important

Items removed from a log are deleted permanently.

Task

1. **Open the Server Task Builder.**
   a. **Select Menu → Automation → Server Tasks.**
   b. **Click New Task.**
2. **Type a name and description for the server task.**
3. **Enable or disable the schedule for the server task, then click Next.**
   The server task does not run until it is enabled.
4. **From the drop-down list, select a purge action, such as Purge Server Task Log.**
5. **Next to Purge records older than, enter a number, then select a time unit, then click Next.**
6. **Schedule the server task, then click Next.**
7. **Review the details of the server task.**
   - To make changes, click **Back**.
   - If everything is correct, click **Save**.

Results

The new server task appears on the **Server Tasks** page. Outdated items are removed from the specified table or log when the scheduled task runs.

Accepted Cron syntax when scheduling a server task

If you select the **Schedule type** → **Advanced** option when scheduling a server task, you can specify a schedule using Cron syntax.

Cron syntax is made up of six or seven fields, separated by a space. Accepted Cron syntax, by field in descending order, is detailed in the following table. Most Cron syntax is acceptable, but a few cases are not supported. For example, you cannot specify both the Day of Week and Day of Month values.

Field name	Allowed values	Allowed special characters
Seconds	0–59	, - * /
Minutes	0–59	, - * /
Hours	0–23	, - * /
Day of Month	1–31	, - * ? / L W C
Month	1–12, or JAN - DEC	, - * /
Day of Week	1–7, or SUN - SAT	, - * ? / L C #
Year (optional)	Empty, or 1970–2099	, - * /

Allowed special characters

- Commas (,) are allowed to specify more values. For example, "`5,10,30`" or "`MON,WED,FRI`".
- Asterisks (*) are used for "every." For example, "`*`" in the minutes field is "every minute".
- Question marks (?) are allowed to specify no specific value in the Day of Week or Day of Month fields.

  Note

  The question mark must be used in one of these fields, but cannot be used in both.

- Forward slashes (/) identify increments. For example, "`5/15`" in the minutes field means the task runs at minutes 5, 20, 35 and 50.

- The letter "L" means "last" in the Day of Week or Day of Month fields. For example, "`0 15 10 ? * 6L`" means the last Friday of every month at 10:15 am.
- The letter "W" means "weekday". So, if you created a Day of Month as "`15W`", this means the weekday closest to the 15th of the month. Also, you can specify "`LW`", which means the last weekday of the month.
- The pound character "#" identifies the "Nth" day of the month. For example, using "`6#3`" in the Day of Week field is the third Friday of every month, "`2#1`" is the first Monday, and "`4#5`" is the fifth Wednesday.

Note

If the month does not have a fifth Wednesday, the task does not run.

Client tasks

Create and schedule client tasks to automate endpoint tasks in your network.

Tip

For information about which client tasks are available and what they can do to help you, see the documentation for your managed products.

Client task example

When you initially start **Trellix ePO - On-prem**, some preconfigured client tasks are automatically installed to help manage your **Trellix** products. These client tasks provide basic security for most users, and run by default.

Client tasks are configured to run using different criteria. For example, some client tasks run:

- Continuously — These client tasks automatically scan programs and files for threats as they occur.
- At configured events — These client tasks run at agent-server communication interval (ASCI) or policy enforcement interval.
- On schedule — These client tasks run at a time configured in the product deployment or policy.

This preconfigured client task, named **Initial Deployment Update My Group**, deploys the **Trellix** software on your managed systems.

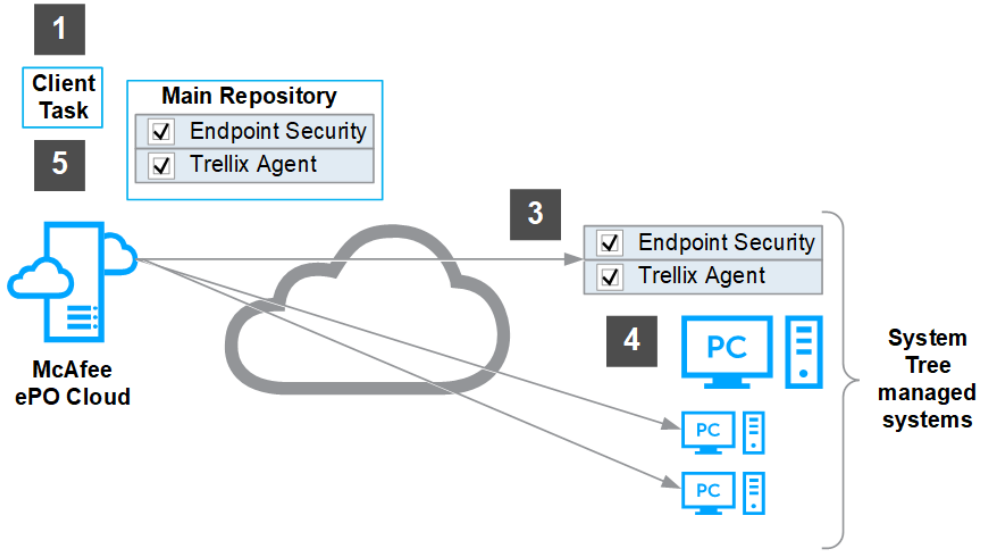
Note

This client task runs continuously to keep the **Trellix** software on all your systems up to date.

This graphic describes how the "Initial Deployment Update My Group" client task works.

1. The client task starts when you run the Smart Installer URL on a system.
2. The client task looks at the list of software saved in the Main Repository and, using a Product Deployment named "Initial Deployment My Group," automatically starts downloading the software to all your managed systems.

3. Once the software is installed, it is run periodically using other client task requests sent from **Trellix ePO - On-prem** to protect your systems.
4. By default, every 60 minutes at the agent-server communication interval (ASCI), the latest versions of all software installed on your managed systems are sent to the **Trellix ePO - On-prem**.
5. The client task continuously compares the software versions installed in the Main Repository to the list of software versions installed on your managed systems. If a more recent version of software exists in the Main Repository, that software is automatically downloaded using Product Deployment to your managed systems.



How the Client Task Catalog works

Use the **Client Task Catalog** to create client task objects you can reuse to help manage systems in your network.

The **Client Tasks Catalog** applies the concept of logical objects to **Trellix ePO - On-prem** client tasks. You can create client task objects for various purposes without the need to assign them immediately. As a result, you can treat these objects as reusable components when assigning and scheduling client tasks.

You create client task assignments to:

- Link System Tree groups or tagged systems to a client task.
- Schedule the client task to run.
- Set stop tasks, randomization, and rerun delays for the client task.

Client tasks can be assigned at any level in the **System Tree**. Groups and systems lower in the tree inherit client tasks. As with policies and policy assignments, you can break the inheritance for an assigned client task.

Client task objects can be shared across multiple registered **Trellix ePO - On-prem** servers in your environment. When client task objects are set to be shared, each registered server receives a copy after your **Share Client Task** server task runs. Any changes made to the task are updated each time it runs. When a client task object is shared, only the owner of the object can modify its settings.

Note

Administrators on the target server that receives a shared task is not an owner for that shared task. None of the users on the target server is owner for any shared task objects the target receives.

Deployment tasks

Deployment tasks are client tasks that are used to deploy managed security products to your managed systems from the **Main Repository**.

You can create and manage individual deployment task objects using the **Client Task Catalog**, then assign them to run on groups or individual system. Alternatively, you can create Product Deployment projects to deploy products to your systems. Product Deployment projects automate the process of creating and scheduling client task objects individually. They also provide additional automated management functionality.

Important considerations

When deciding how to stage your Product Deployment, consider:

- Package size and available bandwidth between the **Main Repository** and managed systems. **In addition to potentially overwhelming the Trellix ePO - On-prem server or your network, deploying products to many systems can make troubleshooting problems more complicated.**
- A phased rollout to install products to groups of systems at a time. If your network links are fast, try deploying to several hundred clients at a time. If you have slower or less reliable network connections, try smaller groups. As you deploy to each group, monitor the deployment, run reports to confirm successful installations, and troubleshoot any problems with individual systems.

Deploying products on selected systems

If you are deploying **Trellix** products or components that are installed on a subset of your managed systems:

1. Use a tag to identify these systems.
2. Move the tagged systems to a group.
3. Configure a Product Deployment client task for the group.

Deployment packages for products and updates

The **Trellix ePO - On-prem** software deployment infrastructure supports deploying products and components, as well as updating both.

Each product that **Trellix ePO - On-prem** can deploy provides a product deployment package .zip file. The .zip file contains product installation files, which are compressed in a secure format. **Trellix ePO - On-prem** can deploy these packages to any of your managed systems.

The software uses these .zip files for both detection definition (DAT) and engine update packages.

You can configure product policy settings before or after deployment. We recommend configuring policy settings before deploying the product to network systems. Configuring policy settings saves time and ensures that your systems are protected as soon as possible.

These package types can be checked in to the **Main Repository** with pull tasks, or manually.

Supported package types

Package type	Description	Origination
SuperDAT files (SDAT.exe) files File type: SDAT.exe	The SuperDAT files contain both DAT and engine files in a single update package. If bandwidth is a concern, we recommend updating DAT and engine files separately.	**Trellix** website. Download and check SuperDAT files into the **Main Repository** manually.
Supplemental detection definition (Extra.DAT) files File type: Extra.DAT	The Extra.DAT files address one or more specific threats that have appeared since the last DAT file was posted. If the threat has a high severity, distribute the Extra.DAT files immediately, rather than wait until the signature is added to the next DAT file. Extra.DAT files are from the **Trellix** website. You can distribute them through **Trellix ePO - On-prem**. Pull tasks do not retrieve Extra.DAT files.	**Trellix** website. Download and check supplemental DAT files in to the **Main Repository** manually.
Product deployment and update packages File type: zip	A product deployment package contains installation software.	Product CD or downloaded product .zip file. Check product deployment packages into the **Main Repository** manually. For specific locations, see the documentation for that product.
Trellix Agent language packages File type: zip	A **Trellix Agent** language package contains files necessary to	**Main Repository** — Checked in at installation. For future versions of the **Trellix Agent**,

Package type	Description	Origination
	display **Trellix Agent** information in a local language.	you must check **Trellix Agent** language packages into the **Main Repository** manually.

Package signing and security

All packages created and distributed by **Trellix** are signed with a key pair using the DSA (Digital Signature Algorithm) signature verification system. The packages are encrypted using 168-bit 3DES encryption. A key is used to encrypt or decrypt sensitive data.

You are notified when you check in packages that **Trellix** has not signed. If you are confident of the content and validity of the package, continue with the check-in process. These packages are secured in the same manner previously described, but **Trellix ePO - On-prem** signs them when they are checked in.

The **Trellix Agent** only trusts package files signed by **Trellix ePO - On-prem** or **Trellix**. This feature protects your network from receiving packages from unsigned or untrusted sources.

Package ordering and dependencies

If one product update depends on another update, check in the update packages to the **Main Repository** in the required order. For example, if Patch 2 requires Patch 1, you must check in Patch 1 before Patch 2. Packages cannot be reordered once they are checked in. You must remove them and check them in again, in the proper order. If you check in a package that supersedes an existing package, the existing package is removed automatically.

Product and update deployment

The **Trellix ePO - On-prem** repository infrastructure allows you to deploy product and update packages to your managed systems from a central location. Although the same repository is used, there are differences.

Product deployment vs. update packages

Product deployment packages	Update packages
Must be manually checked in to the **Main Repository**.	DAT and Engine update packages can be copied from the source site automatically with a pull task. All other update packages must be checked in to the **Main Repository** manually.
Can be replicated to the **Main Repository** and installed automatically on managed systems using a deployment task.	Can be replicated to the **Main Repository** and installed automatically on managed systems with global updating.

Product deployment packages	Update packages
If not implementing global updating for product deployment, a deployment task must be configured and scheduled for managed systems to retrieve the package.	If not implementing global updating for product updating, an update client task must be configured and scheduled for managed systems to retrieve the package.

Product deployment and updating process

Follow this high-level process for distributing DAT and Engine update packages.

1. Check in the update package to the **Main Repository** with a pull task, or manually.
2. Do one of the following:
    - If you are using global updating, create and schedule an update task for laptop systems that leave the network.
    - If you are not using global updating, perform the following tasks.
        - Use a replication task to copy the contents of the **Main Repository**.
        - Create and schedule an update task for agents to retrieve and install the update on managed systems.

Deployment tags

When a deployment task is created, a tag with the task name is automatically created and applied to the systems on which the task is enforced. These tags are only created for a fixed deployment. Does not apply to continuous deployment.

These tags are added to the **Deployment Tags** group on the **Tag Catalog** page every time a deployment task is created and enforced to systems. This group is a read-only group, and tags in this group can't be manually applied, changed, deleted, or used in a criteria configuration to filter systems.

Client task approvals

Create client task users

You can create different task user levels with different permission sets that allow users to create and modify tasks, and allows an administrator to approve or decline task changes.

Before you begin

You must have administrator rights to create users.

Task

1. **Open the User Management page: select Menu → User Management → Users.**
2. **Click New User.**
3. **Type a user name. For example,** `taskUser` **or** `taskAdmin`**.**
4. **Select Enable for the logon status of this account.**
5. **Select whether the new account uses Trellix ePO - On-prem authentication, Windows authentication, or certificate-based authentication, and provide the required credentials or browse and select the certificate.**

Note

The **Trellix ePO - On-prem** authentication password is for one-time use only and must be changed during the next logon.

6. **(Optional) Provide the user's full name, email address, phone number, and a description.**
7. **Select the task user permission set you created, then click Save.**
   The new user or administrator appears in the **Users** list of the **User Management** page.

Results

You have two task users. A task user who can change tasks and a task administrator who can approve or decline those changes.

Create client task permission sets

As an administrator, you can create permission sets for different user levels. Based on the permission sets users can either create and modify client tasks, or approve or reject tasks created by other users.

Before you begin

You must have administrator rights to change permission sets.

To manage task creation, you can create permission sets for users who can create and modify specific tasks. For example, you can create permission sets that allow one user to change tasks and another user permission to approve or reject those changes.

- **Task User permission set** — The task user can create and modify specific product tasks, but the changes must be approved before the task is saved.
- **Task Administrator permission set** — The task administrator can create and modify specific tasks, and approve or reject the changes made by task users, and other administrators.

Task

1. **Select Menu → User Management → Permission Sets, then click New Permission Sets.**
2. **To create the task administrator permission set, type the name, for example, `taskAdminPS`, then click Save.**
   a. **Select the taskAdminPS permission set, scroll down to the Client Task Management row, then click Edit.**
   b. **Select Can approve or decline the task changes submitted by other users, and click Save.**
      This allows the task administrator to respond to others' task changes without administrator approval.
   c. **Scroll down to a parameter that you want to edit, for example, the Endpoint Security Common, and click Edit.**
   d. **Select View and change policy and task settings and click Save.**
      This allows the task administrator user to make task changes to **Endpoint Security Common** tasks.
   e. **Configure the edit permissions for different parameters as needed.**
3. **To duplicate the task administrator permission set and create the policy user permission set, click Actions → Duplicate.**
   a. **Type the name of the task user permission set, for example, `taskUserPS` and click OK.**
      A duplicate task administrator permission set is created.
   b. **From the Permission Sets list, click the taskUserPS permission set.**
   c. **Scroll down to the Client Task Management row and click Edit.**
   d. **Select No Permissions for Task Approval, and click Save.**

This setting forces the users assigned with this permission set to request approval from the administrator before they can save a new or changed policy.

Results

Now, you have created two permission sets; one to assign to a task user and another one to assign to a task administrator.

Configure approval settings for Task changes

You can choose whether a user needs approval to make client task changes.

Before you begin

You must have administrator rights.

Task

1. **Select Menu → Configuration → Server Settings.**
2. **Click Approvals on the Setting Categories pane.**
3. **Click Edit.**
   a. **Select Users need approval for client task changes if task users have to seek approval to make changes.**
   b. **Select Administrators and Approvers need approval for client task changes if the administrators and approvers also need to seek approval to make changes.**

Note

If you change these settings when a client task is submitted for review, it is rejected automatically.

Submit task changes for review

All users, including administrators and approvers, can create and change tasks. However, if configured by the administrator, it must be reviewed by the administrator or a user with approval permissions. Only tasks that are approved are available for task assignment.

Before you begin

The **Server Settings** and user permission sets must be configured to allow users to submit client tasks for approval.

Task

1. **Create client tasks.**

Note

Users only have access to tasks that are configured by the administrator in their assigned permission set.

2. **To save the task, click Submit for Review.**
3. **A pop-up dialog box appears to confirm your submission and you must enter comments about the changes (existing task) or the purpose (new task).**

This sends the task to the administrator to approve or reject.

4. **To check the approval status, select Menu → Client Task Catalog.**
   a. **Select Pending Approvals in the Client Task Types pane.**
   b. **Click the task in the Pending Approvals pane.**
      The latest 10 actions on the task are displayed on the **Task Details** pane.
   c. **Click View Full Task History to see the status of the task on the Comment History page.**
   d. **Use the Product, Category, and Name filters to select Task History entries to check.**
   e. **The Status column displays one of these entries:**
      - **Submit for review** — Has not been reviewed
      - **Rejected** — Has been rejected and not saved
      - **Approved** — Has been approved and saved

Note

The notification icon indicates if an action was taken on the task submitted for review. If you have configured an automatic response, you also receive an email notification.

Cancel or update a client task review

You can update or cancel a task that you have submitted for review.

Warning

You must be the user who submitted the client task for review.

Task

1. **Select Menu → Client Task Catalog.**
2. **Select Pending Approvals from the Client Task Types pane.**
3. **Select the task review that you want to cancel or update and submit again.**
4. **Click Cancel Review on the Task Details pane or click Update Review to edit the task and submit again for approval. Alternately, you can click Review on the Pending Approvals pane and click Cancel Review or Update Review.**
5. **Enter comments and click OK on the pop-up dialog box that appears.**

Results

This action deletes the task if it is a new task that was not saved earlier.

Review client task changes

As an administrator or approver, you need to periodically approve or reject requests submitted by users and other administrators or approvers. You receive notifications when a user submits a task for approval.

Before you begin

Server Settings and user permission sets must be configured to allow users to submit tasks for approval.

Task

1. **To change the status of the task submitted for review, select Menu → Client Task Catalog.**
2. **Select Pending Approvals from the Client Task Types pane and select the task you want to review.**
3. **View all proposed changes on the Task Details pane.**
4. **Click Approve or Reject. When prompted to confirm your decision, enter your comments in the text box and click OK. Alternately, you can click Review on the Pending Approvals pane to open the task and click Approve or Reject on this page.**

Results

If you approve the changes, the task is saved; otherwise the task is sent back to the submitter.

Configure email notifications using Automatic Response

You can set up an automatic response to receive email notifications when a task is submitted for approval, or when a task submitted for approval is approved or rejected.

Before you begin

Your email server must be configured and registered in **Server Settings** to complete this task.

Task

1. **Select Menu → Automation → Automatic Responses.**
2. **Click New Response.**
    a. **Enter a name for the new response and provide a description.**
    b. **Select ePO Approval Events in the Event group drop-down list.**
    c. **Select Task Approval in the Event type drop-down list.**
3. **Click Next to set filters to define when to trigger an email notification.**
4. **Click Next to set aggregation.**
5. **Click Next and select Send emails in the Actions drop-down list.**

    Note

    You receive a warning message that the email server is not configured if you have not registered and configured your email server.

6. **Enter details for the email to be triggered as an automatic response and click Next.**
7. **Verify the settings of the automatic response on the Summary tab and click Save.**

Results

You have set up an automatic response that triggers an email notification when a task is approved, rejected, or submitted for approval.

Deploy products to managed systems

Configure a deployment task for groups of managed systems

Configure a product deployment task to deploy products to groups of managed systems in the **System Tree**.

Task

1. **Open the New Task dialog box.**
    a. **Select Menu → Policy → Client Task Catalog.**
    b. **Under Client Task Types, select a product, then click New Task.**
2. **Select Product Deployment, then click OK.**
3. **Type a name for the task you are creating and add any notes.**
4. **Next to Target platforms, select the types of platform to use the deployment.**
5. **Next to Products and components, set the following:**
    - Select a product from the first drop-down list. **The products listed are products that you have checked in to the Main Repository. If you do not see the product you want to deploy listed here, check in the product package.**
    - Set the **Action** to **Install**, then select the **Language** of the package, and the **Branch**.
    - To specify command-line installation options, type the options in the **Command line** text field. See the product documentation for information on command-line options of the product you are installing.

    Note

    You can click **+** or **–** to add or remove products and components from the list displayed.

6. **If you want to automatically update your security products, select Auto Update.**
    This also deploys the hotfixes and patches for your product automatically.

    Note

    If you set your security product to update automatically, you cannot set the **Action** to **Remove**.

7. **(Windows only) Next to Options, select whether you want to run this task for every policy process, then click Save.**
8. **Select Menu → Systems Section → System Tree → Assigned Client Tasks, then select the required group in the System Tree.**
9. **Select the Preset filter as Product Deployment (McAfee Agent).**
    Each assigned client task per selected category appears in the **details** pane.
10. **Click Actions → New Client Task Assignment.**
11. **On the Select Task page, select Product as McAfee Agent and Task Type as Product Deployment, then select the task you created to deploy your product.**
12. **Next to Tags, select the platforms you are deploying the packages to, then click Next:**
    - **Send this task to all computers**

- **Send this task to only computers that have the following criteria** — Click **edit** next to the criteria to configure, select the tag group, select the tags to use in the criteria, then click **OK**.

Tip

To limit the list to specific tags, type the tag name in the text box under **Tags**.

13. **On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.**
14. **Review the summary, then click Save.**

Results

At every scheduled run, the deployment task installs the latest sensor package to systems that meet the specified criteria.

Configure a deployment task to install products on a managed system

Deploy products to a single system using a product deployment task.

Create a product deployment client task for a single system when that system requires:

- A product installed that other systems within the same group do not require.
- A different schedule than other systems in the group. For example, if a system is located in a different time zone than its peers.

Task

1. **Open the New Task dialog box.**
   a. **Select Menu → Policy → Client Task Catalog.**
   b. **Under Client Task Types, select a product, then click New Task.**
2. **Ensure that Product Deployment is selected, then click OK.**
3. **Type a name for the task you are creating and add any notes.**
4. **Next to Target platforms, select the types of platform to use the deployment.**
5. **Next to Products and components set the following:**
   - Select a product from the first drop-down list. **The products listed are those products for which you have already checked in a package to the Main Repository. If you do not see the product you want to deploy listed here, check in that product's package.**
   - Set the **Action** to **Install**, then select the **Language** and **Branch** of the package.
   - To specify command-line installation options, type the command-line options in the **Command line** text field. See the product documentation for information on command-line options of the product you are installing.

Note

You can click **+** or **–** to add or remove products and components from the list displayed.

6. **If you want to automatically update security products that are already deployed, including hotfixes and patches, select Auto Update.**

Note

If you set your security product to update automatically, you cannot set the **Action** to **Remove**.

7. **Next to Options, select if you want to run this task for every policy enforcement process (Windows only), then click Save.**
8. **Select Menu → Systems → System Tree → Systems, select the system on which you want to deploy a product, then click Actions → Agent → Modify Tasks on a single system.**
9. **Click Actions → New Client Task Assignment.**
10. **On the Select Task page, select Product as McAfee Agent and Task Type as Product Deployment, then select the task you created for deploying product.**
11. **Next to Tags, select the platforms to which you are deploying the packages, then click Next:**
    - **Send this task to all computers**
    - **Send this task to only computers that have the following criteria** — Click **edit**, select the tag group and tags to use in the criteria, then click **OK**.

    Tip

    To limit the list to specific tags, type the tag name in the text box under **Tags**.

12. **On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.**
13. **Review the summary, then click Save.**

Updating tasks

If you do not use global updating, determine when agents on managed systems go for updates.

You can create and update client tasks to control when and how managed systems receive update packages.

If you use global updating, this task is not needed, although you can create a daily task for redundancy.

Considerations when creating or updating client tasks

Consider the following when scheduling client update tasks:

- Create a daily update client task at the highest level of the **System Tree**, so that all systems inherit the task. If your organization is large, you can use randomization intervals to mitigate the bandwidth impact. For networks with offices in different time zones, balance network load by running the task at the local system time of the managed system, rather than at the same time for all systems.
- If you are using scheduled replication tasks, schedule the task at least an hour after the scheduled replication task.
- Run update tasks for DAT and Engine files at least once a day. Managed systems might be logged off from the network and miss the scheduled task. Running the task frequently ensures that these systems receive the update.
- Maximize bandwidth efficiency and create several scheduled client update tasks that update separate components and run at different times. For example, you can create one task to update only DAT files, then create another to update both DAT and Engine files weekly or monthly (Engine packages are released less frequently).

- Create and schedule more tasks to update products that do not use the **Trellix Agent** for Windows.
- Create a task to update your main workstation applications, to ensure that they all receive the update files. Schedule it to run daily or several times a day.

View assigned client task

During the **Initial Product Deployment** process, **Trellix ePO - On-prem** automatically creates a product deployment client task. You can use this assigned client task as a basis for creating other product deployment client tasks.

Before you begin

You must run the **Initial Product Deployment** to create the initial product deployment client task.

Task

1. **To see the initial product deployment client task, select Menu → Client Task Catalog.**
2. **Find the initial product deployment client task: from the Client Task Types list, select McAfee Agent → Product Deployment.**
   The initially created product deployment client task uses the name of the **System Tree** group that you configured in the **Agent Deployment URL** as **InitialDeployment_<groupName>**. For example, "InitialDeployment_AllWindowsSystems." This task appears in the **Name** column of the **McAfee Agent → Product Deployment** table.
3. **To open the client task and view its details, click the name of the task configured in the Agent Deployment URL.**
4. **To close the page, click Cancel.**

Results

Now you know the location and configuration of the default product deployment client task. You can duplicate this client task to, for example, deploy the **Trellix Agent** to platforms using different operating systems.

Update managed systems regularly with a scheduled update task

Create and configure update tasks. **If you use global updating, we recommend using a daily update client task to ensure systems are current with the latest DAT and engine files.**

Task

1. **Open the New Task dialog box.**
   a. **Select Menu → Policy → Client Task Catalog.**
   b. **Under Client Task Types, select a product, then click New Task.**
2. **Verify that Product Update is selected, then click OK.**
3. **Type a name for the task you are creating and add any notes.**
4. **Next to the Update in Progress dialog box, select if you want the users to be aware an update is in process, and if you want to allow them to postpone the process.**
5. **Select a package type, then click Save.**

Note

When configuring individual signatures and engines, if you select **Engine** and deselect **DAT**, when the new engine is updated a new DAT is automatically updated to ensure complete protection.

6. **Select Menu → Systems → System Tree, click the Systems tab, then select the system where you want to deploy the product update, then click Actions → Agent → Modify Tasks on a single system.**
7. **Click Actions → New Client Task Assignment.**
8. **On the Select Task page, make the following selections:**
   - **Product** — Select **McAfee Agent**.
   - **Task Type** — Select **Product Update**.

   Then select the task you created to deploy the product update.
9. **Next to Tags, select the platforms where you are deploying the packages, then click Next:**
   - **Send this task to all computers.**
   - **Send this task to only computers that have the following criteria** — Click **edit** next to the criteria to configure, select the tag group, select the tags to use in the criteria, then click **OK**.

   Tip

   To limit the list to specific tags, type the tag name in the text box under **Tags**.

   Once you select the criteria, the number of systems that fall into that criteria is displayed on top of the page. For example, if you create a tag for a domain group and apply this tag to 5 systems in a group, the page displays "**5 systems are affected**" in red colored font.
10. **On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.**
11. **Review the summary, then click Save.**

Results

The task is added to the list of client tasks for the groups and systems where it is applied. Agents receive the new update task information the next time they communicate with the server. If the task is enabled, the update task runs at the next occurrence of the scheduled day and time.

Each system updates from the appropriate repository, depending on how the policies for that client's agent are configured.

Evaluate new DATs and engines before distribution

You might want to test DAT and engine files on a few systems before deploying them to your entire organization. You can test update packages using the **Evaluation** branch of your Main Repository.

The **Trellix ePO - On-prem** software provides three repository branches for this purpose.

Task

1. **Create a scheduled Repository Pull task that copies update packages in the Evaluation branch of your Main Repository. Schedule it to run after Trellix releases updated DAT files.**
2. **Create or select an evaluation group in the System Tree, then create a Trellix Agent policy for the systems to use only the Evaluation branch.**
    a. **Select the Evaluation branch on the Updates tab in the Repository Branch Update Selection section.**

   The policies take effect the next time the **Trellix Agent** calls into the server. The next time the agent updates, it retrieves them from the **Evaluation** branch.
3. **Create a scheduled update client task for the evaluation systems that updates DAT and engine files from the Evaluation branch of your repository. Schedule it to run one or two hours after your Repository Pull task is scheduled to begin.**

   The evaluation update task created at the evaluation group level causes it to run only for that group.

4. **Monitor the systems in your evaluation group until satisfied.**
5. **Move the packages from the Evaluation branch to the Current branch of your Main Repository. Select Menu → Software → Main Repository to open the Main Repository page.**
   Adding them to the **Current** branch makes them available to your production environment. The next time any client task retrieves packages from the **Current** branch, the new DAT and engine files are distributed to systems that use the task.

Manage client tasks

Create client tasks

Use client tasks to automatically perform product updates. The process is similar for all client tasks.

In some cases, you must create a new client task assignment to associate a client task to a **System Tree** group.

Task

1. **Open the New Task dialog box.**
    a. **Select Menu → Policy → Client Task Catalog.**
    b. **Under Client Task Types, select a product, then click New Task.**
2. **Select a task type from the list, then click OK to open the Client Task Builder.**
3. **Enter a name for the task, add a description, then configure the settings specific to the task type you are creating.**

   Note

   The configuration options depend on the task type selected.

4. **Review the task settings, then click Save.**

Results

The task is added to the list of client tasks for the selected client task type.

Edit client tasks

You can edit any previously configured client task settings or schedule information.

Task

1. **Select Menu → Policy → Client Task Catalog.**
2. **Select the Client Task Type from the navigation tree on the left.**
   The available client tasks appear in the window on the right.
3. **Click the client task name to open the Client Task Catalog dialog box.**
4. **Edit the task settings as needed, then click Save.**

Results

The managed systems receive the changes you configured the next time the agents communicate with the server.

Compare client tasks

The **Client Task Comparison** tool determines which client task settings are different and which are the same.

Many of the values and variables included on this page are specific to each product. For option definitions not included in the table, see the documentation for the product that provides the client task that you want to compare.

Task

1. **Select Menu → Client Task Comparison, then select a product, client task type, and show settings from the lists.**
   These settings populate the client tasks to compare in the **Client Task 1** and **Client Task 2** lists.
2. **Select the client tasks to compare in the Compare Client Tasks row from the Client Task 1 and the Client Task 2 column lists.**
   The top two rows of the table display the number of settings that are different and identical. To reduce the amount of data, change the **Show** setting from **All Client Task Settings** to **Client Task Differences** or **Client Task Matches**.
3. **Click Print to open a printer-friendly view of this comparison.**

View client tasks assigned to a specific system

View a list of all client tasks assigned to a system from one central location, the **System Tree**.

Task

1. **Select Menu → Systems → System Tree, click the Systems tab, then select a group in the System Tree.**
   All systems belonging to the group appear in the details pane.
2. **Click the name of a system to drill into the System Information page, then click the Applied Client Tasks tab.**

Setting up automatic responses

Take immediate action against threats and outbreaks by automatically executing commands or sending emails when events occur.

Trellix ePO - On-prem responds when the conditions of an automatic response rule are met. You specify the actions that make up the response, and the type and number of events that must meet the condition to trigger the response.

By default, an automatic response rule can include these actions:

- Create an issue.
- Execute server tasks.
- Run external commands.
- Run system commands.
- Send an email message.
- Send SNMP traps.

Note

You can also configure external tools installed on the **Trellix ePO - On-prem** server to run an external command.

Managed products increase the number of actions you can select.

The products that you manage with **Trellix ePO - On-prem** determine the types of events you can create an automatic response rule for.

Here are some typical conditions that might trigger an automatic response:

- Detection of threats by your antivirus software.
- Outbreak situations. For example, 1,000 virus-detected events are received in five minutes.
- High-level compliance of **Trellix ePO - On-prem** server events. For example, a repository update or a replication task failed.

Using Automatic Responses

You can specify which events trigger a response, and what that response is.

The complete set of event types for which you can configure an automatic response depends on the software products you are managing with **Trellix ePO - On-prem**.

By default, your response can include these actions:

- Create issues.
- Execute server tasks.

- Run external commands.
- Run system commands.
- Send an email message to multiple recipients.
- Send SNMP traps.

Note

You can also configure external tools installed on the **Trellix ePO - On-prem** server to run an external command.

This feature is designed to create user-configured notifications and actions when the conditions of a rule are met. These conditions include, but are not limited to:

- Detection of threats by your anti-virus software product.
- Outbreak situations. For example, 1000 virus-detected events are received in five minutes.
- High-level compliance of **Trellix ePO - On-prem** server events. For example, a repository update or a replication task failed.

Event thresholds

Setting event thresholds lets you tailor the frequency of automatic responses to fit the needs and realities of your environment.

Aggregation

Use aggregation to set the number of events that occur before triggering an automatic response.

For example, you can configure an automatic response rule to send an email message based on the thresholds you select. First, set the **Trigger this response if multiple events occur within:** field to 30 minutes.

Next, select an option:

- **Option 1** — Select **When the number of distinct values for an event property is at least a certain value**. When **Property:** is set as **Agent GUID** and **Number of distinct values:** is **10**, the response is triggered when 10 unique GUIDs report this event in 30 minutes.
- **Option 2** — Set the **When the number of events is at least:** count to **10**. The response is triggered if 10 event IDs are reported within 30 minutes. The response is triggered whether a single computer reports 10 events or multiple computers trigger the total number of events.

Throttling

Once you have configured the rule to notify you of a possible outbreak, use throttling to make sure that you do not receive too many notification messages. If you are securing a large network, you might receive tens of thousands of events in an hour, generating thousands of email messages. Throttling allows you to limit the number of notification messages you receive based on one rule. For example, you can configure a response rule so that you don't receive more than one notification message in an hour.

Grouping

Use grouping to combine multiple aggregated events. For example, events with the same severity can be combined into one group. Grouping provides these benefits:

- Respond to all events with the same or higher severity at once.
- Prioritize events that are generated.

Default automatic response rules

Enable the default **Trellix ePO - On-prem** response rules for immediate use while you learn more about the feature.

Before enabling any of the default rules, perform these actions:

- Specify the email server (select **Menu** → **Configuration** → **Server Settings**) that sends the notification messages.
- Make sure that the recipient email address is correct. This address is configured on the **Actions** page of the **Automatic Response Builder**.

Rule name	Associated events	Email sent when...
Distributed repository update or replication failed	Distributed repository update or replication failed	Any update or replication fails.
Malware detected	Any events from any unknown products	These criteria are met: • The number of events is at least 1,000 in an hour. • The number of selected distinct values is 500. • At most, once every 2 hours. The email includes the source system IP address, threat names, product information, and other parameters.
Main Repository update or replication failed	Main Repository update or replication failed	Any update or replication fails.
Noncompliant computer detected	Noncompliant Computer Detected events	Any event is received from the **Generate Compliance Event** server task.

Response planning

Before creating automatic response rules, think about the actions you want the **Trellix ePO - On-prem** server to take.

Plan for these items:

- The event types that trigger messages in your environment.
- Who receives which messages. For example, you might not need to notify all administrators about a failed product upgrade, but you might want them to know that an infected file was discovered.
- The types and levels of thresholds that you want to set for each rule. For example, you might not want to receive an email message every time an infected file is detected during an outbreak. Instead, you can choose to send one message for every 1,000 events.
- The commands or registered executables you want to run when the conditions of a rule are met.
- The server task you want to run when the conditions of a rule are met.

Determine how events are forwarded

Determine when events are forwarded and which events are forwarded immediately.

The server receives event notifications from agents. You can configure **Trellix Agent** policies to forward events either immediately to the server or only after agent-server communication intervals.

If you choose to send events immediately (as set by default), the **Trellix Agent** forwards all events when they are received.

If you choose not to have all events sent immediately, the **Trellix Agent** forwards immediately only events that are designated by the issuing product as high priority. Other events are sent only at the agent-server communication.

Determine which events are forwarded immediately

Determine whether events are forwarded immediately or only during agent-server communication.

If the currently applied policy is not set for immediate uploading of events, either edit the currently applied policy or create a **Trellix Agent** policy. This setting is configured on the **Threat Event Log** page.

Task

1. **Select Menu → Policy → Policy Catalog, then select Trellix Agent on the Products pane and expand General category.**
2. **Click an existing agent policy.**
3. **On the Events tab, select Enable priority event forwarding.**
4. **Select the event severity.**
   Events of the selected severity (and greater) are forwarded immediately to the server.
5. **To regulate traffic, type an Interval between uploads (in minutes).**
6. **To regulate traffic size, type the Maximum number of events per upload.**
7. **Click Save.**

Determine which events are forwarded to the server

You can determine which events are forwarded to the server using server settings and event filtering.

Note

These settings affect the bandwidth used in your environment, and the results of event-based queries.

Task

1. **Select Menu → Configuration → Server Settings, select Event Filtering, then click Edit at the bottom of the page.**
2. **Select the events you want forwarded, either all or individual events.**
    - To forward all available events, select **All events to the server**.

      Note

      Select All and **Deselect All** are disabled when you select **All events to the server**.

    - To forward only the events you specified, select **Only selected events to the server**.
3. **Select where you want the selected events stored.**
    - Click **Store selected in McAfee ePO** — Store all selected events in the **Trellix ePO - On-prem** database.
    - Click **Forward selected to syslog** — Forward all selected events to syslog.
    - Click **Store selected in both** — Store all selected events in both the **Trellix ePO - On-prem** and forward to syslog. This is the default setting.

    Note

    If a product extension provides an event storage option for an event type during registration, that event storage option is saved. If a product extension does not provide an event storage option for an event type during registration, the default is to store in both.

4. **Select event source.**
    - **Events from any source**—Any source includes the **Trellix Agent**, **Trellix ePO - On-prem**, and more.
    - **Events that were generated by the sending agent**—Only events generated by the **Trellix Agent**.
5. **Click Save.**

Results

Changes to these settings take effect after all agents have communicated with the **Trellix ePO - On-prem** server.

Configure Automatic Responses

Assign permissions to notifications

Notifications permissions enable users to view, create, and edit registered executables.

Task

1. **Select Menu → User Management → Permission Sets, then either create a permission set or select an existing one.**
2. **Next to Event Notifications, click Edit.**
3. **Select the notifications permission you want:**
    - **No permissions**
    - **View registered executables**
    - **Create and edit registered executables**
    - **View rules and notifications for entire System Tree (overrides System Tree group access permissions)**
4. **Click Save.**
5. **If you created a permission set, select Menu → User Management → Users.**
6. **Select a user to assign the new permission set to, then click Edit.**
7. **Next to Permission sets, select the checkbox for the permission set with the notifications permissions you want, then click Save.**

Assign permissions to Automatic Responses

Assign permssions to responses when you need to limit the types of responses users can create.

Before you begin

To create a response rule, users need permissions for the Threat Event Log, System Tree, Server Tasks, and Detected Systems features.

Task

1. **Select Menu → User Management → Permission Sets, then create a permission set or select an existing one.**
2. **Next to Automatic Response, click Edit.**
3. **Select an Automatic Response permission:**
    - **No permissions**
    - **View Responses; view Response results in the Server Task Log**
    - **Create, edit, view, and cancel Responses; view Response results in the Server Task Log**
4. **Click Save.**
5. **If you created a permission set, select Menu → User Management → Users.**
6. **Select a user to assign the new permission set to, then click Edit.**
7. **Next to Permission sets, select the checkbox for the permission set with the Automatic Response permissions you want, then click Save.**

Manage SNMP servers

Configure responses to use your SNMP (Simple Network Management Protocol) server.

You can configure responses to send SNMP traps to your SNMP server. You can receive SNMP traps at the same location where you can use your network management application to view detailed information about the systems in your environment.

Note

You do not need to make other configurations or start any services to configure this feature.

SNMP server actions

1. Select **Menu** → **Configuration** → **Registered Servers**.
2. From the list of registered servers, select an SNMP server, then click **Actions** and a change available from the Registered Servers page.

Action	Description
Edit	Edit the server information as needed, then click **Save**.
Delete	Deletes the selected SNMP server. When prompted, click **Yes**.

Import .MIB files

Import .mib files before you set up rules to send notification messages to an SNMP server using an SNMP trap.

You must import three .mib files from **\Program Files\McAfee\ePolicy Orchestrator\MIB**. The files must be imported in the following order:

1. NAI-MIB.mib
2. TVD-MIB.mib
3. EPO-MIB.mib

These files allow your network management program to decode the data in the SNMP traps into meaningful text. The EPO-MIB.mib file depends on the other two files to define the following traps:

- **epoThreatEvent** — This trap is sent when an Automatic Response for an **Trellix ePO - On-prem** Threat Event is triggered. It contains variables that match properties of the Threat event.

- **epoStatusEvent** — This trap is sent when an Automatic Response for an **Trellix ePO - On-prem** Status Event is triggered. It contains variables that match the properties of a (Server) Status event.
- **epoClientStatusEvent** — This trap is sent when an Automatic Response for an **Trellix ePO - On-prem** Client Status Event is triggered. It contains variables that match the properties of the Client Status event.
- **epoTestEvent** — This is a test trap that is sent when you click **Send Test Trap** in the **New SNMP Server** or **Edit SNMP Server** pages.

For instructions on importing and implementing .mib files, see the product documentation for your network management program.

Choose a notification interval

This setting determines how often the automatic response system is notified that an event has occurred.

These events generate notifications:

- **Client events** — Events that occur on managed systems. For example, **Product update succeeded**.
- **Threat events** — Events that indicate possible threats are detected. For example, **Virus detected**.
- **Server events** — Events that occur on the server. For example, **Repository pull failed**.

An automatic response can be triggered only after the automatic response system receives a notification. Specify a short interval for sending notifications, and choose an evaluation interval that is frequent enough to ensure that the automatic response system can respond to an event in a timely manner.

Task

1. **Select Menu → Configuration → Server Settings, select Event Notifications from the Setting Categories, then click Edit.**
2. **Specify a value between 1 and 9,999 minutes for the Evaluation Interval (1 minute by default), then click Save.**

Create and edit Automatic Response rule

Define a rule

When creating a rule, include information that other users might need to understand the purpose or effect of the rule.

Task

1. **Select Menu → Automation → Automatic Responses, then click New Response, or click Edit next to an existing rule.**
2. **On the Description page, type a unique name and any notes for the rule. A good name gives users a general idea of what the rule does. Use notes to provide a more detailed description.**
3. **From the Language menu, select the language that the rule uses.**
4. **Select the Event group and Event type that trigger this response.**
5. **Next to Status, select Enabled or Disabled. The default is Enabled.**
6. **Click Next.**

Set filters for the rule

To limit the events that can trigger the response, set the filters for the response rule on the **Filters** page of the **Response Builder**.

Task

1. **From the Available Properties list, select a property and specify the value to filter the response result.**
   Available Properties depend on the event type and event group selected on the **Description** page.
2. **Click Next.**

Set Aggregation and grouping criteria for the rule

Define when events trigger a rule on the **Aggregation** page of the **Response Builder**.

A rule's thresholds are a combination of aggregation, throttling, and grouping.

Task

1. **Next to Aggregation, select an aggregation level.**
   - To trigger the response for every event, select **Trigger this response for every event**.
   - To trigger the event after multiple events occur, perform these steps.
     - Select **Trigger this response if multiple events occur within**, then define the amount of time in seconds, minutes, hours, or days.
     - Select the aggregations conditions.
       - **When the number of distinct values for an event property is at least a certain value** — This condition is used when a distinct value of occurrence of event property is selected.
       - **When the number of events is at least** — Type the minimum defined number of events.
2. **Next to Grouping, select whether to group the aggregated events. If you do, specify the property of the event on which they are grouped.**
3. **As needed, next to Throttling, select At most, trigger this response once every and define an amount of time that must pass before this rule can send another notification message.**
   The amount of time can be defined in minutes, hours, or days.
4. **Click Next.**

Configure the actions for an automatic response rule

Configure the responses triggered by the rule on the **Actions** page of the **Response Builder**.

Configure multiple actions by using the **+** and **-** buttons next to the drop-down list for the type of notification.

Task

1. **Configure each action that occurs as part of the response.**
   After configuring the options for an action, click **Next** if finished, or click **+** to add another action.
   - To send an SNMP trap, select **Send SNMP Trap** from the drop-down list.
     - Select an SNMP server from the drop-down list.
     - Select the value types that you want to send in the SNMP trap. Some events do not include all information specified. If a selection you made is not represented, the information was not available in the event file.
   - To send an email as part of the response, select **Send Email** from the drop-down list.

    - Next to **Recipients**, click **...** and select the recipients for the message. The list of available recipients is taken from Contacts (**Menu** → **User Management** → **Contacts**). Or, you can manually type email addresses, separated by a comma. Recipients can also be added in the BCC field.
    - Select the importance of the email.
    - Type the **Subject** of the message or insert any of the available variables directly into the subject.
    - Type any text that you want to appear in the body of the message or insert any of the available variables directly into the body.
- To run a scheduled task, select **Execute Server Task** from the drop-down list.
    - Select the task that you want to run from the **Task to execute** drop-down list.
    - Click **Next** if finished, or click **+** to add another notification.
- To run an external command, select **Run External Command** from the drop-down list.
    - Select the Registered Executables and type any arguments for the command.
- To create an issue, select **Create issue** from the drop-down list.
    - Select the type of issue that you want to create.
    - Type a unique name and any notes for the issue or insert any of the available variables directly into the name and description.
    - Select the **State**, **Priority**, **Severity**, and **Resolution** for the issue from the respective drop-down list.
    - Type the name of the assignee in the text box.
    - Click **Next** if finished, or click **+** to add another notification.

2. **On the Summary page, verify the information, then click Save.**

Results

The new rule appears in the **Responses** list.

Note

Automatic response rules do not have a dependency order.

Manage registered executables and external commands

The registered executables you configure are run when the conditions of a rule are met. Automatic Responses trigger the registered executable commands to run.

Note

You can run registered executable commands only on console applications.

Task

1. **Select Menu → Configuration → Registered Executables.**
2. **Select one of these actions.**

Action	Steps
Add a registered executable	a. Click **Actions → Registered Executable**. b. Type a name for the registered executable. c. Type the path and select the registered executable that you want a rule to execute when triggered. d. Modify the user credentials, if needed. e. Test the executable and confirm that it worked using the **Audit Log**. f. Click **Save**. The new registered executable appears in the **Registered Executables** list.
Edit a registered executable	a. Find the registered executable to edit in the **Registered Executable** page, then click **Edit**. b. Change the information as needed and click **Save**.
Duplicate a registered executable	a. Find the registered executable to duplicate in the **Registered Executable** page, then click **Duplicate**. b. Type a name for the registered executable, then click **OK**. The duplicated registered executable appears in the **Registered Executables** list.

Action	Steps
Delete a registered executable	a. Find the registered executable to delete in the **Registered Executable** page, then click **Delete**. b. When prompted, click **OK**. The deleted registered executable no longer appears in the **Registered Executables** list.

Agent-server communication

Client systems use the **Trellix Agent** and agent-server communications to communicate with your **Trellix ePO - On-prem** server.

For version-specific information about your agents, see the ***Trellix Agent*** *Product Guide*.

How agent-server communication works

Trellix Agent communicates with the **Trellix ePO - On-prem** server periodically using agent-server communication to send events and ensure that all settings are up to date.

During each agent-server communication, the **Trellix Agent** collects its current system properties, and events that have not yet been sent, and sends them to the server. The server sends new or changed policies and tasks to the **Trellix Agent**, and the repository list if it has changed since the last agent-server communication.

See the ***Trellix Agent*** *Product Guide* for details about:

- How agent-server communication works
- How SuperAgents work to use bandwidth and **Trellix ePO - On-prem** performance
- Collect **Trellix Agent** statistics
- Queries provided by the **Trellix Agent**

Estimating and adjusting the ASCI

Estimating the best ASCI: best practice

To improve the **Trellix ePO - On-prem** server performance, you might need to adjust the ASCI setting for your managed network.

To determine whether to change your ASCI, ask how often changes occur to endpoint policies on your **Trellix ePO - On-prem** server. For most organizations, once your policies are in place, they don't often change. Some organizations change an endpoint policy less frequently than once every few months. That means a system calling in every 60 minutes looking for a policy change, about eight times in a typical work day, might be excessive. If the agent does not find any new policies to download, it waits until the next agent-server communication, then checks again at its next scheduled check-in time.

To estimate the ASCI, your concern is not wasting bandwidth because agent-server communications are only a few kilobytes per communication. The concern is the strain put on the **Trellix ePO - On-prem** server with every communication from every agent in larger environments. All your agents need at least two communications a day with the **Trellix ePO - On-prem** server. This requires a 180–240 minute ASCI in most organizations.

For organizations with fewer than 10,000 nodes, the default ASCI setting is not a concern at 60 minutes. But for organizations with more than 10,000 nodes, change the default setting of 60 minutes setting to about 3–4 hours.

For organizations with more than 60,000 nodes, the ASCI setting is much more important. If your **Trellix ePO - On-prem** server is not having performance issues, you can use the 4-hour ASCI interval. If there are any performance issues, consider increasing

your ASCI to 6 hours; possibly even longer. This change significantly reduces the number of agents that are simultaneously connecting to the **Trellix ePO - On-prem** server and improves the server performance.

Note

You can determine how many connections are being made to your **Trellix ePO - On-prem** server by using the **Trellix ePO - On-prem** Performance Counters.

This table lists basic ASCI guidelines.

Node count	Recommended ASCI
100–10,000	60–120 minutes
10,000–50,000	120–240 minutes
50,000 or more	240–360 minutes

Configure the ASCI setting: best practice

After you estimate the best ASCI setting, reconfigure the setting in the **Trellix ePO - On-prem** server.

The ASCI is set to 60 minutes by default. If that interval is too frequent for your organization, change it.

Task

1. **Select Menu → Policy → Policy Catalog, then select Trellix Agent from the Product list and General from the Category list.**
2. **Click the name of the policy you want to change and the General tab.**
3. **Next to Agent-to-server communication interval, type the number of minutes between updates.**
   This example shows the interval set to 60 minutes.
4. **Click Save.**
   If you send a policy change or add a client task immediately, you can execute an agent wake-up call.

Managing agent-server communication

Allow agent deployment credentials to be cached

Administrators must provide credentials to successfully deploy agents from your Trellix ePO server to systems in your network. You can choose whether to allow agent deployment credentials to be cached for each user.

Once a user's credentials are cached, that user can deploy agents without having to authenticate again. Credentials are cached per user, so a user who has not previously provided credentials can't deploy agents without providing their own credentials first.

Task

1. **Select Menu → Configuration → Server Settings, select Agent Deployment Credentials from the Setting Categories, then click Edit.**
2. **Select the checkbox to allow agent deployment credentials to be cached.**

Change agent communication ports

You can change some of the ports used for agent communication on your Trellix ePO server.

You can modify the settings for these agent communication ports:

- **Agent-to-server communication secure port**
- **Agent wake-up communication port**
- **Agent broadcast communication port**

Task

1. **Select Menu → Configuration → Server Settings, select Ports from the Setting Categories, then click Edit.**
2. **Select whether to enable port 443 for agent-server communications, enter the ports to be used for agent wake-up calls and broadcasts, then click Save.**

Automating and optimizing Trellix ePO - On-prem workflow

You can create queries and tasks to automatically run for improved server performance, easier maintenance, and to monitor threats.

Note

When you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change.

Best practice: Find systems with the same GUID

You can use preconfigured server tasks that runs queries and targets systems that might have the same GUIDs.

This task tells the agent to regenerate the GUID and fix the problem.

Task

1. **Select Menu → Automation → Server Tasks to open the Server Tasks Builder.**
2. **Click Edit in the Actions column for one of the following preconfigured server tasks.**
    - **Duplicate Agent GUID - Clear error count**
    - **Duplicate Agent GUID - Remove systems that potentially use the same GUID**
3. **On the Description page, select Enabled, then click:**
    - **Save** — Enable the server task and run it from the **Server Task** page.
    - **Next** — Schedule the server task to run at a specific time and perform the task.

Results

This clears the error count and removes any systems with the same GUID, and assigns the systems a new GUID.

Best practices: Purging events automatically

Periodically purge the events that are sent daily to your **Trellix ePO - On-prem** server. These events can eventually reduce performance of the **Trellix ePO - On-prem** server and SQL Servers.

Events can be anything from a threat being detected, to an update completing successfully. In environments with a few hundred nodes, you can purge these events on a nightly basis. But in environments with thousands of nodes reporting to your **Trellix ePO - On-prem** server, it is critical to delete these events as they become old. In these large environments, your database size directly impacts the performance of your **Trellix ePO - On-prem** server, and you must have a clean database.

You must determine your event data retention rate. The retention rate can be from one month to an entire year. The retention rate for most organizations is about six months. For example, six months after your events occur, on schedule, they are deleted from your database.

Important

Trellix ePO - On-prem does not come with a preconfigured server task to purge task events. This means that many users never create a task to purge these events and, over time, the **Trellix ePO - On-prem** server SQL database starts growing exponentially and is never cleaned.

Create a purge events server task best practice

Create an automated server task that deletes all events in the database that are older and no longer needed.

Note

Some organizations have specific event retention policies or reporting requirements. Make sure that your purge event settings conform to those policies.

Task

1. **To open the Server Task Builder dialog box, select Menu → Automation → Server Tasks, then click Actions → New Task.**
2. **Type a name for the task, for example** Delete client events**, add a description, then click Next.**
3. **On the Actions tab, configure these actions from the list:**
    - **Purge Audit Log** — Purge after 6 months.
    - **Purge Client Events** — Purge after 6 months.
    - **Purge Server Task Log** — Purge after 6 months.
    - **Purge Threat Event Log** — Purge every day.
    - **Purge SiteAdvisor Enterprise Events** — Purge after 10 days.

    Note

    You can chain the actions all in one task so that you don't have to create multiple tasks.

    This example purges **SiteAdvisor Enterprise** events because they are not included in the normal events table and require their own purge task. The **SiteAdvisor Enterprise** events are retained for only 10 days because they collect all URLs visited by managed systems. These events can save a large amount of data in environments with more than 10,000 systems. Therefore, this data is saved for a much shorter time compared to other event types.
4. **Click Next and schedule the task to run every day during non-business hours.**
5. **Click the Summary tab, confirm that the server task settings are correct, then click Save.**

Purge events by query

You can use a custom configured query as a base to delete client events.

Before you begin

You must have created a query to find the events you want purged before you start this task.

There are reasons why you might need to purge data or events based on a query. For example, there can be many specific events overwhelming your database. In this example, you might not want to wait for the event to age out if you are keeping your events for six months. Instead you want that specific event deleted immediately or nightly.

Purging these events can significantly improve the performance of your **Trellix ePO - On-prem** server and database.

Configure purging data based on the results of a query.

Task

1. **Select Menu → Automation → Server Tasks, then click Action → New Task to open the Server Task Builder.**
2. **Type a name for the task, for example** Delete 1059 client events**, then on the Actions tab, click Purge Client Events from the Actions list.**
3. **Click Purge by Query, then select the custom query that you created.**

   Note

   This menu is automatically populated when table queries are created for client events.

4. **Schedule the task to run every day during non-business hours, then click Save.**

Best practice: Creating an automatic content pull and replication

Pulling content daily from the public **Trellix** servers is a primary functions of your **Trellix ePO - On-prem** server. Regularly pulling content keeps your protection signatures up to date for **Trellix** products.

Pulling the latest DAT and content files keeps your protection signatures up to date for **Trellix** products like **VirusScan Enterprise** and **Host Intrusion Prevention**.

The primary steps are:

1. Pull content from **Trellix** into your Main Repository, which is always the **Trellix ePO - On-prem** server.
2. Replicate that content to your distributed repositories. This ensures that multiple copies of the content are available and remain synchronized. This also allows clients to update their content from their nearest repository.

The most important content are the DAT files for **VirusScan Enterprise**, released daily at approximately 3 p.m. Eastern Time (19:00 UTC or GMT).

Optionally, many users with larger environments choose to test their DAT files in their environment before deployment to all their systems.

Pull content automatically: best practice

Pull the **Trellix** content from the public **Trellix** servers. This pull task keeps your protection signatures up to date.

You must schedule your pull tasks to run at least once a day after 3 p.m. Eastern Time (19:00 UTC or GMT). In the following example, the pull is scheduled for twice daily, and if there is a network problem at 5 p.m., the task occurs again at 6 p.m.. Some users like to pull their updates more frequently, as often as every 15 minutes. Pulling DATs frequently is aggressive and unnecessary because DAT files are typically released only once a day. Pulling two or three times a day is adequate.

Note

Testing your DAT files before deployment requires a predictable pull schedule.

Task

1. **Select Menu → Automation → Server Tasks, then click Actions → New task.**
2. **In the Server Task Builder dialog box, type a task name and click Next.**
3. **Specify which signatures to include in the pull task.**
    a. **In the Actions dialog box, from the Actions list, select Repository Pull, then click Selected packages.**
    b. **Select the signatures that apply to your environment.**

Tip

Best practice: When you create a pull task for content, select only the packages that apply to your environment instead of selecting **All packages**. This keeps the size of your **Main Repository** manageable. It also reduces the bandwidth used during the pull from the **Trellix** website and during replication to your distributed repositories.

4. **Click Next.**
5. **Schedule your pull task to run at least once a day after 3 p.m. Eastern Time, then click Next.**
6. **Click the Summary tab, confirm that the server task settings are correct, then click Save.**

Results

Now you have created a server task that automatically pulls the **Trellix** DAT files and content from the public **Trellix** servers.

Best practices: Filtering 1051 and 1059 events

1051 and 1059 events can make up 80 percent of the events stored in your database. If enabled, make sure that you periodically purge these events.

If you have not looked at Event Filtering on your **Trellix ePO - On-prem** server in a long time, run the custom **Event Summary Query** and check the output.

The two most common events seen in customer environments are:

- 1051 — Unable to scan password-protected file

- 1059 — Scan timed out

These two events can be enabled on the **Trellix ePO - On-prem** server. If you never disabled them, you might find a significant number of these events when you run the **Event Summary Query**. These two events can, for some users, make up 80 percent of the events in the database, use a tremendous amount of space, and impact the performance of the database.

Caution

The 1059 events indicate that a file was not scanned, but the user was given access. Disabling the 1059 event means that you lose visibility of a security risk.

So why are these events in there? These events have historic significance and go back several years and are meant to tell you that a file was not scanned by **VirusScan Enterprise**. This failure to scan the file might be due to one of two reasons:

- The scan timed out due to the size of the file, which is a 1059 event.
- It was inaccessible due to password protection or encryption on the file, which is a 1051 event.

Disable these two events under event filtering, to prevent a flood of these events into your database. By disabling these events, you are effectively telling the agent to stop sending these events to **Trellix ePO - On-prem**.

Note

VirusScan Enterprise still logs these events in the On-access scanner log file for reference on the local client.

Optionally, you can disable additional events, but this is not typically needed because most of the other events are important and are generated in manageable numbers. You can also enable additional events, as long as you monitor your event summary query to make sure that the new event you enabled does not overwhelm your database.

Best practice: Filter 1051 and 1059 events

Disable 1051 and 1059 events if you find a significant number of them when you run the **Event Summary Query**.

Task

1. **Select Menu → Configuration → Server Settings, in the Setting Categories list select Event Filtering, then click Edit.**
2. **In list on the Edit Event Filtering page, scroll down until you see these events, then deselect them:**
    - **1051: Unable to scan password protected (Medium)**
    - **1059: Scan Timed Out (Medium)** This figure shows the 1051 and 1059 events deselected on the **Server Settings** page.
3. **Click Save.**

Results

Now these two events are no longer saved to the **Trellix ePO - On-prem** server database when they are forwarded from the agents.

Best practice: Finding systems that need a new agent

If you suspect some of your managed systems might not have the same **Trellix Agent** installed, perform these tasks to find the systems with the older agent versions, then select those systems for a **Trellix Agent** upgrade.

Create an Agent Version Summary query best practice

Find systems with old **Trellix Agent** versions using a query to generate a list of all agent versions that are older than the current version.

Task

1. **To duplicate the Agent Versions Summary query, select Menu → Reporting → Queries & Reports, then find the Agent Versions Summary query in the list.**
2. **In the Actions column of the Agent Versions Summary query, click Duplicate. In the Duplicate dialog box, change the name, select a group to receive the copy of the query, then click OK.**
3. **Navigate to the duplicate query that you created, then click Edit in the Actions column to display the preconfigured Query Builder.**
4. **In the Chart tab, in the Display Results As list, expand List and select Table.**
5. **To configure the Sort by fields, in the Configure Chart: Table page, select Product Version (Agent) under Agent Properties in the list, click Value (Descending), then click Next.**
6. **In the Columns tab, remove all preconfigured columns except System Name, then click Next.**
7. **In the Filter tab, configure these columns, then click Run:**
    a. **For the Property column, select Product Version (Agent) from the Available Properties list.**
    b. **For the Comparison column, select Less than.**
    c. **For the Value column, type the current Trellix Agent version number.**

Note

Typing the current agent number means that the query finds only versions "earlier than" that version number.

Results

Now your new query can run from a product deployment to update the old **Trellix Agent** versions.

Update Trellix Agent with a product deployment project best practice

Update the old **Trellix Agent** versions found using an **Agent Version Summary** query and a **Product Deployment** task.

Task

1. **Select Menu → Software → Product Deployment, then click New Deployment.**
2. **From the New Deployment page, configure these settings:**
    a. **Type a name and description for this deployment. This name appears on the Product Deployment page after the deployment is saved.**
    b. **Next to Type, select Fixed.**

c. **Next to Package, select the Trellix Agent that you want installed on the systems. Select the language and repository branch (Evaluation, Current, or Previous) that you want to deploy from.**
d. **Next to Command line, specify any command-line installation options. See the *Trellix Agent Product Guide* for information on command-line options.**
e. **In the Select the systems group, click Select Systems, and from the dialog box, click the Queries tab and configure these options, then click OK:**
    - Select the Agent Version Summary table query that you created.
    - Select the system names displayed in the **Systems** list.

    The **Total** field displays the number of systems selected.
f. **Next to Select a start time, select Run Immediately from the list.**

3. **Click Save.**

Results

The **Product Deployment** project starts running and allows you to monitor the deployment process and status.

Finding inactive systems: best practice

Most environments are changing constantly, new systems are added and old systems removed. These changes create inactive **Trellix Agent** systems that, if not deleted, can ultimately skew your compliance reports.

As systems are decommissioned, or disappear because of extended travel, users on leave, or other reasons, remove them from the System Tree. An example of a skewed report might be your DAT report on compliance. If you have systems in your System Tree that have not reported into the **Trellix ePO - On-prem** server for 20 days, they appear as out of date by 20 days and ultimately skew your compliance reports.

Initial troubleshooting

Initially, when a system is not communicating with the **Trellix ePO - On-prem** server, try these steps:

1. From the **System Tree**, select the system and click **Actions** → **Agents** → **Wake Up Agents**.

Note

Configure a **Retry interval** of, for example, 3 minutes.

2. To delete the device from **Trellix ePO - On-prem**, but not remove the agent in the **System Tree**, select the system and click **Actions** → **Directory Management** → **Delete**. Do not select **Remove agent on next agent-server communication**.
3. Wait for the system to communicate with **Trellix ePO - On-prem** again.

Note

The system appears in the **System Tree Lost and Found** group.

Dealing with inactive systems

You can create a query and report to filter out systems that have not communicated with the **Trellix ePO - On-prem** server in **X** number of days. Or your query and report can delete or automatically move these systems.

It's more efficient to either delete or automatically move these inactive systems. Most organizations choose a deadline of between 14–30 days of no communication to delete or move systems. For example, if a system has not communicated with the **Trellix ePO - On-prem** server after that deadline you can:

- Delete that system.
- Move that system to a group in your tree that you can designate as, for example, ***Inactive Agents***.

Note

A preconfigured **Inactive Agent Cleanup Task** exists, disabled by default, that you can edit and enable on your server.

Change the Inactive Agents query: best practice

If the default **Inactive Agents** query is not configured to match your needs, you can duplicate the query and use it as a base to create your custom query.

Deleting the inactive agents that have not communicated in last month is the default setting for the preconfigured **Inactive Agents** query. If you want to change the default timer setting, make a copy of the **Inactive Agents** query.

The instructions in this task describe how to create a copy of the existing **Inactive Agents** query to change the deadline to 2 weeks.

Task

1. **To duplicate the Inactive Agents query, select Menu → Reporting → Queries & Reports, then find the Inactive Agents query in the list.**
2. **In the Actions column of the Inactive Agents query, click Duplicate.**
3. **In the Duplicate dialog box change the name, select a group to receive the copy of the query, then click OK.**
4. **Navigate to the duplicate query that you created and, in the Actions column, click Edit to display the preconfigured Query Builder.**
5. **To change the Filter tab settings from once a month to every two weeks, set the Last Communications property, Is not within the last comparison, to 2 Weeks value.**

   Note

   Don't change the **and Managed State** property, **Equals** comparison, or the **Managed** value.

6. **Click Save.**

Results

Now your new **Inactive Agents** query is ready to run from a server task to delete systems with an inactive agent.

Delete inactive systems: best practice

Use the **Inactive Agent Cleanup** server task with the preconfigured query named **Inactive Agents** to automatically delete inactive systems.

Before you begin

You must have enabled or duplicated the **Inactive Agents** query.

Note

Deleting a system from the **System Tree** deletes only the record for that system from the **Trellix ePO - On-prem** database. If the system physically exists, it continues to perform normally with the last policies it received from the **Trellix ePO - On-prem** server for its applicable products.

Task

1. **To create a duplicate of the Inactive Agent Cleanup Task, select Menu → Automation → Server Tasks, then find the Inactive Agent Cleanup Task in the server tasks list.**
2. **Click the preconfigured Inactive Agent Cleanup Task, click Actions → Duplicate.**
3. **In the Duplicate dialog box, change the server task name, then click OK.**
4. **In the server task row you created, click Edit to display the Server Task Builder page.**
5. **From the Descriptions tab, type any needed notes, click Enabled in Schedule status, then click Next.**
6. **From the Actions tab, configure these settings:**
    a. **From the Actions list, select Run Query,**
    b. **For Query, click ... to open the Select a query from the list dialog box.**
    c. **Click the group tab where you saved your copy of the Inactive Agents query, select your query, then click OK.**
    d. **Select your language.**
    e. **In Sub-Actions, select Delete Systems from the list.**

    Caution

    Do **not** click **Remove agent**. This setting causes **Trellix ePO - On-prem** to delete the **Trellix Agent** from the inactive systems when they are removed from the System Tree. Without the agent installed, when the removed system reconnects to the network it cannot automatically start communicating with the **Trellix ePO - On-prem** server and reinsert itself back into the System Tree.

    (Optional) Instead of using the default subaction **Delete Systems**, you can select **Move Systems to another Group.** This moves the systems found by the query to a designated group, for example, **Inactive Systems** in your **System Tree**.
7. **Click Next, schedule when you want this server task to run, then save the server task.**

Results

Now any inactive systems are automatically removed from the **Trellix ePO - On-prem** server, and your system compliance reports provide more accurate information.

Measuring malware events best practice

Counting malware events provides an overall view of attacks and threats being detected and stopped. With this information, you can gauge the health of your network over time and change it as needed.

Creating a query that counts total infected systems cleaned per week is the first step in creating a benchmark to test your network malware status. This query counts each system as a malware event occurs. It counts the system only once even if it generated thousands of events.

Once this query is created, you can:

- Add it as a dashboard to quickly monitor your network malware attacks.
- Create a report to provide history of your network status.
- Create an Automatic Response to notify you if a threshold of systems is affected by malware.

Create a query that counts systems cleaned per week best practice

Creating a query to count the number of systems cleaned per week is a good way to benchmark the overall status of your network.

Task

1. **Select Menu → Reporting → Queries & Reports, then click Actions → New.**
2. **On the Query Wizard Result Types tab for the Feature Group, select Events, then in the Result Types pane, click Threat Events, then click Next.**
3. **On the Chart tab, in the Display Results As list, select Single Line Chart.**
4. **In the Configure Chart: Single Line Chart pane, configure these settings, then click Next:**
    - In **Time base is**, select **Event Generated Time**.
    - In **Time unit**, select **Week**.
    - In **Time Sequence is**, select **Oldest First**.
    - In **Line values are**, select **Number of**.
    - Select **Threat Target Host Name**.
    - Click **Show Total**.
5. **In the Columns tab, in the Available Columns list select these columns to display, then click Next:**
    - **Event Generated time**
    - **Threat Target Host Name**
    - **Threat Target IPv4 Address**
    - **Event Category**
    - **Threat Severity**
    - **Threat Name**
6. **In the Filter tab, Available Properties list, configure this Required Criteria:**
    - For **Event Generated Time**, select these settings from the **Is within the last** list, **3** and **Months**.
    - For **Event Category**, select these settings from the **Belongs to list**, **Malware**.
    - For **Action Taken**, select these settings from the lists **Equals** and **Deleted**.

7. **Click Save to display the Save Query page, then configure these settings:**
    - For **Query Name**, type a query name, for example, `Total Infected Systems Cleaned Per Week`.
    - For **Query Description**, type a description of what this query does.
    - For **Query Group**, click **New Group**, type the query group name, then click **Public**.
8. **Click Save.**

Results

When you run this query, it returns the number of infected systems cleaned per week. This information provides a benchmark of the overall status of your network.

Finding malware events per subnet: best practice

Finding threats by subnet IP address shows you whether a certain group of users needs process changes or additional protection on your managed network.

For example, if you have four subnets, and only one subnet is continuously generating threat events, you can narrow down the cause of those threats. Perhaps users on that subnet have been sharing infected USB drives.

Create a query to find malware events per subnet best practice

Create a query to find malware events and sort them by subnet. This query helps you find networks in your environment that are under attack.

Task

1. **To duplicate the existing Threat Event Descriptions in the Last 24 Hours query, select Menu → Reports → Queries & Reports, then find and select the Threat Target IP Address query in the list.**
2. **Click Actions → Duplicate and in the Duplicate dialog box, edit the name, select the group to receive the copy, then click OK.**
3. **In the Queries list, find the new query that you created and click Edit.**
   The duplicated query is displayed in the **Query Builder** with the **Chart** tab selected.
4. **In the Display Results As list, select Table under List.**
5. **In the Configure Chart: Table dialog box, select Threat Target IPv4 Address from the sort by list and Value (Descending), then click Next.**
6. **In the Columns tab, you can use the preselected columns.**

   Tip

   It might help to move the **Threat Target IPv4 Address** closer to the left of the table, then click **Next**.

   Don't change the default **Filter** tab settings.
7. **Click the Summary tab, confirm that the query settings are correct, then click Save.**
8. **In the Queries list, find the query that you created, then click Run.**

Results

Now you have a query to find malware events and sort them by IP subnet address.

Create an automatic compliance query and report best practice

You can create a compliance query and report to find which of your managed systems meet specific criteria.

For example, you can find systems that don't have the latest DATs or have not contacted the **Trellix ePO - On-prem** server in over 30 days.

To find this important information automatically, use these tasks.

Create a server task to run compliance queries best practice

You must create a server task to run your compliance queries weekly to automate generating your managed systems' compliance report.

Follow these steps to create a server task that runs your compliance queries every Sunday morning at 2:00 a.m.. Running the queries on Sunday morning allows you to run the report on Monday morning at 5:00 a.m. and deliver it by email to the administrators.

Task

1. **Select Menu → Automation → Server Tasks, then click Actions → New Task.**
2. **In the Server Task Builder:**
    a. **In the, Descriptions tab, type a name and notes.**
    b. **In the Schedule status, click Enabled.**
    c. **Click Next.**
3. **In the Actions tab, configure these settings.**
    a. **In the Actions list, select Run Query and configure these settings:**
        - For **Query**, select **VSE: Compliance Over the Last 30 Days**.
        - Select your language.
        - For **Sub-Actions**, select **Export to File** then click **OK**.
        - For C:\reports\, type a valid file name.
        - For **If file exists**, select **Overwrite**.
        - For **Export**, select **Chart data only**.
        - For **Format**, select **CSV**.
    b. **Click + to create another action, and in the second Actions list, select Run Query and configure these settings, then Next.**
        - For **Query**, select **Inactive Agents**.
        - Select your language.
        - For **Sub-Actions**, select **Export to File**.
        - For C:\reports\, type a valid file name.

- For **If file exists**, select **Overwrite**.
- For **Export**, select **Chart data only**.
- For **Format**, select **CSV**.

4. **In the Schedule tab, change these settings, then click Next.**
   a. **For Schedule type, click Weekly.**
   b. **For Start date, select today's date.**
   c. **For End date, click No end date.**
   d. **Change the Schedule settings to configure the task to run on Monday at 2:00 AM.**

   Note

   You can set the schedule to run when and as often as you want.

   e. **Confirm that all settings are correct in the Summary tab, then click Save.**

Results

That completes creating the server task to automatically run the two compliance queries, then save the output of the queries to CSV files.

Create a report to include query output best practice

Once you have the query data saved, you must create a report to contain the information from the queries you ran before you can send it to the administrator team.

Before you begin

You must know the format of the queries you are adding to the report.

In this example the queries have these formats:

- **VSE: Compliance Over the Last 30 Days** — Chart
- **Inactive Agents** — Table

Create a report that contains the data captured from your compliance queries, which is run automatically using a server task, then emailed to the administrators every Monday morning.

Task

1. **Select Menu → Reporting → Queries & Reports, then select the Report tab.**
2. **Click Actions → New.**
   A blank **Report Layout** page appears.
3. **Click Name and type a name for the report, click Description and, optionally, type a description, click Group, and select an appropriate group to receive the report, then click OK.**
4. **In the Report Layout pane, drag and drop these query input formats from the Toolbox list:**
   - For the **VSE: Compliance Over the Last 30 Days** chart query, drag the **Query Chart** tool into the **Report Layout** pane, then from the **Query Chart** list select **VSE: Compliance Over the Last 30 Days**, then click **OK**.

- For the **Inactive Agents** table query, drag the **Query Table** tool into the **Report Layout** pane, then from **Query** table list, select **Inactive Agents**, then click **OK**.

5. **Click Save, and the new compliance report is listed in the Reports tab.**
6. **To confirm that your report is configured correctly, click Run in the Actions column for your report, then verify that the Last Run Status displays Successful.**
7. **To see the report, click the link in the Last Run Result column, then open or save the report.**

Results

That completes creating the report to display the two compliance queries and save their output to a PDF file.

Create a server task to run and deliver a report: best practice

You must create a server task to automatically run the report and send the compliance report to your administrators.

Before you begin

You must have already:

- Created and scheduled a server task that runs the compliance queries.
- Created the report that includes the output of these queries.

Follow these steps to:

- Automatically run a report that contains the data captured from your compliance queries.
- Use a server task to email the report to the administrators every Monday morning at 5:00 a.m.

Task

1. **Select Menu → Automation → Server Tasks, then click Actions → New Task.**
2. **In the Server Task Builder, configure these settings, then click Next.**
   a. **In the Descriptions tab, type a name and notes.**
   b. **In the Schedule status, click Enabled.**
3. **In the Actions tab, select Run Report, configure these settings, then click Next.**
   a. **For Select a report to run, select the compliance report you configured.**
   b. **Select your language.**
   c. **For Sub-Actions, select Email file.**
   d. **For Recipients, type the email addresses of your administrators.**

      Note

      Separate multiple email addresses with commas.

   e. **For Subject, type the information you want to appear in the subject line of the email.**
4. **In the Schedule tab, change these settings, then click Next.**
   a. **For Schedule type, click Weekly.**
   b. **For Start date, select today's date.**
   c. **For End date, click No end date.**

d. **Change the Schedule settings to configure the task to run on Monday at 5:00 AM.**

Note

You can set the schedule to run when and as often as you want.

e. **Confirm that all settings are correct in the Summary tab, then click Save.**

Results

That completes the final task to create a compliance report that runs automatically and is delivered to your administrators every Monday morning at 5 a.m.

Repositories

Repositories house your security software packages and their updates for distribution to your managed systems.

Security software is only as effective as the latest installed updates. For example, if your DAT files are out of date, even the best anti-virus software cannot detect new threats. It is critical that you develop a strong updating strategy to keep your security software as current as possible.

The **Trellix ePO - On-prem** repository architecture offers flexibility to ensure that deploying and updating software is as easy and automated as your environment allows. Once your repository infrastructure is in place, create update tasks that determine how, where, and when your software is updated.

What repositories do

The agents on your managed systems obtain their security content from repositories on the **Trellix ePO - On-prem** server. This content keeps your environment up to date.

Repository content can include the following:

- Managed software to deploy to your clients
- Security content such as DATs and signatures
- Patches and any other software needed for client tasks that you create using **Trellix ePO - On-prem**

Unlike your server, repositories ***do not*** manage policies, collect events, or have code installed on them. A repository is nothing more than a file share located in your environment that your clients can access.

Repository types and what they do

To deliver products and updates throughout your network, **Trellix ePO - On-prem** software offers several types of repositories that create a strong infrastructure for updating.

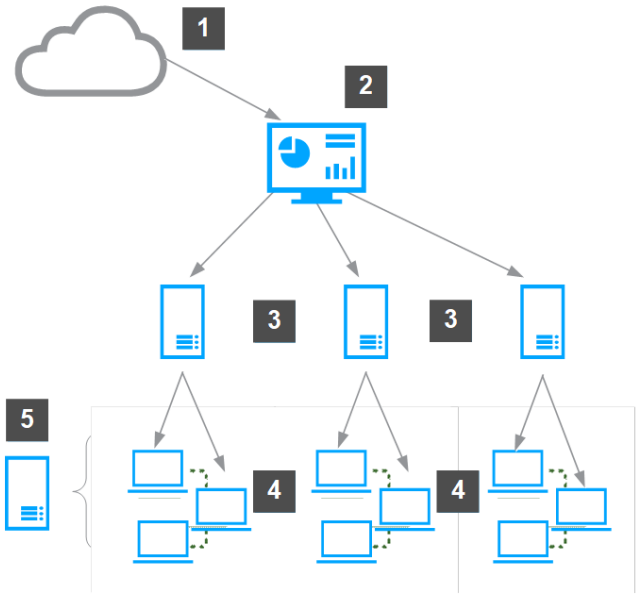
How repository components work together

The repositories work together in your environment to deliver updates and software to managed systems. Depending on the size and geographic distribution of your network, you might need distributed repositories.

1. **Source site —** The source site is updated daily by **Trellix**.
2. **Main Repository —** The Main Repository regularly pulls DAT and engine update files from the source site.
3. **Distributed repositories —** The Main Repository replicates the packages to distributed repositories in the network.
4. **Managed systems —** The managed systems in the network retrieve updates from a main or distributed repository.
5. **Fallback site —** If managed systems can't access the distributed repositories or the Main Repository, they retrieve updates from the fallback site.

These components give you the flexibility to develop an updating strategy so that your systems are always current.

Source sites and repositories delivering packages to systems



Source site

The source site provides all updates for your **Main Repository**. The default source site is the **Trellix http** update site, but you can change the source site or create multiple source sites.

We recommend using the **Trellix http** or **Trellix ftp** update sites as your source site.

Note

Source sites are not required. You can download updates manually and check them into your **Main Repository**. But, using a source site automates this process.

Trellix posts software updates to these sites regularly. For example, DAT files are posted daily. Update your **Main Repository** with updates as they are available.

Use pull tasks to copy source site contents to the **Main Repository**.

Trellix update sites provide updates to detection definition (DAT) and scanning engine files, and some language packs. Manually check in all other packages and updates, including service packs and patches, to the **Main Repository**.

Main Repository

The **Main Repository** maintains the latest versions of security software and updates for your environment. This repository is the source for the rest of your environment.

Note

By default, **Trellix ePO - On-prem** uses Microsoft Internet Explorer proxy settings.

Distributed repositories

Distributed repositories host copies of your **Main Repository**. Consider using distributed repositories and placing them throughout your network. This configuration ensures that managed systems are updated while network traffic is minimized, especially across slow connections.

As you update your **Main Repository**, **Trellix ePO - On-prem** replicates the contents to the distributed repositories.

Replication can occur:

- Automatically when specified package types are checked in to the **Main Repository**, as long as global updating is enabled.
- On a recurring schedule with **Replication** tasks.
- Manually, by running a **Replicate Now** task.

Caution

Do not configure distributed repositories to reference the same directory as your **Main Repository**. This locks the files on the **Main Repository**. This can cause failure for pulls and package check-ins, and can leave the **Main Repository** in an unusable state.

A large organization can have multiple locations with limited bandwidth connections between them. Distributed repositories help reduce updating traffic across low-bandwidth connections, or at remote sites with many endpoints. If you create a distributed repository in the remote location and configure the systems in that location to update from this distributed repository, the updates are copied across the slow connection only once — to the distributed repository — instead of once to each system in the remote location.

If global updating is enabled, distributed repositories update managed systems automatically, when selected updates and packages are checked in to the **Main Repository**. Update tasks are not needed. But, if you want automatic updating, create SuperAgents in your environment. Create and configure repositories and the update tasks.

Caution

If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. To avoid replicating a newly checked-in package, deselect it from each distributed repository or disable the replication task before checking in the package.

Fallback site

The fallback site is a source site enabled as the backup site. Managed systems can retrieve updates when their usual repositories are inaccessible. For example, when network outages or virus outbreaks occur, accessing the established location might be hard.

Managed systems can remain up-to-date using a fallback site. The default fallback site is the **Trellix http** update site. You can enable only one fallback site.

If managed systems use a proxy server to access the Internet, configure agent policy settings to use proxy servers when accessing the fallback site.

Repository branches and their purposes

You can use the three **Trellix ePO - On-prem** repository branches to maintain up to three versions of the packages in your main and distributed repositories.

The repository branches are **Current**, **Previous**, and **Evaluation**. By default, **Trellix ePO - On-prem** uses only the **Current** branch. You can specify branches when adding packages to your **Main Repository**. You can also specify branches when running or scheduling update and deployment tasks, to distribute different versions to different parts of your network.

Update tasks can retrieve updates from any branch of the repository, but you must select a branch other than the **Current** branch when checking in packages to the **Main Repository**. If a non-Current branch is not configured, the option to select a branch other than **Current** does not appear.

To use the **Evaluation** and **Previous** branches for packages other than updates, you must configure this in the **Repository Packages** server settings.

Current branch

The **Current** branch is the main repository branch for the latest packages and updates. Product deployment packages can be added only to the **Current** branch, unless support for the other branches has been enabled.

Evaluation branch

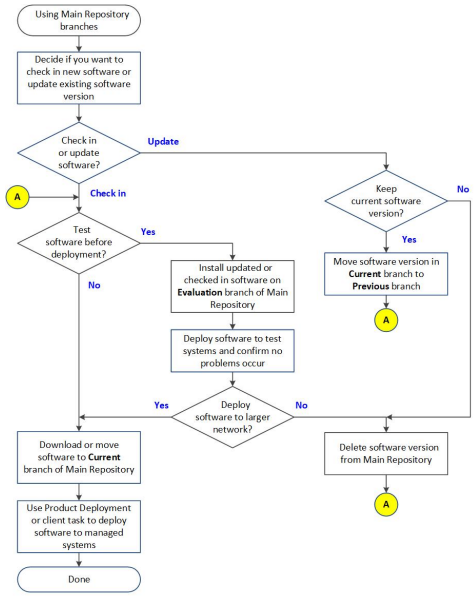
You might want to test new DAT and engine updates with a few network segments or systems before deploying them to your entire organization. Specify the **Evaluation** branch when checking in new DATs and engines to the **Main Repository**, then deploy them to a few test systems. After monitoring the test systems for several hours, you can add the new DATs to your **Current** branch and deploy them to your entire organization.

Previous branch

Use the Previous branch to save and store prior DAT and engine files before adding the new ones to the **Current** branch. If you experience an issue with new DAT or engine files in your environment, you have a copy of a previous version that you can redeploy to your systems if necessary. **Trellix ePO - On-prem** saves only the most immediate previous version of each file type.

You can populate the **Previous** branch by selecting **Move existing packages to Previous branch** when you add new packages to your **Main Repository**. The option is available when you pull updates from a source site and, when you manually check in packages to the **Current** branch.

This flowchart describes when to use these three different branches of the Main Repository.



Using repositories

Distributed repositories work as file shares that store and distribute security content for your managed endpoints.

Repositories play an important role in your **Trellix ePO - On-prem** infrastructure. How you configure repositories and deploy them depends on your environment.

Distributed repository types

Before you create distributed repositories, it is important to understand which type of repository to use in your managed environment.

The **Trellix ePO - On-prem** server always acts as the **Main Repository**. It keeps the primary copy of all content needed by your agents. The server replicates content to each of the repositories distributed throughout your environment. As a result, your agents can retrieve updated content from an alternate and closer source.

Note

Your **Trellix ePO - On-prem** server does not require configuration to make it the **Main Repository**. It is the **Main Repository** by default.

Distributed repository types include:

- FTP repositories
- HTTP repositories
- UNC share repositories

- SuperAgents

Consider the following when planning your distributed repositories:

- The **Trellix ePO - On-prem** server requires that you use certain protocols for the repositories, but any server vendor can provide those protocols. For example, if you use an HTTP repository, you can use either Microsoft Internet Information Services (IIS) or Apache server (Apache is the faster option).
- There is no operating system requirement for the systems that host your repository. As long as your **Trellix ePO - On-prem** server can access the folders you specify to copy its content to, and as long as the agents can connect to these folders to download their updates, everything works as expected.
- Your agent updates and **Trellix ePO - On-prem** replication tasks are only as good as your repositories. If you are already using one of these repositories and your environment works well, do not change the configuration.

Note

If you are starting with a new installation with no repositories, use a SuperAgent because they are easy to configure and are reliable.

Unmanaged repositories

If you are unable to use managed systems as distributed repositories, you can create and maintain unmanaged distributed repositories but a local administrator must keep the distributed files up-to-date manually.

Once the distributed repository is created, use **Trellix ePO - On-prem** to configure managed systems of a specific **System Tree** group to update from it.

Note

Manage all distributed repositories through **Trellix ePO - On-prem**. This ensures your managed environment is up to date. Use unmanaged distributed repositories only if your network or organization's policy doesn't allow managed distributed repositories.

FTP repositories

FTP servers can host a distributed Trellix ePO server repository. You might already have FTP servers in your environment, and you can store **Trellix** content there as well.

FTP repositories are:

- Fast
- Able to manage extensive loads from the clients pulling data
- Helpful in a DMZ where HTTP might not be optimal and UNC shares can't be used

Using FTP servers, your clients do not need authentication and can use an anonymous log on pull their content. No authentication reduces the chance that a client fails to pull its content.

You can use an FTP server to host a distributed repository. Use FTP server software, such as Microsoft Internet Information Services (IIS), to create a folder and site location for the distributed repository. See your web server documentation for details.

HTTP repositories

HTTP servers can host a distributed Trellix ePO server repository. You might already have HTTP servers in your environment.

HTTP servers can be fast serving out files to large environments. Your HTTP servers allow clients to pull their content without authentication, which reduces the chance that a client might fail to pull its content.

You can use an HTTP server to host a distributed repository. Use HTTP server software, such as Microsoft IIS, to create a folder and site location for the distributed repository. See your web server documentation for details.

UNC share repositories best practice

Universal Naming Convention (UNC) shares can host your Trellix ePO server repository.

You can create a UNC shared folder to host a distributed repository on an existing server. Make sure to enable sharing across the network for the folder, so that the **Trellix ePO - On-prem** server can copy files to it and agents can access it for updates.

Note

The correct permissions must be set to access the folder.

Because most administrators are familiar with the concept of UNC shares, UNC shares might seem like the easiest method to choose, but that's not always the case.

If you use UNC shares to host your Trellix ePO server repository, you must correctly configure the account and shares. See the *Recommendations for download credentials when using UNC shares as software repositories in ePolicy Orchestrator*, KB70999, for details.

If you choose to use UNC shares, you must:

1. Create the folder.
2. Adjust share permissions.
3. Change the NTFS permissions.
4. Create two accounts, one with read access and one with write access.

If your IT group has password rules, such as changing a password every 30 days even for service accounts, changing those passwords in Trellix ePO can be cumbersome. You must change the password for access to each of the distributed repository shares in the Windows operating system and in the configuration settings for each of the UNC Distributed Repositories in Trellix ePO. Access the Trellix ePO UNC Distributed Repositories settings using **Menu** → **Software** → **Distributed Repositories**.

All these tasks increase the chance of failure because these processes must be completed manually. Your agents might not properly update if your agents cannot authenticate to your UNC share because they are not part of the domain or the credentials are incorrect.

Best practice: SuperAgent repositories

You can create a **SuperAgent** repository to act as an intermediary between the Trellix ePO server and other agents.

The **SuperAgent** caches information received from a **Trellix ePO - On-prem** server, the Main Repository, or a mirrored Distributed Repository, and distributes it to the nearest agents. The Lazy Caching feature allows **SuperAgents** to retrieve data from **Trellix ePO - On-prem** servers only when requested by a local agent node. Creating a hierarchy of **SuperAgents** along with lazy caching further saves bandwidth and minimizes the wide-area network traffic.

A **SuperAgent** also broadcasts wake-up calls to other agents using that **SuperAgent** repository. When the **SuperAgent** receives a wake-up call from the **Trellix ePO - On-prem** server, it wakes up the agents using its repository connection.

Note

This is an alternative to sending ordinary wake-up calls to each agent in the network or sending an agent wake-up task to each computer.

For detailed information about **SuperAgents** and how to configure them, see the ***Trellix Agent*** *Product Guide*.

SuperAgent repositories

Use systems hosting SuperAgents as distributed repositories. SuperAgent repositories have several advantages over other types of distributed repositories:

- Folder locations are created automatically on the host system before adding the repository to the repository list.
- SuperAgent repositories don't require additional replication or updating credentials — account permissions are created when the agent is converted to a **SuperAgent**.

Tip

Although functionality of **SuperAgent** broadcast wake-up calls requires a **SuperAgent** in each broadcast segment, broadcast wake-up calls are not a requirement for the **SuperAgent** repository. But, managed systems must have access to the system hosting the repository.

SuperAgent considerations

When you configure systems as **SuperAgents**, follow these guidelines.

- Use existing file repositories in your environment, for example Microsoft System Center Configuration Manager (SCCM).
- You don't need a **SuperAgent** on every subnet.
- Turn off **Global Updating** to prevent unwanted updates of new engines or patches from the Main Repository.

SuperAgent and its hierarchy

A hierarchy of **SuperAgents** can serve agents in the same network with minimum network traffic utilization. A **SuperAgent** caches the content updates for the **Trellix ePO - On-prem** server or distributed repository and distributes content updates to the agents in the network, reducing the wide area network traffic. It is always ideal to have more than one **SuperAgent** to balance the network load.

You use the Repository policy to create the **SuperAgent** hierarchy. We recommend that you have a three-level hierarchy of **SuperAgents** in your network.

See ***Trellix Agent*** *Product Guide* for details about creating a hierarchy of SuperAgents, SuperAgent caching (lazy caching), and communication interruptions.

Create a SuperAgent

Creating a **SuperAgent** requires these tasks.

1. Create a new **SuperAgents** policy.
2. Create a new group in the **System Tree**, for example named **SuperAgents**
3. Assign the new **SuperAgent** policy to the new **SuperAgents** group.
4. Drag a system into the new **SuperAgents** group.

Once you have created the new **SuperAgents** group, you can drag any system into that group and it becomes a **SuperAgent** the next time it communicates with the **Trellix ePO - On-prem** server.

Create SuperAgent policy

To convert endpoints to **SuperAgents**, you must assign a SuperAgent policy to those systems.

Task

1. **Select Menu → Policy → Policy Catalog to open the Policy Catalog page.**
2. **To duplicate the My Default policy from the Product drop-down list, select McAfee Agent, and from the Category drop-down list, select General.**
3. **In the My Default policy row, in the Actions column, click Duplicate.**

   Note

   The **McAfee Default** policy cannot be changed.

4. **In the Duplicate Existing Policy dialog box, change the policy name, add any notes for reference, and click OK.**
5. **From the Policy Catalog page, click SuperAgents tab, select Convert agents to SuperAgents to convert the agent to a SuperAgent and update its repository with the latest content.**
6. **Select Use systems running SuperAgents as distributed repositories to use the systems that host SuperAgents as update repositories for the systems in its broadcast segment, then provide the Repository path.**
7. **Select Enable Lazy caching to allow the SuperAgents to cache content when it is received from the Trellix ePO - On-prem server.**

8. **Click Save.**

Best practice: Create a group in the System Tree

Adding a SuperAgent group to your **System Tree** allows you to assign a SuperAgent policy to the group.

Task

1. **Select Menu → Systems Section → System Tree, click System Tree Actions → New Subgroups, and give it a distinctive name, for example *SuperAgents*.**
2. **Click OK. The new group appears in the System Tree list.**

Best practice: Assign the new SuperAgents policy to the new SuperAgent group

Assigning the SuperAgent policy to the new group completes the configuration of the SuperAgent group.

Task

1. **In the System Tree, select the SuperAgent group that you created, select the Assigned Policies tab, then select McAfee Agent from the Product list.**
2. **From the Actions column for the General category, click Edit Assignment.**
3. **From the McAfee Agent: General page, click Break inheritance and assign the policy and settings below. Select the SuperAgent policy that you created from the Assigned Policy list, then click Save.**

Best practice: Assign a system to the new SuperAgent group

After the SuperAgent group is configured, you can assign the SuperAgent policies to individual endpoints by dragging them into that group. These policies convert the endpoints into SuperAgents.

Task

1. **In the System Tree, click the Systems tab and find the system that you want to change to a SuperAgent repository.**
2. **Drag that row with the system name and drop it into the new SuperAgent group you created in the System Tree.**
   Once the system communicates with the **Trellix ePO - On-prem** server, it changes to a SuperAgent repository.
3. **To confirm that the system is now a SuperAgent repository, select Menu → Software → Distributed Repositories and select SuperAgent from the Filter list. The new SuperAgent repository appears in the list.**

Note

Before the system appears as a SuperAgent in the group, two agent-server communications must occur. First, the system must receive the policy change and second, the agent must respond back to the **Trellix ePO - On-prem** server that is now a SuperAgent. This conversion might take some time depending on your ASCI settings.

Repository list files

The repository list files (**SiteList.xml** and **SiteMgr.xml**) contain the names of all repositories you are managing.

The repository list include the location and encrypted network credentials that managed systems use to select the repository and retrieve updates. The server sends the repository list to the **Trellix Agent** during agent-server communication.

If needed, you can export the repository list to external files (**SiteList.xml** or **SiteMgr.xml**). The two files have different uses:

SiteList.xml file

- Import to a **Trellix Agent** during installation.

SiteMgr.xml file

- Back up and restore your distributed repositories and source sites if you have to reinstall the server.
- Import the distributed repositories and source sites from a previous installation of the **Trellix ePO - On-prem** software.

Best practice: Where to place repositories

You must determine how many repositories are needed in your environment and where to locate them.

To answer these questions, you must look at your **Trellix ePO - On-prem** server managed systems and your network geography.

Consider the following factors:

- How many nodes do you manage with the **Trellix ePO - On-prem** server?
- Are these nodes located in different geographic locations?
- What connectivity do you have to your repositories?

Remember, the purpose of a repository is to allow clients to download the large amount of data in software updates locally instead of connecting to the **Trellix ePO - On-prem** server and downloading the updates across the slower WAN links. At a minimum, your repository is used to update your signature, or DAT files for **VirusScan Enterprise** daily. In addition, your repository is used by your agents to download new software, product patches, and other content, for example **Host Intrusion Prevention** content.

Typically you can create a repository for each large geographic location, but there are several caveats. Plus, you must avoid the most common mistakes of having too many or too few repositories and overloading your network bandwidth.

Best practice: Global Updating restrictions

Global Updating is a powerful feature, but if used incorrectly it can have a negative impact in your environment.

Global Updating is used to update your repositories as quickly as possible when the **Main Repository** changes. Global Updating is great if you have a smaller environment (fewer than 1,000 nodes) with no WAN links. Global Updating generates a huge amount of traffic that could impact your network bandwidth. If your environment is on a LAN, and bandwidth is not a concern, then use Global Updating. If you are managing a larger environment and bandwidth is critical, disable Global Updating.

Note

Global Updating is disabled by default when you install **Trellix ePO - On-prem** software.

To confirm the **Global Updating** setting, select **Menu** → **Configuration** → **Server Settings** and select **Global Updating** from the **Setting Categories** list. Confirm that the status is disabled. If not, click **Edit** and change the status.

If you are a user with a large environment and where bandwidth is critical, you can saturate your WAN links if you have Global Updating enabled. You might think having Global Updating enabled makes you receive their DATs quickly. But eventually, **Trellix**, for example releases an update to its **Trellix Endpoint Security (ENS)** engine that can be several megabytes, compared to the 400-KB DAT files. This engine update typically occurs twice a year. When that release occurs the **Trellix ePO - On-prem** server pulls the engine from **Trellix**, starts replicating it to the distributed repositories, and starts waking up agents to receive the new engine immediately. This engine update can saturate your WAN links and roll out an engine that you might prefer to upgrade in a staged release.

Note

If you have a large environment, you can still use Global Updating, but you must disable it when a new engine or product patch is released or the updates could saturate your WAN links.

For additional information see these KnowledgeBase articles:

- How to prevent **Trellix ePO - On-prem** 5.X from automatically updating to the latest posted Engine, KB77901
- **ePolicy Orchestrator - On-prem** prematurely deploys McAfee product software patch, KB77063

How Global Updating works

If your **Trellix ePO - On-prem** server is scheduled to pull the latest DATs from the **Trellix** website at 2 p.m. Eastern time (and the scheduled pull changes the contents of your **Main Repository**), your server automatically initiates the Global Update process to replicate the new content to all your distributed repositories.

The Global Updating process follows this sequence of events:

1. Content or packages are checked in to the **Main Repository**.
2. The **Trellix ePO - On-prem** server performs an incremental replication to all distributed repositories.
3. The **Trellix ePO - On-prem** server issues a wake-up call to all SuperAgents in the environment.
4. The SuperAgent broadcasts a global update message to all agents in the SuperAgent subnet.
5. Upon receipt of the broadcast, the agent is supplied with a minimum catalog version needed.
6. The agent searches the distributed repositories for a site that has this minimum catalog version.
7. Once a suitable repository is found, the agent runs the update task.

Setting up repositories for the first time

Follow these high-level steps when creating repositories for the first time.

1. Decide which types of repositories to use and their locations.
2. Create and populate your repositories.

Manage source and fallback sites best practice

You can change the default source and fallback sites from the **Server Settings**. For example, you can edit settings, delete existing source and fallback sites, or switch between them.

Note

You must be an administrator or have appropriate permissions to define, change, or delete source or fallback sites.

Use the default source and fallback sites. If you require different sites for this purpose, you can create new ones.

Create source sites

Create a source site from **Server Settings**.

Task

1. **Select Menu → Configuration → Server Settings, then select Source Sites.**
2. **Click Add Source Site. The Source Site Builder wizard appears.**
3. **On the Description page, type a unique repository name and select HTTP, UNC, or FTP, then click Next.**
4. **On the Server page, provide the web address and port information of the site, then click Next.**

   HTTP or FTP server type:

   - From the **URL** drop-down list, select **DNS Name**, **IPv4**, or **IPv6** as the type of server address, then enter the address.

Option	Definition
DNS Name	Specifies the DNS name of the server.
IPv4	Specifies the IPv4 address of the server.
IPv6	Specifies the IPv6 address of the server.

   - Enter the port number of the server: FTP default is 21; HTTP default is 80.

   UNC server type:

   - Enter the network directory path where the repository resides. Use this format: **\\<COMPUTER>\<FOLDER>**.

5. **On the Credentials page, provide the Download Credentials used by managed systems to connect to this repository.**
   Use credentials with read-only permissions to the HTTP server, FTP server, or UNC share that hosts the repository.

   HTTP or FTP server type:

   - Select **Anonymous** to use an unknown user account.
   - Select **FTP** or **HTTP authentication** (if the server requires authentication), then enter the user account information.

   UNC server type:

   - Enter domain and user account information.

6. **Click Test Credentials. After a few seconds, a confirmation message appears that the site is accessible to systems using the authentication information. If credentials are incorrect, check the:**

- User name and password.
- URL or path on the previous panel of the wizard.
- The HTTP, FTP or UNC site on the system.

7. **Click Next.**
8. **Review the Summary page, then click Save to add the site to the list.**

Switch source and fallback sites best practice

Use **Server Settings** to change source and fallback sites.

Depending on your network configuration, you might want to switch the source and fallback sites if you find that HTTP or FTP updating works better.

Task

1. **Select Menu → Configuration → Server Settings.**
2. **Select Source Sites, then click Edit. The Edit Source Sites page appears.**
3. **From the list, locate the site that you want to set as fallback, then click Enable Fallback.**

Edit source and fallback sites best practice

Use **Server Settings** to edit the settings of source or fallback sites, such as URL address, port number, and download authentication credentials.

Task

1. **Select Menu → Configuration → Server Settings.**
2. **Select Source Sites, then click Edit.**
3. **Locate the site in the list, then click the name of the site.**
4. **From the Source Site Builder, edit the settings on the builder pages as needed, then click Save.**

Delete source sites or disabling fallback sites best practice

If a source or fallback site is no longer in use, delete or disable the site.

Task

1. **Select Menu → Configuration → Server Settings.**
2. **Select Source Sites, then click Edit. The Edit Source Sites page appears.**
3. **Click Delete next to the required source site. The Delete Source Site dialog box appears.**
4. **Click OK.**

Results

The site is removed from the **Source Sites** page.

Verify access to the source site best practice

You must make sure that the **Trellix ePO - On-prem Main Repository** and managed systems can access the Internet when using the TrellixHttp and TrellixFtp sites as source and fallback sites.

This section describes the tasks for configuring the connection the **Trellix ePO - On-prem Main Repository** and the **Trellix Agent** use to connect to the download site directly or via a proxy. The default selection is **Do not use proxy**.

Configure proxy settings

To update your repositories, configure proxy settings to pull DATs.

Task

1. **Select Menu → Configuration → Server Settings.**
2. **From the list of setting categories, select Proxy Settings, then click Edit.**
3. **Select Configure the proxy settings manually.**
    a. **Next to Proxy server settings, select whether to use one proxy server for all communication, or different proxy servers for HTTP and FTP proxy servers. Type the IP address or fully-qualified domain name and the port number of the proxy server.**

    Note

    If you are using the default source and fallback sites, or if you configure another HTTP source site and FTP fallback site, configure both HTTP and FTP proxy authentication information here.

    b. **Next to Proxy authentication, configure the settings according to whether you pull updates from HTTP repositories, FTP repositories, or both.**
    c. **Next to Exclusions, select Bypass Local Addresses, then specify distributed repositories that the server can connect to directly by typing the IP addresses or the fully-qualified domain name of those systems, separated by semicolons.**
    d. **Next to Exclusions, select Bypass Local Addresses, then specify distributed repositories that the server can connect to directly by typing the IP addresses or the fully-qualified domain name of those systems, separated by semicolons.**
4. **Click Save.**

Configure proxy settings for the Trellix Agent

Configure the proxy settings the **Trellix Agent** uses to connect to the download site.

Task

1. **Select Menu → Policy → Policy Catalog, then from the Product list click Trellix Agent , and from the Category list, select Repository.**
   A list of agents configured for the Trellix ePO server appears.
2. **On the My Default agent, click Edit Settings.**

The **edit settings** page for the **My Default** agent appears.

3. **Click the Proxy tab.**
   The **Proxy Settings** page appears.
4. **Select Use Internet Explorer settings (Windows only) for Windows systems, and select Allow user to configure proxy settings, if appropriate.**
   There are multiple methods to configuring Internet Explorer for use with proxies. **Trellix** provides instructions for configuring and using **Trellix** products, but does not provide instructions for non-**Trellix** products. For information on configuring proxy settings, see Internet Explorer Help and Microsoft Support.
5. **Select Configure the proxy settings manually to configure the proxy settings for the agent manually.**
6. **Type the IP address or fully-qualified domain name and the port number of the HTTP or FTP source where the agent pulls updates. Select Use these settings for all proxy types to make these settings the default settings for all proxy types.**
7. **Select Specify exceptions to designate systems that do not require access to the proxy. Use a semicolon to separate the exceptions.**
8. **Select Use HTTP proxy authentication or Use FTP proxy authentication, then provide a user name and credentials.**
9. **Click Save.**

Configure settings for global updates best practice

Global updates automate repository replication in your network. You can use the **Global Updating** server setting to configure the content that is distributed to repositories during a global update.

Global updates are disabled by default. We recommend that you enable and use them as part of your updating strategy. You can specify a randomization interval and package types to be distributed during the update. The randomization interval specifies the time period in which all systems are updated. Systems are updated randomly in the specified interval.

Task

1. **Select Menu → Configuration → Server Settings, select Global Updating from the Setting Categories, then click Edit.**
2. **Set the status to Enabled and specify a Randomization interval between 0 and 32,767 minutes.**
3. **Specify which Package types to include in the global updates:**
   - **All packages** — Select this option to include all signatures and engines, and all patches and Service Packs.
   - **Selected packages** — Select this option to limit the signatures and engines, and patches and Service Packs included in the global update.

Note

When using global updating, schedule a regular pull task (to update the Main Repository) at a time when network traffic is minimal. Although global updating is much faster than other methods, it increases network traffic during the update.

Configure agent policies to use a distributed repository best practice

Customize how agents select distributed repositories to minimize bandwidth use.

Task

1. **Select Menu → Policy → Policy Catalog, then select the Product as McAfee Agent and Category as Repository.**
2. **Click an existing agent policy, then select the Repositories tab.**
3. **From Repository list selection, select either Use this repository list or Use other repository list.**
4. **Under Select repository by, specify the method to sort repositories:**
    - **Ping time** — Sends an ICMP ping to the closest five repositories (based on subnet value) and sorts them by response time.
    - **Subnet distance** — Compares the IP addresses of endpoints and all repositories and sorts repositories based on how closely the bits match. The more closely the IP addresses resemble each other, the higher in the list the repository is placed.

      Note

      You can set the **Maximum number of hops**.

    - **User order in repository list** — Selects repositories based on their order in the list.
5. **Modify settings in the Repository list as needed:**
    - Disable repositories by clicking **Disable** in the **Actions** field.
    - Click **Move to Top** or **Move to Bottom** to specify the order in which you want endpoints to select distributed repositories.
6. **Click Save when finished.**

Use SuperAgents as distributed repositories

Create and configure distributed repositories on systems that host **SuperAgent**s. **SuperAgent**s can minimize network traffic.

Important

To convert an agent to a **SuperAgent**, the agent must be part of a Windows domain.

Create SuperAgent distributed repositories

To create a **SuperAgent** repository, the **SuperAgent** system must have a **Trellix Agent** installed and running. We recommend using **SuperAgent** repositories with global updating.

This task assumes that you know where the **SuperAgent** systems are located in the **System Tree**. We recommend creating a **SuperAgent** tag so that you can easily locate the **SuperAgent** systems with the **Tag Catalog** page, or by running a query.

Task

1. **From the Trellix ePO - On-prem console, select Menu → Policy → Policy Catalog, then from the Product list click McAfee Agent, and from the Category list, select General.**

A list of available general category policies available for use on your **Trellix ePO - On-prem** server appears.

2. **Create a policy, duplicate an existing one, or open one that's already applied to systems that hosts a SuperAgent where you want to host SuperAgent repositories.**
3. **Select the General tab, then ensure Convert agents to SuperAgents (Windows only) is selected.**
4. **Select Use systems running SuperAgents as distributed repositories, then type a folder path location for the repository. This location is where the Main Repository copies updates during replication. You can use a standard Windows path, such as C:\SuperAgent\Repo.**

   Note

   All requested files from the agent system are served from this location using the agent's built-in HTTP webserver.

5. **Click Save.**
6. **Assign this policy to each system that you want to host a SuperAgent repository.**

Results

The next time the agent calls into the server, the new policy is retrieved. If you do not want to wait for the next agent-server communication interval, you can send an agent wake-up call to the systems. When the distributed repository is created, the folder you specified is created on the system if it did not exist.

In addition, the network location is added to the repository list of the **SiteList.xml** file. This network location makes the site available for updating by systems throughout your managed environment.

Replicate packages to SuperAgent repositories

Select which repository-specific packages are replicated to distributed repositories.

Task

1. **Select Menu → Software → Distributed Repositories.**
   A list of all distributed repositories appears.
2. **Locate and click the SuperAgent repository.**
   The **Distributed Repository Builder** opens.
3. **On the Package Types page, select the required package types.**

   Note

   Ensure that all packages required by any managed system using this repository are selected. Managed systems go to one repository for all packages — the task fails for systems that are expecting to find a package type that is not present. This feature ensures packages that are used only by a few systems are not replicated throughout your entire environment.

4. **Click Save.**

Delete SuperAgent distributed repositories

Remove SuperAgent distributed repositories from the host system and the repository list (SiteList.xml). New configurations take effect during the next agent-server communication.

Task

1. **From the Trellix ePO - On-prem console, click Menu → Policy → Policy Catalog, then click the name of the SuperAgent policy you want to modify.**
2. **On the General tab, deselect Use systems running SuperAgents as distributed repositories, then click Save.**

Note

To delete a limited number of your existing SuperAgent distributed repositories, duplicate the **Trellix** policy assigned to these systems and deselect **Use systems running SuperAgents as distributed repositories** before saving it. Assign this new policy as-needed.

Results

The SuperAgent repository is deleted and removed from the repository list. However, the agent still functions as a SuperAgent as long as you leave the **Convert agents to SuperAgents** option selected. Agents that have not received a new site list after the policy change continue to update from the SuperAgent that was removed.

Create and configure repositories on FTP or HTTP servers and UNC shares

You can host distributed repositories on existing FTP or HTTP servers, or UNC shares. Although a dedicated server is not required, the system must be robust enough to handle the load when your managed systems connect for updates.

Create a folder location

Create the folder that hosts repository contents on the distributed repository system. Different processes are used for UNC share repositories and FTP or HTTP repositories.

Task

- **For UNC share repositories, create the folder on the system and enable sharing.**
- **For FTP or HTTP repositories, use your existing FTP or HTTP server software, such as Microsoft Internet Information Services (IIS), to create a folder and site location. See your web server documentation for details.**

Add the distributed repository to Trellix ePO - On-prem

Add an entry to the repository list and specify the folder the new distributed repository uses.

Caution

Do not configure distributed repositories to reference the same directory as your **Main Repository**. Doing so locks files on the **Main Repository**, causing pulls and package check-ins to fail and leaving the **Main Repository** in an unusable state.

Task

1. **Select Menu → Software → Distributed Repositories, then click Actions → New Repository. The Distributed Repository Builder opens.**
2. **On the Description page, type a unique name and select HTTP, UNC, or FTP, then click Next. The name of the repository does not need to be the name of the system hosting the repository.**
3. **On the Server page, configure one of the following server types.**
   HTTP server type or **FTP server type**
   - From the **URL** drop-down list, select **DNS Name**, **IPv4**, or **IPv6** as the type of server address, then enter the address.

Option	Definition
DNS Name	Specifies the DNS name of the server.
IPv4	Specifies the IPv4 address of the server.
IPv6	Specifies the IPv6 address of the server.

   - Enter the port number of the server: HTTP default is 80. FTP default is 21.
   - For HTTP server types, specify the Replication UNC path for your HTTP folder.

   UNC server type
   - Enter the network directory path where the repository resides. Use this format: **\\<COMPUTER>\<FOLDER>**.
4. **Click Next.**
5. **On the Credentials page:**
   a. **Enter Download credentials. Use credentials with read-only permissions to the HTTP server, FTP server, or UNC share that hosts the repository.**
      HTTP or FTP server type
      - Select **Anonymous** to use an unknown user account.
      - Select **FTP** or **HTTP authentication** (if the server requires authentication), then enter the user account information.

      UNC server type
      - Select **Use credentials of logged-on account** to use the credentials of the currently logged-on user.
      - Select **Enter the download credentials**, then enter domain and user account information.

   b. **Click Test Credentials. After a few seconds, a confirmation message appears, stating that the site is accessible to systems using the authentication information. If credentials are incorrect, check the following:**
      - User name and password

- URL or path on the previous panel of the Builder
- HTTP, FTP, or UNC site on the system

6. **Enter Replication credentials.**
   The server uses these credentials when it replicates DAT files, engine files, or other product updates from the **Main Repository** to the distributed repository. These credentials must have both read and write permissions for the distributed repository:
   - For **FTP**, enter the user account information.
   - For **HTTP** or **UNC**, enter domain and user account information.
   - Click **Test Credentials**. After a few seconds, a confirmation message appears that the site is accessible to systems using the authentication information. If credentials are incorrect, check the following:
     - User name and password
     - URL or path on the previous panel of the Builder
     - HTTP, FTP, or UNC site on the system
7. **Click Next. The Package Types page appears.**
8. **Select whether to replicate all packages or selected packages to this distributed repository, then click Next.**
   - If you choose the **Selected packages** option, manually select the **Signatures and engines** and **Products, patches, service packs, etc.** you want to replicate.
   - Optionally select to **Replicate legacy DATs**.

Note

Ensure all packages required by managed systems using this repository are not deselected. Managed systems go to one repository for all packages — if a needed package type is not present in the repository, the task fails. This feature ensures packages that only a few systems use are not replicated throughout your whole environment.

9. **Review the Summary page, then click Save to add the repository. The Trellix ePO - On-prem software adds the new distributed repository to its database.**

Avoid replication of selected packages

If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. Depending on your requirements for testing and validating, you might want to avoid replicating some packages to your distributed repositories.

Task

1. **Select Menu → Software → Distributed Repositories, then click a repository. The Distributed Repository Builder wizard opens.**
2. **On the Package Types page, deselect the package that you want to avoid being replicated.**
3. **Click Save.**

Disable replication of selected packages

If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. To disable the impending replication of a package, disable the replication task before checking in the package.

Task

1. **Click Menu → Automation → Server Tasks, then select Edit next to a replication server task.**
   The **Server Task Builder** opens.
2. **On the Description page, select the Schedule status as Disabled, then click Save.**

Enable folder sharing for UNC and HTTP repositories

On an HTTP or UNC distributed repository, you must enable the folder for sharing across the network, so that your **Trellix ePO - On-prem** server can copy files to the repository.

Task

1. **On the managed system, locate the folder you created using Windows Explorer.**
2. **Right-click the folder, then select Sharing.**
3. **On the Sharing tab, select Share this folder.**
4. **Configure share permissions as needed.**
   Systems updating from the repository require only read access, but administrator accounts, including the account used by the **Trellix ePO - On-prem** server service, require write access. See your Microsoft Windows documentation to configure appropriate security settings for shared folders.
5. **Click OK.**

Edit distributed repositories

Edit a distributed repository configuration, authentication, and package selection options as needed.

Task

1. **Select Menu → Software → Distributed Repositories, then click a repository.**
   The **Distributed Repository Builder** wizard opens, displaying the details of the distributed repository.
2. **Change configuration, authentication, and package selection options as needed.**
3. **Click Save.**

Delete distributed repositories

Delete **HTTP**, **FTP**, or **UNC** distributed repositories.

Task

1. **Click Menu → Software → Distributed Repositories, then click Delete next to a repository.**
2. **On the Delete Repository dialog box, click OK.**

Note

Deleting the repository does not delete the packages on the system hosting the repository.

Results

Deleted repositories are removed from the repository list.

Using UNC shares as distributed repositories

Follow these guidelines when using UNC shares as distributed repositories.

UNC shares use the Microsoft Server Message Block (SMB) protocol to create a shared drive. Create a user name and password to access this share.

Correctly configure the share

Make sure that the UNC share is correctly configured.

- **Use an alternate method to write to your repository** — Log on to the server using other methods (another share, RDP, locally) to write to your repository. Do not mix the repository you read from with the repository you write to. Read credentials are shared with endpoints, and write credentials are used exclusively by the **Trellix ePO - On-prem** server to update your distributed repository content.
- **Do not use a share on your Domain Controller** — Create a share off your domain controller. A local user on a domain controller is a domain user.

Secure the account you use to read from the UNC share

Follow these guidelines to make sure the account used to access the UNC share is secure.

- **Grant your UNC share account read-only rights for everyone except the Trellix ePO - On-prem server main repository** — When you set up your share, make sure that the account you created has read-only rights to the directory and to the share permissions. Do not grant remote writing to the share (even for administrators or other accounts). The only account allowed access is the account you recently created.

  Important

  The **Trellix ePO - On-prem** server Main Repository must be able to write files to the UNC share account.

- **Create the account locally** — Create the account on the file share, not on the domain. Accounts created locally do not grant rights to systems in the domain.
- **Use a specific account** — Create an account specifically for sharing repository data. Do not share this account with multiple functions.
- **Make the account low privilege** — Do not add this account to any groups it does not need, which includes "Administrators" and "Users" groups.
- **Disable extraneous privileges** — This account does not need to log on to a server. It is a placeholder to get to the files. Examine this account's permissions and disable any unnecessary privileges.

- **Use a strong password** — Use a password with 8–12 characters, using multiple character attributes (lowercase and uppercase letters, symbols, and numbers). We recommend using a random password generator so that your password is complex.

Protect and maintain your UNC share

- **Firewall your share** — Always block unnecessary traffic. We recommend blocking outgoing and incoming traffic. You can use a software firewall on the server or a hardware firewall on the network.
- **Enable File Auditing** — Always enable security audit logs to track access to your network shares. These logs display who accesses the share, and when and what they did.
- **Change your passwords** — Change your password often. Make sure that the new password is strong, and remember to update your **Trellix ePO - On-prem** configuration with the new password.
- **Disable the account and share if it's no longer used** — If you switch to a different repository type other than UNC, remember to disable or delete the account, and close and remove the share.

Use local distributed repositories that are not managed

Copy contents from the Main Repository into an unmanaged distributed repository.

Once an unmanaged repository is created, you must manually configure managed systems to go to the unmanaged repository for files.

Task

1. **Copy all files and subdirectories in the Main Repository folder from the server.**
   For example, using a Windows 2008 R2 Server, this path is the default path on your server: **C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Software**
2. **Paste the copied files and subfolders in your repository folder on the distributed repository system.**
3. **Configure an agent policy for managed systems to use the new unmanaged distributed repository:**
   a. **Select Menu → Policy → Policy Catalog, then select the Product as McAfee Agent and Category as Repository.**
   b. **Click an existing agent policy or create an agent policy.**

      Caution

      Policy inheritance cannot be broken at the level of option tabs that constitute a policy. Therefore, when you apply this policy to systems, ensure that only the correct systems receive and inherit the policy to use the unmanaged distributed repository.

   c. **On the Repositories tab, click Add.**
   d. **Type a name in the Repository Name text field.**
      The name does not have to be the name of the system hosting the repository.
   e. **Under Retrieve Files From, select the type of repository.**
   f. **Under Configuration, type the location of the repository using appropriate syntax for the repository type.**
   g. **Type a port number or keep the default port.**
   h. **Configure authentication credentials as needed.**
   i. **Click OK to add the new distributed repository to the list.**

j. **Select the new repository in the list.**
The type **Local** indicates it is not managed by the **Trellix ePO - On-prem** software. When an unmanaged repository is selected in the **Repository list**, the **Edit** and **Delete** buttons are enabled.
k. **Click Save.**

Results

Any system where this policy is applied receives the new policy at the next agent-server communication.

Work with the repository list files

You can export the repository list files.

- **SiteList.xml** — Used by the agent and supported products.
- **SiteMgr.xml** — Used when reinstalling the **Trellix ePO - On-prem** server, or for importing into other **Trellix ePO - On-prem** servers that use the same distributed repositories or source sites.

Export the repository list SiteList.xml file

Export the repository list (**SiteList.xml**) file for manual delivery to systems, or for import during the installation of supported products.

Task

1. **Select Menu → Software → Main Repository, then click Actions → Export Sitelist.**
The **File Download** dialog box appears.
2. **Click Save, browse to the location to save the SiteList.xml file, then click Save.**

Results

Once you have exported this file, you can import it during the installation of supported products. For instructions, see the installation guide for that product.

You can also distribute the repository list to managed systems, then apply the repository list to the agent.

Export the repository list for backup or use by other servers

Use the exported **SiteMgr.xml** file to restore distributed repositories and source sites. Restore when you reinstall the **Trellix ePO - On-prem** server, or when you want to share distributed repositories or source sites with another **Trellix ePO - On-prem** server.

You can export this file from either the **Distributed Repositories** or **Source Sites** pages. However, when you import this file to either page, it imports only the items from the file that are listed on that page. For example, when this file is imported to the **Distributed Repositories** page, only the distributed repositories in the file are imported. Therefore, if you want to import both distributed repositories and source sites, you must import the file twice, once from each page.

Task

1. **Select Menu → Software → Distributed Repositories (or Source Sites), then click Actions | Export Repositories (or Export Source Sites).**

The **File Download** dialog box appears.

2. **Click Save, browse to the location to save the file, then click Save.**

Import distributed repositories from the repository list

Import distributed repositories from the **SiteMgr.xml** file after reinstalling a server, or when you want one server to use the same distributed repositories as another server.

Note

It is not recommended to import distributed repositories from another server unless the server is inactive and you want to use the existing repositories.

Task

1. **Select Menu → Software → Distributed Repositories, then click Actions → Import Repositories.**
   The **Import Repositories** page appears.
2. **Browse to select the exported SiteMgr.xml file, then click OK. The distributed repository is imported into the server.**
3. **Click OK.**

Results

The selected repositories are added to the list of repositories on this server.

Import source sites from the SiteMgr.xml file

After reinstalling a server, and when you want two servers to use the same distributed repositories, import source sites from a repository list file.

Task

1. **Select Menu → Configuration → Server Settings, then from the Setting Categories list select Source Sites and click Edit.**
2. **Click Import.**
3. **Browse to and select the exported SiteMgr.xml file, then click OK.**
4. **Select the source sites to import into this server, then click OK.**

Results

The selected source sites are added to the list of repositories on this server.

Change credentials on multiple distributed repositories

Change credentials on multiple distributed repositories of the same type. Doing so is valuable in environments where there are many distributed repositories.

Task

1. **Select Menu → Distributed Repositories.**
2. **Click Actions and select Change Credentials.**

The **Change Credentials** wizard opens to the **Repository Type** page.

3. **Select the type of distributed repository for which you want to change credentials, then click Next.**
4. **Select the distributed repositories you want, then click Next.**
5. **Edit the credentials as needed, then click Next.**
6. **Review the information, then click Save.**

Pulling tasks

Use pull tasks to update your **Main Repository** with DAT and Engine update packages from the source site.

DAT and Engine files must be updated often. **Trellix** releases new DAT files daily, and Engine files less frequently. Deploy these packages to managed systems as soon as possible to protect them against the latest threats.

You can specify which packages are copied from the source site to the **Main Repository**.

Note

Extra.DAT files must be checked in to the Main Repository manually. They are available from the **Trellix** website.

A scheduled repository pull server task runs automatically and regularly at the times and days you specify. For example, you can schedule a weekly repository pull task at 5:00 a.m. every Thursday.

You can also use the **Pull Now** task to check updates into the **Main Repository** immediately. For example, when **Trellix** alerts you to a fast-spreading virus and releases a new DAT file to protect against it.

If a pull task fails, you must check the packages into the Main Repository manually.

Once you have updated your **Main Repository**, you can distribute these updates to your systems automatically with global updating or with replication tasks.

Considerations when scheduling a pull task

Consider these variables when scheduling pull tasks:

- **Bandwidth and network usage** — If you are using global updating, as recommended, schedule a pull task to run when bandwidth usage by other resources is low. With global updating, the update files are distributed automatically after the pull task finishes.
- **Frequency of the task** — DAT files are released daily, but you might not want to use your resources daily for updating.
- **Replication and update tasks** — Schedule replication tasks and client update tasks to ensure that the update files are distributed throughout your environment.

Source Sites page (Pull Now)

Use this page to configure and run a pull task immediately. Pull tasks allow you to specify the source or fallback site where you want to retrieve packages. The packages are then integrated into the specified branches in the **Main Repository**.

Option definitions

Option	Definition
Branch	Specifies the branch into which you want packages copied. • **Current** — Use the Current branch when you want the package available to managed systems in your production environment. • **Evaluation** — Use the **Evaluation branch** when you want to test the package on a limited number of systems before making it available to the larger environment. • **Previous** — Use the **Previous branch** to keep previous versions of packages for rollback purposes.
Options	Specifies the options available while pulling content from a source site, including: • **Move the existing package to the Previous branch** — When selected, moves packages in the **Main Repository** from the **Current branch** to the **Previous branch**. Available only when you select **Current** in **Repository branch**.
Source site	Specifies the source site from which to retrieve packages, including: • **TrellixHttp** — Specifies the address of the default HTTP server, where the packages are downloaded. • **TrellixFtp** — Specifies the address of the default FTP server, where the packages are downloaded. .

Package Selection page (Pull Now builder)

Use this page to select the software packages that you want to copy from the source site.

Option definitions

Option	Definition
Package options	Specifies whether to pull all packages or only selected packages.
Package types	Specifies the packages by type that are copied from the source site. These package types are all available for deployment.

Summary page (Pull Now)

Review the selections for this task before starting it.

Option definitions

Option	Definition
Source site	Specifies the source site from which you are pulling content into the **Main Repository**.
Check-in-Branch	Specifies the branch of the **Main Repository** to which contents are copied.
Package types	Specifies the specific types of package that are copied from the source site.
Options	Specifies the options available while pulling content from a source site.
Start Pull	Click to begin pulling content.

Replication tasks

Use replication tasks to copy the contents of the **Main Repository** to distributed repositories.

Unless you have replicated **Main Repository** contents to all your distributed repositories, some systems do not receive them. Make sure that all your distributed repositories are up-to-date.

Note

If you are using global updating for all your updates, replication tasks might not be necessary for your environment, although they are recommended for redundancy. However, if you are not using global updating for any of your updates, you must schedule a Repository Replication server task or run a Replicate Now task.

Scheduling regular Repository Replication server tasks is the best way to ensure that your distributed repositories are up-to-date. Scheduling daily replication tasks ensures that managed systems stay up-to-date. Using Repository Replication tasks automates replication to your distributed repositories.

Occasionally, you might check in files to your **Main Repository** that you want to replicate to distributed repositories immediately, rather than wait for the next scheduled replication. Run a Replicate Now task to update your distributed repositories manually.

Full vs. incremental replication

When creating a replication task, select **Incremental replication** or **Full replication**. Incremental replication uses less bandwidth and copies only the new updates in the **Main Repository** that are not yet in the distributed repository. Full replication copies the entire contents of the **Main Repository**.

Note

Schedule a daily incremental replication task. Schedule a weekly full replication task if it is possible for files to be deleted from the distributed repository outside of the replication functionality of the **Trellix ePO - On-prem** software.

Repository selection

New distributed repositories are added to the repository list file containing all available distributed repositories. The agent of a managed system updates this file each time it communicates with the **Trellix ePO - On-prem** server. The agent performs repository selection each time the agent service starts, and when the repository list changes.

Selective replication provides more control over the updating of individual repositories. When scheduling replication tasks, you can choose:

- Specific distributed repositories to which the task applies. Replicating to different distributed repositories at different times lessens the impact on bandwidth resources. These repositories can be specified when you create or edit the replication task.
- Specific files and signatures that are replicated to the distributed repositories. Selecting only those types of files that are necessary to each system that checks in to the distributed repository lessens the impact on bandwidth resources. When you define or edit your distributed repositories, you can choose which packages you want to replicate to the distributed repository.

Note

This functionality is intended for updating only products that are installed on several systems in your environment, like **VirusScan Enterprise**. The functionality allows you to distribute these updates only to the distributed repositories these systems use.

How agents select repositories

By default, agents can attempt to update from any repository in the repository list file. The agent can use a network ICMP ping or subnet address compare algorithms to find the distributed repository with the quickest response time. Usually, this is the distributed repository closest to the system on the network.

You can also control which distributed repositories agents use for updating by enabling or disabling distributed repositories in the agent policy settings. It is recommended not to disable repositories in the policy settings. Allowing agents to update from any distributed repository ensures that they receive the updates.

Agent Handlers

Agent Handlers route communication between agents and your **Trellix ePO - On-prem** server.

Each **Trellix ePO - On-prem** server contains a primary Agent Handler. Additional Agent Handlers can be installed on systems throughout your network.

Setting up more Agent Handlers provides the following benefits.

- Helps manage an increased number of products and systems managed by a single, logical **Trellix ePO - On-prem** server in situations where the CPU on the database server is not overloaded.
- Provides fault tolerant and load-balanced communication with many agents, including geographically distributed agents.

How Agent Handlers work

Agent Handlers distribute network traffic generated by agent-server communication by directing managed systems or groups of systems to report to a specific Agent Handler. Once assigned, a managed system communicates with the assigned Agent Handler instead of with the main **Trellix ePO - On-prem** server.

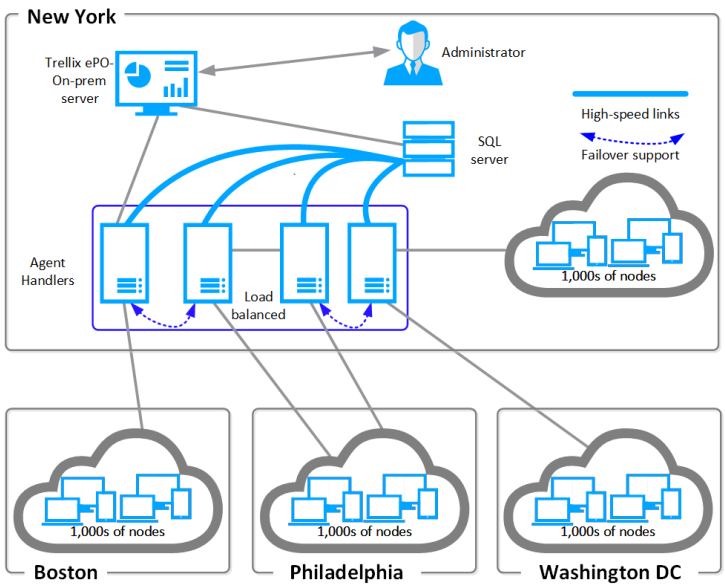
The handler provides updated sitelists, policies, and policy assignment rules, just as the **Trellix ePO - On-prem** server does. The handler also caches the contents of the Main Repository, so that agents can pull product update packages, DATs, and other needed information.

Note

If the handler doesn't have the updates needed when an agent checks in, the handler retrieves them from the assigned repository and caches them, while passing the update through to the agent.

This diagram shows some of the typical connections between **Agent Handlers**, the **Trellix ePO - On-prem** server, and the **Trellix ePO - On-prem** SQL Server.

Agent Handlers in an enterprise network



In this diagram, all **Agent Handlers**:

- Are connected to the **Trellix ePO - On-prem** SQL Server using low-latency high-speed links
- Are located close to the database they write to
- Have failover configured between **Agent Handlers**
- Are managed from the **Trellix ePO - On-prem** server

The **Agent Handlers** in these cities have specific configurations.

Note

A low-latency high-speed link's round-trip latency must be less than about 10 ms. Use the Windows **tracert** command to confirm the round-trip time (RTT) from the Agent Handler to the **Trellix ePO - On-prem** SQL Server.

- **Boston** — The **Agent Handler** for Boston is configured with failover support to the **Agent Handler** for Philadelphia.
- **Philadelphia** — The two **Agent Handlers** have load balancing configured.
- **Washington DC** — The **Agent Handler** uses specific ports to connect to the **Trellix ePO - On-prem** server from behind a firewall.

The Agent Handler must be able to authenticate domain credentials. Or the Agent Handler uses SQL authentication to authenticate to the database. For more information about Windows and SQL authentication, see the Microsoft SQL Server documentation.

For more information about changing authentication modes, see the Microsoft SQL Server documentation. If you do, you must also update the SQL Server connection information.

Run the query **Systems per Agent Handler** to display all Agent Handlers installed and the number of agents managed by each Agent Handler.

When an Agent Handler is uninstalled, it is not displayed in this chart. If an Agent Handler assignment rule exclusively assigns agents to an Agent Handler and if that Agent Handler is uninstalled, it is displayed in the chart with **Uninstalled Agent Handler** and the number of agents still trying to contact this Agent Handler.

If the Agent Handlers are not installed correctly, then the **Uninstalled Agent Handler** message is displayed which indicates that the handler cannot communicate with particular agents. Click the list to view the agents that cannot communicate with the handler.

Multiple Agent Handlers

You can have more than one Agent Handler in your network. You might have many managed systems spread across multiple geographic areas or political boundaries. Whatever the case, you can add an organization to your managed systems by assigning distinct groups to different handlers.

Agent Handler details

Agent Handlers provide specific features that can help grow your network to include many more managed systems.

When to use Agent Handlers

There are many reasons to use Agent Handlers in your network.

- **Hardware is cheaper** — The mid-range server hardware used for Agent Handlers is less expensive than the high-end servers used for **Trellix ePO - On-prem** servers.
- **Scalability** — As your network grows, Agent Handlers can be added to reduce the load on your **Trellix ePO - On-prem** server.

  Note

  Connect no more than five Agent Handlers to one **Trellix ePO - On-prem** server with a maximum of 50,000 nodes connected to each Agent Handler.

- **Network topology** — **Agent Handlers** can manage your agent requests behind a firewall or in an external network.
- **Failover** — Agents can failover between Agent Handlers using a configured fallback priority list.
- **Load Balancing** — Multiple Agent Handlers can load balance the **Trellix Agent** requests in a large remote network.

When *not* to use Agent Handlers

There are some instances not to use Agent Handlers.

- **As distributed repositories** — Repositories, for example SuperAgents, distribute large files throughout an organization. Repositories do not contain any logic. Agent Handlers use logic to communicate events back to the database. These events tell the **Trellix Agent** when to download new products from the distributed repositories. Agent Handlers can

cache files from the distributed repositories, but don't use them to replace distributed repositories. Agent Handlers are used to reduce the event management load on the **Trellix ePO - On-prem** server.

- **Through a slow or irregular connection** — Agent Handlers require a relatively high speed, low latency connection to the database to deliver events sent by the agents.
- **To save bandwidth** —Agent Handlers do not save bandwidth. They actually increase bandwidth use over the WAN connection that connects the clients to the Agent Handler. Use distributed repositories to save bandwidth.

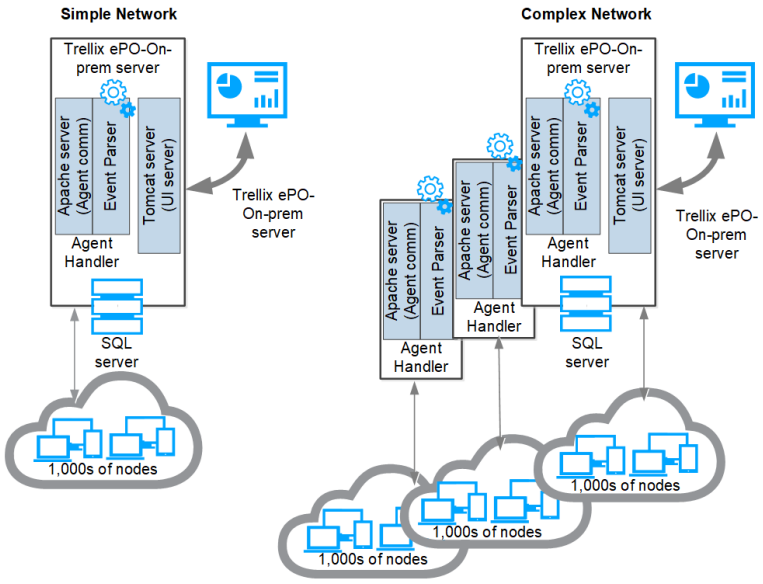
How Agent Handlers work

Agent Handlers use a work queue in the **Trellix ePO - On-prem** database as their primary communication mechanism.

Agent Handlers check the server work queue every 10 seconds and perform the requested action. Typical actions include wake-up calls, requests for product deployment, and data channel messages. These frequent communications to the database require relatively high speed, low latency connection between the Agent Handler and the **Trellix ePO - On-prem** database.

An Agent Handler installation includes only the Apache Server and Event Parser services. You can deploy Agent Handlers on separate hardware, or virtual machines, that coexist in one logical **Trellix ePO - On-prem** infrastructure.

Agent Handler functional diagram



This diagram shows two different network configurations and their Agent Handlers.

- **Simple network** — The primary Agent Handler is installed as a part of the **Trellix ePO - On-prem** server. This is sufficient for many small **Trellix ePO - On-prem** installations; typically additional Agent Handlers are not required.
- **Complex network** — Multiple remote Agent Handlers are installed on separate servers connected to the **Trellix ePO - On-prem** server. Once installed, the additional Agent Handlers are automatically configured to work with the **Trellix ePO - On-prem** server to distribute the incoming agent requests. The **Trellix ePO - On-prem** console is also used to configure

Agent Handler Assignment rules to support more complex scenarios. For example, an Agent Handler behind the DMZ, firewall, or using network address translation (NAT).

Administrators can override the Agent Handler default behavior by creating rules specific to their environment.

Best practice: Agent Handlers eliminate multiple Trellix ePO - On-prem servers

Use **Agent Handlers** in different geographic regions instead of multiple **Trellix ePO - On-prem** servers.

Note

Multiple **Trellix ePO - On-prem** servers cause management, database duplication, and maintenance problems.

Use **Agent Handlers** to:

- Expand the existing **Trellix ePO - On-prem** infrastructure to handle more agents, more products, or a higher load due to more frequent agent-server communication.
- Ensure that agents continue to connect and receive policy, task, and product updates even if the **Trellix ePO - On-prem** server is unavailable.
- Expand **Trellix ePO - On-prem** management into disconnected network segments with high-bandwidth links to the **Trellix ePO - On-prem** database.

Usually, it is more efficient and less expensive to add an **Agent Handler** rather than a **Trellix ePO - On-prem** server.

Note

Use a separate **Trellix ePO - On-prem** server for ***separate*** IT infrastructures, ***separate*** administrative groups, or ***test*** environments.

Agent Handler functionality

Agent Handlers provide horizontal network scalability, failover protection, load balancing, and allow you to manage clients behind a DMZ, firewall, or using network address translation (NAT).

Providing scalability

Agent Handlers can provide scalability for **Trellix ePO - On-prem** managed networks as the number of clients and managed products grow.

One **Trellix ePO - On-prem** server can easily manage up to 200,000 systems with only the **VirusScan Enterprise** product installed. But, as the systems managed and the number of products integrated with your **Trellix ePO - On-prem** server increase the attempts to receive policies or send events to your server increase. This load increase also decreases the maximum number of systems manageable with the same **Trellix ePO - On-prem** server hardware.

Agent Handlers allow you to scale your **Trellix ePO - On-prem** infrastructure to manage more clients and products. You do this by adding Agent Handlers to manage an equivalent or larger number of agents with one logical **Trellix ePO - On-prem** deployment. By default, when you install the Agent Handlers software on a server, all Agent Handlers are used at the same order level unless custom assignment rules are created.

Failover protection with Agent Handlers best practice

Agent Handlers allow any **Trellix Agent** to receive policy and task updates and report events and property changes if the **Trellix ePO - On-prem** server is unavailable. For example, an upgrade or network problem.

Once multiple **Agent Handler** are deployed, they are available to agents as failover candidates. As long as the **Agent Handler** is connected to the database, it can continue serving agents. This includes any policy or task changes resulting from agent properties or from administrator changes before the **Trellix ePO - On-prem** server goes offline.

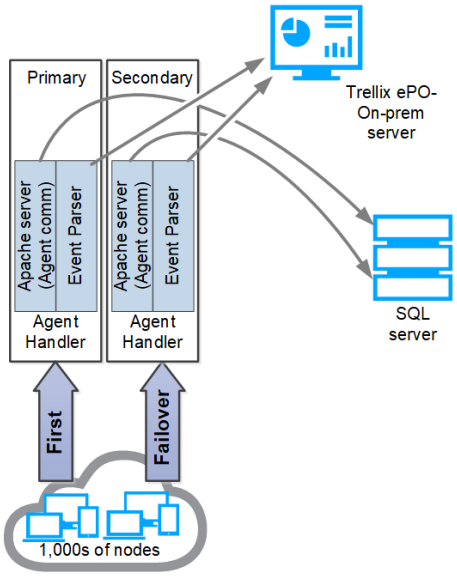
The configuration file shared with the **Trellix Agent** contains a configurable fallback list of **Agent Handlers**. If needed, the **Trellix Agent** tries to connect through the list of **Agent Handlers** until the list ends or it can contact a valid, enabled **Agent Handler**.

Failover between **Agent Handlers** is configured in one of two ways.

Simple deployment failover

In the simple deployment failover, two **Agent Handlers** can be deployed as primary and secondary. All agents initiate communications with the primary **Agent Handler**, and only use the secondary**Agent Handler** if the primary is unavailable. This deployment makes sense if the primary **Agent Handler** has better hardware, and can handle the whole load of the infrastructure.

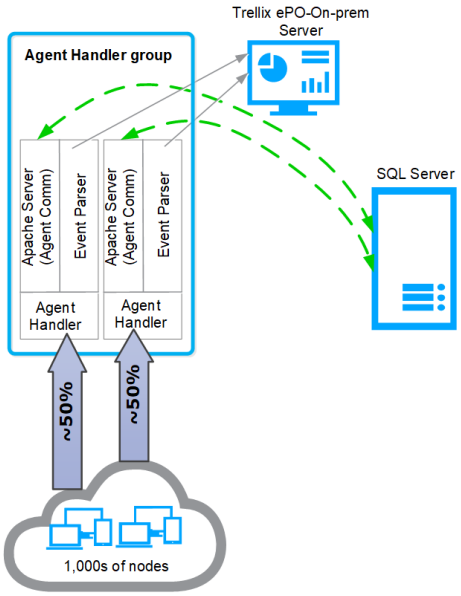
Simple **Agent Handler** failover



Failover with load balancing

The second deployment combines failover with load balancing. Multiple **Agent Handlers** are configured into the same **Agent Handler** group. The **Trellix ePO - On-prem** server inserts each **Agent Handler** in the group into the list of **Agent Handlers** at the same order level. The **Trellix Agent** randomizes **Agent Handlers** at the same order level, which results in an equal load across all **Agent Handlers** in a particular group.

Failover with Agent Handler load balancing



Agents failover between all **Agent Handlers** in a group before failing through to the next **Agent Handler** in the assignment list. Using **Agent Handler** groups results in both load balancing and failover benefits.

Network topology and deployment considerations

Using Agent Handlers behind a DMZ, firewall, or in NAT networks: best practices

Without Agent Handlers, any **Trellix Agent** behind a DMZ, firewall, or in a NAT network can be viewed with the **Trellix ePO - On-prem** server. But you can't manage or directly manipulate those systems in the NAT network.

With an Agent Handler behind the DMZ, you can address systems within the NAT region for wake-up calls, data channel access, and more.

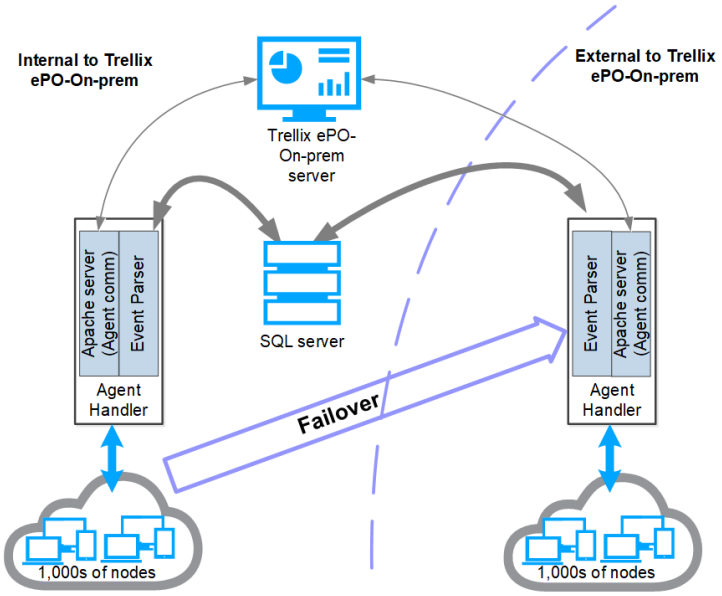
Note

This Agent Handler connection requires access to both the SQL database and the **Trellix ePO - On-prem** server. Some firewall rules are necessary for this configuration.

This diagram shows an Agent Handler with managed systems behind the DMZ and these connections:

- Data Channel connection to the **Trellix ePO - On-prem** server
- Low-latency high-speed connection to the SQL database
- Failover connection between the Agent Handlers

Agent Handler behind the DMZ



This table lists all ports used by the **Trellix ePO - On-prem** server and the other network components.

Important

The ports connecting the Agent Handler to the **Trellix ePO - On-prem** server and SQL database must be open to connect to the Agent Handler through a firewall.

Default ports used

Server	Direction	Connection	Port
Trellix ePO - On-prem	To	Web browser	HTTPS 8443
Trellix ePO - On-prem	To	SQL database	JDBC/SSL 1433
Agent Handler	From	**Trellix ePO - On-prem**	HTTPS 8443 (install), HTTPS 8444

Server	Direction	Connection	Port
Agent Handler	Both	**Trellix ePO - On-prem**	HTTP 80
Agent Handler	To	SQL database	ADO/SSL 1433
Agent Handler	To	Clients	HTTP 8081
Agent Handler	From	Clients	HTTP 80, HTTPS 443

Roaming with Agent Handlers

Agent Handlers allow users who roam between enterprise network sites to connect to the nearest Agent Handler.

Roaming is possible only if the Agent Handlers from all locations are configured in the **Trellix Agent** failover list. You can modify policy and system sorting so that roaming systems can receive a different policy in each location.

Repository cache and how it works

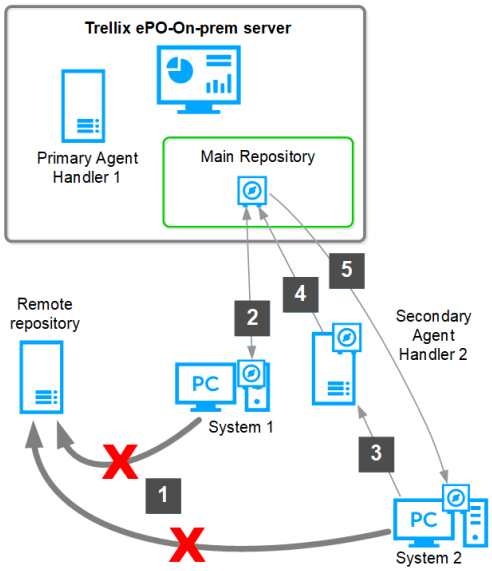
Agent Handlers automatically cache content and product updates if a **Trellix Agent** can't access the content directly from the **Main Repository** on the **Trellix ePO - On-prem** server.

The **Trellix Agent**, by default, uses the primary **Trellix ePO - On-prem** server (same server as Tomcat) as the Main Repository. Agents fail back to the Agent Handler if they are unable to communicate with their configured remote repository to pull content and product updates. Since the Agent Handler might not be running on the same server as the true **Main Repository** (on the **Trellix ePO - On-prem** server), the Agent Handler manages these requests. Agent Handlers transparently handle requests for software and cache the required files after downloading them from the **Main Repository**. No configuration is necessary.

1. Systems 1 and 2 attempt to pull content or product updates from their configured remote repository and the attempt fails.
2. For System 1, the **Trellix Agent** is configured, by default, to use Primary Agent Handler 1 that is part of the **Trellix ePO - On-prem** server. If the connection to the remote repository fails, System 1 requests the content or product updates directly from the **Main Repository** on the **Trellix ePO - On-prem** server.
3. For System 2, the **Trellix Agent** is configured to use Secondary Agent Handler 2, if the connection to the remote repository fails.
4. Secondary Agent Handler 2 requests the content or product updates from the Main Repository.
5. Secondary Agent Handler 2 caches those updates, for any subsequent requests, and delivers them to System 2.

This diagram shows how Agent Handlers cache product update content if the configured remote repository is unavailable to remote systems.

Agent Handler repository caching



Best Practices: Agent Handler installation and configuration

You can configure mid-range servers, located in your network, as Agent Handlers by simply installing the **Agent Handler** software and assigning systems for management.

You can also group **Agent Handlers**, set their failover priority, and create virtual **Agent Handlers** behind a DMZ, firewall, or in NAT networks.

Important

When you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change.

Deployment considerations

Before you deploy **Agent Handlers** in your extended network, consider the health of your existing **Trellix ePO - On-prem** server and database hardware. If this hardware is already overloaded, adding **Agent Handlers** actually decreases **Trellix ePO - On-prem** performance.

A fully configured **Agent Handler** has about the same hardware and database requirements as a **Trellix ePO - On-prem** server. When determining how many **Agent Handlers** you need, first examine the database usage. If the database serving your **Trellix ePO - On-prem** server is under a heavy load, adding **Agent Handlers** does not improve your performance. Upgrade your SQL Server hardware to take advantage of multiple **Agent Handlers**. If the database is currently running at a moderate to low load, then additional **Agent Handlers** can help you expand your logical **Trellix ePO - On-prem** infrastructure.

Trellix testing shows that adding **Agent Handlers** improves performance until your **Trellix ePO - On-prem** database CPU load exceeds 70 percent. Since each **Agent Handler** adds some overhead, for example database connections and management queries to the database, adding **Agent Handlers** beyond 70 percent database CPU load does not help performance.

Agent Handler configuration overview

Agent Handlers can be configured to load balance in groups and as virtual Agent Handlers.

Priority assignment rules enable clients to find Virtual Agent Handlers when the Agent Handlers are using different IP address on multiple network segments.

Configure Agent Handlers list

Use the **Handlers List** to see a list of your Agent Handlers and their detailed information,

Task

1. **Select Menu → Configuration → Agent Handlers.**
2. **Click the Agent Handlers number in the Handler Status of the dashboard, to see a list of your Agent Handlers and their detailed information.**
3. **Click the setting in the Actions column, to disable, enable, and delete Agent Handlers.**
4. **Click the Agent Handler name in the Handler DNS Name column to configure Agent Handler Settings.**
5. **From the Agent Handler Settings page, configure these properties.**
    - **Published DNS Name**
    - **Published IP Address**
6. **Click Save.**

Configure Agent Handlers groups and virtual groups

You can configure your **Agent Handlers** into groups and create virtual handlers to use behind a DMZ, firewall, or in NAT networks.

Task

1. **Select Menu → Configuration → Agent Handlers and, in the Handler Group dashboard, click New Group to create Agent Handler groups.**
2. **From the Agent Handlers Add/Edit Group page, configure these group settings:**
    - **Group Name** — Type a name for the **Agent Handler** group.
    - **Included Handlers** — Allows you to:
        - Click **Use load balancer** to use a third-party load balancer, then type the **Virtual DNS Name** and **Virtual IP address** in the fields (both are required).
        - Click **Use custom handler list** and use **+** and **–** to add and remove additional **Agent Handlers**. Use the drag-and-drop handle to change the priority of **Agent Handlers**.
3. **Click Save**

Configure Agent Handlers priority

You can configure the failover priority of your Agent Handlers by setting their failover priorities.

When you have multiple Agent Handlers, configure the primary Agent Handler in the **Trellix ePO - On-prem** Server as the lowest priority Agent Handler. This priority:

- Forces systems to connect to all other Agent Handlers before connecting to the primary **Trellix ePO - On-prem** Server Agent Handler
- Reduces the **Trellix ePO - On-prem** Server load so that it can perform other tasks like displaying the **Trellix ePO - On-prem** console user interface and running reports and server tasks

Task

1. **Select Menu → Configuration → Agent Handlers, then click Edit Priority to create Agent Handler groups.**
2. **Click and drag the Agent Handlers to create the priority list you need for your network.**
3. **Click Save.**

Configure assignments for Agent Handlers

You can assign agents to use **Agent Handlers** individually or as groups.

Tip

When assigning systems to **Agent Handlers**, consider geographic proximity to reduce unnecessary network traffic.

Task

1. **Select Menu → Configuration → Agent Handlers, then click New Assignment to change the assignments for Agent Handlers.**
2. **From the Agent Handler Assignment page, configure these settings:**
    - **Assignment Name** — Type a name for the assignment.
    - **Agent Criteria** — Choose one of these methods to assign agents to **Agent Handlers**:
        - **System Tree location** — Click **System Tree**, select the **System Tree Group** from the dialog box, then click **OK**.
        - **Agent Subnet** — Type the IPv4/IPv6 address, IPv4/IPv6 address ranges, subnet masks, or subnet masks range.
    - **Handler Priority** — To configure the priority used by the **Trellix Agent**, select:
        - **Use all agent handlers** — Agents randomly select which handler to communicate with.
        - **Use custom handler list** — Use **+** and **–** to add more or remove **Agent Handlers**. Use the drag-and-drop handle to change the priority of handlers.
3. **Click Save.**

Best Practices: Adding an Agent Handler in the DMZ

Agent Handlers in the DMZ allow you to directly manage systems with a **Trellix Agent** installed. Without an **Agent Handler** installed in the DMZ, you can only view those systems with your **Trellix ePO - On-prem** server.

The **Agent Handler** you install in the DMZ has specific hardware and software requirements. These requirements are similar to the **Trellix ePO - On-prem** server requirements. See this information before you begin:

These are the major steps to configure an **Agent Handlers** in the DMZ.

1. Install the Windows Server hardware and software in the DMZ between your networks that are internal and external to **Trellix ePO - On-prem**.
2. Configure all ports on your firewall between your **Trellix ePO - On-prem** server and SQL database and the **Agent Handler**.
3. Install the **Trellix ePO - On-prem** remote **Agent Handler** software using the information in the ***Trellix ePolicy Orchestrator - On-prem*** *Installation Guide*.
4. If needed, create a subgroup of systems to communicate with the **Trellix ePO - On-prem** server through the **Agent Handler**.
5. Create an **Agent Handlers** assignment.
6. Configure the **Agent Handlers** priority list and enable the **Agent Handler** in the DMZ.

Configure hardware, operating system, and ports

Installing the Agent Handler server hardware and software, and configuring the firewall ports are the first steps before using **Trellix ePO - On-prem** to manage systems behind a DMZ.

Before you begin

Make sure that your Agent Handler server meets all hardware and software requirements.

Task

1. **Build the Agent Handler server hardware with the Microsoft Windows Server operating system.**
2. **Install the server in the DMZ behind the firewall in the protected network.**
3. **Configure your Domain Name System (DNS) server to add the Agent Handler server behind the firewall in the protected network.**
4. **Configure these ports on the *internal-facing* firewall to communicate between the Trellix ePO - On-prem server and the Agent Handler in DMZ:**
    - Port 80 — Bidirectional
    - Port 8443 — Agent Handler to the **Trellix ePO - On-prem** server
    - Port 8444 — Agent Handler to the **Trellix ePO - On-prem** server
    - Port 443 — Bidirectional
5. **If your SQL database is installed on a different server than your Trellix ePO - On-prem server, configure these two ports on the *internal-facing* firewall for that connection to the Agent Handler:**
    - Port 1433 TCP — Agent Handler to SQL database server
    - Port 1434 UDP — Agent Handler to SQL database server

6. **Configure these ports on the *public-facing* firewall to communicate between the Trellix ePO - On-prem server and the Agent Handler in the DMZ:**
    - Port 80 TCP — Inbound
    - Port 443 TCP — Inbound
    - Port 8081 TCP — Bidirectional
    - Port 8082 UDP — Bidirectional

Install software and configure the Agent Handler

When you complete the **Trellix ePO - On-prem** Agent Handler software installation and configuration, your Agent Handler allows you to directly manage systems behind the DMZ.

Before you begin

- You must have installed the Agent Handler hardware and operating system in the DMZ of your external network.
- You must have access to the **Trellix ePO - On-prem** executable files located in the downloaded **Trellix ePO - On-prem** installation files.

Task

1. **Install the Trellix ePO - On-prem remote Agent Handler software. See the *Trellix ePolicy Orchestrator - On-prem Installation Guide*.**
2. **Use one of these methods to communicate through the Agent Handler to the Trellix ePO - On-prem server:**
    - Create a subgroup of systems. This task uses a subgroup, **NAT Systems**, in the **System Tree** behind the DMZ.
    - In **Agent Subnet**, type IP addresses, IP address ranges, or subnet masks, separated by commas, spaces, or new lines.
3. **To start the Agent Handler configuration on the Trellix ePO - On-prem server, select Menu → Configuration → Agent Handlers.**
4. **To open the Agent Handler Assignmentpage, select New Assignment.**
5. **Configure these settings:**
    a. **Type an Assignment Name. For example,** NAT Systems Assignment**.**
    b. **Next to Agent Criteria, click Add Tree Locations and the "..." to select a System Tree group (for example, NAT Systems) and click OK.**
    For example, select the **NAT Systems** group.
    c. **Next to Handler Priority, click Use custom handler list and Add Handlers.**
    d. **From the list, select the Agent Handler to handle these selected systems.**
    Disregard the warning that appears.
    e. **Click Save.**
6. **To configure the Agent Handler as the highest priority for the systems behind the DMZ, click Edit Priority and configure these settings, from the Agent Handler Configuration page:**
    a. **Move the Agent Handler to the top of the priority list by moving the Agent Handler names.**
    b. **Click Save.**
7. **From the Agent Handler configuration page, in the Handler Status dashboard, click the number of the Agent Handler to open the Agent Handlers List page.**
8. **From the Agent Handler Settings page, configure these settings and click Save:**

Option	Description
Published DNS Name	Type the configured name for the **Agent Handler**.
Published IP Address	Type the configured IP address for the **Agent Handler**.

9. **From the Handlers List page, in the row for the Agent Handler in the DMZ, click Enable in the Actions column.**
   The systems designated to use the Agent Handler begin getting their changes during the next few agent-server communications.
10. **Confirm that the Agent Handler in the DMZ is managing the systems behind the DMZ:**
    a. **From the Agent Handlers Configuration page, in the Systems per Agent Handler dashboard, click the Agent Handler name in the list or its corresponding color in the pie chart.**
    b. **From the Agents for Agent Handler page, confirm that the correct systems appear in the list.**
    It might take multiple instances of the agent-server communication before all systems appear in the list.

Results

With the Agent Handlers in the DMZ and configured with the **Trellix ePO - On-prem** server, you can now directly manage systems with a **Trellix Agent** installed behind the DMZ.

Connect an Agent Handler in the DMZ to a Trellix ePO - On-prem server in a domain

When your **Trellix ePO - On-prem** server is in a domain, an Agent Handler installed in the DMZ cannot connect to the **Trellix ePO - On-prem** SQL database because the Agent Handler cannot use domain credentials.

To bypass this limitation, configure the Agent Handler to use the SQL database system administrator (sa) account credentials.

Task

1. **Enable the system administrator account.**
   a. **Open SQL Management Studio, expand Security → Logins, then double-click the sa account.**
   b. **On the General tab, enter and confirm your password.**
   c. **On the Status tab, set Login to Enabled, then click OK.**
   d. **Right-click the database instance name and click Properties.**
   The system administrator account is enabled.
2. **Change the system administrator account to connect to the Trellix ePO - On-prem database.**
   You must use SQL authentication to connect to the database. If Agent Handler cannot use domain account and **Trellix ePO - On-prem** uses the domain account for SQL connection, you need to manually deselect the option to use **Trellix ePO - On-prem** database configuration and provide non-domain SQL credentials with appropriate roles to access **Trellix ePO - On-prem** database.
   a. **Open a web browser and go to https://localhost:8443/core/config-auth.**

Note

8443 is the console communication port. If you use a different port to access the **Trellix ePO - On-prem** console, include that port number in the address instead.

b. **Log on with your Trellix ePO - On-prem credentials.**
c. **Delete the entry in the User Domain field, then type sa.**
d. **Provide a password for the system administrator account, then click Test Connection.**
e. **If the test is successful, click Apply.**

Note

If the test is unsuccessful, re-enter your password, then click **Test Connection** again.

Results

The Agent Handler uses the system administrator credentials to communicate with the **Trellix ePO - On-prem** database.

Handler groups and priority

When using multiple Agent Handlers in your network, group and prioritize them to help ensure network connectivity.

Handler groups

With multiple Agent Handlers in your network, you can create handler groups. You can also apply priority to handlers in a group. Handler priority tells the agents which handler to communicate with first. If the handler with the highest priority is unavailable, the agent falls back to the next handler in the list. This priority information is contained in the repository list (sitelist.xml file) in each agent. When you change handler assignments, this file is updated as part of the agent-server communication process. Once the assignments are received, the agent waits until the next regularly scheduled communication to implement them. You can perform an immediate agent wake-up call to update the agent immediately.

Grouping handlers and assigning priority is customizable, so you can meet the needs of your specific environment. Two common scenarios for grouping handlers are:

- **Using multiple handlers for load balancing** You might have many managed systems in your network, for which you want to distribute the workload of agent-server communications and policy enforcement. You can configure the handler list so that agents randomly pick the handler communicate with.
- **Setting up a fallback plan to ensure agent-server communication** You might have systems distributed over a wide geographic area. By assigning a priority to each handler dispersed throughout this area, you can specify which handler the agents communicate with, and in what order. This can help ensure that managed systems on your network stay up-to-date by creating a fallback agent communication, much the same as fallback repositories ensure that new updates are available to your agents. If the handler with the highest priority is unavailable, the agent uses the handler with the next highest priority.

In addition to assigning handler priority within a group of handlers, you can also set handler assignment priority across several groups of handlers. This adds redundancy to your environment to further ensure that your agents can always receive the information they need.

Sitelist files

The agent uses the sitelist.xml files to decide which handler to communicate with. Each time handler assignments and priorities are updated, these files are updated on the managed system. Once these files are updated, the agent implements the new assignment or priority on the next scheduled agent-server communication.

Assign Trellix agents to Agent Handlers

Assign agents to specific handlers. You can assign systems individually, by group, and by subnet.

Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

Task

1. **Select Menu → Configuration → Agent Handlers, then click Actions → New Assignment.**
2. **Specify a unique name for this assignment.**
3. **Specify the agents for this assignment using one or both of the following Agent Criteria options:**
    - Browse to a **System Tree location**.
    - Type the IP address, IP range, or subnet mask of managed systems in the **Agent Subnet** field.
4. **Specify Handler Priority by deciding whether to:**
    - **Use all Agent Handlers** — Agents randomly select which handler to communicate with.
    - **Use custom handler list** — When using a custom handler list, select the handler or handler group from the drop-down menu.

Note

When using a custom handler list, use **+** and **-** to add or remove more Agent Handlers (an Agent Handler can be included in more than one group). Use the drag-and-drop handle to change the priority of handlers. Priority determines which handler the agents try to communicate with first.

Manage Agent Handler assignments

Complete common management tasks for Agent Handler assignments.

To perform these actions, select **Menu → Configuration → Agent Handlers**, then in **Handler Assignment Rules**, click**Actions**.

To do this...	Do this...
Delete a handler assignment	Click **Delete** in the selected assignment row.

To do this...	Do this...
Edit a handler assignment	Click **Edit** for the selected assignment. The **Agent Handler Assignment** page opens, where you can specify: • **Assignment name** — The unique name that identifies this handler assignment. • **Agent criteria** — The systems that are included in this assignment. You can add and remove **System Tree** groups, or modify the list of systems in the text box. • **Handler priority** — Choose whether to use all Agent Handlers or a custom handler list. Agents randomly select which handler to communicate with when **Use all Agent Handlers** is selected. **Tip:** Use the drag-and-drop handle to quickly change the priority of handlers in your custom handler list.
Export handler assignments	Click **Export**. The **Download Agent Handler Assignments** page opens, where you can view or download the AgentHandlerAssignments.xml file.
Import handler assignments	Click **Import**. The **Import Agent Handler Assignments** dialog box opens, where you can browse to a previously downloaded AgentHandlerAssignments.xml file.
Edit the priority of handler assignments	Click **Edit Priority**. The **Agent Handler Assignment | Edit Priority** page opens, where you change the priority of handler assignments using the drag-and-drop handle.
View the summary of handler assignments details	Click **>** in the selected assignment row.

Create Agent Handler groups

Handler groups make it easier to manage multiple handlers throughout your network, and can play a role in your fallback strategy.

Task

1. **Select Menu → Configuration → Agent Handlers, then in Handler Groups, click New Group.**
   The **Add/Edit Group** page appears.
2. **Specify the group name and the Included Handlers details:**
   - Click **Use load balancer** to use a third-party load balancer, then enter the **Virtual DNS Name** and **Virtual IP address** (both are required).
   - Click **Use custom handler list** to specify which **Agent Handlers** are included in this group.

   Note

   When using a custom handler list, select the handlers from the **Included Handlers** drop-down list. Use **+** and **-** to add and remove additional **Agent Handlers** to the list (an Agent Handler can be included in more than one group). Use the drag-and-drop handle to change the priority of handlers. Priority determines which handler the agents try to communicate with first.
3. **Click Save.**

Manage Agent Handler groups

Complete common management tasks for Agent Handler groups.

To perform these actions, select **Menu → Configuration → Agent Handlers**, then click the **Handler Groups** monitor.

Action	Steps
Delete a handler group	Click **Delete** in the selected group row.
Edit a handler group	Click the handler group. The **Agent Handler Group Settings** page opens, where you can specify: • **Virtual DNS Name** — The unique name that identifies this handler group. • **Virtual IP address** — The IP address associated with this group. • **Included handlers** — Choose whether to use a third-party load balancer or a custom handler list.

Action	Steps
	Note: Use a custom handler list to specify which handlers, and in what order, agents assigned to this group communicate with.
Enable or disable a handler group	Click **Enable** or **Disable** in the selected group row.

Move agents between handlers

Assign agents to specific handlers. You can assign systems using Agent Handler assignment rules, Agent Handler assignment priority, or individually using the **System Tree**.

Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

Group agents using Agent Handler assignments

Create **Agent Handler** assignments to group **Trellix Agent**s together.

Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

Tip

When assigning agents to **Agent Handlers**, consider geographic proximity to reduce unnecessary network traffic.

Task

1. **Select Menu → Configuration → Agent Handlers, then click the required Handler Assignment Rule.**
   The **Agent Handler** Assignment page appears.

   Note

   If the **Default Assignment Rules** is the only assignment in the list, you must create an assignment.

2. **Type a name for the Assignment Name.**
3. **You can configure Agent Criteria by System Tree locations, by agent subnet, or individually using the following:**
   - **System Tree Locations** — Select the group from the **System Tree location**.

Note

You can browse to select other groups from the **Select System Tree Group** dialog box and use + and - to add and remove **System Tree** groups that are displayed.

- **Agent Subnet** — In the text field, type IP addresses, IP address ranges, or subnet masks in the text box.
- Individually — In the text field, type the IPv4/IPv6 address for a specific system.

4. **You can configure Handler Priority to Use all Agent Handlers or Use custom handler list. Click Use custom handler list, then change the handler in one of these ways:**
    - Change the associated handler by adding another handler to the list and deleting the previously associated handler.
    - Add additional handlers to the list and set the priority that the agent uses to communicate with the handlers.

    Note

    When using a custom handler list, use + and - to add and remove additional **Agent Handlers** from the list (an **Agent Handler** can be included in more than one group). Use the drag and drop handle to change the priority of handlers. Priority determines which handler the agents try to communicate with first.

5. **Click Save.**

Group agents by assignment priority

Group agents together and assign them to an Agent Handler that is using assignment priority.

Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers. This list defines the order in which agents attempt to communicate using a particular Agent Handler.

Note

When assigning systems to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.

Task

1. **Select Menu → Configuration → Agent Handlers.**

    Note

    If **Default Assignment Rules** is the only assignment in the list, you must create a new assignment.

2. **Edit assignments using the steps in the task *Grouping agents by assignment rules*.**
3. **As needed, modify the priority or hierarchy of the assignments by clicking Actions → Edit Priority.**

Note

Moving one assignment to a priority lower than another assignment creates a hierarchy where the lower assignment is actually part of the higher assignment.

4. **To change the priority of an assignment, which is shown in the Priority column on the left, do one of the following:**
    - Use drag and drop — Use the drag-and-drop handle to drag the assignment row up or down to another position in the Priority column.
    - Click **Move to Top** — In **Quick Actions**, click **Move to Top** to automatically move the selected assignment to the top priority.
5. **When assignment priority is configured correctly, click Save.**

Group agents using the System Tree

Group agents together and assign them to an Agent Handler using the **System Tree**.

Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

Note

When assigning systems to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.

Task

1. **Select Menu → Systems → System Tree → Systems.**
2. **In the System Tree column, navigate to the system or group you want to move.**
3. **Use the drag-and-drop handle to move systems from the currently configured system group to the target system group.**
4. **Click OK.**

Frequently asked questions

Here are answers to frequently asked questions.

What data is sent to the Trellix ePO - On-prem server and what is sent to the database?

A data channel is a mechanism for **Trellix** products to exchange messages between their endpoint plug-ins and their management extensions. The data channel provides most data sent from the **Agent Handler** to the application server. It is used internally by the **Trellix ePO - On-prem** server for agent deployment and wake-up progress messaging. Other functions such as agent properties, tagging, and policy comparisons are performed directly against the **Trellix ePO - On-prem** database.

If the Trellix ePO - On-prem server is not defined in my repository list, does replication still occur?

Yes, if the agent contacts the Agent Handler for software packages, the Agent Handler retrieves them from the **Trellix ePO - On-prem** server **Main Repository**.

How much bandwidth is used for communication between the database and the Agent Handler?

Bandwidth between the Agent Handler and the database varies based on the number of agents connecting to that Agent Handler. But, each Agent Handler places a fixed load on the database server for:

- Heartbeat (updated every minute)
- Work queue (checked every 10 seconds)
- Database connections held open to the database (two connections per CPU for EventParser plus four connections per CPU for Apache)

How many agents can one Agent Handler support?

Agent Handlers for scalability are not required until a deployment reaches 100,000 nodes. Agent Handlers for topology or failover might be required at any stage. A good rule is one Agent Handler per 50,000 nodes.

What hardware and operating system should I use for an Agent Handler?

Use the Microsoft Server Operating System (2008 SP2+ server or 2012 64-bit server).

Note

Non-server Operating System versions have severe (~10) limits set on the number of incoming network connections.

Maintaining your Trellix ePO - On-prem server and SQL databases

Maintaining your Trellix ePO - On-prem server

Generally your **Trellix ePO - On-prem** server does not require periodic maintenance, but if your server performance changes, take these steps before calling technical support.

Note

The SQL database used by the **Trellix ePO - On-prem** server requires regular maintenance and back ups to ensure that **Trellix ePO - On-prem** functions correctly.

Best practices: Monitoring server performance

Periodically check how hard your **Trellix ePO - On-prem** server is working so that you can create benchmarks and avoid performance problems.

If you suspect your **Trellix ePO - On-prem** server is having performance problems, use **Windows Task Manager** and **Windows Server Reliability and Performance Monitor** to check the performance.

Using Windows Task Manager

The first steps to take if your **Trellix ePO - On-prem** server is having performance problems are to start Windows Task Manager on the server and check **Trellix ePO - On-prem** server performance.

- Is there excessive paging?
- Is the physical memory over-utilized?
- Is the CPU over-utilized?

See *How to use and troubleshoot issues with Windows Task Manager* (http://support.microsoft.com/kb/323527), for details.

Using the Windows Reliability and Performance Monitor

When you install **Trellix ePO - On-prem** server, custom counters are added to the built-in Windows Reliability and Performance Monitor. Those counters are informative and can give you an idea of how hard the **Trellix ePO - On-prem** server is working.

Note

You must use the 32-bit version of the **Reliability and Performance Monitor** found at `C:\Windows\SysWOW64\perfmon.exe`. The default 64-bit version of **Reliability and Performance Monitor** does not have the custom **Trellix ePO - On-prem** counters added.

See these links for **Microsoft Windows Performance Monitor** information:

- *Configure the Performance Monitor Display* (**http://technet.microsoft.com/en-us/library/cc722300.aspx**)
- *Working with Performance Logs* (**http://technet.microsoft.com/en-us/library/cc721865.aspx**)

Finding and using Performance Monitor

To use the custom **Trellix ePO - On-prem** counters with the Windows Performance Monitor, you must use the 32-bit version of the tool.

Task

1. **To find the 32-bit version of the Windows Performance Monitor, use Windows Explorer and navigate to C:\Windows\SysWOW64, then find and double-click perfmon.exe.**
2. **To confirm that you opened the 32-bit version of Performance Monitor, click Monitoring Tools → Performance Monitor, Add Counters, then click the + sign to open the Add Counters dialog box.**
3. **To find the Trellix ePO - On-prem server counters, scroll down the list of counters, find ePolicy Orchestrator Server, and expand the list.**

Results

Now you can start using the counters to test and create benchmarks for your **Trellix ePO - On-prem** server performance.

Use perfmon with Trellix ePO - On-prem: best practice

The 32-bit Windows Reliability and Performance Monitor (perfmon) is a tool to develop server benchmarks, which can help you manage your server performance.

Task

1. **Start the Windows Performance Monitor.**
2. **In the Add Counters list, browse or scroll down to the ePolicy Orchestrator Server counters selection, then click + to expand the list of counters.**
3. **To view the output as a report, click the Change Graph Type icon and select Report from the list.**

   For example, the **Open ePO Agent Connections** counter tells you how many agents are communicating with the **Trellix ePO - On-prem** server simultaneously. A healthy **Trellix ePO - On-prem** server keeps this number fairly low, usually under 20. For a **Trellix ePO - On-prem** server that is struggling, this number is over 200 (the maximum is 250) and stays high, and rarely drops below 20.

4. **Click Add to move the selected counter into the Added counters list, then click OK.**
5. **To determine the stress on your Trellix ePO - On-prem server and how quickly it can process events from all your agents, add the following counters, then click OK.**
   - **Completed Agent Requests/sec**
   - **Currently Running Event Parser Threads**
   - **Data Channel saturation**
   - **Data channel threads**
   - **Event Queue Length**
   - **Max Event Parser Threads**
   - **Open ePO Agent Connections**

- **Processor Events/sec**
- **Static event queue length**

Results

The tests listed here are just a few that you can perform with the **Trellix ePO - On-prem** server using the Windows Performance Monitor. For additional Windows Performance Monitor information, see these Microsoft websites:

- *Configure the Performance Monitor Display* (**http://technet.microsoft.com/en-us/library/cc722300.aspx**)
- *Working with Performance Logs* (**http://technet.microsoft.com/en-us/library/cc721865.aspx**)

Check event processing: best practice

The number of events appearing in the **Trellix ePO - On-prem** database events folder can indicate the performance of your **Trellix ePO - On-prem** server.

Task

1. **Using Windows Explorer, navigate to this folder:**
   `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Events`
   At any time, this folder might display a few dozen or a few hundred events.

   Note

   In larger environments, this folder is constantly processing thousands of events per minute.

2. **Click the Refresh icon multiple times, then look at the status bar to see the number of files in this folder changing quickly.**
   If there are thousands of files in this folder and **Trellix ePO - On-prem** is unable to process them, the server is probably struggling to process the events at a reasonable rate.

   Note

   It is normal for this **Events** folder to fluctuate depending on the time of day. But, if there are thousands of files in this folder and it is constantly increasing then that probably indicates a performance issue.

3. **Confirm that the events are not occurring faster than the event parser can process them. This causes this folder to grow quickly. Use these steps to confirm the event parser is running.**
   a. **To open the Windows Services Manager and confirm that the event parser is running, click Start, Run, type** `services.msc` **and click OK.**
   b. **In the Services Manager list, find Trellix ePolicy Orchestrator 5.10.0 Event Parser and confirm it is Started.**
4. **Check the event parser log file for any errors, using these steps.**
   a. **Go to the log file folder at this path:**
      `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Logs`
   b. **Open this log file and check for errors:**
      eventparser_<serverName>.log

5. **Use these steps if the events are still occurring faster than the event parser can process them.**
    a. **Open the Services Managers list again and *temporarily* stop all three of these Trellix ePO - On-prem services:**
        - Application Server
        - Event Parser
        - Server
    b. **Move the contents of the `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Events\` folder to another location, or delete the events, if you're not worried about losing the data.**

Maintaining your SQL database

To help the **Trellix ePO - On-prem** server function correctly, you must have a well performing SQL database. The database is the central storage place for all data your **Trellix ePO - On-prem** server uses, and it requires maintenance.

Maintaining the Trellix ePO - On-prem SQL database best practice

The SQL database requires regular maintenance and back ups to ensure that **Trellix ePO - On-prem** functions correctly.

The **Trellix ePO - On-prem** SQL database houses everything that **Trellix ePO - On-prem** uses to function; your System Tree structure, policies, administrators, client tasks, and configuration settings.

Perform these tasks regularly to maintain your SQL Server:

- Regularly back up the **Trellix ePO - On-prem** SQL database and its transaction log.
- Reindex your database regularly.
- Rebuild your database regularly.
- Purge older events using server tasks.

Back up your SQL database regularly, in case your SQL database or your **Trellix ePO - On-prem** server environment fails. If the **Trellix ePO - On-prem** server must be rebuilt or restored, current back ups ensure that a safe copy is available. In addition, if you are using the information in the Microsoft website, *Full Database Backups (SQL Server)* (**https://msdn.microsoft.com/en-us/library/ms186289.aspx**), your transaction log can continue to grow indefinitely until a full backup is performed.

Table data fragmentation

One of the most significant performance problems found in databases is table data fragmentation. For example, table fragmentation can be compared to an index at the end of a large book. One index entry in this book might select several pages scattered throughout the book. You must then scan each page for the specific information you are looking for.

This fragmented index is different from the index of the telephone book that stores its data in sorted order. A typical query might span multiple consecutive pages, but they are always in a sorted order.

For a database, you start with the data looking like a telephone book and, over time, end up with the data looking more like a large book index. You must occasionally resort the data to re-create the phone book order. This is where reindexing and rebuilding your **Trellix ePO - On-prem** SQL database is critical. Over time your database becomes more fragmented, especially if it manages a larger environment where thousands of events are written to it daily.

Setting up a maintenance task to automatically reindex and rebuild your **Trellix ePO - On-prem** SQL database takes only a few minutes and is essential to maintain proper performance on the **Trellix ePO - On-prem** server. You can include the reindexing as part of your regular backup schedule to combine everything in one task.

Important

Do not shrink your database. Data file shrink causes serious index fragmentation. Shrinking the database is a common mistake that many administrators make when building their maintenance task.

Learn more

Select **Menu** → **Automation** → **Server Tasks** to run the **ePO Database Index Maintenance** server task.

For details about creating your maintenance task, see KB67184.

To learn more about database fragmentation and how to determine the fragmentation of your database, use the DBCC command found here: https://docs.microsoft.com/en-us/sql/t-sql/database-console-commands/dbcc-showcontig-transact-sql.

Best practice: Test SQL database connectivity with test.udl file

For database connection issues, you can use the test.udl file to confirm the database credentials used to access the SQL database from the **Trellix ePO - On-prem** server.

Before you begin

You must know the SQL database server name and database name on the server. Use the **https://<localhost>:8443/core/config-auth** URL to learn this information.

If you are troubleshooting **Trellix ePO - On-prem** database connection problems, you might see this error in the orion.log file:

Login failed for user ''. The user is not associated with a trusted SQL Server connection

Task

1. **On the Trellix ePO - On-prem server, create a file named** test.udl.
2. **Double-click the file you created to display the Data Link Properties user interface.**
3. **Click the Provider tab, select Microsoft OLE DB Provider for SQL Server from the OLE DB Provider(s) list, then click Next.**
4. **On the Connection tab, configure this information:**
    - **Select or enter a server name** — Type the server name, instance, and port using this format: **<servername>\<instancename>,<port>**. If no named database instance is used, use this format: **<servername>,<port>**
    - **Enter information to log on to the server** — Type the SQL database credentials.
    - **Select the database on the server** — Type the database name.
5. **Click Test Connection.**

Results

The Microsoft Data Link dialog box should display **Test connection succeeded**.

Best practices: Recommended tasks

Trellix recommends that you perform certain tasks daily, weekly, and monthly to ensure that your managed systems are protected and your **Trellix ePO - On-prem** server is working efficiently.

Because all networks are different, your environment might require more detailed steps, or only some of the steps, described in this section.

Important

These are suggested best practices and do not guarantee 100-percent protection against security risks.

The processes outlined share these features:

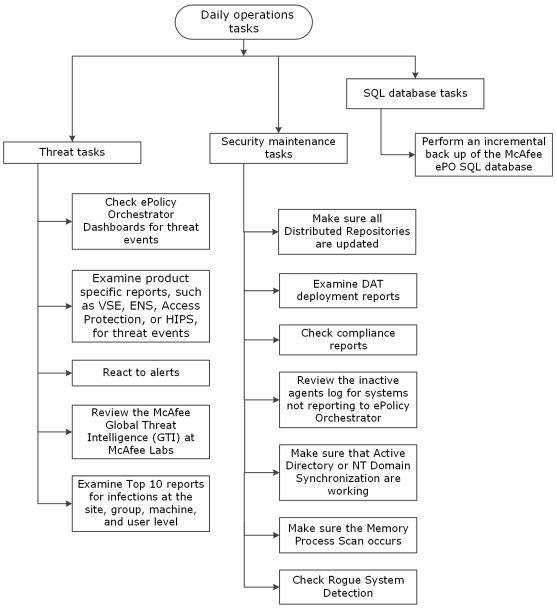
- Once you learn the processes, they don't take too long to perform.
- They are repeatable, manageable, and effective practices.
- They are based on input from **Trellix** experts and IT managers.

Recommended daily tasks: best practice

Perform these **Trellix** recommended tasks at least once a day to ensure that your **Trellix ePO - On-prem** server-managed systems are safe from threats and your **Trellix ePO - On-prem** server is functioning normally.

Note

Before you make any major changes to policies or tasks, **Trellix** recommends that you back up the database or create a snapshot of the records in the **Trellix ePO - On-prem** database.



Note

Where indicated, some of these tasks can be automated. Those instructions are included in this guide.

Recommended Trellix ePO - On-prem daily tasks details

Task	Description
Daily threat tasks	
Periodically check **Trellix ePO - On-prem** Dashboards for threat events.	Throughout the day, review your dashboards for threats, detections, and trends. **Note:** Set up automated responses to send emails to administrators when threat activity thresholds are met.
Examine product-specific reports, such as **VirusScan Enterprise**, **Trellix ENS**, Access Protection, or **McAfee Host IPS**, for threat events	Examine reports for any events that might indicate a new vulnerability in the environment. Create a server task to schedule queries and send the results to you. Using this data, you might create policies or edit existing policies.

Task	Description
React to alerts.	If new alerts are found, follow your company's internal procedure for handling malware. Collect and send samples to **Trellix** and work toward cleaning up the environment. Ensure that signature files are updated and run on-demand scans as needed. See Troubleshooting procedure for finding possible infected files, KB53094. Run queries or review dashboards periodically to check for alerts collected from your managed devices. Also watch for these threat signs: • High CPU usage on undetermined processes • Unusually high increases in network traffic • Services added or deleted by someone other than you • Inability to access network or administrative shares • Applications or files that stop functioning • Unknown registry keys added to start an application • Any browser home page that changed outside your control • Examine the **VSE: Trending Data Dashboard** and look at the **VSE: DAT Deployment** information to determine whether your signature files are up to date. • Files being created or changed on an endpoint (review Access Protection Rules).
Review the **McAfee® Global Threat Intelligence™ (McAfee GTI)** at **Trellix Labs Threat** site at least once a day.	To access the **Trellix Labs** Threat site, select **Menu** → **Reporting** → **Dashboards**. Select the **ePO Summary** dashboard and in **Trellix Links**, click **Global Threat Intelligence**.
Examine Top 10 reports for infections at the site, group, system, and user level.	**Trellix ePO - On-prem** provides preconfigured Top 10 reports that display statistics on infections in your environment. Determine which users, systems, and parts of the network have the most infections or vulnerability. These reports might reveal weakness in the network, where policies must be adjusted.

Task	Description
Daily security maintenance tasks	
Examine the DAT deployment reports.	It is important to have 100 percent deployment of the most recent DAT file to all managed systems. Make sure that clients have an update task configured to run multiple times a day to keep the DAT file current. Run the **VSE: DAT Adoption** and **VSE: DAT Adoption Over the Last 24 Hours** queries or the **VSE: DAT Deployment** query frequently throughout the day to ensure that systems are running the latest DATs.
Check compliance queries and reports.	In **Queries & Reports**, find the compliance queries that identify systems that have not updated a managed product version with an engine, hotfix, or update. Create a process to make sure that systems are up to date. For example, run an update or deployment task to ensure compliance. **Note:** Out-of-compliance system numbers drop until all systems have checked in and updated their software.
Review the inactive agents log to determine which systems are not reporting to **Trellix ePO - On-prem**.	In **Server Tasks**, run the **Inactive Agent Cleanup Task**. This task identifies systems that have not connected to the **Trellix ePO - On-prem** server for a specific number of days, weeks, or months. You can use this task to move inactive systems to a new group in the System Tree, tag the systems, delete the systems, or email a report. If the systems are on the network but having difficulty checking into the **Trellix ePO - On-prem** server, you might perform one of these actions: • Use a **Ping Agent** or **Agent Wake-Up Call** to check if a system is online and able to perform an agent-server communication with the **Trellix ePO - On-prem** server.

Task	Description
	• Reinstall the **Trellix Agent** to ensure that the system is communicating with the **Trellix ePO - On-prem** server.
Ensure that Active Directory or NT Synchronization is working.	Active Directory or NT Domain synchronization pulls in a list of new systems and containers that **Trellix ePO - On-prem** must manage. If they are used, confirm that the Sync task can be configured to run at least once a day and is working. **Caution:** If the synchronization fails, systems are vulnerable on the network and pose a major risk for infection.
Confirm that a **Memory Process Scan** occurs at least daily.	Using the **Threats Dashboard**, confirm that the results of these scans don't indicate an increase in threats. **Tip:** Run memory process scans frequently, because they are quick and unobtrusive.
Check **Rogue System Detection**	**Rogue System Detection** tells you which devices are attached to the network. It reports unmanaged systems, so they can be quickly found and removed from the network.
Daily SQL database tasks	
Perform an incremental backup of the **Trellix ePO - On-prem** database.	Use the Microsoft SQL Enterprise Manager to back up the **Trellix ePO - On-prem** database. Verify that the back up was successful after it has completed.

Task	Description
	Note: You can use the **Trellix ePO - On-prem Disaster Recovery** feature to create a snapshot of the records in the **Trellix ePO - On-prem** database to quickly recover or reinstall your software, if needed. See these documents for additional information: • This guide for Disaster Recovery details. • How to back up and restore the ePO database using SQL Server Management Studio, KB52126 • Trellix ePO server backup and disaster recovery procedure, KB66616

Recommended weekly tasks: best practice

Perform the **Trellix** suggested tasks at least once a week to ensure that your **Trellix ePO - On-prem** server-managed systems are safe from threats and your **Trellix ePO - On-prem** server is functioning normally.

Note

Where indicated, some of these tasks can be automated. Those instructions are included in this guide.

Recommended **Trellix ePO - On-prem** weekly tasks details

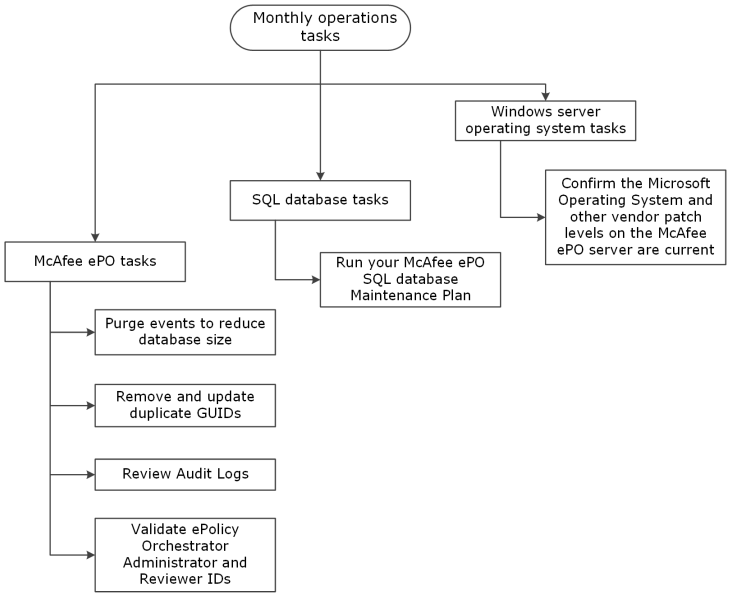
Task	Description
Weekly Trellix ePO - On-prem tasks	
Check for **Trellix** product hotfixes, extensions, and updates on the **Trellix** website or from the Software Catalog.	**Trellix** periodically releases updates and hotfixes, as well as DATs and Engine updates. Check the **Trellix** website and **Trellix ePO - On-prem** Software Catalog frequently for new updates to check in to the **Trellix ePO - On-prem** console for local environment testing. You can also use the Software Catalog to download and check in these updates. **Note:** DAT and Engine files are not updated with the Software Catalog.

Task	Description
Run a full replication to all distributed repositories.	Distributed repositories can become corrupt because of an incomplete replication task. Remove corrupt files in the repositories by running a full replication to all distributed repositories once a week. Full replication tasks delete the existing repository contents and replace them with new files. **Note:** Incremental replication tasks only copy new or non-existent files and can't fix any corrupt files.
Run Distributed Repository Status.	Select **Menu** → **Reports** → **Queries and Reports**. Locate and run the **Distributed Repository Status** report to determine whether there have been any failures to update distributed repositories. If there are failures, run the replication again and ensure that it does not fail again.
Schedule an **On-Demand Scan** of all systems in your environment.	Schedule an on-demand scan of all systems in your environment that runs during off-hours. See these documents for additional information: • Best practices for on-demand scans in **Trellix Endpoint Security (ENS)** and **VirusScan Enterprise**, See KB74059. • How to create a **Trellix ePO - On-prem** report for the event: 1203 (On-Demand Scan Completed), see KB69428. • For details about configuring on-demand scans, see the **Trellix Endpoint Security (ENS)** product documentation.
Weekly SQL database tasks	
Back up the **Trellix ePO - On-prem** SQL database.	Use the Microsoft SQL Enterprise Manager to back up the **Trellix ePO - On-prem** database. Verify that the back-up was successful after it has completed.

Task	Description
	Note: You can use the **Trellix ePO - On-prem** Disaster Recovery feature to create a snapshot of the records in the **Trellix ePO - On-prem** database to quickly recover, or reinstall your software, if needed. See these documents for additional information: • How to back up and restore the **Trellix ePO - On-prem** database using SQL Server Management Studio, see KB52126 • **Trellix ePO - On-prem** server backup and disaster recovery procedure, KB66616
Weekly Windows Server operating system tasks	
Remove inactive systems from Active Directory.	Active Directory pulls in a list of new systems and containers that **Trellix ePO - On-prem** must manage. Confirm that the synchronization task is configured to run at least once a day and is working. **Caution:** If the synchronization fails, systems are vulnerable on the network and pose a major risk for infection.

Recommended monthly tasks: best practice

Perform the **Trellix** suggested tasks at least once a month to ensure that your **Trellix ePO - On-prem** server-managed systems are safe from threats and your **Trellix ePO - On-prem** server is functioning normally.



Note

Where indicated, some of these tasks can be automated. Those instructions are included in this guide.

Recommended Trellix ePO - On-prem monthly tasks details

Task	Description
Monthly Trellix ePO - On-prem tasks	
Purge events to reduce database size.	Purge events automatically.
Remove and update duplicate GUIDs.	Run the Duplicate Agent GUID server tasks to find and fix any duplicate GUIDs in your environment. Also, run these server tasks: • **Duplicate Agent GUID - clear Error Count** • **Duplicate Agent GUID - remove systems with potentially duplicated GUIDs**
Review Audit Logs.	Review the **Trellix ePO - On-prem** Audit Logs to ensure that individuals with administrative rights are making only approved changes to system configurations, tasks, and policies.

Task	Description
Validate **Trellix ePO - On-prem** Administrator and Reviewer IDs	Confirm that only employees authorized to have administrative access have properly configured IDs, with the proper permission sets in the **Trellix ePO - On-prem** system.
SQL database tasks	
Run your **Trellix ePO - On-prem** SQL database Maintenance Plan.	Set up and run your SQL Monthly Maintenance Plan. See Recommended maintenance plan for **Trellix ePO - On-prem** database using SQL Server Management Studio, KB67184.
Monthly Windows Server operating system tasks	
Confirm that the Microsoft Operating System and other vendor update levels on the **Trellix ePO - On-prem** server are current.	Review and implement all Microsoft updates to eliminate vulnerabilities and mitigate risk. **Note:** Other vendor updates might also be released and need updating to reduce vulnerabilities in the environment.

Periodic tasks: best practice

Performing periodic maintenance is important to ensure proper **Trellix ePO - On-prem** server operations. Performing every task daily, weekly, or monthly, is not required. But periodic tasks are important to ensure that overall site health, security, and disaster recovery plans are up to date.

Note

Create a periodic maintenance log to document dates that maintenance was conducted, by whom, and any maintenance-related comments about the task conducted.

Task	Description
Assess your environment, policies, and policy assignments periodically to confirm that they are still applicable.	Organizational needs can change. Periodically review both existing policies and policy assignments to ensure that they still make sense in the environment. Fewer policies simplify server administration.
Review existing client tasks and task assignments periodically to confirm that they are still needed.	Client tasks run scans, deploy product updates, product patches and hotfixes, and more to systems managed by **Trellix ePO - On-prem**. Clean out unused tasks to reduce system complexity which can ultimately affect database size.
Review existing tags and tag criteria to ensure that they are still relevant to your environment.	Use tags as an alternative to **System Tree** groups to combine, or select a group of systems to operate on. For example, to send updates, deploy **Trellix** managed products, or run scans. Tagging is useful, but you must monitor tags to ensure that they are useful and have the impact needed.
Review product exclusions (for example, **VirusScan Enterprise**) and includes/excludes (for example, Access Protection rules) periodically to validate relevancy.	You must keep exclusions as specific as possible in your environment. Products changes can affect the exclusions that you have configured. Periodically review exclusions to ensure that they still accomplish what is needed. Plus, you can use High and Low Risk OnAccess scanning configurations to augment exclusions. Structure the **System Tree**, or use tags as another method to control exclusions.
Make any hardware changes or remove any repositories that you want to decommission.	As your network and organization changes, you might find that changing the location and type of repositories you use provides more efficient and effective coverage.
Validate that you have the required software, such as the latest version of the **Trellix Agent**.	Always use the most current version of **Trellix** managed products to ensure that you have technical support for those products. Plus, you have the latest features and fixes available.

Task	Description
Remove any unsupported software or software for products you aren't using from the main and distributed repositories.	Keeps disk space to a minimum and removes clutter from the **Trellix ePO - On-prem** server and distributed repositories. Only keep those products currently in use in your environment in the **Main Repository**.
Validate your **System Tree** and remove any agents that have not communicated with the **Trellix ePO - On-prem** server in 30 days or that are de-commissioned.	Keep the **System Tree** organized and delete systems that are no longer in use, or reporting to **Trellix ePO - On-prem**. A clean **System Tree** ensures that reports do not contain extraneous information. Set up a server task to delete inactive systems.
Remove server tasks that are no longer used.	Keep only those server tasks that you intend to use in the task listing. You can always disable an unused task that you want to keep, but don't use regularly. Keeping a minimum list of tasks that you use regularly reduces **Trellix ePO - On-prem** complexity.
Remove **Automated Responses** that are no longer relevant.	Automated responses are configured to alert individuals, particularly system administrators; when malware event threats, client treats, or compliance issues must be resolved.
Delete shell systems using a **Trellix ePO - On-prem** server task.	Delete systems with incomplete or missing system and product properties from the **System Tree**. Those systems skew reports and queries, and waste space in the **Trellix ePO - On-prem** database.
Monitor database size	Check the size of the **Trellix ePO - On-prem** database and determine whether, and how often, to purge events reported to **Trellix ePO - On-prem**. See How to identify why the ePolicy Orchestrator database is large, KB76720. To purge events from the database, see How to remove old events and shrink the **ePolicy Orchestrator - On-prem** database, KB68961 and

Task	Description
	how to purge the Audit Log, Server Task Log, and Threat Event Log.

Managing SQL databases

Best practice: Maintaining SQL databases

Your **Trellix ePO - On-prem** databases require regular maintenance to promote optimal performance and to protect your data.

Depending on your deployment of the **Trellix ePO - On-prem** software, plan on spending a few hours each week on regular database backups and maintenance. Perform these tasks regularly, either weekly or daily. But, these tasks are not the only maintenance tasks available. See your SQL documentation for details about what else you can do to maintain your database.

Configure a Snapshot and restore the SQL database

To quickly reinstall a **Trellix ePO - On-prem** server, configure a Disaster Recovery Snapshot to save, or confirm that a snapshot is being saved to the SQL database. Then back up that SQL database, which includes the Snapshot, and copy the database backup file to an SQL Server to create the restoration.

A quick reinstallation of the **Trellix ePO - On-prem** server requires these tasks.

Configure Disaster Recovery Server Task

Use the **Disaster Recovery** Snapshot Server Task to modify the scheduled automatic Snapshots of your **Trellix ePO - On-prem** server configuration saved to the SQL database.

The preconfigured status of your **Disaster Recovery Server Snapshot Task** depends on the SQL database your **Trellix ePO - On-prem** server uses. **Disaster Recovery Snapshot** is enabled, by default, on all Microsoft SQL Servers.

You can only run one **Disaster Recovery Snapshot** at a time. If you run multiple Snapshots, only the last **Snapshot** creates any output and the previous Snapshots are overwritten.

You can modify the default **Disaster Recovery Server Task** as needed.

Task

1. **Select Menu → Automation → Server Tasks, select Disaster Recovery Snapshot Server from the Server Tasks list, and click Edit.**
2. **From the Disaster Recovery Server Task builder Descriptions tab Schedule status, click Enabled or Disabled as needed.**
3. **From the Schedule tab, change the following settings as needed:**
    - **Schedule type** — Set the frequency when the Snapshot is saved.
    - **Start Date** and **End Date** — Set the start and end dates the Snapshots are saved, or click **No End Date** to have the task run continuously.

- **Schedule** — Set the time when the Snapshot is saved. By default, the Snapshot task runs at 1:59 a.m. daily.

Note

Best practice: un the Disaster Recovery Server Task during off hours to minimize the changes to the database during the Snapshot creation process.

4. **From the Summary tab, confirm that the server task is configured correctly and click Save.**

Use Microsoft SQL to back up and restore the database

To save the **Disaster Recovery Snapshot** with the **Trellix ePO - On-prem** server configuration information, use Microsoft SQL Server procedures.

Before you begin

To complete this task, you must have connectivity and authorization to copy files between your primary and restore **Trellix ePO - On-prem** SQL Servers.

After you create a Snapshot of the **Trellix ePO - On-prem** server configuration, you must:

Task

1. **Create a Microsoft SQL Server backup of the database using:**
   - Microsoft SQL Server Management Studio
   - Microsoft Transact-SQL

   See your Microsoft SQL Server documentation for details to complete these processes.

2. **Copy the backup file created to your restore SQL Server.**
3. **Restore the backup of the primary SQL database that includes the Disaster Recovery Snapshot records using:**
   - Microsoft SQL Server Management Studio
   - Microsoft Transact-SQL

   See your Microsoft SQL Server documentation for details to complete these processes.

Results

This creates a duplicate SQL Server ready for restoration, if needed, by connecting it to a new **Trellix ePO - On-prem** installation using the **Restore** option.

Use Microsoft SQL Server Management Studio to find Trellix ePO - On-prem server information

From the Microsoft SQL Server Management Studio, determine your existing **Trellix ePO - On-prem** server information.

Task

1. **Use a Remote Desktop Connection to log on to the Microsoft SQL database server with host name or IP address.**
2. **Open the Microsoft SQL Server Management Studio and connect to the SQL Server.**

3. **From the Object Explorer list, click <Database Server Name> → Databases → <Database name> → Tables.**
4. **Scroll down to find the EPOServerInfo table, right-click the table name, and select Edit top 200 Rows from the list.**
5. **Find and save the information in these database records.**
    - **ePOVersion** — For example **<three-digit ePolicy Orchestrator version>**.
    - **DNSName** — For example **epo-2k8.servercom**.
    - **ComputerName** — For example **EPO-2K8**.
    - **LastKnownTCPIP** — For example **172.10.10.10**.
    - **RmdSecureHttpPort** — For example **8443**.

Make sure that you have this information in case you ever have to restore your **Trellix ePO - On-prem** software.

Common event format

Most managed products now use a common event format. The fields of this format can be used as columns in the Threat Event Log.

These fields include:

- **Action Taken** — Action that the product took in response to the threat.
- **Agent GUID** — Unique identifier of the agent that forwarded the event.
- **DAT Version** — DAT version on the system that sent the event.
- **Detecting Product Host Name** — Name of the system hosting the detecting product.
- **Detecting Product ID** — ID of the detecting product.
- **Detecting Product IPv4 Address** — IPv4 address of the system hosting the detecting product (if applicable).
- **Detecting Product IPv6 Address** — IPv6 address of the system hosting the detecting product (if applicable).
- **Detecting Product MAC Address** — MAC address of the system hosting the detecting product.
- **Detecting Product Name** — Name of the detecting managed product.
- **Detecting Product Version** — Version number of the detecting product.
- **Engine Version** — Version number of the detecting product's engine (if applicable).
- **Event Category** — Category of the event. Possible categories depend on the product.
- **Event Generated Time (UTC)** — Time in Coordinated Universal Time that the event was detected.
- **Event ID** — Unique identifier of the event.
- **Event Received Time (UTC)** — Time in Coordinated Universal Time that **Trellix ePO - On-prem** received the event.
- **File Path** — File path of the system which sent the event.
- **Host Name** — Name of the system which sent the event.
- **IPv4 Address** — IPv4 address of the system which sent the event.
- **IPv6 Address** — IPv6 address of the system which sent the event.
- **MAC Address** — MAC address of the system which sent the event.
- **Network Protocol** — Threat target protocol for network-homed threat classes.
- **Port Number** — Threat target port for network-homed threat classes.
- **Process Name** — Target process name (if applicable).
- **Server ID** — Server ID that sent the event.
- **Threat Name** — Name of the threat.
- **Threat Source Host Name** — System name from which the threat originated.

- **Threat Source IPv4 Address** — IPv4 address of the system from which the threat originated.
- **Threat Source IPv6 Address** — IPv6 address of the system from which the threat originated.
- **Threat Source MAC Address** — MAC address of the system from which the threat originated.
- **Threat Source URL** — URL from which the threat originated.
- **Threat Source User Name** — User name from which the threat originated.
- **Threat Type** — Class of the threat.
- **User Name** — Threat source user name or email address.

View and purge the Threat Event Log

You should periodically view and purge your threat events.

Task

1. **Select Menu → Reporting → Threat Event Log.**
2. **Select one of these actions.**

Action	Steps
View Threat Event Log.	a. Click any of the column titles to sort the events. You can also select **Actions → Choose Columns** and the **Select Columns to Display** page appears. b. From the **Available Columns** list, select different table columns that meet your needs, then click **Save**. c. Select events in the table, then click **Actions** and select **Show Related Systems** to see the details of the systems that sent the selected events.
Purge Threat Events.	a. Select **Actions → Purge**. b. In the **Purge** dialog box, next to **Purge records older than**, type a number and select a time unit. c. Click **OK**. Records older than the specified age are deleted permanently.

Best practice: Schedule purging the Threat Event Log

You can create a server task to automatically purge the **Threat Event Log**.

Task

1. **Open the Server Task Builder.**
    a. **Select Menu → Automation → Server Tasks.**
    b. **Click New Task.**
2. **Name and describe the task. Next to Schedule Status, select Enabled, then click Next.**
3. **Select Purge Threat Event Log from the drop-down list.**
4. **Select whether to purge by age or from a queries result. If you purge by query, pick a query that results in a table of events.**
5. **Click Next.**
6. **Schedule the task as needed, then click Next.**
7. **Review the task's details, then click Save.**

Use a remote command to determine the Microsoft SQL database server and name

The following **Trellix ePO - On-prem** remote command is used to determine the Microsoft SQL database server and database name.

Task

1. **Type this remote command in your browser address bar:**
   `https://<localhost>:8443/core/config`
   In this command:

    - `<localhost>` — Is the name of your **Trellix ePO - On-prem** server.
    - `:8443` — Is the default **Trellix ePO - On-prem** server port number. Your server might be configured to use a different port number.

2. **Save the following information that appears in the Configure Database Settings page:**

    - Host name or IP address
    - Database name

Reporting with queries

Trellix ePO - On-prem provides built in querying and reporting capabilities. These are highly customizable, flexible, and easy to use.

Both the **Query Builder** and **Report Builder** create and run queries and reports that organize user-configured data in user-specified charts and tables. The data for these queries and reports can be obtained from any registered internal or external database used with your **Trellix ePO - On-prem** system.

Reporting features

You can use the preconfigured queries, create custom queries, use the output of the queries to perform tasks, and create reports as output.

Note

Whenever you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change.

To view one of the preconfigured queries, click **Run**. You can then perform the following tasks:

- Save the output as a report.
- Duplicate the query and change the output.
- View results in the query system.
- Take action on the results as you normally would in the System Tree.

Note

As you add new products using extensions to **Trellix ePO - On-prem**, new preconfigured queries and reports become available.

Reporting lag time

When you run **Trellix ePO - On-prem** query reports, you must be aware that reports have a lag-time. This lag-time means information is not added to the report during the time when it's actually being run. This information lag-time begins when you start the query, lasts until the query is done, and varies depending on the time it takes to run the query.

Report lag-time example:

- You run a query hourly and the query takes 10 minutes to run.
- Events that occur during the 10 minutes, while the query is being run, are not included in that report, but are written to the database.
- Those events appear in the next query report run an hour later.

Best practices: How to use custom queries

Creating custom queries on the **Trellix ePO - On-prem** server is easy, plus you can duplicate and change existing queries to suit your needs.

You create custom queries using the **Query Builder** wizard. To access the **Query Builder** wizard, select **Menu** → **Reporting** → **Queries and Reporting**, then click **New Query**.

You can approach custom queries two ways:

1. You can determine exactly which kind of query that you want to create before you create it.
2. You can explore the **Query Builder** wizard and try different variables to see the different types of available queries.

Both approaches are valid and can yield interesting data about your environment. If you are new to the query system, try exploring different variables to see the types of data that **Trellix ePO - On-prem** can return.

Once you have created your report, you can act on the results. The type of action depends on the type of output created by the report. You can do anything that you could do in the **System Tree** for example, you can wake up systems, update them, delete them, or move them to another group. The wake-up action is useful when running reports on systems that:

- Have not communicated with the **Trellix ePO - On-prem** server recently
- Are suspected of not working properly when you try to wake them up
- Need a new agent deployed to them directly from **Trellix ePO - On-prem**

Create custom event queries

You can create a custom query from scratch or duplicate and change an existing query.

Task

1. **Select Menu → Reporting → Queries & Reports, then New Query. The Query wizard opens and displays the Result Types tab.**
   The result types are organized into groups on the left side of the page. Depending on what extensions have been checked in to **Trellix ePO - On-prem**, these groups vary. Most of the result types are self-explanatory, but two of the more powerful result types are Threat Events and Managed Systems. You can access these two events types as shown in the following examples.

   - **Threat Events** — In the **Feature Group**, select **Events**. Under **Result Types**, select **Threat Events**.
   - **Managed Systems** — In the **Feature Group**, select **System Management**. Under **Result Types**, select **Managed Systems**.
2. **Choose your chart type. You have several chart types to choose from and some are more complex than others. The two simplest charts are the pie chart and the single group summary table. The pie chart compares multiple values in a graphic format, and the summary table displays a data set with over 20 results.**

   To create a pie chart, in the **Chart type**, click **Pie Chart**.
3. **Choose the label or variable that you want the report to display.**

Note

Many times the report does not have to return data on **Trellix** products. For example, you can report on the operating system versions used in your environment.

In the list, click **OS Type**.

4. **Choose the columns that you want to see when you drill down on any of the variables in the report. Choosing columns is not a critical component when building a query and can be adjusted later.**

Note

You can also drag-and-drop columns from left to right and add and remove columns to display.

To use the default columns, click **Next**.

You can filter the data that you want the query to return. You can leave the filter area blank, which returns every device in your tree, or specify the return results you are interested in. Examples of filter options include:

- A group in your **System Tree** where the report applies. For example, a geographic location or office.
- Only include laptop or desktop systems.
- Only specific operating system platforms. For example, servers or workstations.
- Only include systems that have an older DAT version.
- Only include systems with an older version of **VirusScan Enterprise**.
- Only return systems that have communicated with the **Trellix ePO - On-prem** server in the past 14 days.

5. **Click Next to not create any filters and display all operating system types.**
6. **Click Run to generate the report and see the results.**

After you create the reports and display the output, you can fine-tune your report without starting again from the beginning. To do this, click **Edit Query**. Clicking Edit allows you to go back and adjust your report and run it again in seconds.

When you are done, click **Save** to save it permanently. Now, this query is included with your dashboards and you can run it any time.

How event summary queries work best practice

Client events and threat events make up most of the event data in your database. Queries help you track how many events are stored in your database.

Event summary queries help you manage any performance problems that these events might cause for your **Trellix ePO - On-prem** server and database.

Client events from your agents relate their task status to **Trellix ePO - On-prem**. Items like update complete, update failed, deployment completed, or encryption started are considered client events. Threat events include a virus was found, a DLP

event was triggered, or an intrusion was detected. Depending on which products you have installed and which events you are collecting, there might be thousands or even millions of these events in your database.

Best practice: Create client event summary queries

To display events sent from your agents to **Trellix ePO - On-prem**, create client event summary queries that send threat notifications to your administrator.

This example creates a client events summary query. It displays events sent from each **Trellix Agent** to **Trellix ePO - On-prem**. Items like update complete, update failed, deployment completed, or encryption started are considered client events.

Task

1. **To create a client events summary query, select Menu → Reporting → Queries & Reports.**
2. **From the Queries page, click New Query.**
3. **From the Query Builder, starting with the Result Types tab, click Events in the Features Group, Client Events in Result Types, then click Next.**
4. **On the Chart page under Summary, click Single Group Summary Table to display a total count of all client events in the events table.**
5. **To create a filter with a good human-readable description of the events, click Event Description, in the Labels are list under Threat Event Descriptions.**

   Optionally, you can filter by the Event ID, which is the number that represents client event data in **Trellix ePO - On-prem**. For details about managed product generated event IDs listed in **Trellix ePO - On-prem**, see KB54677.

6. **If needed, adjust the column information based on the type that you want displayed.**

   Note

   This step is not critical for the creation of the query.

7. **Click Next, the Filter page appears.**
   You do not need any filtering because you want every client event returned in the database. Optionally, you can create a query based on events generated in a certain time, for example, the last 24 hours, or the last seven days.
8. **Click Run to display the query report.**
9. **Click Save and type an appropriate name for the report. For example, `All Client Events by Event Description`.**

Create a threat events summary query: best practice

To provide threat notification to your administrators, create a threat events summary query to display threat events sent from your agents to the **Trellix ePO - On-prem** server.

In this example, threat events include a virus found, a Data Loss Protection event triggered, or an intrusion detected.

Task

1. **To start the query configuration, select Menu → Reporting → Queries & Reports.**

2. **From the Queries page, click New Query.**
3. **From the Query wizard page, starting with the Result Types tab, click Events in the Features Group and Threat Events in the Result Type, and click Next.**
4. **From the Chart page, under Summary, click Single Group Summary Table, to display a total count of all threat events in the events table.**
5. **To create a filter with a good human-readable description of the events, click Event Description, in the Labels are list, under Threat Event Descriptions.**

   Optionally, you can filter by the Event ID which is the number that represents client event data in **Trellix ePO - On-prem**. For details about managed product generated event IDs listed in **Trellix ePO - On-prem**, see KnowledgeBase article McAfee point product generated Event IDs listed in ePO, KB54677.

6. **If needed, adjust the columns information based on the type that you want displayed, then click Next.**
7. **On the Filter page, you do not need any filtering because you want every client event returned in the database. Optionally, you can create a query based on events generated in a certain time, for example the last 24 hours, or the last 7 days. Click Run to display the query report.**
8. **To determine about how many events you should have on your network, use the following formula:**

   (10,000 nodes) x (5 million events) = estimated number of events

   For example, if you have 50,000 nodes, your range is 25 million total client and threat events.

   Note

   This number varies greatly based on the number of products and policies you have and your data retention rate. Do not panic if you exceed this number.

   If you significantly exceed this number, determine why you have so many events. Sometimes this many events are normal if you receive a significant number of viruses in unrestricted networks, such as universities or college campuses. Another reason for a high event count could be how long you keep the events in your database before purging. Here is what to check:

   - Are you purging your events regularly?
   - Is there a specific event in the query that comprises most of your events?

   Remember, it's common to forget to include a purge task. This causes **Trellix ePO - On-prem** to retain every event that has occurred since the **Trellix ePO - On-prem** server was built. You can fix this simply by creating a purge task.

   If you notice one or two events make up a disproportionate number of your events, you can then determine what they are by drilling down into those events. For example, if you see that the event with the most instances is an access protection rule from **VirusScan Enterprise**. This is a common event. If you double-click the **Access Protection rule** event to drill down on the cause, you can see that a few access protection rules are being triggered repeatedly on **VirusScan Enterprise**.

9. **At this point, determine whether these are important events in your organization and if they are being looked at by administrators. Ignoring some events is common by some administrators.**

Ultimately, when dealing with excessive events in your database, you must follow this process:

a. **Create a query that shows all events you are questioning, then use the information in this section to analyze these threat events.**
b. **Determine if anyone is looking at these excessive events in the first place.**
c. **If events are not being analyzed, change your policy to stop the event forwarding.**
d. **If the event is important, make sure that you are monitoring the number of events.**

If no one is looking at these events, you might consider disabling them completely in the **VirusScan Enterprise** access protection policy to stop them from being sent to the **Trellix ePO - On-prem** server. Or, you can adjust your policy to send only the access protection events that you are concerned with instead of excessive events that are not being analyzed. If you do want to see these events, you can leave the policy as configured, but confirm that you are following the rules about purging events from the **Trellix ePO - On-prem** server so that these events do not overrun your database.

Create custom table queries: best practice

Create a query that displays the results in a table so that you can act on the query results.

For example, you might need to purge data or events based on your query. You might have events of a specific type that are overwhelming your database, such as 1051 and 1059 events. You can also use this technique to purge other threat events based on the custom queries you create.

A table query is used to return data in a simple table format, without graphs or charts. Server tasks can act on simple table data. For example, you can automatically delete this data.

This task creates a custom query that returns all 1051 and 1059 events in the database.

Task

1. **To open the Queries dialog box, select Menu → Reporting → Queries & Reports, then click New Query.**
2. **Click Events in the Features Group and Client Events in the Result Types, and click Next.**
3. **In the Display Results As pane, click List, then click Table, then click Next.**
4. **Click Next to skip the Columns dialog box.**

Note

You can skip this step because **Trellix ePO - On-prem** does not use the columns you choose in the server task.

5. **In Available Properties under Client Events, click Event ID to create an Event ID filter.**
   An Event ID row is added in the Filter pane.
6. **Click the plus sign, +, at the right to add another Event ID comparison row, select equals in the Comparison column, add `1051` and `1059` in the Value column; then click Save and Run.**
7. **(Optional) You can select all these 1051 and 1059 events, then click Actions | Purge to purge them in real time. You can filter which events to purge based on those events older than X Days, Weeks, Months, or Years. Or you can Purge using a specific previously defined query.**

Tip

Instead of purging the events in real time during business hours, you can create a server task that runs the purge nightly during off hours.

8. **To create a erver task, select Menu → Automation → Server Tasks and click Actions → New Task.**
9. **Give the task an appropriate name and description; then click Next.**
   For example, Purge of 1051 and 1059 Events Nightly.
10. **Click Purge Threat Event Log from the Actions list, then click Purge by Query.**
11. **In the list, find and click the custom query that you created.**
12. **Schedule the task to run every night, then click Save.**

Multi-server rollup querying

Trellix ePO - On-prem includes the ability to run queries that report on summary data from multiple databases.

Use these result types in the **Query Builder** for this type of querying:

- **Rolled-Up Threat Events**
- **Rolled-Up Client Events**
- **Rolled-Up Compliance History**
- **Rolled-Up Managed Systems**
- **Rolled-Up Applied Policies**

Action commands cannot be generated from rollup result types.

How it works

To roll up data for use by rollup queries, you must register each server (including the local server) that you want to include in the query.

Once the servers are registered, you must configure **Roll Up Data** server tasks on the reporting server (the server that performs the multi-server reporting). **Roll Up Data** server tasks retrieve the information from all databases involved in the reporting, and populate the EPORollup_ tables on the reporting server. The rollup queries target these database tables on the reporting server.

As a prerequisite to running a **Rolled-Up Compliance History** query, you must take two preparatory actions on each server whose data you want to include:

- Create a query to define compliance.
- Generate a compliance event.

Create a Rollup Data server task

Rollup Data server tasks draw data from multiple servers at the same time.

Before you begin

- Register each **Trellix ePO - On-prem** reporting server that you want to include in rollup reporting. Registering each server is required to collect summary data from those servers to populate the EPORollup_ tables of the rollup reporting server.

- The reporting server must also be registered to include its summary data in roll up reporting.

Important

You can't roll up data from registered **Trellix ePO - On-prem** servers at versions that are no longer supported. For example, you can't aggregate data from **Trellix ePO - On-prem** servers at version 4.5 or earlier.

Task

1. **Open the Server Task Builder.**
   a. **Select Menu → Automation → Server Tasks.**
   b. **Click New Task.**
2. **On the Description page, type a name and description for the task, and select whether to enable it, then click Next.**
3. **Click Actions, then select Roll Up Data.**
4. **From the Roll up data from: drop-down menu, select All registered servers or Select registered servers.**
5. **If you chose Select registered servers, click Select. Choose the servers you want data from in the Select Registered Servers dialog box, then click OK.**
6. **Select the data type to be rolled up, then click Next. To select multiple data types, click the + at the end of the table heading.**

   Note

   The data types **Threat Events**, **Client Events**, and **Applied Policies** can be further configured to include the properties **Purge**, **Filter**, and **Rollup Method**. To do so, click **Configure** in the row that describes the available properties.

7. **Schedule the task, then click Next.**
   The **Summary** page appears.

   Note

   If you are reporting on rolled-up compliance history data, make sure that the time unit of the **Rolled-Up Compliance History** query matches the schedule type of the **Generate Compliance Event** server tasks on the registered servers.

8. **Review the settings, then click Save.**

Create a query to define compliance

Compliance queries are required on **Trellix ePO - On-prem** servers whose data is used in rollup queries.

Task

1. **Select Menu → Reporting → Queries & Reports, then click New Query.**
2. **On the Result Type page, select System Management for Feature Group and Managed Systems for Result Types, then click Next.**
3. **Select Boolean Pie Chart from the Display Result As list, then click Configure Criteria.**

4. **Select the properties to include in the query, then set the operators and values for each property. Click OK. When the Chart page appears, click Next.**

   Note

   These properties define compliance for systems managed by this **Trellix ePO - On-prem** server.

5. **Select the columns to be included in the query, then click Next.**
6. **Select the filters to be applied to the query, click Run, then click Save.**

Generate compliance events

Compliance events are used in rollup queries to aggregate data in a single report.

Task

1. **Select Menu → Automation → Server Tasks , then click Actions → New Task.**
2. **On the Description page, type a name for the new task, then click Next.**
3. **From the Actions drop-down menu, select Run Query.**
4. **Click browse (...) next to the Query field and select a query. The Select a query from the list dialog box appears with the My Groups tab active.**
5. **Select the compliance-defining query. This could be a default query, such as McAfee Agent Compliance Summary in the McAfee Groups section, or a user-created query, such as one described in *Creating a query to define compliance*.**
6. **From the Sub-Actions drop-down menu, select Generate Compliance Event and specify the percentage or number of target systems, then click Next.**

   Note

   You can generate events using the **generate compliance event** task if noncompliance rises above a set percentage or set number of systems.

7. **Schedule the task for the time interval needed for Compliance History reporting. For example, if compliance must be collected on a weekly basis, schedule the task to run weekly. Click Next.**
8. **Review the details, then click Save.**

Export query results to other formats

Query results can be exported to these formats: HTML, PDF, CSV, and XML.

Exporting query results differs from creating a report. First, no additional information is added to the export output as you do when you create a report; only the output data is added to the report. Second, more formats are supported. The exported query results can be used for further processing using the supported machine-friendly formats such as XML and CSV. Reports are designed to be human readable, and as such are only output as PDF files.

Unlike query results in the console, exported data is not actionable.

Task

1. **Select Menu → Reporting → Queries & Reports, select a query, then click Run.**
2. **After the query runs, click Options → Export Data.**
   The Export page appears.
3. **Select what to export. For chart-based queries, select Chart data only or Chart data and drill-down tables.**
4. **Select whether the data files are exported individually or in a single archive (.zip) file.**
5. **Select the format of the exported file.**
   - **CSV** — Saves the data in a spreadsheet application (for example, Microsoft Excel).
   - **XML** — Transforms the data for other purposes.
   - **HTML** — Use this report format to view the exported results as a webpage.
   - **PDF** — Print the results.
6. **If exporting to a PDF file, configure the following:**
   - Select the **Page size** and **Page orientation**.
   - (Optional) **Show filter criteria**.
   - (Optional) **Include a cover page with this text** and enter the needed text.
7. **Select whether the files are emailed as attachments to selected recipients, or they are saved to a location on the server to which a link is provided. You can open or save the file to another location by right-clicking it.**
8. **Click Export.**

Results

The files are either emailed as attachments to the recipients, or you are taken to a page where you can access the files from links.

Best practices: Running reports with the web API

The **Trellix ePO - On-prem** API framework allows you to run commands from a web URL or use any scripting language to create command-line scripts to automate common management activities.

This section describes creating web URLs to run queries. For detailed examples of command-line scripts and tools, see the ***Trellix ePolicy Orchestrator - On-prem*** *Web API Scripting Guide*.

Use the web URL API or the Trellix ePO - On-prem user interface

You can run queries using the web URL application programming interface (API) instead of using the **Trellix ePO - On-prem** user interface.

Using the web URL API or the **Trellix ePO - On-prem** user interface, you can:

- Run the URL and display the output as a list of text
- Manipulate the text output using other scripts and tools
- Change the query
- Filter the output using Boolean operators that aren't available in the user interface

For example, you can run the **New Agents Added to ePO per Week** query in the **Trellix ePO - On-prem** user interface and get this output.

To run this query, select **Menu** → **Reporting** → **Queries & reports**, select **New Agents Added to ePO per Week** query, then click **Actions** → **Run**.

Or you can paste this web URL query in your browser address bar.

https://<localHost>:8443/remote/core.executeQuery?queryId=34&:output=terse

```
OK:
count Completion Time (Week)
----- ----------------------
3     4/27/19 - 5/3/19
2     5/4/19 - 5/10/19
6     5/11/19 - 5/17/19
1     5/18/19 - 5/24/19
```

Trellix ePO - On-prem command framework: best practice

The structure of the **Trellix ePO - On-prem** framework allows you to access all **Trellix ePO - On-prem** command objects and their parameters using the API or the user interface.

To understand the **Trellix ePO - On-prem** framework, you can compare how the **AppliedTag** command is accessed from multiple places in the **Trellix ePO - On-prem** user interface and the web URL.

The **AppliedTag** command is accessed from the System Tree page in the **Trellix ePO - On-prem** user interface.

You can find valid **AppliedTag** command parameters using this core.listTables web URL command:

https://<localHost>:8443/remote/core.listTables

The following Web URL command structure, and its parts, are used to find the **AppliedTags** command.

https://<localHost:8443/remote/core.listDatatypes?type=applied_tags

Following are the parts of the web URL command.

- **Basic URL** — Your remote console connection URL. The default port number is 8443.
- **Command name** — Appears before the **?** and is listed in the web API Help.
- **Command argument** — Appears after the **?** and is separated by **&** (ampersands). You can also add S-Expressions to your commands.

Using the web URL Help: best practice

Use the web URL Help to learn which preconfigured queries, SQL tables, and arguments are available for your **Trellix ePO - On-prem** web URL queries.

Use these Help commands when creating web URL queries:

- `https://<localHost>:8443/remote/core.help?`
- `https://<localHost>:8443/remote/core.listQueries?:output=terse`
- `https://<localHost>:8443/remote/core.help?command=core.executeQuery`
- `https://<localHost>:8443/remote/core.listTables`

Using the core.help command

All commands and their basic parameters for creating **Trellix ePO - On-prem** web URLs are listed in the `core.help` command output.

Type this command to see the Help.

`https://<localHost>:8443/remote/core.help?`

Using the core.listQueries Help command

To run an existing query using the **Trellix ePO - On-prem** web URL, use the queryID number appended to the base `core.executeQuery` command. Type this command to see the `listQueries` Help.

`https://<localHost>:8443/remote/core.listQueries?:output=terse`

Type the following command to query with an ID:

`https://<localHost>:8443/remote/core.executeQuery?queryId=<IdNumber>`

Using the core.executeQuery Help command

Before you can create a **Trellix ePO - On-prem** web URL query, or change query parameters exported from an existing query, you must know which commands and arguments are available.

Type this command to see the `core.executeQuery` Help.

`https://<localHost>:8443/remote/core.help?command=core.executeQuery`

This table lists `core.executeQuery` Help.

Note

Optional parameters and options appear in square brackets "[...]."

Web URL core.executeQuery Help

Command	Arguments	Parameters	Options	Description
core.executeQuery	queryId	—	—	Executes a SQUID query. Returns the data from the execution of the

Command	Arguments	Parameters	Options	Description
				query or displays on error.
		[database=<>]	—	The name of the remote database; if blank, the default database for the given database type is used.
core.executeQuery		target=	—	The SQUID target type to query. Optionally, you can add "." and the database type before the target. For example, **databaseType.target**.
			[select=<>]	The SQUID select clause of the query; if blank, all columns are returned.
			[where=<>]	The SQUID where clause of the query; if blank, all rows are returned.
			[order=<>]	The SQUID order-by clause of the query; if blank, database order is returned.

Command	Arguments	Parameters	Options	Description
			[group=<>]	The SQUID group-by clause of the query; if blank, no grouping is performed.
			[database=<>]	The name of the remote database; if blank, the default database for the given database type is used.
			[depth=<>]	The SQUID depth to fetch sub-results. (default: 5).
			[joinTables=<>]	The comma-separated list of SQUID targets to join with the target type; "*" means join all types.

Using the core.listTables Help command

To create a **Trellix ePO - On-prem** web URL query or to change query parameters exported from an existing query, you must know the names of the SQL tables and their parameters. These three commands provide that information.

- **https://<localHost>:8443/remote/core.listTables** — Lists all SQL tables and their parameters
- **https://<localHost>:8443/remote/core.listTables?:output=terse** — Lists a summary of all SQL tables and their parameters
- **https://<localHost>:8443/remote/core.listTables?table=<tableName>** — Lists all arguments for a specific SQL table

Type this command to see the **core.listTables** Help.

https://<localHost>:8443/remote/core.listTables?:output=terse

To list only the parameters for a specific table, use this command:

`https://<localHost>:8443/remote/core.listTables?table=<tableName>`

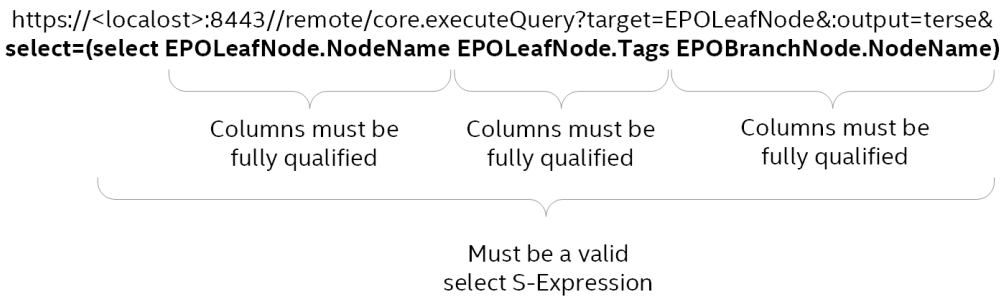
Using S-Expressions in web URL queries: best practice

You can use S-Expressions (Symbolic Expressions) in your **Trellix ePO - On-prem** web URL commands to select specific command objects and their parameters to join tables, then group, sort, and order the output.

Use the `core.executeQuery` command with the `[select=<>]` option to create S-Expressions.

This diagram shows the basic requirements for a fully qualified S-Expression query.

Web URL query with S-Expression



A fully qualified S-Expression has these parts:

- `select=(select ...)` — S-Expression function format.
- `<tableName>.<argumentName>` — The names of the SQL table columns you want to display and manipulate. For example, **EPOLeafNode.NodeName** is a managed system name and **EPOBranchNode.NodeName** is a **System Tree** group name.

In this example web URL query, the **EPOLeafNode** and **EPOBranchNode** tables are automatically joined to fulfill the query.

Note

The two tables in this example must be fully qualified, or related, for the automatic join to work.

Find the valid parameters for the target tables and confirm the table relationships.

Group, sort, order, and filter web URL query output

Within your web URL query S-Expressions, you can group, sort, order, and filter web URL query using the arguments listed for the `core.executeQuery` command.

Ordering the output

Before you can configure a sort order for your web URL query output, you must determine if the data in a table column can be sorted. Use this command to confirm the column data can be sort ordered.

https://<localHost>:8443/remote/core.listTables?table=<tableName>

This example confirms you can sort the **EPOBranchNode** table **NodeName** column data. In the **NodeName** row, **True** is listed in the **Order ?** column.

https://<localHost>:8443/remote/core.listTables?table=EPOBranchNode

This command displays this Help.

```
OK:
Name: Groups
Target: EPOBranchNode
Type: join
Database Type:
Description: null
Columns:
    Name          Type          Select? Condition? GroupBy? Order? Number?
    ------------- ------------- ------- ---------- -------- ------ -------
    AutoID        group         False   True       False    True   True
    NodeName      string        True    False      True     True   False
    L1ParentID    group         False   False      True     True   True
    L2ParentID    group         False   False      True     True   True
    Type          int           False   False      False    True   True
    BranchState   int           False   False      False    True   True
    Notes         string        True    True       False    True   False
    NodePath      string        False   False      False    True   False
    NodeTextPath  string_lookup True    True       True     True   False
    NodeTextPath2 string_lookup True    True       True     True   False
Related Tables:
    Name
    ----
Foreign Keys: None
```

This **Order** command is used to sort the **Trellix ePO - On-prem** branch nodes, or **System Tree Group Names**, in descending order.

```
https://<localHost>:8443//remote/core.executeQuery?target=EPOLeafNode&:output=terse&select=(select
EPOLeafNode.NodeName EPOLeafNode.Tags EPOBranchNode.NodeName&order=(order(desc EPOBranchNode.NodeName)
```

This is the command output.

```
OK:
System Name     Tags         Group Name
--------------- ------------ --------------
DP-2K12R2S-SRVR Server       SuperAgents
DP-2K8ER2EPO510 Server       Servers
DP-W7PIP-1      Workstation  NAT Systems
DP-W7PIP-2      Workstation  NAT Systems
DP-W7PIP-3      Workstation  NAT Systems
```

```
DP-EN-W7E1XP-2               Lost&Found
DP-2K8AGTHDLR   Server, test Agent handlers
```

Grouping the output

This command groups, or counts, the System Tree system names, and groups them by **Trellix ePO - On-prem** branch nodes, or **System Tree Group Names**.

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&:output=terse&select=(select
EPOBranchNode.NodeName (count))&group=(group EPOBranchNode.NodeName)
```

This is the command output.

```
OK:
Group Name     count
-------------- -----
Agent handlers 1
Lost&Found     1
NAT Systems    3
Servers        1
SuperAgents    1
```

Filtering the output using a string

This command filters the **System Tree** system names to display only the names with the string "2k8" in the name.

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&:output=terse&select=(select
EPOLeafNode.NodeName EPOLeafNode.Tags EPOBranchNode.NodeName)&where=(contains EPOLeafNode.NodeName "2k8")
```

This is the command output displaying only the names with the string "2k8" in the name.

```
OK:
System Name     Tags         Group Name
--------------- ------------ --------------
DP-2K8ER2EPO510 Server       Servers
DP-2K8AGTHDLR   Server, test Agent handlers
```

Filtering the output using the top <number> of the list

This command filters the **System Tree** system names to only display the top 3 names in the list.

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&:output=terse&select=(select (top 3)
EPOLeafNode.NodeName EPOLeafNode.Tags EPOBranchNode.NodeName)
```

This is the command output displaying the top 3 names in the list.

```
OK:
System Name     Tags   Group Name
--------------- ------ -----------
```

```
DP-2K8ER2EPO510 Server Servers
DP-2K12R2S-SRVR Server SuperAgents
DP-EN-W7E1XP-2         Lost&Found
```

Filtering the output using common attributes

This command filters the **System Tree** systems to display only a specific number of common attributes.

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&:output=terse&select=(select
EPOLeafNode.NodeName EPOLeafNode.Tags EPOBranchNode.NodeName)&where=(hasTag EPOLeafNode.AppliedTags 4)
```

This is the command output with 4 common attributes.

```
OK:
System Name Tags           Group Name
----------- -------------- -----------
DP-W7PIP-1  7, Workstation Workstation
DP-W7PIP-2  7, Workstation Workstation
DP-W7PIP-3  7, Workstation Workstation
```

You can combine filters

You can use the most common filters **AND** and **OR**. For example:

- **(AND <expression> <expression> ...)**
- **(OR <expression> <expression> ...)**
- They can be combined in any combination. For example: **(AND (hasTag EPOLeafNode.AppliedTags 3) (contains EPOLeafNode.NodeName "100"))**

Note

Parentheses must be matched.

You can also use filters that can't be constructed in the **Trellix ePO - On-prem** user interface. For example:

```
(OR
        (AND (hasTag EPOLeafNode.AppliedTags 3)
                  (contains EPOLeafNode.NodeName “100”))
        (AND (hasTag EPOLeafNode.AppliedTags 4)
                  (contains EPOLeafNode.NodeName “100”))
)
```

Parsing query export data to create web URL queries best practice

You can use the data exported from existing queries to create valid web URL queries and S-Expressions.

The following example is the exported data from the preconfigured VSE: DAT Deployment query. This exported file is used to describe the steps and processes to create a web URL queries.

```
<list id="1">
  <query id="2">
    <dictionary id="3"/>
    <name>VSE: DAT Deployment</name>
    <description>Displays the three highest DAT versions, and a slice for all the other versions.</
description>
    <target>EPOLeafNode</target>
    <table-uri>query:table?
orion.table.columns=EPOComputerProperties.ComputerName%3AEPOComputerProperties.DomainName%3AEPOLeafNode.os%3AEPOComput
table-uri>
    <condition-uri>query:condition?orion.condition.sexp=%28+where+
%28+version_ge+EPOProdPropsView_VIRUSCAN.productversion+%228%22+%29+%29</condition-uri>
    <summary-uri>query:summary?
pie.slice.title=EPOProdPropsView_VIRUSCAN.datver&amp;pie.count.title=EPOLeafNode&amp;orion.query.type=pie.pie&amp;oric
summary-uri>
  </query>
</list>
```

The exported query contains strings that are URL-encoded. Use this table to convert the URL-encoded characters to valid web URL query characters.

Convert URL-encoded characters to web URL query characters

URL-encoded characters	Web URL query characters
%22	quotation marks ""...""
"+"	space " "
%28	opening parenthesis "("
%29	closing parenthesis ")"
&amp	ampersand "&"
az (in an order command)	"asc" = ascending order
za (in an order command)	"desc" = descending order

XML query data file structure

The XML query export data file is separated into sections of data. Some sections aren't used in your final web URL query, and some sections can be used almost as they appear.

Exported query and web URL query data comparison

Note

The commands in the **<summary-uri>query:** code creates the pie chart and are not used to create the web URL query output. The **order=desc** parameter is shown as a sorting and grouping example in the final web URL query.

This table lists the numbers shown in the figure, the major sections of the exported query and the final web URL query, and how they are used.

Convert URL-encoded characters to web URL query characters

Number	Exported query	Web URL query	Description
1	<target>...</target>	target=...	Lists the table parsed in the query.
2	sexp=...	select=(select...	Lists the S-Expressions command objects, their parameters, and joint tables.
3	order=...	order=(order(...	Lists the sort order used in the output.

Web URL query separated into parts

Using the information from the existing query exported XML file, you can create this file, with line breaks for clarity:

```
https://<localHost>8443/remote/core.executeQuery?

target=EPOLeafNode&

select=(select EPOLeafNode.NodeName EPOProdPropsView_VIRUSCAN.datver)&

:output=terse&

order=(order(desc EPOLeafNode.NodeName))
```

Note

The **?** and **&**s indicate the different parts of the web URL query.

When you remove the line breaks, this example is final web URL query.

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&select=(select EPOLeafNode.NodeName
EPOProdPropsView_VIRUSCAN.datver)&:output=terse& order=(order(desc EPOLeafNode.NodeName))
```

Following is the output of the web URL query.

```
OK:
System Name     DAT Version (VirusScan Enterprise)
--------------- ----------------------------------
DP-W7PIP-3      7465.0000
DP-W7PIP-2      7429.0000
DP-W7PIP-1      7437.0000
DP-EN-W7E1XP-2
DP-2K8ER2EPO510 7465.0000
DP-2K8AGTHDLR   7437.0000
DP-2K12R2S-SRVR
```

Run query with ID number: best practice

The quickest way to run a query using a web URL is to use the preconfigured query ID, then use the output from the web browser in other scripts or in an email.

Before you begin

You must have administrator permissions to run the query.

Running web API queries is quicker than running a query using the **Trellix ePO - On-prem** user interface. Plus, you can use their output in scripts and redirect the output and port it for further processing.

For example, to access the query New Agents Added to ePO per Week using the **Trellix ePO - On-prem** user interface, select **Menu** → **Reports** → **Queries & Reports**, select the **New Agents Added to ePO per Week** query, and click **Actions** → **Run**.

As an alternative, you can paste, `https://<localHost>:8443/remote/core.executeQuery?queryId=34` in a browser address bar to display this URL output.

This web URL output is similar to the query output with the user interface, plus it allows you to use the output in another script or manipulate it as needed.

Task

1. **Use your browser to log on to your Trellix ePO - On-prem server.**
2. **To get a list of the preconfigured queries and their ID numbers, type this URL into the browser address bar, then press Enter.**

   `https://<localHost>:8443/remote/core.listQueries?:output=terse`

3. **From the `listQueries` command output, find the query to run.**
   In this example, the `queryId=34` argument is appended to the web URL `https://<localHost>/remote/core.executeQuery?queryId=<number>` to run the New Agents Added to ePO per Week query.

Run query with XML data best practice

Exporting existing query XML definitions is a great way to learn how to create web URL queries.

In this example, export the "VSE: DAT Deployment XML" definition file and use those table objects to create a list of the **VirusScan Enterprise** DAT file versions for each system in your network.

Task

1. **Export the existing query definition XML file and open it in a text editor.**
   Your export files look similar to this VSE: DAT Deployment XML definition file.

```
<list id="1">
  <query id="2">
    <dictionary id="3"/>
    <name>VSE: DAT Deployment</name>
    <description>Displays the three highest DAT versions, and a slice for all the other versions.</
description>
    <target>EPOLeafNode</target>
    <table-uri>query:table?
orion.table.columns=EPOComputerProperties.ComputerName%3AEPOComputerProperties.DomainName%3AEPOLeafNode.os%3AEPOC
table-uri>
    <condition-uri>query:condition?orion.condition.sexp=%28+where+
%28+version_ge+EPOProdPropsView_VIRUSCAN.productversion+%228%22+%29+%29</condition-uri>
    <summary-uri>query:summary?
pie.slice.title=EPOProdPropsView_VIRUSCAN.datver&amp;pie.count.title=EPOLeafNode&amp;orion.query.type=pie.pie&amp
summary-uri>
  </query>
</list>
```

2. **Open an existing web URL query file to use as a template, then save it with a new name. For example, `URL_template`.**
   Following is an example of an existing web URL template file.

```
https://<localHost>:8443/remote/core.executeQuery?
target=<tableTarget>&
select=(select <tableObjectNames>)
```

3. **From the query definition XML file, find the query target listed between the target tags.**
   For example, `<target>EPOLeafNode</target>` and paste the target table name in `target=` of your template URL.
   This is the template the URL with the target table name added.

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&
select=(select <tableObjectNames>)
```

4. **From the query definition XML file, find the S-Expression function, listed between the opening and closing `<condition-uri> ... </condition-uri>` tags, then perform these steps:**
   a. **In the URL template file, paste the object names in the `select=(select` parameter and the closing parenthesis. This example adds the EPOLeafNode.NodeName (system name) and EPOProdPropsView_VIRUSCAN.datver (VirusScan Enterprise DAT version) from the EPOLeafNode (System Tree) table.**

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&
select=(select EPOLeafNode.NodeName EPOProdPropsView_VIRUSCAN.datver)
```

   b. **Add the sort order function. For example, to sort the output by system name, add the string "`& order=(order(desc EPOProdPropsView_VIRUSCAN.datver)`" in the existing S-Expression.**
   The following example sorts the output by the **VirusScan Enterprise** DAT version.

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&
select=(select EPOLeafNode.NodeName EPOProdPropsView_VIRUSCAN.datver&
order=(order(asc EPOProdPropsView_VIRUSCAN.datver))
```

5. **Replace the `<localHost>` variable with your Trellix ePO - On-prem server DNS name, or IP address and paste the URL in your browser address bar. Your output should be similar to this output, but with many entries.**

```
OK:
System Name: DP-2K12R2S-SRVR
DAT Version (VirusScan Enterprise):

System Name: DP-EN-W7E1XP-2
DAT Version (VirusScan Enterprise):

System Name: DP-W7PIP-2
DAT Version (VirusScan Enterprise): 7429.0000

System Name: DP-W7PIP-1
DAT Version (VirusScan Enterprise): 7437.0000
.
.
.
```

6. **(Optional) To have the information appear in table format, paste the string :output=terse& before any ampersand in the URL and rerun the command. This is an example of your template file with :output=terse& added.**

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&:output=terse&select=(select
EPOLeafNode.NodeName EPOProdPropsView_VIRUSCAN.datver)&
order=(order(desc EPOLeafNode.NodeName))
```

Confirm that your output is similar to the following example.

```
OK:
System Name     DAT Version (VirusScan Enterprise)
--------------- ----------------------------------
DP-2K12R2S-SRVR
DP-EN-W7E1XP-2
DP-W7PIP-2      7429.0000
DP-W7PIP-1      7437.0000
DP-2K8AGTHDLR   7437.0000
DP-2K8ER2EPO510 7465.0000
DP-W7PIP-3      7465.0000
.
.
.
```

Results

You have created a web URL query using the information exported from an existing XML query definition.

Run query using table objects, commands, and arguments: best practice

You can create web URL queries using a web query template and the web URL Help.

This example describes creating a simple web URL query that displays this information about your managed systems:

- System name
- **Trellix Agent** version
- When the agent was last updated
- **VirusScan Enterprise** product family
- **VirusScan Enterprise** version
- Displays the information as a table

Task

1. **To find the name of the SQL table with most of your information, use this Help command.**
   https://<localHost>:8443/remote/core.listTables?:output=terse
2. **Using your text editor, type this web URL template command.**
   https://<localHost>:8443/remote/core.executeQuery?target=<tableName>&select=(select <columns>)
3. **Use the information from this command to find the arguments for the system names, Trellix Agent version, and when it was last updated.**
   https://<localHost>:8443/remote/core.listTables?:output=terse&table=EPOLeafNode
   This command displays this information, which you need for your web URL query:

- Query "target" — **EPOLeafNode**
- System name — **EPOLeafNode.NodeName**
- **Trellix Agent** version — **EPOLeafNode.AgentVersion**
- When the agent was last updated — **EPOLeafNode.LastUpdate**
- Products installed on each system — **EPOProductPropertyProducts**

```
OK:
Name: Managed Systems
Target: EPOLeafNode
Type: target
Database Type:
Description: Retrieves information about systems that have been added to your System Tree.
Columns:
    Name                          Type          Select? Condition? GroupBy? Order? Number?
    ----------------------------- ------------- ------- ---------- -------- ------ -------
    AutoID                        int           False   False      False    True   True
    Tags                          string        True    False      False    True   False
    ExcludedTags                  string        True    False      False    True   False
    AppliedTags                   applied_tags  False   True       False    False  False
    LastUpdate                    timestamp     True    True       True     True   False
    os                            string        True    False      False    False  False
    products                      string        False   False      False    False  False
    NodeName                      string        True    True       True     True   False
    ManagedState                  enum          True    True       False    True   False
    AgentVersion                  string_lookup True    True       True     True   False
    AgentGUID                     string        True    False      False    True   False
    Type                          int           False   False      False    True   False
    ParentID                      int           False   False      False    True   True
    ResortEnabled                 boolean       True    True       False    True   False
    ServerKeyHash                 string        True    True       False    True   False
    NodePath                      string_lookup False   False      False    True   False
    TransferSiteListsID           isNotNull     True    True       False    True   False
    SequenceErrorCount            int           True    True       False    True   True
    SequenceErrorCountLastUpdate timestamp     True    True       False    True   False
    LastCommSecure                string_enum   True    True       True     True   False
    TenantId                      int           False   False      False    True   True
Related Tables:
    Name
    --------------------------
    EPOProdPropsView_EEFF
    EPOProdPropsView_VIRUSCAN
    EPOProductPropertyProducts
    EPOProdPropsView_PCR
    EPOBranchNode
    EPOProdPropsView_EPOAGENT
    EPOComputerProperties
    EPOComputerLdapProperties
    EPOTagAssignment
    EPOProdPropsView_TELEMETRY
Foreign Keys:
    Source table Source Columns Destination table          Destination columns Allows inverse? One-to-
one? Many-to-one?
    ------------ -------------- --------------------------- ------------------- ---------------
----------- ------------
    EPOLeafNode  AutoID         EPOComputerProperties      ParentID            False
False       True
    EPOLeafNode  AutoID         EPOTagAssignment           LeafNodeID          False
False       True
    EPOLeafNode  ParentID       EPOBranchNode              AutoID              False
False       True
```

```
    EPOLeafNode  AutoID         EPOComputerLdapProperties  LeafNodeId          False
False       True
    EPOLeafNode  AutoID         EPOProductPropertyProducts ParentID            False
False       True
```

4. **Add the arguments from step 3 to the web URL template command and test it. Confirm that your command looks similar to this example.**

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&select=(select
EPOLeafNode.NodeName EPOLeafNode.AgentVersion EPOLeafNode.LastUpdate)
```

   Confirm that your output is similar to this example.

```
OK:
System Name: DP-2K8ER2EPO510
Agent Version (deprecated): 4.8.0.887
Last Communication: 6/13/14 9:21:49 AM PDT

System Name: DP-2K12R2S-SRVR
Agent Version (deprecated): 4.8.0.887
Last Communication: 6/13/14 9:55:19 AM PDT

System Name: DP-EN-W7E1XP-2
Agent Version (deprecated): null
Last Communication: null

.
.
.
```

5. **Use the `core.listTables` Help command again, but with the `EPOProdPropsView_VIRUSCAN` table. This table lists the VirusScan Enterprise products and versions installed on each system. Confirm that your command looks similar to this example.**

```
https://<localHost>:8443/remote/core.listTables?table=EPOProdPropsView_VIRUSCAN
```

6. **Using the output of step 5, add these parameters to your web URL command and test it.**
   - **VirusScan Enterprise** product family — **`EPOProdPropsView_VIRUSCAN.ProductFamily`**
   - **VirusScan Enterprise** version — **`EPOProdPropsView_VIRUSCAN.productversion`**

   Confirm that your example looks similar to the following.

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&select=(select
EPOLeafNode.NodeName EPOLeafNode.AgentVersion EPOLeafNode.LastUpdate
EPOProdPropsView_VIRUSCAN.ProductFamily EPOProdPropsView_VIRUSCAN.productversion)
```

   Confirm that your example output looks similar to the following.

```
OK:
System Name: DP-2K8ER2EPO510
Agent Version (deprecated): 4.8.0.887
Last Communication: 6/13/14 10:21:50 AM PDT
```

```
ProdProps.productFamily (VirusScan Enterprise): VIRUSCAN
Product Version (VirusScan Enterprise): 8.8.0.1266

System Name: DP-2K12R2S-SRVR
Agent Version (deprecated): 4.8.0.887
Last Communication: 6/13/14 10:55:19 AM PDT
ProdProps.productFamily (VirusScan Enterprise): VIRUSCAN
Product Version (VirusScan Enterprise):

System Name: DP-EN-W7E1XP-2
Agent Version (deprecated): null
Last Communication: null
ProdProps.productFamily (VirusScan Enterprise): VIRUSCAN
Product Version (VirusScan Enterprise):

.
.
.
```

7. **Finally, to show the output as a table, add the command `:output=terse&` after the first ampersand and rerun the command.**

   Confirm that your example command looks similar to the following.

   ```
   https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&:output=terse&select=(select
   EPOLeafNode.NodeName EPOLeafNode.AgentVersion EPOLeafNode.LastUpdate
   EPOProdPropsView_VIRUSCAN.ProductFamily EPOProdPropsView_VIRUSCAN.productversion)
   ```

   Confirm that your example output looks similar to the following.

   ```
   OK:
   System Name     Agent Version (deprecated) Last Communication      ProdProps.productFamily (VirusScan
   Enterprise) Product Version (VirusScan Enterprise)
   --------------- -------------------------- ----------------------
   ---------------------------------------- ------------------------------------
   DP-2K8ER2EPO510 4.8.0.887                  6/13/14 10:21:50 AM PDT
   VIRUSCAN                                       8.8.0.1266
   DP-2K12R2S-SRVR 4.8.0.887                  6/13/14 10:55:19 AM PDT
   VIRUSCAN
   DP-EN-W7E1XP-2  null                       null
   VIRUSCAN
   DP-W7PIP-1      4.8.0.887                  6/13/14 10:37:20 AM PDT
   VIRUSCAN                                       8.8.0.1266
   DP-W7PIP-2      4.8.0.887                  6/13/14 10:36:56 AM PDT
   VIRUSCAN                                       8.8.0.1266
   DP-W7PIP-3      4.8.0.887                  6/13/14 10:37:00 AM PDT
   VIRUSCAN                                       8.8.0.1266
   DP-2K8AGTHDLR   4.8.0.887                  6/13/14 10:25:10 AM PDT
   VIRUSCAN                                       8.8.0.1266
   ```

Troubleshooting for systems that connect over a VPN

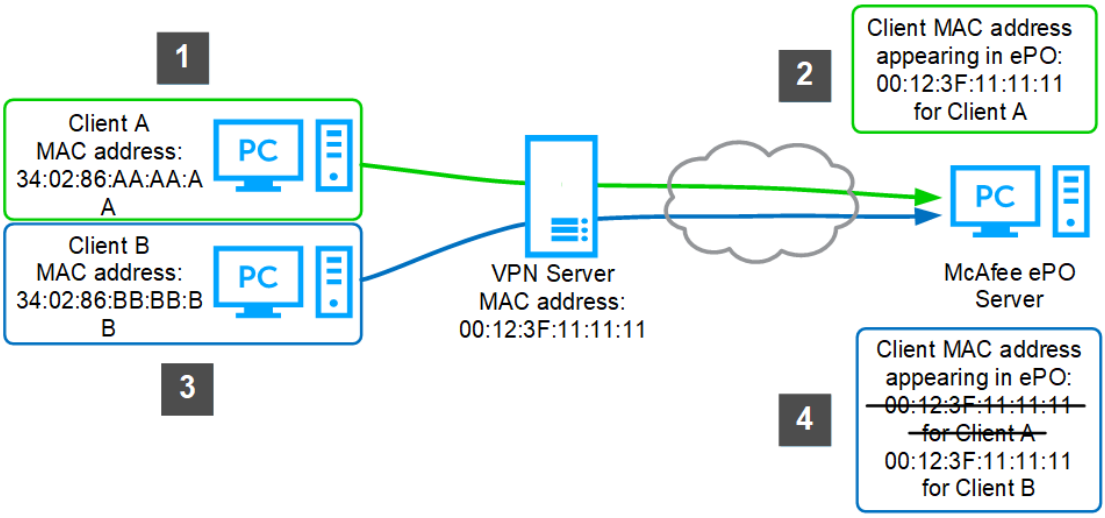
Systems in the System Tree are typically identified with their unique MAC address. But, when systems connect over a VPN they can become associated with the MAC address of the VPN server instead. This can create problems when multiple systems are all connecting through the same VPN. To resolve this, **Trellix** recommends using the Client GUID to uniquely identify systems that use a VPN.

How systems are associated with a MAC address

The following diagram shows how two systems can be associated with the same MAC address in **Trellix ePO - On-prem**.

1. Client A connects to **Trellix ePO - On-prem** over the VPN connection.
2. **Trellix ePO - On-prem** associates the MAC address of the VPN server, 00:12:3F:11:11:11, to Client A rather than the client's actual MAC address.
3. Client B connects to **Trellix ePO - On-prem** over the VPN connection.
4. **Trellix ePO - On-prem** associates the MAC address of the VPN server, also 00:12:3F:11:11:11, to Client B. Now two clients have the same VPN server MAC address.

As a result, Client A is deleted from the System Tree because both clients are associated with the same MAC address.



Preventing MAC address conflicts by using the client GUID instead

To resolve this issue, **Trellix** recommends using client GUIDs instead of MAC addresses to uniquely identify systems.

First, find the Organizationally Unique Identifier (OUI) of the VPN server. The OUI is the first six digits of the MAC address.

Add the VPN server OUI to the virtual MAC vendor values. This change allows **Trellix ePO - On-prem** to identify the VPN server and begin using the client GUID as the unique identifier for systems that connect through it.

Add Virtual MAC Vendor

This feature allows you to add the duplicated MAC address to the **Trellix ePO - On-prem** database and prevent it from matching the used MAC address to another system. Virtual machines are assigned a unique MAC (Media Access Control) address in a particular host system.

Task

1. **Click Menu → Configuration → Server Settings.**
2. **In the Server Settings page, click Virtual MAC Vendors in the Setting Categories pane.**
   You see a list of vendors and their respective ID.
3. **Click Edit.**
4. **In the Add New Virtual MAC Vendor area, enter a value in the Vendor ID field.**
   The Vendor ID must consist of six characters. It can be numeric (0–9), alphabetical (A to Z), or alphanumeric (combination of numbers and alphabets). A Vendor ID cannot have special characters.
5. **Enter the details in the Vendor Name/Note field.**
   You can enter details such as the name of the organization, the reason to add the vendor, and you can also enter comments that you would like to add. This field does not accept these special characters:
   - {
   - }
   - ;
   - <
   - >
   - ?
6. **Click Add MAC Vendor to add more vendors.**
7. **Click Save.**

Results

Note

The vendor name and ID are added to the list of vendors.
You can also edit or delete existing Vendors.

Use the System Tree to find the MAC address of the VPN

To prevent MAC address duplication when systems connect through a VPN, first determine the MAC address of the VPN server. The primary way to learn the MAC address is to access one of the systems that connects through the VPN.

Before you begin

Ensure that you have a remote connection to systems connecting to **Trellix ePO - On-prem** through a VPN server.

Task

1. **Remotely connect to a system that uses the VPN.**
2. **Click the Trellix Agent icon to open the Trellix Agent Status Monitor.**
   If you don't see the **Trellix Agent** icon, you can run the application from a command line:
   a. From the command prompt, change directories to this default folder: `C:\Program Files\McAfee\Common Framework\`

b. Type: `CmdAgent.exe /s`

The **McAfee Agent Status Monitor** opens.

3. **Click Collect and Send Props.**
   This process collects system properties and sends the information to the **Trellix ePO - On-prem** server.
4. **From the Trellix ePO - On-prem console, select Menu → Systems → System Tree.**
5. **Locate the system and double-click the system name.**
6. **Click the System Properties tab, then click Customize on the right of the display.**
7. **From the Properties list, find MAC Address, click Move to Top, and click Save.**
   The MAC address appears at the top of the list.
8. **Make note of the first six digits of the system MAC address. This is the OUI value.**

Results

Use the OUI value in the SQL Server Management Studio to update the virtual MAC vendor ID.

Create a report to find the MAC address of the VPN

To prevent MAC address duplication when systems connect through a VPN, first determine the MAC address of the VPN server. An alternative way to learn the MAC address is to create a report and identify the systems that share an address.

Task

1. **Select Menu → Reporting → Queries & Reports.**
2. **Click New Query to display the Result Type tab, configure these settings:**
   - In the **Feature Group** list, select **System Management**.
   - In **Result Types** pane, select **Systems**.
3. **Click Next.**
4. **From the Chart tab, configure these settings:**
   - In the **Summary** list, select **Single Group Summary Table**.
   - In the **Labels** list, under **Computer Properties**, select **MAC Address**.
5. **Click Next.**
6. **In the Columns tab, from the Available Columns list under Computer Properties, select MAC Address, then click Next**
7. **In the Filter tab, configure these settings:**
   - In the **Available Properties** list, expand **Systems** and click **Managed State**.
   - In the **Managed State** settings, select **Equals** from the **Comparison** drop-down list and **Managed** from the **Values** drop-down list.
   - In the **Available Properties** list, expand **Computer Properties** and click **MAC Address**.
   - In the **MAC Address** settings, select **Value is not Blank** from the **Comparison** drop-down list.
8. **Click Run.**
9. **In the output of the query, find any two systems with the same MAC address. This MAC address probably belongs to the VPN server connecting the systems to Trellix ePO - On-prem. Make note of the first six digits of the system MAC address, which is the OUI of the VPN server.**

Results

Use the OUI value in the SQL Server Management Studio to update the virtual MAC vendor ID.

Registered servers

Access additional servers by registering them with your **Trellix ePO - On-prem** server. Registered servers allow you to integrate your software with other, external servers. For example, register an LDAP server to connect with your Active Directory server.

Trellix ePO - On-prem can communicate with:

- Other **Trellix ePO - On-prem** servers
- Additional, remote, database servers
- LDAP servers
- SNMP servers
- Syslog servers

Each type of registered server supports or supplements the functionality of **Trellix ePO - On-prem** and other **Trellix** and third-party extensions and products.

We recommend that you use certificates with RSA public key lengths of 2048 bits or greater for the registered servers that connect to **Trellix ePO - On-prem**. For more information, including additional supported public key algorithms and key lengths, see KB87731.

Note

TLS 1.0 is disabled by default for communication to external servers, such as SQL Server. For more information about TLS support, see KB90222.

Register Trellix ePO - On-prem servers

You can register additional **Trellix ePO - On-prem** servers for use with your main **Trellix ePO - On-prem** server to collect or aggregate data, or to allow you to transfer managed systems between the registered servers.

Before you begin

To register one **Trellix ePO - On-prem** server with another, you need to know detailed information about the **Trellix ePO - On-prem** server SQL database of the server you are registering. You can use the following remote command to determine the Microsoft SQL database server name, database name, and more:

`https://<server_name>:<port>/core/config`

These are the variables in the remote command:

- `<server_name>` — The DNS server name or IP address of the remote **Trellix ePO - On-prem** server
- `<port>` — The assigned **Trellix ePO - On-prem** server port number, usually "`8443`", unless your server is configured to use a different port number

Task

1. **Select Menu → Configuration → Registered Servers and click New Server.**
2. **From the Server type menu on the Description page, select ePO, specify a unique name and any notes, then click Next.**
3. **Specify the following options to configure the server:**

Option	Definition
Authentication type	Specifies the type of authentication to use for this database, including: • **Windows authentication** • **SQL authentication**
Client task sharing	Specifies whether to enable or disable client task for this server.
Database name	Specifies the name for this database.
Database port	Specifies the port for this database.
Database server	Specifies the name of the database for this server. You can specify a database**Trellix ePO - On-prem** using DNS Name or IP address (IPv4 or IPv6).
ePO Version	Specifies the version of the server being registered.
Password	Specifies the password for this server.
Policy sharing	Specifies whether to enable or disable policy sharing for this server.
SQL Server instance	Allows you to specify whether this is the default server or a specific instance, by providing the Instance name.

Option	Definition
	Note: Ensure that the SQL browser service is running before connecting to a specific SQL instance using its instance name. Specify the port number if the SQL browser service is not running. Select the **Default SQL** server instance and type the port number to connect to the SQL server instance.
SSL communication with database server	Specifies whether **Trellix ePO - On-prem** uses SSL (Secure Socket Layer) communication with this database server including: • **Try to use SSL** • **Always use SSL** • **Never use SSL**
Test connection	Verifies the connection for the detailed server. **Note:** If you register a server with a different **Trellix ePO - On-prem** version, this information-only warning appears: **Warning Version mismatch!**
Transfer systems	Specifies whether to enable or disable the ability to transfer systems for this server. When enabled, select **Automatic sitelist import** or **Manual sitelist import**.

Option	Definition
	Note: When choosing **Manual sitelist import**, it is possible to cause older versions of **Trellix Agent** (version 4.0 and earlier) to be unable to contact their Agent Handler. This can happen when: • Transferring systems from this **Trellix ePO - On-prem** server to the registered **Trellix ePO - On-prem** server • An Agent Handler name appears alpha-numerically earlier than the **Trellix ePO - On-prem** server name in the supplied sitelist • Older agents use that Agent Handler
Use NTLMv2	Optionally choose to use NT LAN Manager authentication protocol. Select this option when the server you are registering uses this protocol.
User name	Specifies the user name for this server.

4. **Click Save.**

Using database servers

Trellix ePO - On-prem can retrieve data from not only its own databases, but from some extensions as well.

You might need to register several different server types to accomplish tasks within **Trellix ePO - On-prem**. These can include authentication servers, Active Directory catalogs, **Trellix ePO - On-prem** servers, and database servers that work with specific extensions you have installed.

Database types

An extension can register a database type, otherwise known as a schema or structure, with **Trellix ePO - On-prem**. If it does, that extension can provide data to queries, reports, dashboard monitors, and server tasks. To use this data, you must first register the server with **Trellix ePO - On-prem**.

Database server

A database server is a combination of a server and a database type installed on that server. A server can host more than one database type, and a database type can be installed on multiple servers. Each specific combination of the two must be registered separately and is referred to as a database server.

After you register a database server, you can retrieve data from the database in queries, reports, dashboard monitors, and server tasks. If more than one database using the same database type is registered, you are required to select one of them as the default for that database type.

Register a database server

Before **Trellix ePO - On-prem** can retrieve data, you must register it with the database server.

Task

1. **Open the Registered Servers page: select Menu → Configuration → Registered Servers, then click New Server.**
2. **Select Database server in the Server type drop-down list, enter a server name and an optional description, then click Next.**
3. **Choose a Database type from the drop-down list of registered types. Indicate if you want this database type to be as the default.**
   If there is already a default database assigned for this database type, it is indicated in the **Current Default database for database type** row.
4. **Indicate the Database Vendor. Currently, only Microsoft SQL Server and MySQL are supported.**
5. **Enter the connection specifics and logon credentials for the database server.**
6. **To verify that all connection information and logon credentials are entered correctly, click Test Connection.**
   A status message indicates success or failure.
7. **Click Save.**

Modify a database registration

If connection information or logon credentials for a database server changes, you must modify the registration to reflect the current state.

Task

1. **Open the Registered Servers page by selecting Menu → Configuration → Registered Servers.**
2. **Select a database to edit, then click Actions → Edit.**
3. **Change the name or notes for the server, then click Next.**
4. **Modify the information as appropriate. To verify the database connection, click Test Connection.**
5. **Click Save to save your changes.**

Remove a registered database

You can remove databases from the system when they are no longer needed.

Task

1. **Open the Registered Servers page: select Menu → Configuration → Registered Servers.**
2. **Select a database to delete, and click Actions → Delete.**
3. **When the confirmation dialog appears, click Yes to delete the database.**

Results

The database has been deleted. Any queries, reports, or other items within **Trellix ePO - On-prem** that used the deleted database is designated as invalid until updated to use a different database.

Register SNMP servers

To receive an SNMP trap, you must add the SNMP server's information, so that **Trellix ePO - On-prem** knows where to send the trap.

Task

1. **Select Menu → Configuration → Registered Servers, then click New Server.**
2. **From the Server Type menu on the Description page, select SNMP Server, provide the name and any additional information about the server, then click Next.**
3. **From the URL drop-down list, select one of these types of server address, then enter the address:**
    - **DNS Name** — Specifies the DNS name of the registered server.
    - **IPv4** — Specifies the IPv4 address of the registered server.
    - **IPv6** — Specifies the DNS name of the registered server which has an IPv6 address.
4. **Select the SNMP version that your server uses:**
    - If you select **SNMPv1** or **SNMPv2c** as the SNMP server version, type the community string of the server under **Security**.
    - If you select **SNMPv3**, provide the **SNMPv3 Security** details.
5. **Click Send Test Trap to test your configuration.**
6. **Click Save.**

Results

The added SNMP server appears on the **Registered Servers** page.

What is a syslog server?

Syslog is a protocol used by network devices to send event messages to a logging server – known as a syslog server. Event log forwarding consolidates all event logs in a central location such as a syslog server. Consolidation reduces the hassle of logging into every server to check logs individually.

Syslog server must be SSL enabled. **Trellix ePO - On-prem** server syslog client supports SyslogNG RFC 5424 + 5425 only which requires TCP, and Transport Layer Security (TLS). There is no support for UDP or unencrypted TCP syslog receivers.

How does event log forwarding work?

The **Trellix Agent** sends events to the Agent Handler. You need to store these events in a server. Use **Trellix ePO - On-prem** to configure syslog server and forward events to the syslog server or store the events on the SQL database server.

Register syslog servers

You can enable **Trellix ePO - On-prem** to synchronize with your syslog server. A syslog is a way for network devices to send event messages to a separate logging server. For example, you can use syslog to collect information about specific threat events.

Before you begin

You must have the domain name or IP address for your syslog server. To know how to create a syslog server, see KB87927 **Trellix ePO - On-prem** syslog forwarding only supports the TCP protocol, and requires Transport Layer Security (TLS). For more information, see KB91194.

Task

1. **Select Menu → Configuration → Registered Servers, then click New Server.**
2. **From the Server type menu on the Description page, select Syslog Server, specify a unique name and any details, then click Next.**
3. **From the Registered Server Builder page, configure these settings:**
    a. **Server name — Use DNS-style domain names (for example, `internaldomain.com`) and fully qualified domain names or IP addresses for servers. (for example, `server1.internaldomain.com` or `192.168.75.101`)**
    b. **TCP port number — Type the syslog server TCP port. The default is 6514.**
    c. **Enable event forwarding — Click to enable event forwarding from Agent Handler to this syslog server.**
    d. **Test — Click Test Connection to verify the connection to your syslog server.**
4. **Click Save.**

Results

After you register the syslog server, you can set **Trellix ePO - On-prem** to send events to your syslog server. This log file includes any syslog server errors that might occur.

Register LDAP servers

You must have a registered LDAP (Lightweight Directory Access Protocol) server to use Policy Assignment Rules, to enable dynamically assigned permission sets, and to enable Active Directory User Login.

Important

Trellix ePO - On-prem only supports Microsoft Active Directory to synchronize and import systems into the System Tree, apply policies on those systems, and apply user-based policies based on LDAP users and groups. No other LDAP server types are supported.

Task

1. **Select Menu → Configuration → Registered Servers, then click New Server.**
2. **From the Server type menu on the Description page, select LDAP Server, specify a unique name and any details, then click Next.**
3. **Choose whether you are registering an OpenLDAP or Active Directory server in the LDAP server type list.**

Note

The rest of these instructions assume that an Active Directory server is being configured. OpenLDAP-specific information is included where required.

4. **Choose if you are specifying a Domain name or a specific server name in the Server name section.**
   Use DNS-style domain names. For example, `internaldomain.com` and fully qualified domain names or IP addresses for servers, and `server1.internaldomain.com` or 192.168.75.101.

   Using domain names gives failover support, and allows you to choose only servers from a specific site if wanted.

   Note

   You must use server names with OpenLDAP servers. You can't use domain names with OpenLDAP servers.

5. **Choose if you want to Use Global Catalog.**
   This option is deselected by default. Selecting **Use Global Catalog** can provide significant performance benefits. Only select this option if the registered domain is the parent of only local domains. If non-local domains are included, chasing referrals could cause significant non-local network traffic, possibly severely impacting performance.

   Note

   Use Global Catalog is not available for OpenLDAP servers.

6. **If you have chosen to not use the Global Catalog, choose whether to Chase referrals or not.**
   Chasing referrals can cause performance problems if it leads to non-local network traffic, whether a Global Catalog is used.
7. **Choose whether to Use SSL when communicating with this server or not.**
8. **If you are configuring an OpenLDAP server, enter the Port.**
9. **Enter a User name and Password as indicated.**
   These credentials must be for an admin account on the server. Use `domain\username` format on Active Directory servers and `cn=User,dc=realm,dc=com` format on OpenLDAP servers.
10. **Either enter a Site name for the server, or select it by clicking Browse and navigating to it.**
11. **Click Test Connection to verify communication with the server as specified. Change information as needed.**
12. **Click Save to register the server.**

Mirroring an LDAP server

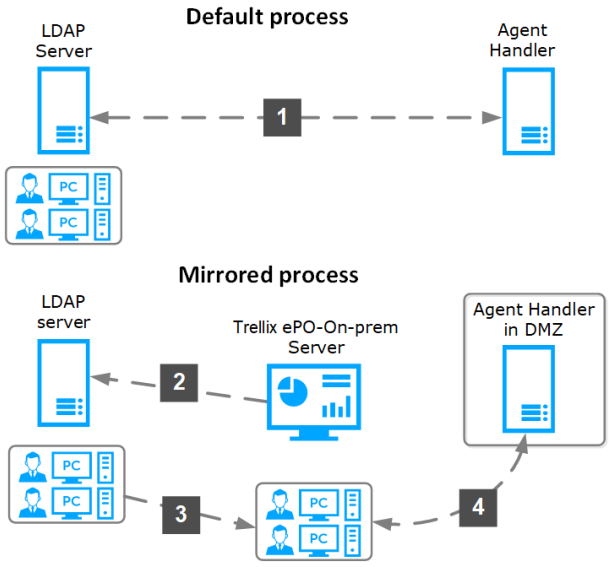
LDAP server mirroring to the **Trellix ePO - On-prem** database increases performance on any product which uses user-based policies (UBP) and allows LDAP access to Agent Handlers behind a DMZ.

This diagram shows the default LDAP server to Agent Handler connection process and the mirrored LDAP connection process.

1. Default connection process from the configured LDAP server to the Agent Handler.
2. Mirrored LDAP connection with the LDAP Synchronize server task requesting user information from the LDAP server.

3. Shows the LDAP server user information mirrored to the **Trellix ePO - On-prem** database.
4. Shows an Agent Handler behind the DMZ accessing the mirrored LDAP server information in the **Trellix ePO - On-prem** database.

Default and LDAP mirrored connection processes



Why use LDAP mirroring?

When the LDAP server user information is mirrored to the **Trellix ePO - On-prem** database:

- Medium to large organizations can access that user information used by the Agent Handler from the database faster to satisfy LDAP requests for UBPs.
- Agent Handlers behind a DMZ can access the LDAP user information.

Note

The LDAP information in the database can't be accessed or queried from the **Trellix ePO - On-prem** user interface.

By default, the LDAP information in the database is updated every 8 hours by the **LdapSync: Sync across users from LDAP** server task unless:

- An "LDAP change notification" is sent to the Agent Handler from the **Trellix ePO - On-prem** server.

  Note

  By default, the LDAP user information cache in the Agent Handler is updated every 30 minutes.

- You manually run the server task.

Sharing objects between servers

Export objects and data from your Trellix ePO - On-prem server

Exported objects and data can be used for backing up important data, and to restore or configure the **Trellix ePO - On-prem** servers in your environment.

Most objects and data used in your server can be exported or downloaded for viewing, transforming, or importing into another server or applications. The following table lists the various items you can act on. To view data, export the tables as HTML or PDF files. To use the data in other applications, export the tables or to CSV or XML files.

An exported XML file usually contains an element named `<list>` in the event multiple items are being exported. If only one object is exported, this element might be named after the object. (For example `<query>`). Any more detailed contents are variable depending on the exported item type.

The following items can be exported. Installed extensions can add items to this list. Check the extension documentation for details.

- Dashboards
- Permission Sets
- Queries
- Reports
- Server Tasks
- Users
- Automatic Responses

You can also export items from:

- Policy Catalog
- Client Task Catalog
- Tag Catalog

The following items can have a table of their current contents exported.

- Audit Log
- Issues

Task

1. **From the page displaying the objects or data, click Actions and select an option. For example, when exporting a table, select Export Table, then click Next.**
2. **When exporting content that can be downloaded in multiple formats, such as Query data, an Export page with configuration options appears. Specify your preferences, then click Export.**
3. **When exporting objects or definitions, such as client task objects or definitions, one of the following occurs:**
    - A browser window opens where you can choose **Open** or **Save**.

- An **Export** page with a link to the file opens. Left-click the link to view the file in your browser, or right-click the link to save the file.

Importing items into Trellix ePO - On-prem

Items exported from a **Trellix ePO - On-prem** server can be imported into another server.

Trellix ePO - On-prem exports items into XML. These XML files contain exact descriptions of the exported items.

Importing items

When importing items into **Trellix ePO - On-prem**, certain rules are followed:

- All items except users are imported with private visibility by default. You can apply other permissions either during or after import.
- If an item exists with the same name, **"(imported)"** or **"(copy)"** is appended to the imported item's name.
- Imported items requiring an extension or product that does not exist on the new server is designated as invalid.

Trellix ePO - On-prem only import XMLs files exported by **Trellix ePO - On-prem**.

Specific details on how to import different kinds of items can be found in the documentation for the individual items.

Issues

Issues and how they work

Issues are managed by users with proper permissions and the installed managed product extensions.

An issue's state, priority, severity, resolution, assignee, and due date are all user-defined, and can be changed at any time. You can also specify default issue responses from the **Automatic Responses** page. These defaults are automatically applied when an issue is created, based on a user-configured response. Responses also allow multiple events to be aggregated into a single issue so that the **Trellix ePO - On-prem** server is not overwhelmed with large numbers of issues.

Issues can be deleted manually, and closed issues can be manually purged based on their age and automatically purged through a user-configured server task.

View issues

The **Issues** page provides a list of current and closed issues.

Task

1. **Open the Issues page: select Menu → Automation → Issues.**
2. **Sort and filter the table to focus on relevant entries.**
    - To change which columns are displayed, from the **Actions** menu, click **Choose Columns.**
    - To order table entries, click a column title.
    - To show or hide entries, select a filter option.
3. **To view additional details, click an entry.**

Remove closed issues from the Issues table

Periodically remove closed issues from the **Issues** table to improve database performance.

Important

Items removed from the **Issues** table are deleted permanently.

Task

1. **Open the Issues page: select Menu → Automation → Issues.**
2. **Click Purge.**
3. **In the Purge dialog box, enter a number, then select a time unit.**
4. **Click OK.**

Results

Any items of the specified age or older are deleted, including items not in the current view. The number of removed items is displayed in the lower right corner of the page.

Tip
Create a server task to automatically remove outdated items.

Create issues manually

Create an issue when you have an item for administrators to address. Provide enough information so that other users understand why you created the issue.

Task

1. **Select Menu → Automation → Issues, then click New Issue.**
2. **In the New Issue dialog box, select an issue type from the Create issue of type drop-down list, then click OK. If you are unsure which issue type to select, choose Basic.**
3. **Configure the new issue. Any due dates you specify must be in the future.**
4. **Click Save.**

Configure responses to automatically create issues

Use responses to automatically create issues when certain events occur.

Task

1. **Open the Response Builder.**
    a. **Select Menu → Automation → Automatic Responses.**
    b. **Click New Response.**
2. **Complete the fields, then click Next.**
3. **Select properties to narrow the events that trigger the response, then click Next.**
4. **Specify these additional details, then click Next.**
    - The frequency of events required to generate a response.
    - A method to group events.
    - The maximum time period that you want this response to occur.
5. **Select Create issue from the drop-down list, then select the type of issue to create.**
   This choice determines the options that appear on this page.
6. **Type a name and description for the issue. Optionally, select one or more variables for the name and description.**
   This feature provides a number of variables providing information to help fix the issue.
7. **Type or select any additional options for the response, then click Next.**
8. **Review the details for the response, then click Save.**

Manage issues

You can add comments, assign, delete, edit, and view details of issues.

Task

1. **Select Menu → Automation → Issues.**
2. **Perform any of the following tasks.**

Option	Definition
Adding comments to issues	a. Select the checkbox next to each issue you want to comment, then click **Action → Add comment**. b. In the **Add comment** panel, type the comment you want to add to the selected issues. c. Click **OK** to add the comment.
Assigning issues	Select the checkbox next to each issue you want to assign, then click **Assign to user**.
Display required columns on Issues page	Click **Actions → Choose Columns**. Select columns of data to be displayed on the Issues page.
Deleting issues	a. Select the checkbox next to each issue you want to delete, then click **Delete**. b. Click **OK** to delete the selected issues.
Editing issues	a. Select the checkbox next to an issue, then click **Edit**. b. Edit the issue as needed. c. Click **Save**.
Exporting the list of issues	a. Click **Actions → Export Table** to open the **Export** page. b. From the **Export** page, you can specify the format of files to be exported, as well as how they are packaged.
Viewing issue details	• Select an issue. The **Issue Details** page shows all settings for the issue as well as the **Issues Activity Log**.

Use tickets with Trellix ePO - On-prem

To integrate automatic ticketing with **Trellix ePO - On-prem**, you or **Trellix** Professional Services can use issue APIs to configure a remote server.

Issues - Options definitions

Edit Issue page

Use this page to edit the details of an existing issue.

Option definitions

Option	Definition
Name	Specifies the name of the issue.
Description	Specifies the description of the issue.
State	Specifies the state of the issue. • **Assigned** • **Closed** • **New** • **Resolved** • **Unknown**
Priority	Specifies the priority of the issue. • **High** • **Highest** • **Low** • **Lowest** • **Medium** • **Unknown**
Severity	Specifies the severity of the issue. • **High** • **Highest** • **Low** • **Lowest** • **Medium**

Option	Definition
	• **Unknown**
Resolution	Specifies the resolution of the issue. • **Fixed** • **None** • **Waived** • **Will not fix**
Assignee	Specifies the user name of the user assigned to the issue.
Due Date	Specifies whether the issue has a due date and, if so, the date and time the issue is due.

Issue Details page

Use this page to view details about the selected issue, to edit, delete, and assign the issue, and to add a comment to the issue.

Option definitions

Option	Definition
Name	Specifies the name of the selected issue.
Type	Specifies the type of the selected issue. Product extensions can have more than one type of issue.
Description	Specifies any additional information about the issue.
State	Specifies the state of the selected issue.
Priority	Specifies the priority of the selected issue.
Severity	Specifies the severity of the selected issue.
Resolution	Specifies the resolution of the selected issue.

Option	Definition
Creator	Specifies the name of the user who created the issue.
Assignee	Specifies the name of the user assigned to the issue.
Created	Specifies the date and time the issue was created.
Due	Specifies the date and time the issue is due. If the issue is overdue, a message also appears.
Ticket	Specifies the ticket ID of the ticket added to this issue.
Ticket Server	Specifies the ticket server address of the ticket added to this issue.
Issue Activity Log	Specifies the entries in the **Issues Activity Log** for this issue, including: • **Date** — Specifies the date and time the activity occurred. • **Details** — Specifies the details of the activity. • **Title** — Specifies the title of the activity. • **Username** — Specifies the name of the user who conducted the activity.
Actions	Specifies the actions you can take on this issue, including; • **Add comment** — Adds a user-specified comment to the issue. • **Assign to user** — Adds a user-specified assignee to the issue. • **Delete** — Deletes the selected issue. • **Edit** — Opens the **Edit Issue** page. Use this action to edit the details of the selected issue.

Issue activity details page

Use this page to view details about the selected activity for the issue.

Option definitions

Option	Definition
Date	Specifies the date and time the activity log entry was created.
Title	Specifies the title assigned to the activity log entry.
Details	Specifies the detailed information added to the activity log entry.
User	Specifies the name of the user who generated the activity log entry.

Issues page

Use this page to view and manage issues in your environment.

Option definitions

Category	Option	Definition
Common actions	**New Issue**	Opens the **New Issue** dialog box.
	Purge	Deletes all closed issues older than the specified age.
Filter options	**Hide Filter/Show Filter**	Hides or shows the options used to filter the displayed issues.
	Preset	Select one of the available filters. • **All Issues** — Lists all issues. • **Issues assigned to me** — Lists only issues assigned to the logged-on user.

Category	Option	Definition
		• **Issues that I authored** — Lists only issues that the logged-on user created. • **New Issues** — Lists only new issues. • **Ticketed Issues** — Lists only issues that have a corresponding ticket. • **Closed Issues** — Lists only closed issues. • **Only Basic Issues** — Does not list any user-defined issues. **Note:** Custom filters appear at the bottom of the list.
	Custom	Allows you to add custom filters to find issues. Custom filters appear at the bottom of the **Preset** drop-down list.
	Quick find	Allows you to type search strings to find specific issues. Click **Apply** to perform the search.
	Clear	Removes the entry in the **Quick find** text box.
	Show selected rows	Displays only the rows you selected.
Default table columns	**Name**	Displays the user assigned to the issue.
	Type	Displays the type assigned to the issue.

Category	Option	Definition
	Description	Displays the description assigned to the issue.
	State	Lists the state of the issue. • **Assigned** • **Closed** • **New** • **Resolved** • **Unknown**
	Priority	Lists the priority of the issue. • **High** • **Highest** • **Low** • **Lowest** • **Medium** • **Unknown**
	Severity	Lists the severity of the issue. • **High** • **Highest** • **Low** • **Lowest** • **Medium** • **Unknown**
	Resolution	Lists the resolution of the issue. • **Fixed** • **None** • **Waived** • **Will not fix**
	Creator	Specifies the person who created the issue.

Category	Option	Definition
	Assignee	Specifies the name of the person assigned the issue.
	Created	Specifies the date and time the issue was created.
	Due	Specifies the date the issue is due to be fixed or **No Due Date**.
Actions	**Add comment**	Adds a user-specified comment to the selected issue.
	Assign to user	Adds a user-specified assignee to the selected issue.
	Choose Columns	Opens the **Select the Columns to Display** page. Use this action to select the columns that are displayed on the Issues page.
	Delete	Deletes the selected issue.
	Edit	Opens the **Edit Issue** page. Use this action to edit the details of the selected issue.
	Export Table	Opens the **Export** page. From this page, you can specify file formats, packaging (for example, placing files in a .zip file), and file actions (for example, emailing files as an attachment).

New Issue page

Use this page to add new issues.

Option definitions

Option	Definition
Name	Specifies the name of the issue.
Description	Specifies any additional information about the issue.
State	Specifies the state of the issue. • **Assigned** • **Closed** • **New** • **Resolved** • **Unknown**
Priority	Specified the priority of the issue. • **High** • **Highest** • **Low** • **Lowest** • **Medium** • **Unknown**
Severity	Specifies the severity of the issue. • **High** • **Highest** • **Low** • **Lowest** • **Medium** • **Unknown**
Resolution	Specifies the resolution of the issue. • **Fixed** • **None** • **Waived** • **Will not fix**
Assignee	Specifies the name of the user assigned to the issue.

Option	Definition
Due Date	Specifies whether the issue has a due date and, if so, the date and time the issue is due. Due dates that are in the past are not allowed.

Disaster Recovery example scenarios

Perform failover of your small and medium-sized Trellix ePO - On-prem server (example)

This example task shows how to use the Disaster Recovery Snapshot in the SQL database for recovery if the primary **Trellix ePO - On-prem** server fails.

Before you begin

- If the **Trellix ePO - On-prem** server is damaged, you must restore the SQL database from the backup before performing the failover process.
- See the *Small and medium-sized **Trellix ePO - On-prem** Disaster Recovery network configuration* graphic to reference names and connections described in these steps.

Task

1. **From the primary Trellix ePO - On-prem server, stop these services:**
   a. **Click Start → Run, type** services.msc**, and click OK.**
   b. **Right-click each of the following services and select Stop:**
      - **Trellix ePolicy Orchestrator - On-prem** Application Server
      - **Trellix ePolicy Orchestrator - On-prem** Event Parser
      - **Trellix ePolicy Orchestrator - On-prem** Server
   c. **Double-click each of the following services and change the Startup type to Disabled:**
      - **Trellix ePolicy Orchestrator - On-prem** Application Server
      - **Trellix ePolicy Orchestrator - On-prem** Event Parser
      - **Trellix ePolicy Orchestrator - On-prem** Server
2. **(Optional) If you have remote Agent Handlers, use Windows Services on all Agent Handlers, and stop the Event Parser and Apache services. This step is only required if the primary Agent Handlers aren't used in failover situations.**
3. **On the restore server, install Trellix ePO - On-prem using the same version as the Snapshot:**
   a. **When prompted, click Restore ePO from an existing database Snapshot.**
   b. **Point to the Trellix ePO - On-prem database on SQL-DC1 or SQL-DC2 using a Windows or Active Directory account with local administrator permissions on the Trellix ePO - On-prem server.**
   c. **Use the same drive and directory location used for the Trellix ePO - On-prem software on the EPO-DC1.**
   d. **Point Trellix ePO - On-prem to the SQL-DC1 or SQL-DC2, the physical node hosting the Trellix ePO - On-prem database.**
   e. **Use Windows Active Directory or Server Administration account credentials to access to the Trellix ePO - On-prem database.**
   f. **Confirm the port information is correct.**
   g. **Provide the Trellix ePO - On-prem administrator account and password.**
   h. **Provide the Keystore Password. Recovery takes about 15 minutes, depending on the performance of the Trellix ePO - On-prem server and SQL Server.**
4. **On the DNS server, change the CNAME record in epo.customer.net to point to the restore Trellix ePO - On-prem server.**

5. **(Optional) If you have remote Agent Handlers, change their configuration to use epo.customer.net and to find the restore Trellix ePO - On-prem server based on the CNAME.**
6. **Complete the Trellix ePO - On-prem software installation process using the documented steps until your new Trellix ePO - On-prem server is up and running.**
7. **Confirm your managed systems and remote Agent Handlers (if used) can connect to the restore Trellix ePO - On-prem server.**

Perform failover of your enterprise Trellix ePO - On-prem server (example)

This example task shows how to use the Disaster Recovery Snapshot for recovery if the primary **Trellix ePO - On-prem** server fails.

Before you begin

- If the **Trellix ePO - On-prem** server is damaged, you must restore the SQL database from the backup before performing the failover process.
- You must have a Snapshot and backup of the database on your SQL Server.

Task

1. **From the EPO-DC1 Trellix ePO - On-prem server, stop these services:**
   a. **Click Start → Run, type** services.msc**, and click OK.**
   b. **Right-click each of the following services and select Stop:**
      - **Trellix ePolicy Orchestrator - On-prem** Application Server
      - **Trellix ePolicy Orchestrator - On-prem** Event Parser
      - **Trellix ePolicy Orchestrator - On-prem** Server
   c. **Double-click each of the following services and change the Startup type to Disabled:**
      - **Trellix ePolicy Orchestrator - On-prem** Application Server
      - **Trellix ePolicy Orchestrator - On-prem** Event Parser
      - **Trellix ePolicy Orchestrator - On-prem** Server
2. **Using Windows Services on all Agent Handlers, stop the Event Parser and Apache services. Make sure the Agent Handlers in DC1 aren't active.**
3. **On the SQL Server "Virtual-SQL-name," disable Always On Group.**
4. **On the DNS server, identify the physical node hosting the Trellix ePO - On-prem SQL database. The recovery installation must point to the physical SQL Server (SQL-DC1 or SQL-DC2) during recovery installation, and then change the name to "Virtual-SQL-name" after recovery installation.**
5. **On the restore server, Trellix ePO - On-prem Server-DC2, confirm Trellix ePO - On-prem isn't installed. Delete Trellix ePO - On-prem if it is installed.**
6. **On the restore server, follow the steps to install Trellix ePO - On-prem:**
   a. **When prompted, click Restore ePO from an existing database Snapshot.**
   b. **Point to the Trellix ePO - On-prem database on SQL-DC1 or SQL-DC2 using a Windows or Active Directory account with local administrator permissions on the Trellix ePO - On-prem server.**
   c. **Use the same drive and directory location used for the Trellix ePO - On-prem software on EPO-DC1.**

d. **Point Trellix ePO - On-prem to the SQL-DC1 or SQL-DC2, the physical node hosting the Trellix ePO - On-prem database.**
e. **Use Windows Active Directory or Server Administration account credentials to access to the Trellix ePO - On-prem database.**
f. **Confirm the port information is correct. For detailed port requirements, see *Port configuration from failed to restored McAfee ePO server*.**
g. **Provide the Trellix ePO - On-prem administrator account and password.**
h. **Provide the Keystore Password. Recovery takes about 15 minutes, depending on the performance of the Trellix ePO - On-prem server and SQL Server.**
i. **Install Trellix ePO - On-prem hotfixes in sequential order.**

7. **Change the CNAME record in the DNS for epo.customer.net to point to EPO-DC2 in DC2.**
8. **On the SQL Server "Virtual-SQL-name," enable Always On Group.**
9. **Reconfigure Trellix ePO - On-prem to use the shared SQL resource “Virtual-SQL-name.”**

Note

All Agent Handlers are configured to use epo.customer.net and to find the restored **Trellix ePO - On-prem** server based on the CNAME. For steps on how to set up the published DNS name, see *Configure Agent Handlers list*.

10. **Browse to https://epo.customer.net:8443/core/config and change the host name of the SQL Server to “Virtual-SQL-name.”**
11. **Make sure Trellix ePO - On-prem is uninstalled on EPO-DC1.**
    Follow these steps when reverting **Trellix ePO - On-prem** back from DC2 to DC1.

Small and medium-sized Trellix ePO - On-prem network configuration and components (example)

This is an example of a simple **Trellix ePO - On-prem** network and how it recovers after a **Trellix ePO - On-prem** server failure.

Create a Snapshot of your current **Trellix ePO - On-prem** server and make sure the server task is finished before starting the restore process.

1. **Trellix ePO - On-prem server**
   a. Primary **Trellix ePO - On-prem** server — Used for day-to-day activities. The **Trellix ePO - On-prem** snapshots of the SQL database are completed automatically or initiated manually just after updates occur.

   Note

   By default, server tasks automate snapshots every night.

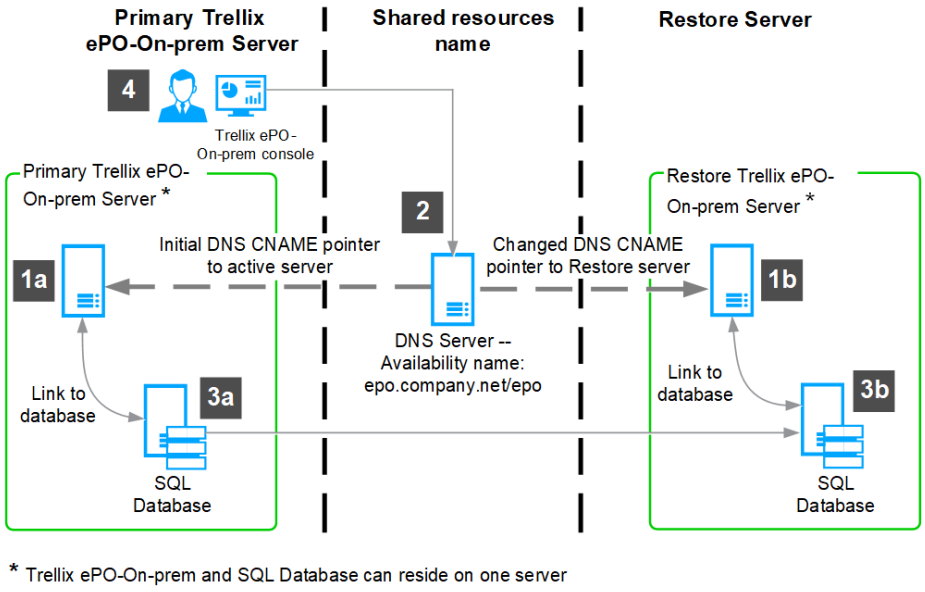
   b. Restore **Trellix ePO - On-prem** server — This server is running with only the SQL database installed. This is where you copy the Disaster Recovery snapshot and SQL database backups from the primary **Trellix ePO - On-prem** server.

Note

After a primary **Trellix ePO - On-prem** server failure, reinstall the **Trellix ePO - On-prem** software using the restore option during the **Trellix ePO - On-prem** setup process.

2. **Shared resource** — The DNS server configured with an availability name (for example, epo.customer.net) uses CNAME to point to the primary **Trellix ePO - On-prem** server, and is configured to point to the restore **Trellix ePO - On-prem** server after a failure.
3. **SQL database servers**
   a. Primary SQL database — Used for day-to-day activities. Use either a Microsoft SQL Server Management Studio or the BACKUP (Transact-SQL) command-line process to copy the Disaster Recovery Snapshots and database backups daily to the Restore SQL database.
   b. Restore SQL database — Used for running and receiving the Disaster Recovery Snapshots and database backups daily from the Primary SQL database.
4. **Trellix ePO console** — Depending on the DNS server configuration, the console is connected to either the primary or restore **Trellix ePO - On-prem** server. The console is used to manage systems, run the SQL backups, and install the **Trellix ePO - On-prem** software.

Small and medium-sized business **Trellix ePO - On-prem** Disaster Recovery network configuration



Enterprise Trellix ePO - On-prem network configuration and components (example)

This is an example of a complex **Trellix ePO - On-prem** network and how it recovers after a **Trellix ePO - On-prem** server failure.

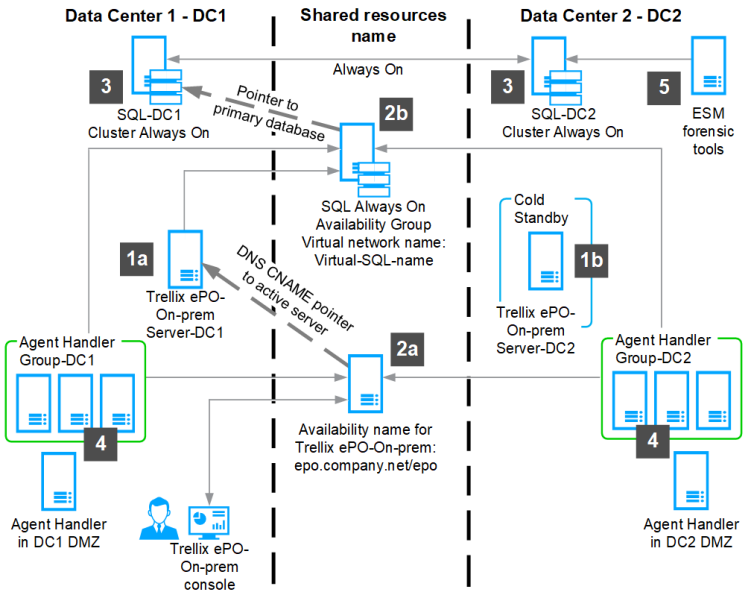
You must create a Snapshot of your current **Trellix ePO - On-prem** server before a failover occurs. Make sure the server task is finished before starting the restore process.

1. **Trellix ePO - On-prem server**
    a. **Trellix ePO - On-prem** server-DC1 — This is the primary **Trellix ePO - On-prem** server used for day-to-day activities. The **Trellix ePO - On-prem** snapshots of the SQL database are completed automatically or initiated manually just after updates occur.

    Note

    By default, server tasks automate snapshots every night.

    b. **Trellix ePO - On-prem** server-DC2 is installed and running in DC2 — This is the ***Cold Standby*** or recovery **Trellix ePO - On-prem** server.
2. **Shared resources**
    a. A **Trellix ePO - On-prem** shared resource name configured using DNS (for example, epo.customer.net) uses CNAME to point to the active **Trellix ePO - On-prem** server, and is configured to point to **Trellix ePO - On-prem** Server-DC1 or **Trellix ePO - On-prem** Server-DC2.
    b. SQL database configured with Always on Availability Groups — The SQL Server is reachable by a virtual name of SQL Availability Group. For example, Virtual-SQL-name. The Snapshots of the SQL database are completed daily and sent to the SQL databases SQL-DC1 and SQL-DC2.
3. **SQL database servers** — Use SQL replication or SQL Log Shipping to copy the **Trellix ePO - On-prem** database from the primary site SQL-DC1 to the secondary site's SQL Server SQL-DC2 in real time.
4. **Agent Handlers** — Agent Handler Groups and Agent Handlers in the DMZ are configured in DC1 and DC2 to use the SQL resource "Virtual-SQL-name."
    - Active-Passive Data Center strategy — Configure all Agent Handlers in DC2 to passive while DC1 is active, and make sure that all Agent Handlers in DC2 aren't running. This is only needed if the date center strategy for Agent Handlers is active-passive. The Agent Handler servers can be in "cold" standby and only turned on when a failover from DC1 to DC2 is initiated. If the Agent Handler servers are running, make sure the two Agent Handler services are stopped and disabled. The DC2 Agent Handlers listed in the Agent Handler Assignment still need to be listed as enabled, so the **Trellix Agent** is aware of their existence and starts looking for them if all DC1 Agent Handlers are unavailable.
    - Active-Active Data Center strategy — All services, except the **Trellix ePO - On-prem** server must be installed and running in both data centers. With this strategy, Agent Handlers are available and running in both data centers. You must have a good network connection between the two data centers because there's heavy traffic between the Agent Handler in one data center and the SQL Server available in the other data center.
5. **Trellix ESM or forensic tools** — These tools can use the second SQL database to relieve the active SQL Server. These tools often only require read-only access to the **Trellix ePO - On-prem** database, SQL-DC2, to monitor events in the database.



Example DNS configuration

Name	Type	Value
epo.customer.net	CNAME	EPO-DC1 or EPO-DC2
EPO-DC1	A	10.1.1.100
EPO-DC2	A	10.2.2.200

How Trellix Agent responds to a restored Trellix ePO - On-prem server

Changes made to a restored **Trellix ePO - On-prem** server cause minimum impact to an existing **Trellix Agent**. **Trellix Agent** communication doesn't change because the Agent Handler IP addresses and FQDN didn't change.

By default, the **Trellix Agent** tries connecting to the **Trellix ePO - On-prem** server in this order, depending on the Agent Handler configuration:

1. IP address of the Agent Handler and **Trellix ePO - On-prem** server.
2. FQDN of the Agent Handler and **Trellix ePO - On-prem** server.
3. NetBIOS name the Agent Handler and **Trellix ePO - On-prem** server.

If you change any of these items, make sure the **Trellix Agent** has a way to locate the server. For example, using the CNAME record, change the existing DNS record so it directs to the new IP address. After the **Trellix Agent** successfully connects to the **Trellix ePO - On-prem** server, it downloads an updated Sitelist.xml with the current information.

SSL certificates

Browsers supported by **Trellix ePO - On-prem** warn about a server's SSL certificate if the browser cannot verify whether a TrustedSource signed the certificate. Creating a self-signed certificate with OpenSSL stops the browser warning.

Creating a self-signed certificate can provide the basic security and functionality needed for systems used on internal networks, or if you don't want to wait for a certification authority to authenticate a certificate.

Create a self-signed certificate with OpenSSL

Sometimes you might not be able to, or want to, wait for a certification authority to authenticate a certificate. During initial testing or for systems used on internal networks, a self-signed certificate can provide the basic security and functionality needed.

Before you begin

To create a self-signed certificate, install the OpenSSL for Windows software. OpenSSL is available from:

http://www.slproweb.com/products/Win32OpenSSL.html

To create and self-sign a certificate to use with your **Trellix ePO - On-prem** server, use OpenSSL for Windows software. There are many tools you can use to create a self-sign a certificate. This task describes the process using OpenSSL.

Note

To have a third party, for example Verisign or Microsoft Windows Enterprise Certificate Authority, create a signed certificate for **Trellix ePO - On-prem**, see How to generate a custom SSL certificate for use with ePO using the OpenSSL toolkit, KB72477.

The file structure used in the following task is:

Note

OpenSSL does not create these folders by default. They are used in these examples and can be created to help you find your output files.

- **C:\ssl** — Installation folder for OpenSSL.
- **C:\ssl\certs** — Used to store the certificates created.
- **C:\ssl\keys** — Used to store the keys created.
- **C:\ssl\requests** — Used to store the certification requests created.

Note

We recommend that you use certificates with RSA public key lengths of 2048 bits or greater.

Task

1. **To generate the initial certificate key, type the following command at the command line:**

   C:\ssl\bin>openssl genrsa -des3 -out C:/ssl/keys/ca.key 2048

   The following screen appears.

```
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....................++++++
.++++++
unable to write 'random state'
e is 65537 (ox10001)
Enter pass phrase for keys/ca.key:
Verifying - Enter pass phrase for keys/ca.key:

C:\ss\bin>
```

2. **Enter a passphrase at the initial command prompt and verify the pass phase at the second command prompt.**

   Note

   Make a note of the passphrase you enter. You need it later in the process.

   The file name **ca.key** is generated and stored in the path **C:\ssl\keys**.

   The key looks similar to the following example.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE327E8D510D1882

4Evg9bqeteKbo6OWyOcFh6o8gUhcOTDn/odppSeykvQBAasEhFfcF+nHLort8KkS
bS9WDAqczf6SdKMxoGbi9m57X/PZ+7dcTH7YyKNKskfoqED7/VZXktAEhA1Vw+wj
.
.
.
im2DEkLWQ3kI+6HdaQHoOFe99ReHZJzvAU6F6LbUNULLpDe3wvnGwMI681fAF9C3
4+KDIt1RhfK3piLpCOM+8L1DpdOg5FC723Z1Drr0uwghKdyDlGRKLw==
-----END RSA PRIVATE KEY-----
```

3. **To self-sign the certificate key you created, type the following command at the command line:**

   openssl req -new -x509 -days 365 -key C:/ssl/keys/ca.key -out C:/ssl/certs/ca.cer

   The following screen appears.

```
Enter pass phrase for ca.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Oregon
Locality Name (eg, city) []:Beaverton
Organization Name (eg, company) [Internet Widgits Pty Ltd]:McAfee
Organizational Unit Name (eg, section) []:Enterprise
Common Name (eg, YOUR name) []:ePO_Server
Email Address []:tester@mcafee.com

C:\ssl\bin>
```

Type the information needed after the following command prompts:

- **Country Name (two letter code) [AU]:**
- **State or Province Name (full name) [Some-State]:**
- **Locality Name (for example, city) []:**
- **Organization Name (for example, company) [Internet Widgits Pty Ltd]:**
- **Organizational Unit Name (for example, section) []:**
- **Common Name (for example, YOUR name) []:**

  Note

  At this command prompt, type the name of your server, for example your **Trellix ePO - On-prem** server name.

- **Email Address []:**

The file named **ca.cer** is generated and stored in the path **C:\ssl\certs**.

The self-signed certificate looks similar to the following example.

```
-----BEGIN CERTIFICATE-----
MIIDdTCCAt6gAwIBAgIJAJe1id+Ih0GDMA0GCSqGSIb3DQEBBQUAMIGEMQswCQYD
VQQGEwJVUzEPMA0GA1UECBMGT1JFR090MRIwEAYDVQQHEwlCRUFWRVJUT04xDzAN
.
.
.
NF/Om6VMhuUy4Cyc5CIyTmGzVPDEo8dK20kdLR+tQhDsdqM5qpfd6w52ew20RKo/
dLGiMtraicXeR2GyWrKJjywow3xBtkvyQQj2xmMWUmDwYjC0YH0lKjV0X+fGwcdX
jWTfB10HV8507ASU0qte0we/BSTMuZWgMA==
-----END CERTIFICATE-----
```

4. **To upload the self-signed certificate, open the Edit Server Certificate page.**
    a. **Select Menu → Configuration → Server Settings.**
    b. **From the Setting Categories list, select Server Certificate, and click Edit.**
5. **Browse to the server certificate file, then click Open.**
   In this example, browse to **C:\ssl\certs** and select **ca.cer**.
6. **If needed, type the PKCS12 certificate password.**
7. **If needed, type the certificate alias name.**
8. **Browse to the private key file, then click Open.**
   In this example, browse to **C:\ssl\keys** and select **ca.key**.
9. **If needed, type the private key password, then click Save.**
10. **Restart Trellix ePO - On-prem for the change to take effect.**

Other useful OpenSSL commands

You can use other OpenSSL commands to extract and combine the keys in generated PKCS12 certificates. You can also convert a password protected private key PEM file to a non-password protected file.

Commands to use with PKCS12 certificates

Use these commands to create a PKCS12 certificate with both the certificate and key in one file.

Description	OpenSSL command format
Create a certificate and key in one file	**openssl req -x509 -nodes -days 365 -newkey rsa:1024 -config *path* \openssl.cnf -keyout *path* \pkcs12Example.pem -out *path* \pkcs12Example.pem**
Export the PKCS12 version of the certificate	**openssl pkcs12 -export -out *path* \pkcs12Example.pfx -in *path* \pkcs12Example.pem -name " *user_name_string* "**

Use these commands to separate the certificate and key from a PKCS12 certificate with them combined.

Description	OpenSSL command format
Extracts the .pem key out of .pfx	**openssl pkcs12 -in pkcs12ExampleKey.pfx -out pkcs12ExampleKey.pem**
Removes password on key	**openssl rsa -in pkcs12ExampleKey.pem -out pkcs12ExampleKeyNoPW.pem**

Description	OpenSSL command format
	Note: The **Trellix ePO - On-prem** server can then use the **pkcs12ExampleCert.pem** as the certificate and the **pkcs12ExampleKey.pem** as the key (or the key without a password **pkcs12ExampleKeyNoPW.pem**).

Command to convert a password protected private key PEM file

To convert a password protected private key PEM file to a non-password protected file, type:

```
openssl rsa -in C:\ssl\keys\key.pem -out C:\ssl\keys\keyNoPassword.pem
```

Note

In the previous example, **C:\ssl\keys** is the input and output paths for the file names **key.pem** and **keyNoPassword.pem**.

Convert an existing PVK file to a PEM file

The **Trellix ePO - On-prem** software supports PEM-encoded private keys, including both password protected and non-password protected private keys. Using OpenSSL you can convert a PVK-formatted key to a PEM format.

Before you begin

To convert the PVK formatted file, install the OpenSSL for Windows software. This software is available from:

http://www.slproweb.com/products/Win32OpenSSL.html

Using the OpenSSL for Windows software, convert your PVK format certificate to PEM format.

Task

1. **To convert a previously created PVK file to a PEM file, type the following at the command line:**
   ```
   openssl rsa -inform PVK -outform PEM -in C:\ssl\keys\myPrivateKey.pvk -out C:\ssl\keys\myPrivateKey.pem -passin pass:p@$$w0rd -passout pass:p@$$w0rd
   ```

   Note

   In this example, **-passin** and **-passout** arguments are optional.

2. **If prompted, type the password used when you originally created the PVK file.**
   If the **-passout** argument is not used in the example, the newly created PEM-formatted key is not password protected.

Migrate Certificate Authority Hashing Algorithm from SHA-1 to SHA-2 or higher

To remediate vulnerabilities in your **Trellix ePO - On-prem** environment, migrate your existing certificates to more secure algorithm certificates or regenerate them.

The SHA-1 algorithm has reached end-of-life (EOL). Many organizations are deprecating TLS/SSL certificates signed by the SHA-1 algorithm. If you continue to use SHA-1 certificates, browsers such as Google Chrome or Microsoft Internet Explorer will flag the **Trellix ePO - On-prem** console as an unsecure HTTPS site.

If you have upgraded **Trellix ePO - On-prem** from an older version, migrate **Trellix ePO - On-prem** certificates to the latest hash algorithm. A fresh installation of **Trellix ePO - On-prem** installs the latest hash algorithm certificates.

The **Certificate Manager** allows you to:

- Migrate certificates that are signed by older signing algorithm to the new algorithm such as SHA-1 to SHA-256.
- Regenerate your certificates when your existing certificates are compromised due to vulnerabilities in your environment.
- Migrate or regenerate certificates for managed products that are derived from **Trellix ePO - On-prem** root CA.

This task replaces certificates that are used for:

- Agent-server communication
- Authenticating to browsers
- Certificate-based user authentication

Important

Read these instructions carefully before proceeding with the steps. If you activate the new certificates before they are populated on the systems in your network, those systems won't be able to connect to your **Trellix ePO - On-prem** server until the agents on those systems are re-installed.

Task

1. **Log on as an administrator, then select Menu → Configuration → Certificate Manager.**
   The Certificate Manager page provides information about the installed Root Certificate, Agent Handler certificates, server certificates, and other certificates that are derived from **Trellix ePO - On-prem** root Certificate Authority (CA).
2. **Click Regenerate Certificate, then click OK to confirm.**
   The **Trellix ePO - On-prem** root CA and other certificates that are derived from the root CA are regenerated and stored in a temporary location on the server. The time required to complete the process depends on the number of Agent Handlers and extensions that derive certificates from **Trellix ePO - On-prem** root CA.
3. **After the certificates regenerate, wait for sufficient saturation of the new certificates throughout your environment.**
   As agents communicate to the **Trellix ePO - On-prem** server, they are given the new certificate. The percentage of agents that have received the newly-generated certificates is provided in the **Certificate Manager** under **Product: Agent Handler → Status**.

Important

Make sure that the distribution percentage is as close to 100% as possible before you continue. Otherwise, pending systems might not receive the newly generated certificates and won't be able to communicate with the **Trellix ePO - On-prem** after the certificates are activated. You can stay in this state for as long as is necessary to achieve sufficient saturation.

4. **Once you've achieved a distribution percentage close to 100%, click Activate Certificates to carry out all future operations using the new certificates.**
   A backup of the original certificates is created, and a message appears.
5. **Click OK.**
6. **Stop and start these services:**
   a. **Stop the Agent Handler services.**
   b. **Restart the Trellix ePO - On-prem services.**
   c. **Start the Agent Handler services.**
7. **Monitor your environment and make sure that your agents are successfully communicating.**
   You can cancel the migration at this point to roll back the certificate and restore agent-to-server communication; however, this is not possible after you have completed the next step.
8. **Click Finish Migration to complete the certificate migration.**
   For any issues during the migration, click **Cancel Migration** to revert to the previous certificates. If you cancel the migration, stop the Agent Handler services, restart the **Trellix ePO - On-prem** service, and start the Agent Handler service again.

   You can start the certificate migration again after fixing any issues.

9. **Re-install any agents that use the old certificates to restore agent-server communication.**

Security keys and how they work

The **Trellix ePO - On-prem** server relies on three security key pairs.

The three security pairs are used to:

- Authenticate agent-server communication.
- Verify the contents of local repositories.
- Verify the contents of remote repositories.

Each pair's secret key signs messages or packages at their source, while the pair's public key verifies the messages or packages at their target.

Agent-server secure communication (ASSC) keys

- The first time the agent communicates with the server, it sends its public key to the server.
- From then on, the server uses the agent public key to verify messages signed with the agent's secret key.
- The server uses its own secret key to sign its message to the agent.
- The agent uses the server's public key to verify the server's message.
- You can have multiple secure communication key pairs, ***but only one can be designated as the main key***.

- When the client agent key updater task runs (**Trellix ePO Agent Key Updater**), agents using different public keys receive the current public key.
- When you upgrade, existing keys are migrated to your **Trellix ePO - On-prem** server.

Local main repository key pairs

- The repository secret key signs the package before it is checked in to the repository.
- The repository public key verifies repository package contents.
- The agent retrieves available new content each time the client update task runs.
- This key pair is unique to each server.
- By exporting and importing keys among servers, you can use the same key pair in a multi-server environment.

Other repository key pairs

- The secret key of a trusted source signs its content when posting that content to its remote repository. Trusted sources include the **Trellix** download site and the **Trellix** Security Innovation Alliance (SIA) repository.

  ⚠ Caution

  If this key is deleted, you cannot perform a pull, even if you import a key from another server. Before you overwrite or delete this key, make sure to back it up in a secure location.

- The **Trellix Agent** public key verifies content that is retrieved from the remote repository.

Main Repository key pair

The **Main Repository** private key signs all unsigned content in the **Main Repository**.

Agents use the public key to verify the repository content that originates from the **Main Repository** on this **Trellix ePO - On-prem** server. If the content is unsigned, or signed with an unknown repository private key, the downloaded content is considered invalid and deleted.

This key pair is unique to each server installation. However, by exporting and importing keys, you can use the same key pair in a multi-server environment. Doing so ensures that agents can always connect to one of your Main Repositories, even when another repository is down.

Other repository public keys

Keys, other than the main key pair, are the public keys that agents use to verify content from other main Repositories in your environment or from **Trellix** source sites. Each agent reporting to this server uses the keys in the **Other repository public keys** list to verify content that originates from other **Trellix ePO - On-prem** servers in your organization, or from **Trellix** sources.

If an agent downloads content that originated from a source where the agent does not have the appropriate public key, the agent discards the content.

These keys are a new feature, and only agents 4.0 and later are able to use the new protocols.

Manage repository keys

Use one Main Repository key pair for all servers

You can ensure that all **Trellix ePO - On-prem** servers and agents use the same **Main Repository** key pair in a multi-server environment using **Server Settings**.

This process consists of first exporting the key pair you want all servers to use, then importing the key pair into all other servers in your environment.

Task

1. **Select Menu → Configuration → Server Settings, select Security Keys from the Setting Categories list, then click Edit.**
2. **From the Edit Security Keys page next to Local main repository key pair, click Export Key Pair.**
3. **Click OK. The File Download dialog box appears.**
4. **Click Save, browse to a location that is accessible by the other servers, where you want to save the .zip file containing the secure-communication key files, then click Save.**
5. **Next to Import and back up keys, click Import.**
6. **Browse to the .zip file containing the exported Main Repository key files, then click Next.**
7. **Verify that these are the keys you want to import, then click Save.**

Results

The imported **Main Repository** key pair replaces the existing key pair on this server. Agents begin using the new key pair after the next agent update task runs. Once the **Main Repository** key pair is changed, an ASSC must be performed before the agent can use the new key.

Use Main Repository keys in multi-server environments

Make sure that agents can use content originating from any **Trellix ePO - On-prem** server in your environment using **Server Settings**.

The server signs all unsigned content that is checked in to the repository with the **Main Repository** private key. Agents use repository public keys to validate content that is retrieved from repositories in your organization or from **Trellix** source sites.

The **Main Repository** key pair is unique for each installation of **Trellix ePO - On-prem**. If you use multiple servers, each uses a different key. If your agents can download content that originates from different Main Repositories, you must make sure that agents recognize the content as valid.

You can complete this process in two ways:

- Use the same **Main Repository** key pair for all servers and agents.
- Make sure that agents are configured to recognize any repository public key that is used in your environment.

This task exports the key pair from one **Trellix ePO - On-prem** server to a target **Trellix ePO - On-prem** server, then, at the target **Trellix ePO - On-prem** server, imports, and overwrites the existing key pair.

Task

1. On the Trellix ePO - On-prem server with the Main Repository key pair, select Menu → Configuration → Server Settings, select Security Keys from the Setting Categories list, then click Edit.
2. Next to Local main repository key pair, click Export Key Pair, then click OK.
3. In the File Download dialog box, click Save.
4. Browse to a location on the target Trellix ePO - On-prem server to save the .zip file. Change the name of the file if needed, then click Save.
5. On the target Trellix ePO - On-prem server where you want to load the Main Repository key pair, select Menu → Configuration → Server Settings, select Security Keys from the Setting Categories list, then click Edit.
6. On the Edit Security Keys page:
    a. Next to Import and back up keys, click Import.
    b. Next to Select file, browse to and select the main key pair file you saved, then click Next.
    c. If the summary information appears correct, click Save. The new main key pair appears in the list next to Agent-server secure communication keys.
7. From the list, select the file you imported in the previous steps, then click Make Main. This setting changes the existing main key pair to the new key pair you imported.
8. Click Save to complete the process.

Agent-server secure communication (ASSC) keys

Agents use ASSC keys to communicate securely with the server.

You can make any ASSC key pair the main, which is the key pair currently assigned to all deployed agents. Existing agents that use other keys in the **Agent-server secure communication keys** list do not change to the new main key unless there is a client agent key updater task scheduled and run.

⚠ Caution

Make sure to wait until all agents have updated to the new main before deleting older keys.

Manage ASSC keys

Generate, export, import, or delete agent-server secure communication (ASSC) keys from the **Server Settings** page.

Task

1. Select Menu → Configuration → Server Settings, select Security Keys, then click Edit.
2. Select one of these actions.

Action	Steps
Generate and use new ASSC key pairs	a. Next to the **Agent-server secure communication keys** list, click **New Key**. In

Action	Steps
	the dialog box, type the name of the security key. b. If you want existing agents to use the new key, select the key in the list, then click **Make main**. Agents begin using the new key after the next **Trellix Agent** update task is complete. Make sure that there is an Agent Key Updater package for each version of the **Trellix Agent** managed by **Trellix ePO - On-prem**. ⚠ **Caution:** In large installations, only generate and use new main key pairs when you have specific reason to do so. We recommend performing this procedure in phases so that you can more closely monitor progress. c. After all agents have stopped using the old key, delete it. In the list of keys, the number of agents currently using that key is displayed to the right of every key. d. Back up all keys.
Export ASSC keys	Export ASSC keys from one **Trellix ePO - On-prem** server to a different **Trellix ePO - On-prem** server, to allow agents to access the new **Trellix ePO - On-prem** server. a. In the **Agent-server secure communication keys** list, select a key, then click **Export**. b. Click **OK**. Your browser prompts you to download the **sr<ServerName>.zip** file to the specified location.

Action	Steps
	Note: If you specified a default location for all browser downloads, this file might be automatically saved to that location.
Import ASSC keys	Import ASSC keys that were exported from a different **Trellix ePO - On-prem** server, allowing agents from that server to access this **Trellix ePO - On-prem** server. a. Click **Import**. b. Browse to and select the key from the location where you saved it (by default, on the desktop), then click **Open**. c. Click **Next** and review the information about the Import Keys page. d. Click **Save**.
Designate an ASSC key pair as the main	Change which key pair is specified as the main. Specify a main key pair after importing or generating a new key pair. a. From the **Agent-server secure communication keys** list, select a key, then click **Make main**. b. Create an update task for the agents to run immediately, so that agents update after the next agent-server communication. **Note:** Make sure that the Agent Key Updater package is checked in to the **Trellix ePO - On-prem main Repository**. Agents begin using the new key pair after the next update task for the **Trellix Agent** is complete. At any time, you can see which agents are using any of the ASSC key pairs in the list. c. Back up all keys.

Action	Steps
Delete ASSC keys	**Caution:** Do not delete any keys that are being used by any agents. If you do, those agents cannot communicate with the **Trellix ePO - On-prem** server. a. From the **Agent-server secure communication keys** list, select the key that you want to remove, then click **Delete**. b. Click **OK** to delete the key pair from this server.

View systems that use an ASSC key pair

You can view the systems whose agents use a specific agent-server secure communication key pair in the **Agent-server secure communication keys** list.

After making a specific key pair as the main, you might want to view the systems that are still using the previous key pair. Do not delete a key pair until you know that no agents are still using it.

Task

1. **Select Menu → Configuration → Server Settings, select Security Keys from the Setting Categories list, then click Edit.**
2. **In the Agent-server secure communication keys list, select a key, then click View Agents.**

Results

This **Systems using this key** page lists all systems whose agents are using the selected key.

Use the same ASSC key pair for all servers and agents

Verify that all **Trellix ePO - On-prem** servers and agents use the same agent-server secure communication (ASSC) key pair.

Tip

If you have many managed systems in your environment, **Trellix** recommends performing this process in phases so you can monitor agent updates.

Task

1. **Create an agent update task.**
2. **Export the keys chosen from the selected Trellix ePO - On-prem server.**
3. **Import the exported keys to all other servers.**

4. **Designate the imported key as the main on all servers.**
5. **Perform two agent wake-up calls.**
6. **When all agents are using the new keys, delete any unused keys.**
7. **Back up all keys.**

Use a different ASSC key pair for each Trellix ePO - On-prem server

You can use a different ASSC key pair for each **Trellix ePO - On-prem** server to ensure that all agents can communicate with the required **Trellix ePO - On-prem** servers in an environment where each server must have a unique agent-server secure communication key pair.

Note

Agents can communicate with only one server at a time. The **Trellix ePO - On-prem** server can have multiple keys to communicate with different agents, but the opposite is not true. Agents cannot have multiple keys to communicate with multiple **Trellix ePO - On-prem** servers.

Task

1. **From each Trellix ePO - On-prem server in your environment, export the main agent-server secure communication key pair to a temporary location.**
2. **Import each of these key pairs into every Trellix ePO - On-prem server.**

Back up and restore keys

Periodically back up all security keys, and always create a backup before changing the key management settings.

Store the backup in a secure network location, so that the keys can be restored easily in the unexpected event any are lost from the **Trellix ePO - On-prem** server.

Task

1. **Select Menu → Configuration → Server Settings, select Security Keys from the Setting Categories list, then click Edit.**
2. **From the Edit Security Keys page, select one of these actions.**

Action	Steps
Back up all security keys.	a. Click **Back Up All** near the bottom of the page. The Backup Keystore dialog box appears. b. You can optionally enter a password to encrypt the Keystore .zip file or click **OK** to save the files as unencrypted text. c. From the File Download dialog box, click **Save** to create a .zip file of all security keys. The Save As dialog box appears.

Action	Steps
	d. Browse to a secure network location to store the .zip file, then click **Save**.
Restore security keys.	a. Click **Restore All** near the bottom of the page. The Restore Security Keys page appears. b. Browse to the .zip file containing the security keys, select it, and click **Next**. The Restore Security Keys wizard opens to the Summary page. c. Browse to the keys you want to replace your existing key with, then click **Next**. d. Click **Restore**. The Edit Security Keys page reappears. e. Browse to a secure network location to store the .zip file, then click **Save**.
Restore security keys from a backup file.	a. Click **Restore All** near the bottom of the page. The Restore Security Keys page appears. b. Browse to the .zip file containing the security keys, select it, and click **Next**. The Restore Security Keys wizard opens to the Summary page. c. Browse to and select the backup .zip file, then click **Next**. d. Click **Restore All** at the bottom of the page. The Restore Security Keys wizard opens. e. Browse to and select the backup .zip file, then click **Next**. f. Verify that the keys in this file are the ones you want to overwrite your existing keys, then click **Restore All**.

Edit Product Improvement Program page

The **Trellix Product Improvement Program** helps improve **Trellix** products. It collects data proactively and periodically from the client systems managed by the **Trellix ePO - On-prem** server.

Option definitions

Option	Definition
Allow McAfee to collect anonymous diagnostic and usage data	• **Yes** — Allows the data collection. • **No** — Stops the data collection.

Ports overview

Change console-to-application server communication port

If the **Trellix ePO - On-prem** console-to-application server communication port is in use by another application, follow these steps to specify a different port.

Before you begin

- Back up your registry and understand the restore process. For more information, see the Microsoft documentation.
- Make sure that you run only **.reg** files that are not confirmed to be genuine registry import files.

Important

This topic contains information about opening or modifying the registry. This information is intended for use by network and system administrators only. Registry modifications are irreversible and can cause system failure if done incorrectly.

Task

1. **Stop the Trellix ePO - On-prem services:**
   a. **Close all Trellix ePO - On-prem consoles.**
   b. **Click Start → Run, type** services.msc**, then click OK.**
   c. **Right-click each of these services and select Stop:**
      - **Trellix ePolicy Orchestrator Application Server**
      - **Trellix ePolicy Orchestrator Event Parser**
      - **Trellix ePolicy Orchestrator Server**
2. **In the registry editor, select this key: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{53B73DFD-AFBE-4715-88A1-777FE404B6AF}]**
3. **In the right pane, double-click TomcatSecurePort.SQL and change the value data to reflect the required port number (default is 8443).**
4. **Open a text editor and paste this line into a blank document:**

   ```
   UPDATE EPOServerInfo SET rmdSecureHttpPort =8443
   ```

   Change 8443 to the new port number.
5. **Name the file TomcatSecurePort.sql and save it to a temporary location on the SQL Server.**
6. **Use Microsoft SQL Server Management Studio to install the** TomcatSecurePort.SQL **file that you created.**
   a. **Click Start → All Programs → Microsoft SQL Server Management Studio.**
   b. **On the Connect to Server dialog box, click Connect.**
   c. **Expand Databases, then select ePO database.**
   d. **From the toolbar, select New Query.**
   e. **Click File → Open → File..., then browse to the TomcatSecurePort.sql file.**

f. **Select the file, click Open → Execute.**

7. **In Windows Explorer, browse to this directory:**
   \Program Files (x86)**Trellix****Trellix ePO - On-prem**\Server\conf\
8. **In Notepad, open Server.xml and replace all entries for port 8443 with the new port number.**
9. **Click Start → Run, type** services.msc**, then click OK.**
10. **Right-click each of these services and select Start:**
    - **Trellix ePolicy Orchestrator Application Server**
    - **Trellix ePolicy Orchestrator Event Parser**
    - **Trellix ePolicy Orchestrator Server**

Change agent-server communication port

Follow these steps to change the agent-server communication port.

Before you begin

Important

This topic contains information about opening or modifying the registry. This information is for network and system administrators only. Registry modifications are irreversible and can cause system failure if done incorrectly.

- We strongly recommend that you back up your registry and understand the restore process. For more information, see the Microsoft documentation.
- Make sure that you run only .REG files that are confirmed to be genuine registry import files.

Modifying the agent-server communication port requires five steps and one optional step if you are using remote **Agent Handlers**.

1. Stop the **Trellix ePO - On-prem** services
2. Modify the port value in the registry
3. Modify the value in the **Trellix ePO - On-prem** database
4. Modify the port value in the **Trellix ePO - On-prem** configuration files
5. Restart the **Trellix ePO - On-prem** services
6. **(Optional)** Modify settings on remote Agent Handlers

Task

1. **Stop the Trellix ePO - On-prem services:**
   a. **Close all Trellix ePO - On-prem consoles.**
   b. **Click Start → Run, type** services.msc**, then click OK.**
   c. **Right-click each of these services and select Stop:**
      - **McAfee ePolicy Orchestrator Application Server**
      - **McAfee ePolicy Orchestrator Event Parser**
      - **McAfee ePolicy Orchestrator Server**
2. **Modify the port value in the registry:**

a. **Click Start → Run, type `regedit`, then click OK.**
b. **Navigate to the key that corresponds to Trellix ePO - On-prem:** [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{ 53B73DFD-AFBE-4715-88A1-777FE404B6AF}]
c. **Modify the string value `AgentPort` to reflect the appropriate port, then close the registry editor. The default value for this port is `80`.**

3. **Modify the value in the Trellix ePO - On-prem database:**
   a. **Open a text editor, and add these lines to the blank document:**

```
UPDATE EPOServerInfo
ServerHTTPPort=80
```

   b. **Save the file as DefaultAgentPort.SQL in a temporary location on the SQL Server.**
   c. **Click Start → All Programs → Microsoft SQL Server Management Studio to use Microsoft SQL Server Management Studio to install the DefaultAgentPort.sql file.**
   d. **On the Connect to Server dialog box, click Connect.**
   e. **Expand Databases, then select ePO database.**
   f. **From the toolbar, select New Query.**
   g. **Click File → Open → File, browse to and select the DefaultAgent.SQL file, then click Open → Execute.**
   h. **Paste this line into a blank document:**

```
UPDATE EPOServerInfo SET ServerHTTPPort =80
```

   Change `80` to the new port number.
   i. **Name the file `DefaultAgentPort.SQL` and save it to a temporary location on the SQL Server.**
   j. **Use Microsoft SQL Server Management Studio to install the `DefaultAgentPort.SQL` file.**

- Click **Start → All Programs → Microsoft SQL Server Management Studio**.
- On the **Connect to Server** dialog box, click **Connect**.
- Expand **Databases**, then select **ePO database**.
- From the toolbar, select **New Query**.
- Click **File → Open → File**, browse to and select the DefaultAgentPort.SQL file, then click **Open → Execute.**

4. **Modify the port value in the Trellix ePO - On-prem configuration files:**
   a. **Navigate to C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\....**
   b. **Using a text editor, open Server.ini and change the value for `HTTPPort=80` to reflect the new number, then save the file.**
   c. **Using a text editor, open Siteinfo.ini and change the value for `HTTPPort=80` to reflect the new number, then save the file.**
   d. **Navigate to C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Apache2\conf\..., open httpd.conf, then change these lines to reflect the new port number:**

```
Listen 80
ServerName<YourServerName>: 80
```

If using VirtualHosts, change:

```
NameVirtualHost *:80
<VirtualHost *:80>
```

e. Save the file and exit the text editor.

5. Restart the Trellix ePO - On-prem services:
   a. Click Start → Run, type services.msc, then click OK.
   b. Right-click each of these services and select Start:
      - McAfee ePolicy Orchestrator Application Server
      - McAfee ePolicy Orchestrator Event Parser
      - McAfee ePolicy Orchestrator Server
6. (Optional) Modify settings on remote Agent Handlers:
   a. Make sure that all Trellix ePO - On-prem consoles are closed, then click Start → Run, type services.msc and click OK.
   b. Right-click each of these services and select Start:
      - McAfee ePolicy Orchestrator Event Parser
      - McAfee ePolicy Orchestrator Server

      Note

      This server might be listed as MCAFEEAPACHESRV if the server wasn't restarted since the Agent Handler was installed.

   c. Navigate to C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Apache2\conf\..., using a text editor open httpd.conf, then change these lines to reflect the new port number:

```
Listen 80
ServerName<YourServerName>: 80
```

   If using VirtualHosts, change:

```
NameVirtualHost *:80
<VirtualHost *:80>
```

   d. Save the file and exit the text editor.
   e. Click Start → Run, type services.msc, then click OK.
   f. Right-click each of these services and select Start.
      - McAfee ePolicy Orchestrator Event Parser
      - McAfee ePolicy Orchestrator Server

Note

This server might be listed as MCAFEEAPACHESRV if the server has not been restarted since the Agent Handler was installed.

If you previously deployed agents to clients, reinstall the agent on all clients using the /forceinstall switch to overwrite the existing Sitelist.xml file. For more information about specific **Trellix Agent** versions that allow the /forceinstall switch to work successfully, see **Trellix** KnowledgeBase article KB60555.

Ports required for communicating through a firewall

Use these ports to configure a firewall to allow traffic to and from your **Trellix ePO - On-prem** server.

Relevant terms

- *Bidirectional* — The remote or local system can initiate the connection.
- *Inbound* — The remote system initiates the connection.
- *Outbound* — The local system initiates the connection.

Trellix ePO - On-prem server

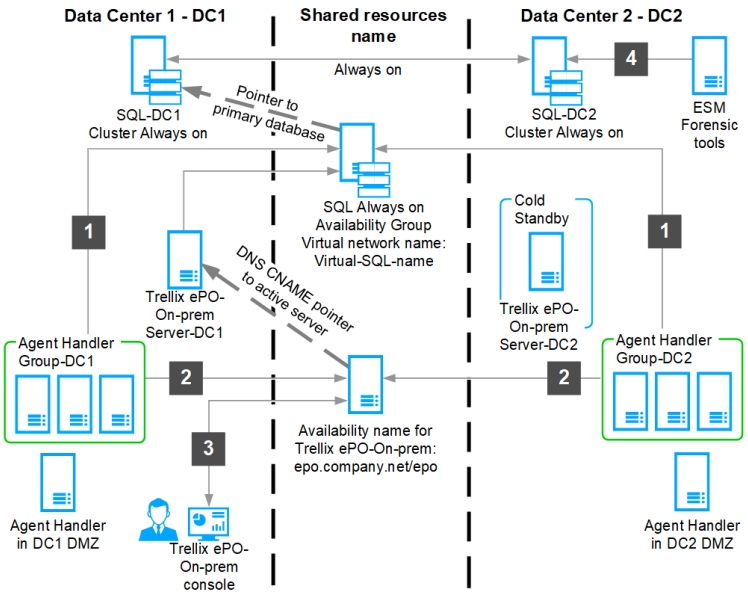
Port	Default	Description	Traffic direction
Agent-server communication port	80	TCP port opened by the **Trellix ePO - On-prem** server service to receive requests from agents.	Bidirectional between the **Agent Handler** and the **Trellix ePO - On-prem** server and inbound from **Trellix Agent** to **Agent Handlers** and **Trellix ePO - On-prem** server.
Agent communicating over SSL	443	By default, agents must communicate over SSL (443 by default). This port is also used for the **Remote Agent Handler** to communicate with the **Trellix ePO - On-prem main Repository**.	Inbound connection to the **Trellix ePO - On-prem** server from agents or **Agent Handlers** to the **main Repository**. Inbound connection: • Agent to **Trellix ePO - On-prem** • **Agent Handler** to **main Repository** • **Trellix ePO - On-prem** to **main Repository**

Port	Default	Description	Traffic direction
			• Agent to **Agent Handler**
Agent wake-up communication port SuperAgent repository port	8081	TCP port opened by agents to receive agent wake-up requests from the **Trellix ePO - On-prem** server. TCP port opened to replicate repository content to a **SuperAgent** repository.	Outbound connection from the **Trellix ePO - On-prem** server and **Agent Handler** to the **Trellix Agent**.
Agent broadcast communication port	8082	UDP port opened by **SuperAgent** to forward messages from the **Trellix ePO - On-prem** server and **Agent Handler**.	Outbound connection from the **SuperAgent** to other agents.
Console-to-application server communication port	8443	HTTPS port opened by the **Trellix ePO - On-prem** Application Server service to allow web browser console access.	Inbound connection to the **Trellix ePO - On-prem** server from the **Trellix ePO - On-prem** console.
Client-to-server authenticated communication port	8444	Used by the **Agent Handler** to communicate with the **Trellix ePO - On-prem** server to get required information (for example, LDAP servers).	Outbound connection from remote **Agent Handlers** to the **Trellix ePO - On-prem** server.
SQL Server TCP port	1433	TCP port used to communicate with the SQL Server. This port is specified or determined	Outbound connection from the **Trellix ePO - On-prem** server and

Port	Default	Description	Traffic direction
		automatically during the setup process.	**Agent Handler** to the SQL Server.
SQL Server UDP port	1434	UDP port used to request the TCP port that the SQL instance hosting the **Trellix ePO - On-prem** database is using.	Outbound connection from the **Trellix ePO - On-prem** server and **Agent Handler** to the SQL Server.
Default LDAP server port	389	LDAP connection to look up computers, users, groups, and Organizational Units for User-Based Policies.	Outbound connection from the **Trellix ePO - On-prem** server and **Agent Handler** to an LDAP server.
Default SSL LDAP server port	636	User-Based Policies use the LDAP connection to look up users, groups, and Organizational Units.	Outbound connection from the **Trellix ePO - On-prem** server and **Agent Handler** to an LDAP server.

Port configuration from failed to restored Trellix ePO - On-prem server

Use these port configurations when restoring a failed McAfee ePO server.



Number	Ports	Connections
1	SQL 1433 (SSL)	Agent Handler group to virtual SQL name
2	80, 443, 8443, 8444	Agent Handler group to **Trellix ePO - On-prem** virtual name
3	8443	**Trellix ePO - On-prem** virtual name to **Trellix ePO - On-prem** console
4	Read only access to secondary replica	ESM to SQL-DC2

Traffic quick reference

Use this port and traffic direction information to configure a firewall to allow traffic to and from your **Trellix ePO - On-prem** server.

Relevant terms

- *Bidirectional* — A local or remote system can initiate the connection.
- *Inbound* — A remote system can initiate the connection.
- *Outbound* — A local system can initiate the connection.

Agent Handler

Default port	Protocol	Traffic direction on Trellix ePO - On-prem server	Traffic direction on Agent Handler
80	TCP	Bidirectional connection to and from **Trellix ePO - On-prem** server.	Bidirectional connection to and from **Agent Handler**.
389	TCP	Outbound connection from **Trellix ePO - On-prem** server.	Outbound connection from **Agent Handler**.
443	TCP	Inbound connection to **Trellix ePO - On-prem** server.	Inbound connection to the **Agent Handler**.
636	TCP	Outbound connection from **Trellix ePO - On-prem** server.	Outbound connection from **Agent Handler**.
1433	TCP	Outbound connection from **Trellix ePO - On-prem** server.	Outbound connection from **Agent Handler**.
1434	UDP	Outbound connection from **Trellix ePO - On-prem** server.	Outbound connection from **Agent Handler**.

Default port	Protocol	Traffic direction on Trellix ePO - On-prem server	Traffic direction on Agent Handler
8081	TCP	Outbound connection from **Trellix ePO - On-prem** server.	
8443	TCP	Inbound connection to **Trellix ePO - On-prem** server.	Outbound connection from **Agent Handler**.
8444	TCP	Inbound connection to **Trellix ePO - On-prem** server.	Outbound connection from **Agent Handler**.

Trellix Agent

Default port	Protocol	Traffic direction
80	TCP	Outbound connection to **Trellix ePO - On-prem** server and **Agent Handler**.
443	TCP	Outbound connection to the **Trellix ePO - On-prem** server and **Agent Handler**.
8081	TCP	Inbound connection from the **Trellix ePO - On-prem** server and **Agent Handler**. **Note:** If the agent is a **SuperAgent** repository, the inbound connection is from other agents.
8082	UDP	Inbound connection to agents.

Default port	Protocol	Traffic direction
		Note: Inbound and outbound connection is from or to a **SuperAgent**.

SQL Server

Default port	Protocol	Traffic direction
1433	TCP	Inbound connection from **Trellix ePO - On-prem** server and **Agent Handler**.
1434	UDP	Inbound connection from **Trellix ePO - On-prem** server and **Agent Handler**.

COPYRIGHT

Trellix