BeyondTrust

Endpoint Privilege Management for Windows
ePO Extension 23.10 Installation Guide

TC:1/23/2024

Table of Contents

Endpoint Privilege Management for Windows ePO Extension Installation

Endpoint Privilege Management for Windows combines privilege management and application control technology in a single, lightweight agent. This scalable solution allows global organizations to eliminate admin rights across the entire business.

Actionable intelligence is provided by an enterprise class reporting solution with endpoint analysis, dashboards, and trend data for auditing and compliance.

This guide assumes that you have set up your ePO server and you now need to install the Endpoint Privilege Management ePO Extension.

This guide shows you how to install the Endpoint Privilege Management ePO Extension, create a client task to deploy Endpoint Privilege Management to your endpoints, and configure your ePO server for Endpoint Privilege Management tasks.

If you are upgrading an existing BeyondTrust Endpoint Privilege Management ePO Extension, please see "Install the Endpoint Privilege Management ePO Extension" on page 5.

BeyondTrust Endpoint Privilege Management App

Starting in version 23.10, we are updating and enhancing the policy editing and reporting experience for our Endpoint Privilege Management for Windows and Mac solution deployed via Trellix ePolicy Orchestrator (ePO). This new experience will mean policy editing and reporting will happen outside of the ePO extension and will instead be delivered via a new Electron-based application called the BeyondTrust Endpoint Privilege Management App, published by BeyondTrust.

For more information, please see:

- *BeyondTrust Endpoint Privilege Management App User Guide*
- *BeyondTrust Endpoint Privilege Management App Frequently Asked Questions*

Install the Endpoint Privilege Management ePO Extension

The Endpoint Privilege ManagementePO Extension:

- Allows you to use Trellix ePolicy Orchestrator to manage your endpoints.
- The installer is a ZIP file and includes the build number in its name.

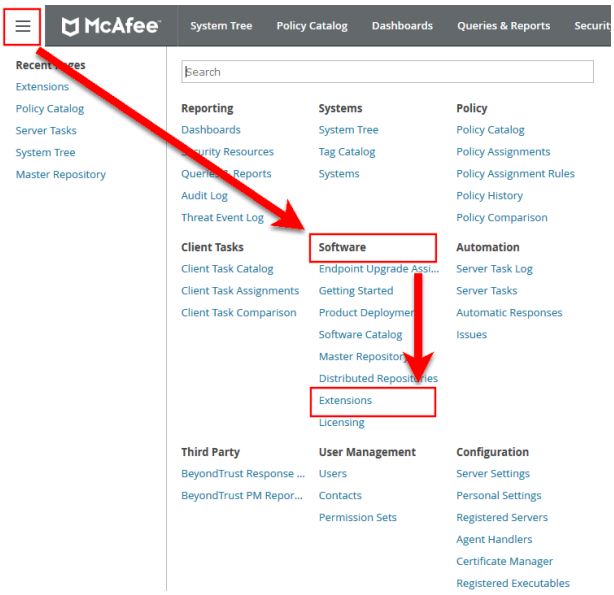
Requirements

> *For more information, please see Endpoint Privilege Management ePO Extension 22.7 Release Notes at https://www.beyondtrust.com/docs/release-notes/privilege-management/windows-and-mac/epo-extension/epo-extension-22-7.htm.*

Install the Extension

To install the Endpoint Privilege Management ePO Extension extension:

1. Log in to Trellix ePolicy Orchestrator and navigate to **Menu > Software > Extensions**.



2. Click **Install Extension** in the top-left corner. The **Install Extension** dialog box appears.
3. Enter or browse to the location of the Endpoint Privilege Management server extension package **Defendpoint_x_x_x_xx.zip** and click **OK**.
4. On the **Install Extension** summary screen, click **OK** in the bottom-right corner to proceed with the installation.

The BeyondTrust Endpoint Privilege Management ePO Extension is now installed on your ePO server.

Configure ePO User Permission Sets

There are four permission sets in ePO by default. You can view these at **Menu > User Management > Permission Sets**, on the left menu. Installing the Endpoint Privilege Management ePO Extension grants some privilege management permissions to the following default ePO permissions sets:

- **Executive Reviewer:** Privilege Management Policy Permission: View and Change Settings

  This enables the user to access the policy catalog, but not to view or change the policy. The user requires **Run permission for BeyondTrust Endpoint Privilege Management** under **BeyondTrust Endpoint Privilege Management** to view policy.

- **Global Reviewer:** Privilege Management Policy Permission: View Settings

  This enables the user to access the policy catalog, but not to view or change the policy. The user requires **Run permission for BeyondTrust Endpoint Privilege Management** under **BeyondTrust Endpoint Privilege Management** to view policy.

- **Group Admin:** No Endpoint Privilege Management permissions.
- **Group Reviewer:** No Endpoint Privilege Management permissions.

> ***Note:*** *Users need to be members of the permission sets required for Endpoint Privilege Management. Please refer to Trellix documentation for how to add users to permission sets.*

Alternatively, you can create your own permission sets in ePO by selecting **New Permission Set**. After this is selected, you can name the permission set and assign users. Once you click **Save**, you can apply permissions.

If a user needs to view or change BeyondTrust policies, they require the **Run permission for BeyondTrustEndpoint Privilege Management** permission under **BeyondTrustEndpoint Privilege Management** and the **View settings** or **View and change settings** permission under **BeyondTrustEndpoint Privilege Management Policy**.

Assign Endpoint Privilege Management Permissions

Permissions that can be configured for each Endpoint Privilege Management permission set are:

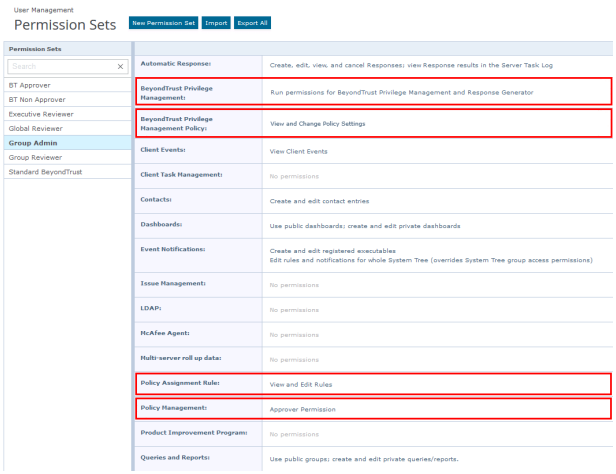
- Endpoint Privilege Management
- Endpoint Privilege Management Policy
- Policy Assignment Rule
- Policy Management

Configure Permissions

To configure user permissions for Endpoint Privilege Management in the ePO Server.

1. In **Trellix ePolicy Orchestrator**, navigate to **Menu > User Management > Permission Sets**.

2. Select the permission set that you want to configure.



Endpoint Privilege Management

1. Locate **BeyondTrust Endpoint Privilege Management** and click **Edit**.
2. Select a permission:
    - **Run permission for BeyondTrustEndpoint Privilege Management**: Users can manage Endpoint Privilege Management only.
    - **Run permission for BeyondTrust Response Generator**: Users can manage the Endpoint Privilege Management ePO Response Generator only.
    - **Run permissions for BeyondTrustEndpoint Privilege Management and for Response Generator**: Users can manage both.
    - **No permissions**: Users cannot manage either component.
3. Click **Save**.

Endpoint Privilege Management Policy

1. Locate **BeyondTrust Endpoint Privilege Management Policy** and click **Edit**.
2. Select a permission:
    - **View and change task settings**: Users can edit policy and Workstyles.
    - **View settings**: Users can read but not edit policy and Workstyles.
    - **No permissions**: Users cannot read or edit policy and Workstyles.
3. Click **Save**.

Policy Assignment Rule

1. Locate **Policy Assignment Rule** in the list and click **Edit**.
2. Select a permission:
    - **View and Edit Rules**: Users can manage policy rules.

- **View Rules**: Users can view but not manage policy rules.
- **No permissions**: Users cannot view or manage policy rules.

3. Click **Save**.

Policy Management

Add users who can make policy changes independently, including approving or rejecting policy change requests.

1. Locate **Policy Management** in the list and click **Edit**.
2. Select one of the following:
   - **No Permission - Users with this permission must submit policy changes for approval**
   - **Approver Permission - Users with this permission can make policy changes independently. This includes the ability to approve or reject policy change requests**
3. Click **Save**.

Configure Additional Permissions

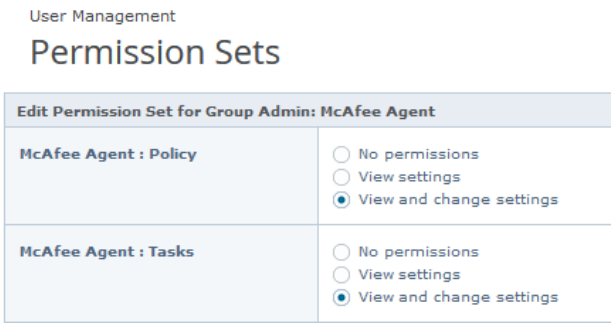
Other user permissions you, as an admin, may want to consider granting include those below, in order to:

- Modify deployment of the Endpoint Privilege Management endpoint client
- Access the **System Tree** tab
- Edit the groups and systems within the System Tree
- Wake and deploy agents
- Assign policies or client tasks to a group
- Create client tasks with the software or with the Software Catalog

To edit the permissions, navigate to **Menu > User Management > Permission Sets** and select the appropriate permission set. Alternatively, create a permission set by clicking the **New Permission Set** button. A list of settings you can edit appears in the right panel. Click **Edit** on the appropriate setting to edit it. Once finished, click **Save**.

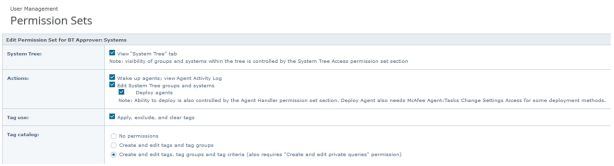
Trellix Agent: Policy and Trellix Agent: Tasks

A user may need **Trellix Agent** permissions if they need to view or change client deployment tasks of Endpoint Privilege Management for Windows or Endpoint Privilege Management for Mac.



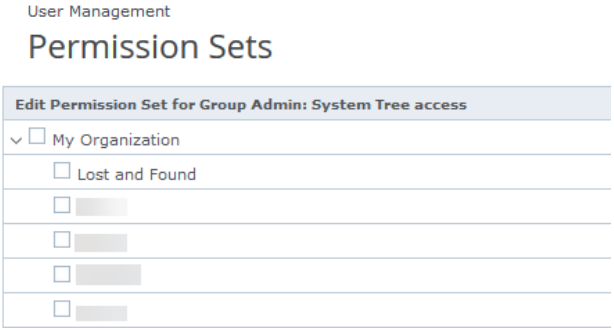
Systems

A user may need the **Systems** permission so they can access the **System Tree** tab, wake up agents, edit the groups and systems in the System Tree, and deploy agents.



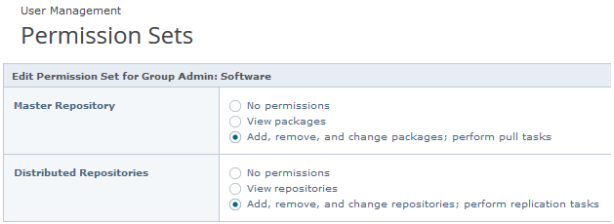
System Tree

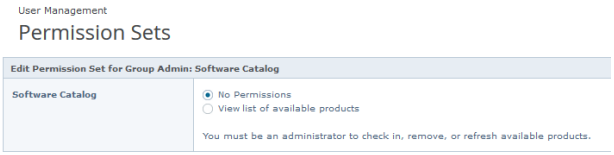
A user may need the **System Tree access** permission if they need access to certain groups (assigning policies or client tasks to a group, for example).



Software and Software Catalog

A user may need the **Software** and **Software Catalog** permissions if they need to create client tasks with software.





Upgrade Endpoint Privilege Management for Windows

Recommended Steps

- Step 1: Upgrade Application Groups to Match Publisher Name BeyondTrust Corporation
- Step 2: Upgrade the Endpoint Privilege Management ePO Extension
- Step 3: Upgrade Endpoint Privilege Management Reporting (if in use)
- Step 4: Upgrade Endpoint Privilege Managementfor WindowsClients
- Step 5: Delete Old Application Definitions (Upgrade from 5.4)

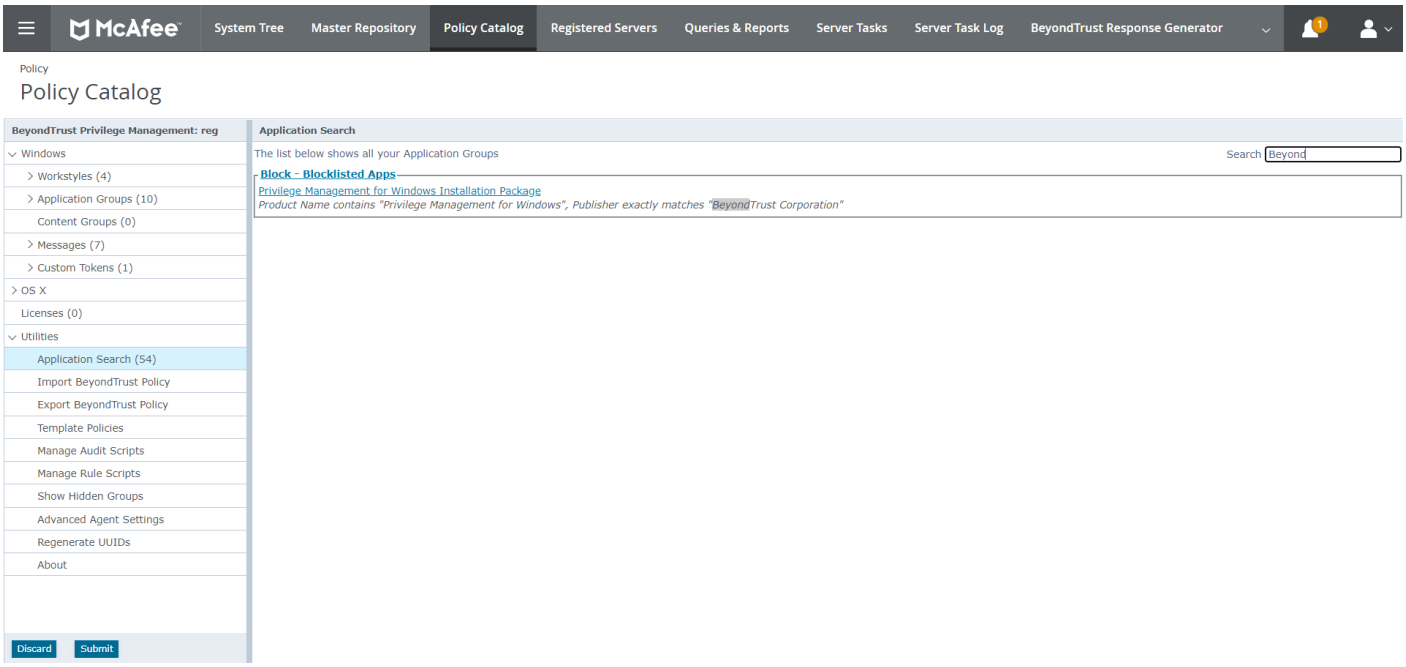
IMPORTANT!

As of release 5.5, all releases of this product are signed with BeyondTrust Corporation, rather than Avecto, as the software publisher name. If prior to 5.5 you used the QuickStart Policy Template as a starting point, it is likely that your configuration includes Application Groups which target our own applications based on a publisher match to Avecto. An upgrade to 5.5 or beyond requires you to update your configuration so that it continues to match the versions of the applications and tools that you use. We recommend you add a copy of any existing application definitions that target Avecto and update those copies to target BeyondTrust Corporation instead; the presence of both sets of application definitions ensures they continue to match both new and existing versions during the implementation of 5.5. It is critical that you roll out your configuration changes before you update your Endpoint Privilege Management for Windows software to version 5.5 or later.

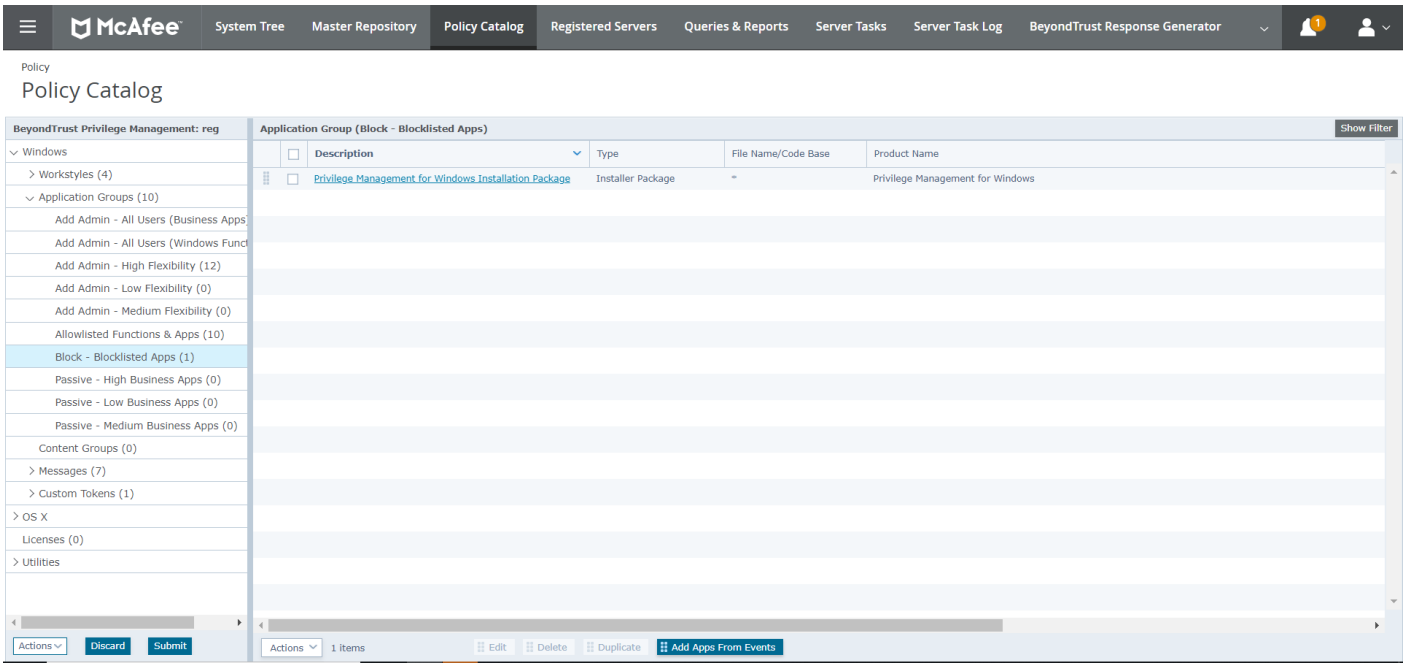
Step 1: Upgrade Application Groups to Match Publisher Name BeyondTrust Corporation

This section applies to upgrades to Version 5.5.

1. Locate all **Avecto** matches:
    - In the policy tree, navigate to **Utilities > Application Search**.
    - Type **Avecto** into the **Search applications** box to filter.



2. Create a copy of all definitions in each Application Group found that contain a publisher match on **Avecto:**
    - Make a note of the name of the application definition which contains a publisher match on Avecto, and click on its Application Group name in **Application Search**. This takes you to the Application Group.
    - Select the application definition and click **Duplicate**.



> ***Tip:*** *Rename one of the copies to* ***OLD****, so it's easy to tell which to delete after the new application definitions take effect.* ***OLD*** *can be deleted once the 5.5 upgrade is complete.*

3. Update the new application definitions to match publisher **BeyondTrust Corporation**.
4. Test the updated configuration against the new 5.5 applications.

At this point, you can continue with upgrading the remaining components.

The product code for Endpoint Privilege Management for Windows version 5 was updated from version 4. This means that the Endpoint Privilege Management ePO Extension must be upgraded before the Endpoint Privilege Management for Windows version 5 clients are installed.

> ***Note:*** *ePO will not recognize Endpoint Privilege Management for Windows if you upgrade the Endpoint Privilege Management for Windows clients before the Endpoint Privilege Management ePO extension. In addition, ePO Threat events will be rejected if this order is not followed, although they can be recovered once the upgrade to the Endpoint Privilege Management ePO Extension has been completed.*

Version 5 of the Endpoint Privilege Management ePO Extension is compatible with older Endpoint Privilege Management for Windows clients.

The recommended order to upgrade BeyondTrust Endpoint Privilege Management for Windows software is:

- Upgrade the Endpoint Privilege Management ePO Extension
- Upgrade Endpoint Privilege Management Reporting (if in use)
- Upgrade Endpoint Privilege Management Clients

> ***Note:*** *If you have a requirement to upgrade BeyondTrust software in a different order from that listed above, please contact your BeyondTrust representative.*

Step 2: Upgrade the Endpoint Privilege Management ePO Extension

When you are upgrading, the newer version of the Endpoint Privilege Management ePO Extension recognizes the existing Endpoint Privilege Management ePO Extension installation and prompts you to upgrade it. We recommend upgrading, as removing the installed Endpoint Privilege Management ePO Extension deletes your settings.

To upgrade the Endpoint Privilege Management ePO Extension, you need to use ePO to install the latest extension from **Software > Extensions**. When you upload the new Endpoint Privilege Management ePO Extension, ePO prompts you that this newer version of the ePO Extension will replace the previous extension. Click **OK** to upgrade the Endpoint Privilege Management ePO Extension. You do not need to restart ePO for the upgrade to take effect. Existing registered servers, client tasks, and server tasks are not affected.

> ***Note:*** *If you see an error message that states "Please stop CopyFromStaging from running before upgrading the database," make sure that no new events are being processed by querying the above tables and try again.*

This upgrade path can be applied to both standalone Reporting configurations and to configurations spread over multiple machines.

Step 4: Upgrade Endpoint Privilege Management for Windows Clients

You can upload a newer version of the Endpoint Privilege Management for Windows client to ePO and deploy it as required.

Depending on the type of installation, a restart of the endpoint may be required. When installing in silent mode, a reboot occurs automatically.

The Endpoint Privilege Management ePO Extension maintains backwards compatibility with the Endpoint Privilege Management for Windows client. You can use a later version of the Endpoint Privilege Management ePO Extension with an earlier version of the Endpoint Privilege Management for Windows client. However, not all features in the Endpoint Privilege Management ePO Extension are supported with earlier versions of the client.

For more information, please see the Endpoint Privilege Management for Windows Administration Guide, at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm.

Upgrade the Reporting Database Using SQL Scripts

Use these instructions to upgrade the Endpoint Privilege Management Reporting database where you cannot use the installer or need to do a manual installation, for example, EPM in Azure. SQL scripts are provided to manage these upgrades.

To upgrade an Endpoint Privilege Management Reporting database using SQL scripts:

1. The SQL scripts are provided as part of the Reporting installers. Alternatively, you can contact BeyondTrust Technical Support for them.

Note: *There is a README file provided in this directory to assist you.*

2. Run the following SQL query to find the current version of the database. This returns the version of the database.

```
select * from DatabaseVersion
```

Note: *This SQL query works for Endpoint Privilege Management Reporting databases 4.5 and later.*

3. Execute the upgrade script where the name is the next version number and carry on applying these until the desired version is reached.

Example: *If your current database version is **4.3.16** and you want to upgrade to version **5.0.0**, execute the following scripts in order:*

1. ***Script_4.5.0_Updates.sql***
2. ***Script_5.0.0_Updates.sql***

Please check the SQL log for any errors and contact BeyondTrust Technical Support if necessary.

Deploy Endpoint Privilege Management for Windows

Use the following steps to import the Endpoint Privilege Management client for ePO into the ePO server and create a client task to deploy it to your endpoints:

- Import the package into ePO.
- If using **Trellix Endpoint Security (ENS)**, configure Endpoint Privilege Management for Windows with **Trellix Endpoint Security**.
- Create and assign a client task to deploy Endpoint Privilege Management.
- Assign and run the client task to deploy the agent.
- Verify the Endpoint Privilege Management for Windows deployment.

For more information, please see the following:

- *"Import Endpoint Privilege Management for Windows Package into ePO" on page 14*
- *"Endpoint Privilege Management for Windows with Trellix Endpoint Security (ENS)" on page 15*
- *"Create and Assign a Client Task" on page 15*
- *"Assign and Run the Client Task to Deploy the Agent" on page 16*
- *"Verify the Deployment" on page 17*

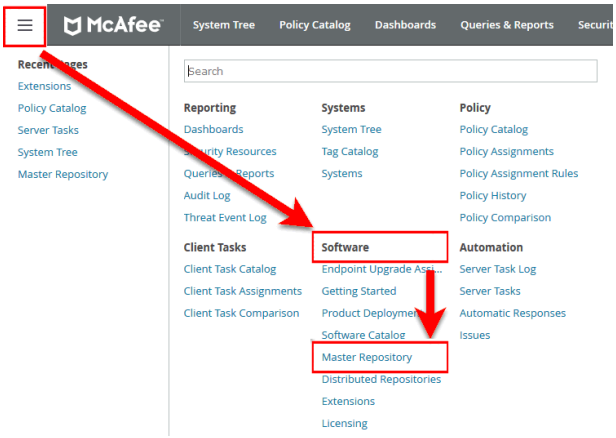
Import Endpoint Privilege Management for Windows Package into ePO

If you use Trellix ePolicy Orchestrator to deploy Endpoint Privilege Management for Windows to your endpoints, you need the Endpoint Privilege Management zip file package for your operating system.

The client package is a zip file that takes the form which includes both 32-bit and 64-bit versions of Endpoint Privilege Management client for Windows.

To install the Defendpoint package:

1. Log in to **ePolicy Orchestrator** and navigate to **Menu > Software > Master Repository**.



2. Click **Check In Package** at the top-left of the screen. The **Check In Package** wizard appears.
3. Leave **Package Type** as the default **Product or Update (.ZIP)** selection and click **Browse**.

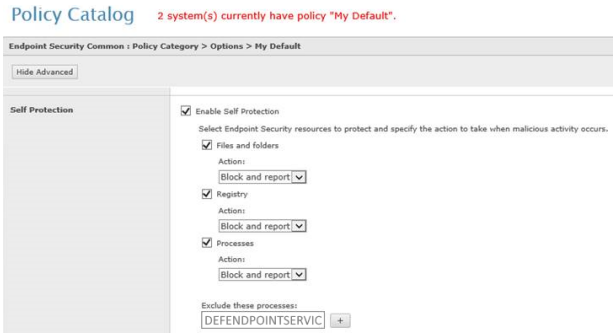
4. Navigate to and select the Endpoint Privilege Management for Windows package that you want to use on your local machine.
5. Click **Open** and then click **Next** at the bottom-right of the screen.
6. Leave the **Current** selection as the **Branch** option and click **Save** at the bottom-right of the screen to save the client package to the master repository.

The Endpoint Privilege Management for Windows package is displayed in the **Packages in Master Repository** list.

Endpoint Privilege Management for Windows with Trellix Endpoint Security (ENS)

If you are using **Trellix Endpoint Security (ENS)**, you need to do an additional task. Follow the steps below to configure Endpoint Privilege Management for Windows with **Trellix Endpoint Security**. If you're not using ENS, you can skip this section.

1. Navigate to **Policy Catalog** and select **Trellix Endpoint Security** from the **Product** dropdown menu.
2. In the **Self Protection** section, if the **Enable Self Protection** box is checked:
    - Check the three boxes shown for **Files and folders**, **Registry** and **Processes**.
    - Type **DEFENDPOINTSERVICE.EXE** into the **Exclude these processes** text box and click **Save**.



Create and Assign a Client Task

Endpoint Privilege Management for Windows is deployed to client computers using **ePolicy Orchestrator** client tasks. Client tasks are assigned to groups within the **System Tree**. This section guides you through the creation of a client task for Endpoint Privilege Management for Windows, and the assignment of the client task to the group in the **System Tree**.

If you previously installed the Endpoint Privilege Management client with a switch, you must ensure that when you upgrade the Endpoint Privilege Management client you use with the same switch. If you do not use the same switch, the new installation parameters will apply (including any added switches) and any functionality relating to previous installation switches will be lost. Endpoint Privilege Management client switches can be set in the **Command Line** field in **Products and Components**.

To create a client task for Endpoint Privilege Management for Windows package:

1. Log in to **ePolicy Orchestrator** and navigate to **Menu > Client Tasks > Client Task Catalog**.
2. Select **Trellix Agent > Product Deployment** from the left pane and click **New Task** on the top-left of the page.
3. Select **Product Deployment** from the **Task Types** dropdown menu and click **OK**.
4. Enter the following options:

Field	Description
Task Name	Name the task **Endpoint Privilege Management x.x.xxx**, where **x** represents the full version of Endpoint Privilege Management you're deploying.
Description	This is an optional field you can use if required.

Field	Description
Target platforms	This is the operating system of your endpoints. Check the **Mac** box. ***Note:*** *The Endpoint Privilege Management for Windows package includes both 32-bit and 64-bit versions of the client. The correct version is automatically installed based on the characteristics of the target client computer.*
Products and components	Select **BeyondTrust Endpoint Privilege Management for Windows x.x.xxx** from the dropdown menu. Confirm **Action** is set to **Install**, **Language** is set as **English**, and **Branch** is set to **Current**. Set any switches in the **Command Line** field that you want to install Endpoint Privilege Management for Windows with.
Postpone Deployment	Use this option to allow your users to postpone the deployment of Endpoint Privilege Management on their machines.

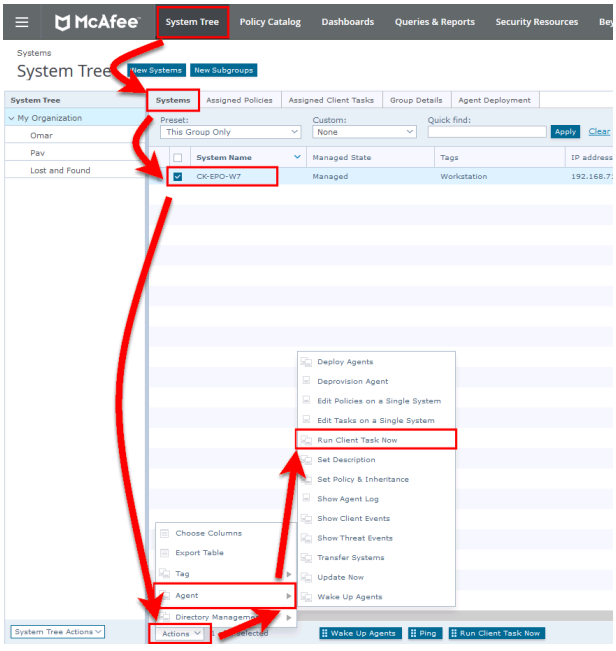
5. Click **Save** to finish creating the client task.

The client task is displayed in the **Product Deployment** list, and is now ready for assignment to a group or client computer in the **System Tree** prior to running it.

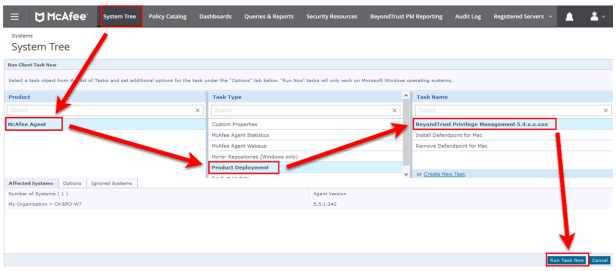
Assign and Run the Client Task to Deploy the Agent

The Trellix Agent must be installed on your endpoints prior to installing Endpoint Privilege Management for Windows.

1. Navigate to the **System Tree > Systems** tab and select the endpoint or group containing your endpoints. You may need to drill down to the location using the tree on the left.
2. Click **Actions** on the bottom of the screen and select **Agent > Run Client Task Now**.



3. Leave the **Product** as **Trellix Agent**.
4. Select **Product Deployment** from the **Task Type**.
5. Select your Endpoint Privilege Management for Windows client from the **Task Name** list. This is the name of the client task that you created to deploy Endpoint Privilege Management for Windows .
6. Your list of endpoints is shown in the bottom panel. Click **Run Task Now**.
7. The **Running Client Task Status** page appears. The **Status** bar may not show completed until the client computer has been restarted.



Once you have deployed the Endpoint Privilege Management for Windows package, the endpoints automatically send a manifest of product information to the ePO server. This information is stored as a property of the client computer in the **System Tree** on the **Products** tab.

Verify the Deployment

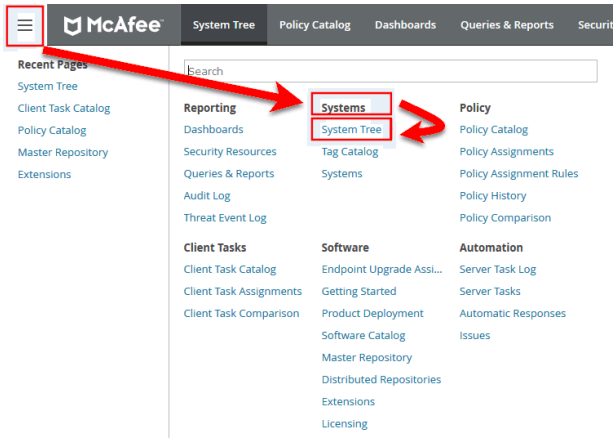
You can verify the Endpoint Privilege Management for Windows deployment from the server and client.

> ***Note:*** *You may not be able to verify deployments if your endpoints are pending a restart.*

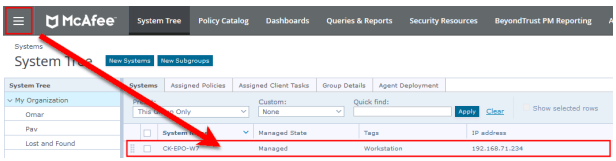
Server Verification

To verify that the Endpoint Privilege Management for Windows package has been successfully deployed:

1. Log in to **ePolicy Orchestrator** and navigate to **Systems > System Tree**. The **System Tree** is also available as a shortcut in ePO on the top-menu bar.



2. The **Systems** tab is the default view. Click the row of the client computer you want to check.



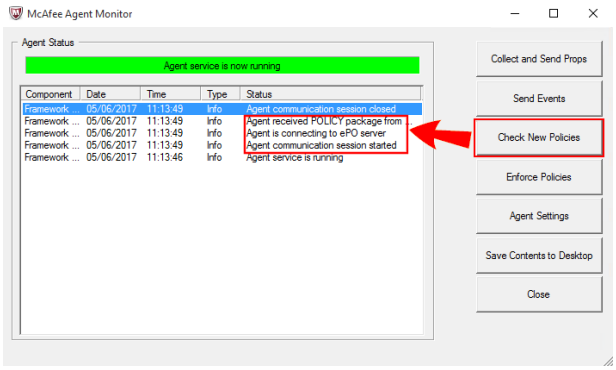
3. Click the **Products** tab and then select **BeyondTrust Endpoint Privilege Management** from the product list. Here you can check the status of the deployment and deployed files.

> ***Note:*** *In certain cases there may be a delay in the client connecting back to the ePO server. Click* ***Wake Up Agents****, check the* ***Force complete policy and task update*** *box, and click* ***OK*** *to force the connection.*

Client Verification

To verify that the Endpoint Privilege Management client is connected to the ePO server:

1. From the client computer, right-click on the Trellix icon in the system tray and select the **McAfee Agent Status Monitor**. The **Agent Status** dialog box appears. If the agent doesn't appear in the task bar, you can run it manually. To do this, open a Windows command prompt and change the directory to the installation folder of the Trellix agent. By default, this is **C:\Program Files\McAfee\Agent**. Run the following command from the Windows command prompt.




```
cmdagent.exe -s
```

2. Click **Check New Policies**. This allows you to check the communication between your endpoint and the ePO server.

> ***Note:*** *Sometimes there is a delay in the client connecting to the ePO server. Click* ***Check New Policies*** *and select* ***Enforce Policies*** *to force a policy update. If you see the endpoint receiving policies from the ePO server, then the connection is successful.*

Endpoint Privilege Management and ePO Events and Reporting

There are two types of reporting available:

- Trellix ePO reporting, threat events only
- Endpoint Privilege Management reporting. Starting in version 23.10, you can deploy the BeyondTrust Endpoint Privilege Management App to run reports on your ePO Endpoint Privilege Management environment.

Trellix ePO Reports

No additional configuration is required to use Trellix ePO Reporting.

ePO Reporting is available by default and allows you to build complex queries to analyze your data. ePO Reporting uses threat events on the **Queries and Dashboards** page and the **Dashboards** page.

ePO Reporting can also report on report events in the **Queries and Dashboards** page if **BeyondTrust Reporting** is configured.

There are four **Dashboards** and twelve default **Queries and Reports** available by default for BeyondTrust Endpoint Privilege Management for Windows. You can configure dashboards, charts, and tabular reports on the **Dashboards** and **Queries and Reports** pages. These can incorporate data from other ePO server products in ePO.

All the events are stored in the ePO database.

Configure BeyondTrust Reporting in ePO

BeyondTrust Reporting is an optional Reporting suite that is integrated into ePO.

BeyondTrust Reporting is available in two places in the ePO server interface:

- **Queries and Reports** page
- **BeyondTrust Endpoint Privilege Management Reporting** page

BeyondTrust Endpoint Privilege Management Reporting integrates with Intel Security Threat Intelligence Exchange (TIE), so it has additional support for application reputation using Data Exchange Layer (DXL) and VirusTotal.

Note: *Times on reports are shown using the time zone of the ePO server. All events are stored in the database in UTC.*

Set up a New SQL Server Instance for BeyondTrust Endpoint Privilege Management Reporting

For BeyondTrust Endpoint Privilege Management Reporting functionality, you can either use the same installation of SQL Server as the ePO server or you can use a different SQL installation. A new database is created for BeyondTrust Endpoint Privilege Management Reporting by the BeyondTrust Database installation.

The following SQL server versions are supported:

- SQL 2012 Standard or Enterprise
- SQL 2014 Standard or Enterprise
- SQL 2016 Standard or Enterprise
- Azure SQL Server

Note: *Express SQL versions may be used for evaluation and demonstration purposes.*

Please refer to the SQL documentation to create a new installation of SQL server, if required.

Create the Required Database User Accounts

You can either use a system administration account for the registered servers required for BeyondTrust Endpoint Privilege Management Reporting or you can use the default user accounts that are configured as part of the Endpoint Privilege Management database installation. This section describes using the least privilege default user accounts that are configured by the Endpoint Privilege Management database installer.

If you plan to use a system administration account for the BeyondTrust reporting registered servers, you do not need to complete the steps in this section.

We recommend that you use the accounts that the Endpoint Privilege Management database installer configures. These are:

- **ReportReader** user: Permissions include Read and Execute on the appropriate database objects.
- **EventParser** user: Permissions include Write access to certain database tables. Membership of local Event Log Readers group.
- **DataAdmin** user: Permissions include Read and Execute on the appropriate database objects

In addition to the users that the Endpoint Privilege Management database installer configures, you need to choose the user that you'll use to install the Endpoint Privilege Management database. This is known as the *DatabaseCreator* user.

This account must be able to execute installers on the machine with administrative privileges. Alternatively, you can use a SQL account for the DatabaseCreator user. This can be configured in the installer when you run it.

The DatabaseCreator user also needs SQL sysadmin permissions.

To grant the **sysadmin** permission for the DatabaseCreator user:

1. Open SQL Server Management Studio and connect to the SQL instance that you're going to use for the BeyondTrust Endpoint Privilege Management Reporting installation.
2. Navigate to the **Security > Logins** folder.
3. You must add your user to this folder if it hasn't previously been used to authenticate with SQL Server. To do this:
    - Right-click on the **Logins** folder and click **New Login**.
    - Click **Search** to the right of the **Login name** option. If you know the domain and user name you need to add you can type it here, and then click **Check Name**. If you're not sure about the user's details you can click **Advanced** to browse to the user you want to use. Click **OK** and **OK** again to finish adding the user.
4. In the **Logins** folder, right-click on the user to use as the **DatabaseCreator** and select **Properties**.
5. Click **Server Roles** from the left menu and check the **sysadmin** box.
6. Click **OK** to add the **sysadmin** privilege to the user.

> ***Note:*** *If Windows Authentication is specified for the SQL connection, and you're not using an admin account, the user must have* ***Alter Any Login*** *and* ***Create Any Database*** *permissions on the SQL server instance, in order for the* ***Reporting Services Instance User*** *to be created. If you receive error 15247, verify these permissions have been granted.*

ReportReader User

The *ReportReader* user is a Windows or SQL account that is used by the Endpoint Privilege Management ePO Extension to read report events from the Endpoint Privilege Management database. The registered server **BeyondTrust Endpoint Privilege Management Reporting** uses this account, so you should make a note of it.

If this is a Windows account, you need to grant the following permission:

- Requires the **Allow Log on Locally** permission to the server hosting SSRS. This is granted automatically if the account is in the Administrators user group.

Some domain groups have this permission set. It's up to you how you configure this account as long as it has the **Allow log on Locally** permission granted through group membership or as an exception.

EventParser User

The *EventParser* user is used by the Endpoint Privilege Management ePO Extension to read data from the ePO database and write it to the Endpoint Privilege Management Reporting database. The registered server **BeyondTrust Staging** uses this account, so you should make a note of it.

This account needs to be able to authenticate on the database machine. If the two databases are on different machines, then this account needs to be on a shared domain.

DataAdmin User

The *DataAdmin* user is a Windows or SQL account that is used by the Endpoint Privilege Management ePO Extension to write to the Endpoint Privilege Management for Windows database. The registered server **BeyondTrust Purge** uses this account by default.

If this is a Windows account, you need to grant the following permission:

- Requires the **Allow Log on Locally** permission to the server hosting SSRS. This is granted automatically if the account is in the Administrators group.

Some domain groups have this permission set. It's up to you how you configure this account as long as it has the **Allow log on Locally** permission granted through group membership or as an exception.

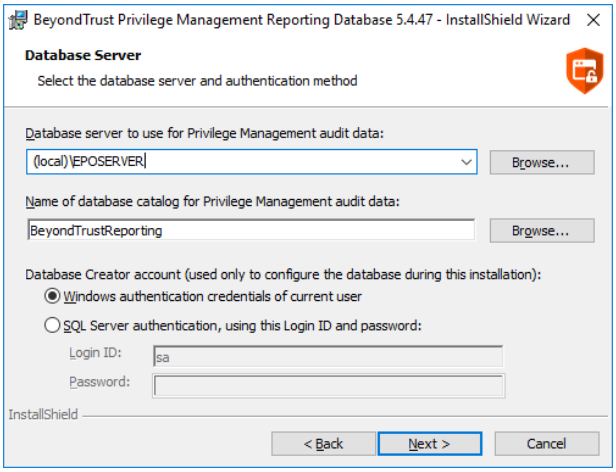
Install the Endpoint Privilege Management Reporting Database

To install Endpoint Privilege Management Reporting database, run the Endpoint Privilege Management Reporting Database installation package with the **Database Creator** user that you set up when you created the required user accounts.

- If you are running the installer on the same machine as the database, use **Endpoint Privilege Management ReportingDatabase.msi**.
- If you are running the installer on a client machine, use **Endpoint Privilege Management ReportingDatabase.exe**. This includes the SQL Native Client Redistributable package.

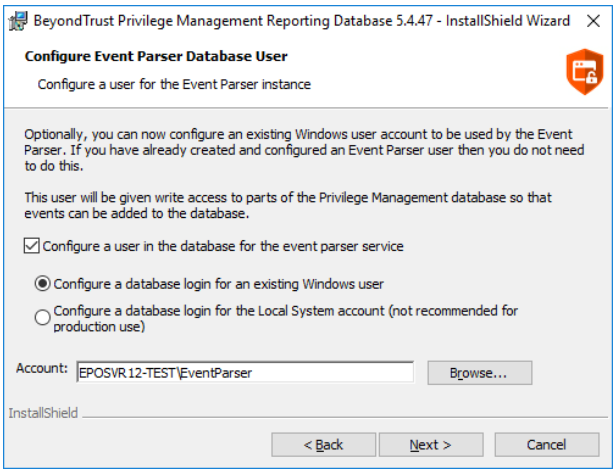
> ***Note:*** *The Endpoint Privilege Management Reporting Database installer assigns specific privileges to the user accounts that you created previously.*

1. Run the installation package and click **Next** to continue. The **License Agreement** dialog box appears.
2. To accept the agreement, select **I accept the terms in the license agreement** and click **Next**. The **Database Server** dialog box appears.
3. Set the **Database server to use for Endpoint Privilege Management audit data** as **(local)** if you are using the same machine for your database server and you didn't create an instance. If you did create an instance, you need to add it here, for example **(local)\BeyondTrustReporting**, where the instance is **BeyondTrustReporting**. The database servers are available from the dropdown menu.
4. Type a new name in the **Name of database catalog for Endpoint Privilege Management audit data** field.
5. Select to either use the Windows credentials of the current user or you can use SQL server authentication. If you choose SQL server authentication you need to enter the **Login ID** and **Password** before you can proceed.



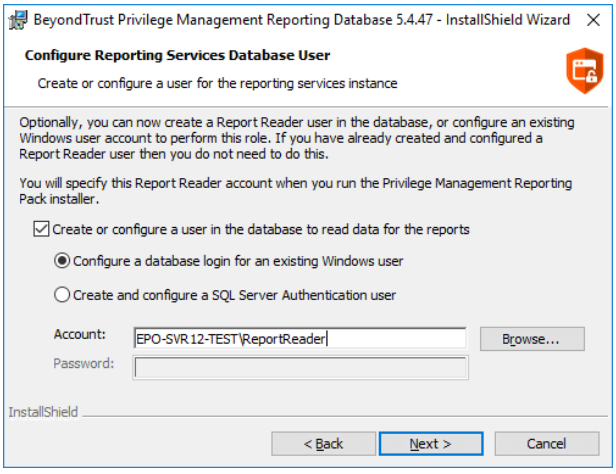
6. Click **Next**. The **Configure Event Parser Database User** dialog box appears.
7. If you are using the default Endpoint Privilege Management Reporting database users for BeyondTrust Reporting, check the **Configure a user in the database for the event parser service** box. Select your **EventParser** user. In this example we are using a Windows user that we've previously created.

8. Click **Browse** and navigate to the **EventParser** user that you created.



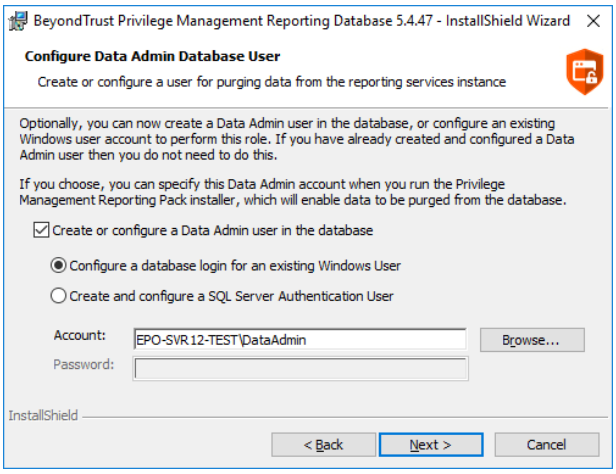
> ***Note:*** *Once you have selected a local or domain machine, ensure you select a user that you know exists in that location; otherwise, the installation will fail.*

9. Click **Next**. The **Configure Reporting Services Database User** dialog box appears.
10. If you are using the default Reporting users for Endpoint Privilege Management Reporting, check the **Create or configure a user in the database to read data for the reports** box. Select to either use an existing Windows user or create a new SQL server user. In this example we use a Windows user that we previously created.
11. Click **Browse** to navigate to the **ReportReader** user that you created.



> ***Note:*** *Once you have selected a local or domain machine, ensure you select a user that you know exists in that location; otherwise, the installation will fail.*

12. Click **Next**. The **Configure Data Admin Database User** dialog box appears.



13. If you are using the default Reporting users for Endpoint Privilege Management Reporting, check the **Create or configure a Data Admin user in the database** box. Select to either use an existing Windows user or create a new SQL server user. In this example we use a Windows user that we previously created.
14. Click **Browse** to navigate to the **DataAdmin** user that you created.

> ***Note:*** *Ensure you select a user that you know exists on the domain or local machine that you've selected; otherwise, the installation will fail.*

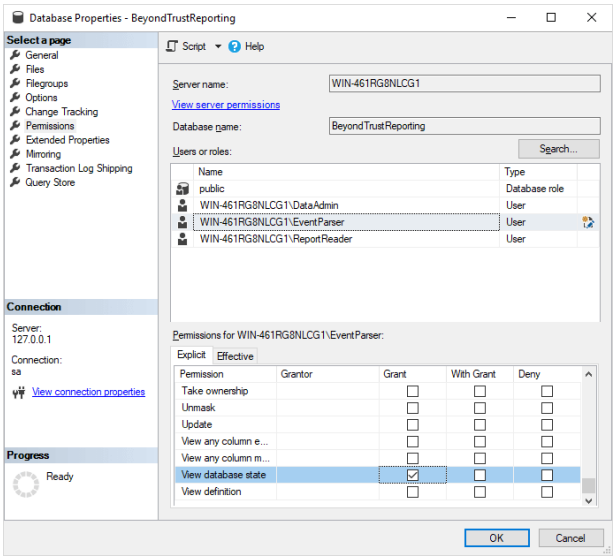
15. Click **Next** and then **Install** to finish the installation. You have now installed the Endpoint Privilege Management Reporting database.

> *For more information, please see "Create the Required Database User Accounts" on page 22.*

Configure Permissions for the EventParser User

You must grant the **View database state** permission on the Reporting database for the EventParser user that you created during the database installation. This permission is already granted on the ePO database by the installer.

1. Open SQL Server Management Studio and connect to your Reporting database.
2. Right-click on the Reporting database, select **Properties** from the Reporting database, and click **Permissions** on the left menu.
3. Select the **EventParser** user from the **Users or roles** section.
4. Check the **Grant** box for the **View database state** permission.



Create Registered Servers for your Deployment

There are three registered servers you can configure in the Endpoint Privilege Management ePO Extension for Reporting. What you need to configure will depend on your setup.

Compulsory: BeyondTrust Endpoint Privilege Management Reporting

You need to configure this registered server if you are using Endpoint Privilege Management Reporting.

Server tasks that use the Reporting registered server:

- BeyondTrust Endpoint Privilege Management Reputation Update to update the reputation.

This registered server uses the ReportReader account that was configured by the Endpoint Privilege Management database installer. Alternatively, you can use a system administration account.

> *For information on how to set up your BeyondTrust Reporting registered server, please see "Configure the BeyondTrust Reporting Registered Server" on page 29.*

Optional: BeyondTrust Reporting Staging

This registered server allows you to use the EventParser user to move events to the staging table.

Server tasks that user the Reporting registered server:

- BeyondTrust Endpoint Privilege Management Reporting Event Staging. If it's not configured, it uses the BeyondTrust Reporting registered server.

This registered server uses the EventParser user account that was configured by the Endpoint Privilege Management database installer. Alternatively, you can use a system administration account.

> *For information on how to set up your BeyondTrust Reporting registered server, please see "Configure the BeyondTrust Endpoint Privilege Management Reporting Staging Registered Server" on page 29.*

Optional: BeyondTrust Admin

This registered server allows you to use the DataAdmin user to manage the purging of data.

Server tasks that user the Reporting registered server:

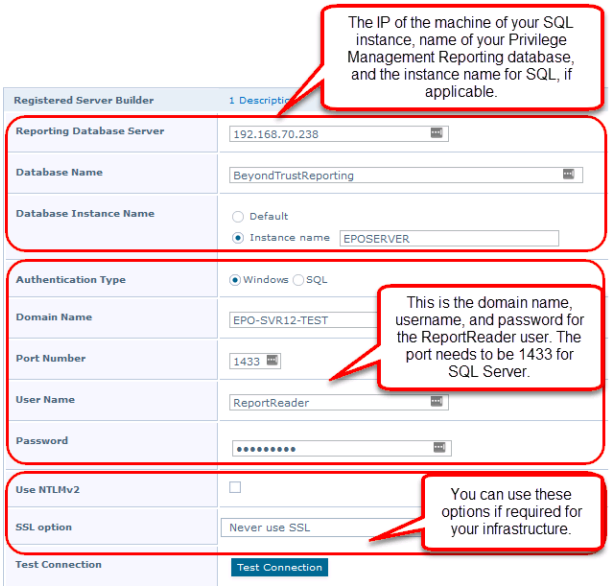
- BeyondTrust Reporting Purge. If it's not configured, it uses the BeyondTrust staging registered server if that has been configured; if not, it uses the Reporting registered server user instead.

This registered server uses the DataAdmin account that was configured by the Endpoint Privilege Management database installer. Alternatively, you can use a system administration account.

> *For information on how to set up your BeyondTrust Reporting registered server, please see "Configure the BeyondTrust Admin Registered Server" on page 30.*

Configure the BeyondTrust Reporting Registered Server

1. Log in to **ePolicy Orchestrator**, navigate to **Menu > Configuration > Registered Servers**, and select **New Server**.
2. On the next page, select **BeyondTrustEndpoint Privilege Management Reporting** from the **Server type** dropdown menu and enter an appropriate name (**BeyondTrust Reporting ER Server**, for example). Click **Next**.



> ***Note:*** *This screen shot shows example data.*

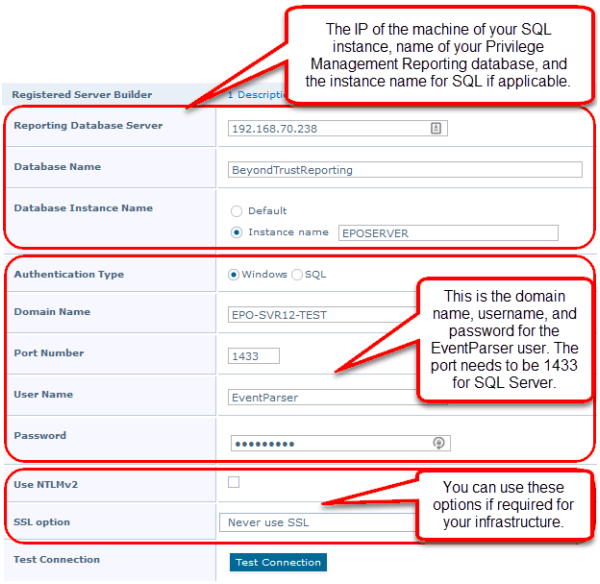
3. Complete the configuration page with the server details. The **Port Number** should be set to 1433.
4. Click **Test Connection**. On successful connection, click **Save**.

Configure the BeyondTrust Endpoint Privilege Management Reporting Staging Registered Server

> ***Note:*** *If this is an upgrade, and you do not have a registered server for BeyondTrust Endpoint Privilege Management Reporting Staging, the server tasks attempt to use the Reporting registered server. Please see "Configure the BeyondTrust Reporting Registered Server" on page 29. This is for backwards compatibility and additional permissions are required.*

> ***Note:*** *The screen shot shows example data.*

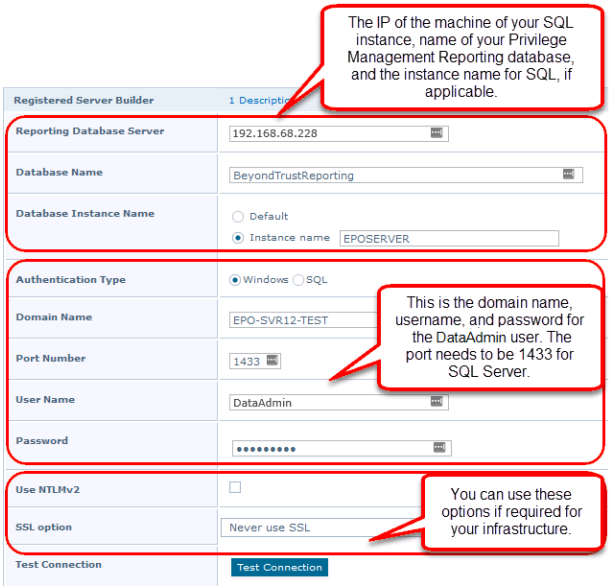
1. Log in to **ePolicy Orchestrator**, navigate to **Menu > Configuration > Registered Servers**, and click **New Server**.
2. On the next page, select **BeyondTrust Endpoint Privilege Management Reporting Staging** from the **Server type** dropdown menu and enter an appropriate name (**BeyondTrust Staging Server**, for example). Click **Next**.
3. Complete the configuration page and click **Test Connection**. On successful connection, click **Save**.



Configure the BeyondTrust Admin Registered Server

1. Log in to **ePolicy Orchestrator**, navigate to **Menu > Configuration > Registered Servers**, and click **New Server**.
2. On the next page, select **BeyondTrust Endpoint Privilege Management Reporting Admin** from the **Server type** dropdown menu and enter an appropriate name (**BeyondTrust Admin Purge Server**, for example). Click **Next**.

This screen shot shows example data.



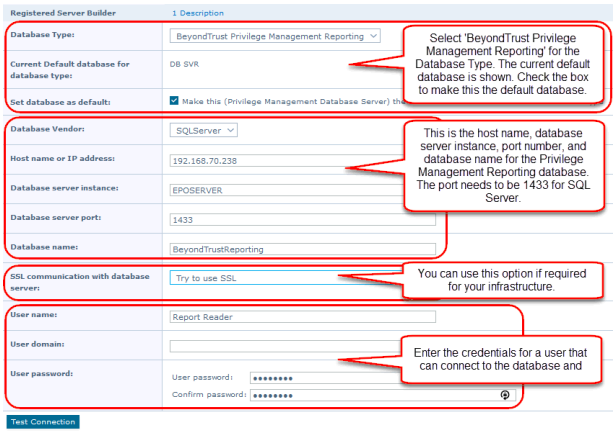
3. Complete the configuration page and click **Test Connection**. On successful connection, click **Save**.

Configure the Database Server Registered Server

A Database server registered server allows you to query Endpoint Privilege Management events in the Endpoint Privilege Management database using the **Queries and Reports** capability in ePO.

> ***Note:*** *This screen shot shows example data.*

1. Log in to **ePolicy Orchestrator**, navigate to **Menu > Configuration > Registered Servers**, and click **New Server**.
2. On the next page, select **Database Server** from the **Server type** dropdown menu and enter an appropriate name (**Endpoint Privilege Management Database Server**, for example). Click **Next**.



3. Complete the configuration page and click **Test Connection**. On successful connection, click **Save**.

Create Automated Tasks Using ePO Server Tasks

You use ePO server tasks to create an automated schedule of tasks that you want your ePO server to perform. The following ePO server tasks are used for Endpoint Privilege Management for Windows:

- **Create the BeyondTrust Endpoint Privilege Management Reputation Update Server Task:** Optional to update the reputation from VirusTotal and/or TIE.
- **Create the Purge Threat Event Log Server Task:** Optional to purge the ePO threat event log.

There is an additional server task that you can create if you have a business need to purge the events from the BeyondTrust table in the ePO database only.

We recommend you use the built-in ePO server task called **Purge Rolled up Data** rather than this server task. This will remove all the events from the BeyondTrust table in the ePO database and the Endpoint Privilege Management Reporting database.

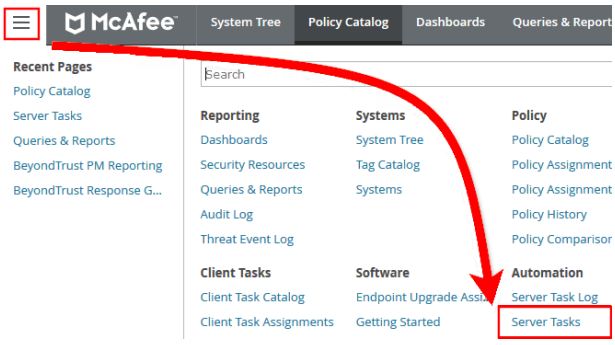
For more information, please see the following:

- *"Create the Endpoint Privilege Management Reporting Reputation Update Server Task" on page 34*
- *"Create the Purge Threat Event Log Server Task" on page 34*

Create the Endpoint Privilege Management Reporting Event Staging Server Task

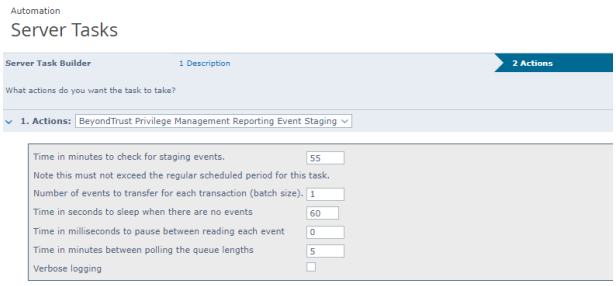
The **Reporting Event Staging** server task takes report events from the ePO database and inserts them into the BeyondTrust Endpoint Privilege Management Reporting database. You need to create this task to view BeyondTrust reports.

1. Navigate to **Menu > Automation > Server Tasks** and select **New Task**.



2. Enter an appropriate name (**BeyondTrust Event Staging**, for example), leave the **Schedule status** as **Enabled**, and click **Next**.
3. Select **BeyondTrust Endpoint Privilege Management Reporting Event Staging** from the **Actions** dropdown menu and click **Next**.

4. Adjust the times to check for events to suit your environment and click **Next**.

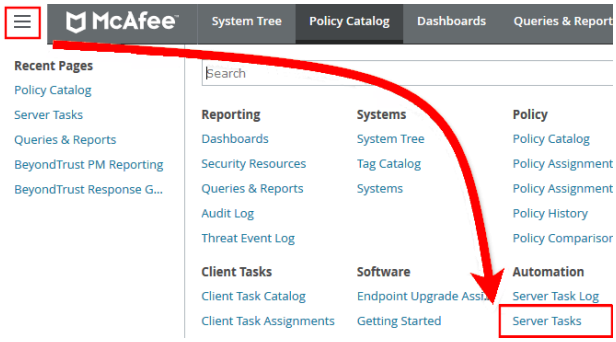


   - **Time in minutes to check for staging events**: The recommended value is 55 minutes.
   - **Number of events to transfer for each transaction (batch size)**: The default value is 1. Only increase the value if there is a lag in performance throughput between ePO to Endpoint Privilege Management Reporting.
   - **Time in seconds to sleep when there are no events**: The recommended value is 60 seconds.
   - **Time in milliseconds to pause between reading each event**: The default and recommended value is 0.
   - **Time in minutes between polling the queue lengths**: The recommended value is 5 minutes.
   - **Verbose logging**: By default, verbose logging is turned off. Only use verbose logging when you need more details about the events being collected.
5. On the **Schedule** page, set the **Schedule type** to your preference.
6. Select the **Start date** and **End date** if required. By default, **No end date** is selected.
7. Adjust the time that you want the schedule to run. This is the time of the machine running the ePO server. Click **Next**. You are presented with a summary of the server task.
8. Select **Save** to finish creating the server task.

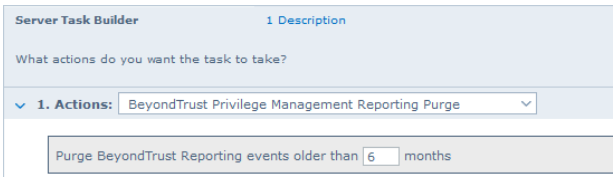
Create the Endpoint Privilege Management Reporting Purge Server Task

You can purge Reporting database events that are older than a defined period in order to manage the size of your database.

1. Navigate to **Menu > Automation > Server Tasks** and select **New Task**.



2. Enter an appropriate name (**BeyondTrust Purge**, for example), leave **Schedule status** as **Enabled**, and click **Next**.
3. Select **BeyondTrust Endpoint Privilege Management Reporting Purge** from the **Actions** dropdown menu.
4. Choose the number of months to purge events older than.



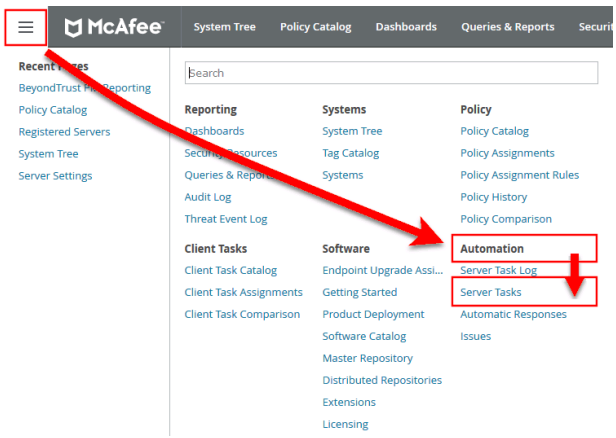
5. On the **Schedule** page set the **Schedule type** to your preference.
6. Select the **Start date** and **End date**, if required. By default, **No end date** is selected.

7. Adjust the time that you want the schedule to run. This is the time of the machine running the ePO server. Click **Next**. You are presented with a summary of the server task.
8. Click **Save** to finish creating the server task.

Create the Endpoint Privilege Management Reporting Reputation Update Server Task

You can update the reputation, provided that it is configured using this server task.

1. Navigate to **Menu > Automation > Server Tasks** and click **New Task**.



2. Enter an appropriate name, such as **BeyondTrust Reputation Update**, leave **Schedule status** as **Enabled**, and click **Next**.
3. Select **BeyondTrust Endpoint Privilege Management Reputation Update** from the **Actions** dropdown menu.
4. Check the boxes adjacent to the reputations you want to update. You can then select from **Add Reputation to entries with no reputation** or **Update Reputation for entries with old reputation**. If you select the latter option, you can choose the number of days. Click **Next**.
5. On the **Schedule** page set the **Schedule type** to your preference.
6. Select the **Start date** and **End date**, if required. By default, **No end date** is selected.
7. Adjust the time that you want the schedule to run. This is the time of the machine running the ePO server. Click **Next**. You are presented with a summary of the server task.
8. Click **Save** to finish creating the server task.

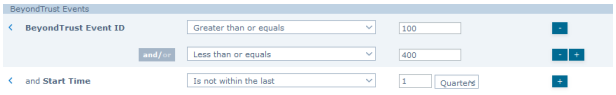
Create the Purge Threat Event Log Server Task

You can purge threat events from the event log using this server task. Before you use this server task you need to create a query for it to use.

Create the Purge Threat Event Log Query

1. Click **Queries and Reports** and click **New Query**.
2. From the left side, click **BeyondTrust Endpoint Privilege Management** and click **Next**.
3. Select **List > Table** from the left side and click **Next**.
4. Click **Next** on the **Select Columns** page.

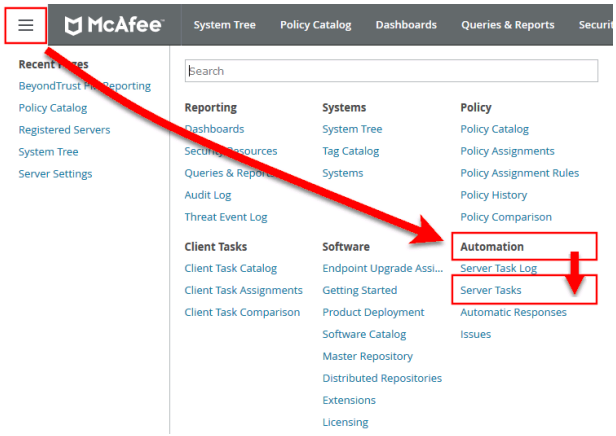
5. On the **Filter** page click **BeyondTrust Event ID**.
6. Select **Greater than or equals** and enter **100** for the **Value**.
7. Click the plus symbol (**+**) and change the filter to **and**.
8. Select **Less than or equals** and enter **400** for the **Value**.
9. On the same **Filter** page, click **Start Time**.
10. Select **Is not within the last** and configure the time period to say how many days/months/years of data you want to keep.



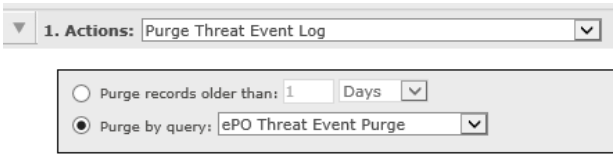
11. Click **Save** and give the query a name, such as **ePO Purge Threat Event**.

Create the ePO Purge Threat Event Server Task

1. Select **Menu > Automation > Server Tasks** and select **New Task**.

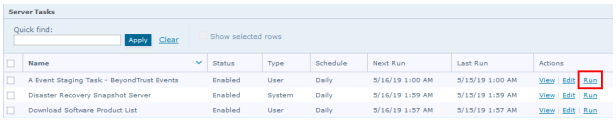


2. Enter an appropriate name (**Purge Threat Event Log**, for example), leave **Schedule status** as **Enabled**, and click **Next**.
3. Select **Purge Threat Event Log** from the **Actions** dropdown menu.
4. Select from **Purge records older than** or **Purge by query** and choose your criteria.



5. On the **Schedule** page set the **Schedule type** to your preference.
6. Select the **Start date** and **End date**, if required. By default, **No end date** is selected.
7. Adjust the time that you want the schedule to run. This is the time of the machine running the ePO server. Click **Next**. You are presented with a summary of the server task.
8. Click **Save** to finish creating the server task.

Run an Automated Task Outside the Scheduled Time



You can run the server tasks you have created from the **Server Tasks** page in ePO. This lists all the server tasks. You can run a task by clicking the **Run** link on the right side of the row:

Performance Tuning on the ePO Server

The default configuration of an ePO Server allows two concurrent tasks that share a single processor core. For larger systems, this may have a performance implication. Your ePO Server can be configured to make better use of the processor cores for scheduled tasks.

1. Navigate to **Menu > Server Settings > Scheduler Tasks**.
2. Click **Edit**.
3. From **Total maximum tasks**, select **Absolute maximum calculation**.

This ensures you are not restricted to using only a single core for calculations.

Note: *Your ePO Server must be restarted for these changes to take effect.*