



BeyondTrust

Endpoint Privilege Management for Windows BeyondInsight Integration Guide

Table of Contents

Integrate Endpoint Privilege Management for Windows with BeyondInsight	4
Overview	4
Architecture	5
Prerequisites	5
Integration Workflow	7
Configure U-Series Appliance	8
Primary/Secondary Deployment Model	8
Configure BeyondInsight and EPM via OAuth	10
Installing EPM with an OAuth activation secret	10
Configure BeyondInsight and Endpoint Privilege Management	11
Generate Client Certificate MSI	11
Deploy the Certificate MSI	12
Install Endpoint Privilege Management for Windows	14
Verify Endpoints are Registered in BeyondInsight	15
Use Smart Rules to Assign Policy	16
Create a Smart Rule to Assign Policy to Assets	16
Create a Smart Rule to Assign Policy to Users	17
Grant Users Permissions to Log in to the Policy Editor	18
Install Web Policy Editor in BeyondInsight Instance	19
Install Endpoint Privilege Management WPE and the BeyondInsight WPE Plugin	19
Upgrade the Endpoint Privilege Management WPE	20
Install Endpoint Privilege Management Reporting in BeyondInsight	22
Prerequisites	22
Install BeyondTrust Endpoint Privilege Management Reporting Database	23
Install BeyondTrust Endpoint Privilege Management Reporting UI	25
Install the BeyondTrust EPM Event Collector	25
Upgrade Endpoint Privilege Management Reporting in BeyondInsight	27
Prerequisites	27
Upgrade BeyondTrust Endpoint Privilege Management Reporting Database	28
Upgrade BeyondTrust Endpoint Privilege Management Reporting UI	29
Configure Endpoint Privilege Management Reporting in BeyondInsight	38

Configure Endpoint Privilege Management Reporting Database in BeyondInsight	38
Assign Permissions to Users to Access Reports in BeyondInsight	40
Configure Endpoint Endpoint Privilege Management Policy Editor to Raise Events in BI	40
Configure Advanced SQL and Event Collector Settings for PMR in BI Integration	42
SQL Connection Options (Including SSL Configuration)	42
SQL Always On Availability Group Support	43
Install and Configure External Event Collector Worker Nodes	44
Troubleshoot	45
Use the EndpointUtility.exe Tool	45
Use the Capture Config Utility	46

Integrate Endpoint Privilege Management for Windows with BeyondInsight

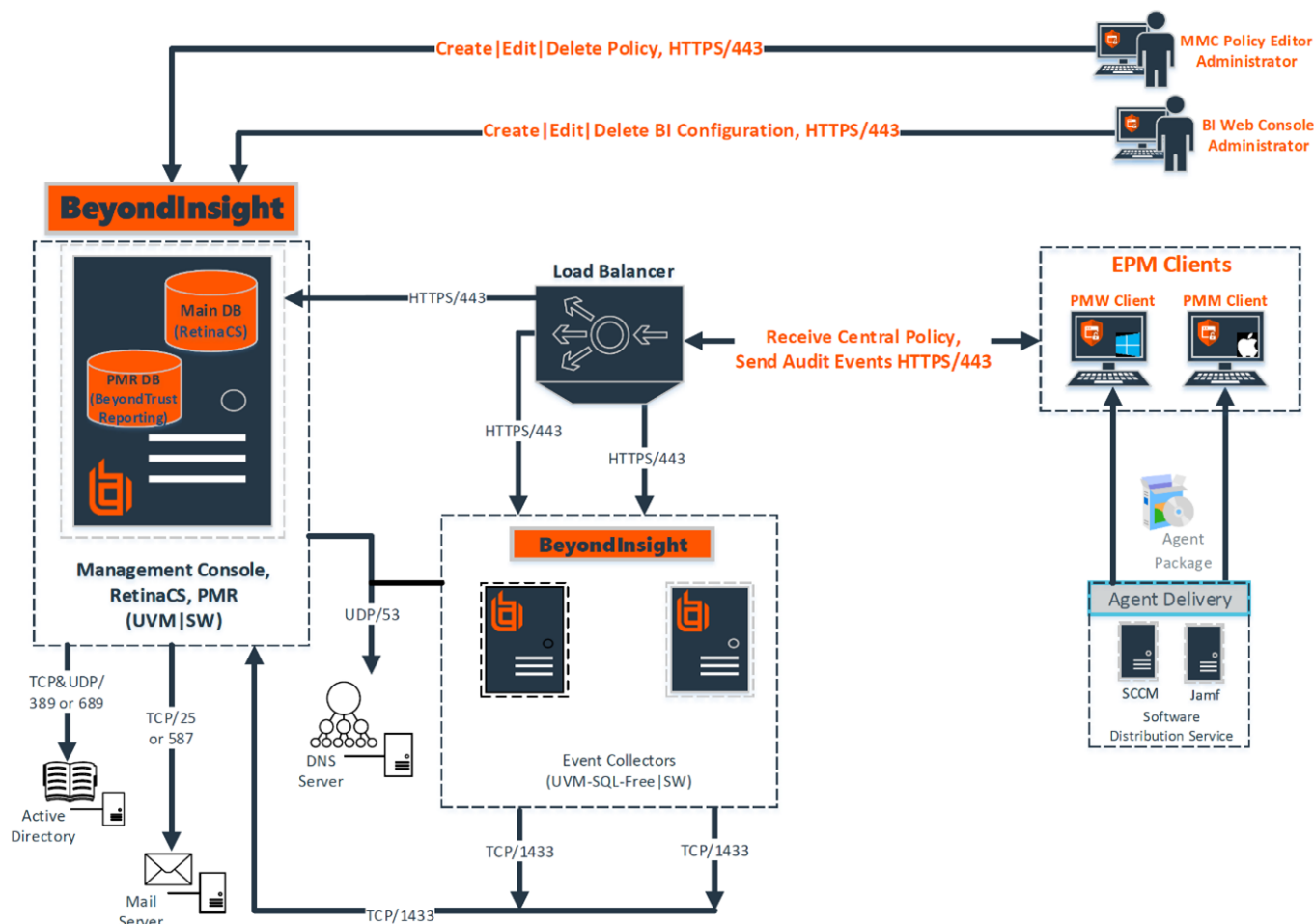
Overview

Endpoint Privilege Management combines privilege management and application control technology in a single lightweight agent. This scalable solution allows global organizations to reduce the attack surface of their endpoint estate by eliminating local admin rights, enforcing application controls and protecting against the techniques used by modern malware.

With the integration between U-Series Appliance, BeyondInsight, and Endpoint Privilege Management, you have a proven privilege management solution that transmits data about your endpoints and policies to a centralized management console with the reporting and analytic capabilities needed to reduce risk, maximize security, and empower users to work effectively.

Architecture

Endpoint Privilege Management – BeyondInsight Architecture



Prerequisites

- BeyondInsight version 6.9.0.712 or later
- Endpoint Privilege Management for Windows 5.4.228.0 or later

The Endpoint Privilege Management endpoints and the U-Series-BeyondInsight appliance communicate using TLS certificates for authentication of both parties. This guide details how to use the BeyondInsight default client certificate (**eEyeEmsClient**), but you may prefer to use your own Public Key Infrastructure (PKI).

i For more information, see [Use a Domain PKI for BeyondInsight Communication in the BeyondInsight Installation Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/install/certificates.htm#UseDomainPKI), at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/install/certificates.htm#UseDomainPKI>.

Port Requirements

TCP Port 443	<p>An event service is used to communicate between Endpoint Privilege Management and BeyondInsight using port 443. Events from Endpoint Privilege Management are sent to BeyondInsight using this service. Communications over this channel is secured by means of a client certificate.</p> <p>This connection is from the endpoint to the appliance where BeyondInsight is hosted. No ports need to be open on the client side.</p>
TCP Port 1443	<p>Required for the SQL Server database connection from the event server to the server where the database is hosted.</p>

i For information on integrating BeyondTrust Endpoint Privilege Management for Mac with BeyondInsight, see the [Endpoint Privilege Management for Mac Integration Guide](https://www.beyondtrust.com/docs/privilege-management/integration/pmm-beyondinsight/index.htm), at <https://www.beyondtrust.com/docs/privilege-management/integration/pmm-beyondinsight/index.htm>.

Web Policy Editor and Reporting

- The Web Policy Editor (WPE) is available in BeyondInsight versions 22.1 and later.
- Endpoint Privilege Management Reporting (PMR) is available in BeyondInsight versions 6.10 and later.

Note: To integrate PMR in versions of BeyondInsight prior to 23.1, please contact your BeyondTrust representative for assistance with installing and configuring.

The Web Policy Editor and Endpoint Privilege Management Reporting features are not installed out of the box with BeyondInsight.

i For more information on installing and configuring WPE and PMR with BeyondInsight, see:

- ["Install Web Policy Editor in BeyondInsight Instance" on page 19](#)
- ["Install Endpoint Privilege Management Reporting in BeyondInsight" on page 22](#)
- ["Upgrade Endpoint Privilege Management Reporting in BeyondInsight " on page 27](#)
- ["Configure Endpoint Privilege Management Reporting in BeyondInsight" on page 38](#)

Detailed documentation on using WPE and PMR is available in the BeyondInsight User Guide.

i For more information, see:

- [Manage Endpoint Privilege Management Policies](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/epm/policies.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/epm/policies.htm>.
- [View Endpoint Privilege Management Reports](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/epm/reporting/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/epm/reporting/index.htm>.

Integration Workflow

After you set up the appliances, and verify BeyondInsight and Endpoint Privilege Management are correctly installed, set up the communication between the two.

High-level integration steps:

1. Create and deploy the BeyondInsight client certificate to all potential Endpoint Privilege Management for Windows endpoints or policy editor machines.
2. Using your method of choice, deploy the Endpoint Privilege Management for Windows client and BeyondInsight adapter on all endpoints, using the **BIMODE=1** install flag.
3. Verify BeyondInsight is receiving heartbeats and information from Endpoint Privilege Management for Windows endpoints.
4. Configure the policy editor to communicate with BeyondInsight and test the connection.
5. Create a policy in the editor.
6. Create a Smart Rule in BeyondInsight.
7. Assign and deploy a policy from BeyondInsight.

Configure U-Series Appliance

If you deploy Endpoint Privilege Management to a BeyondInsight and U-Series Appliance environment, use the following information as supplementary guidance to installing and configuring a U-Series Appliance.

Appliances can be set up across your environment, each one configured to host one or more roles. We recommend working with your BeyondTrust representative to determine the appliance architecture best suited for your estate. This is especially important if you plan to integrate Endpoint Privilege Management into an existing U-Series Appliance-BeyondInsight-Password Safe deployment.

i For more information, see *U-Series Appliance Technical Documentation* at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/index.htm>.

Primary/Secondary Deployment Model

An example deployment model for a U-Series-BeyondInsight-Endpoint Privilege Management integration includes two appliances.

- **Primary appliance:** Hosts the reporting server and the BeyondInsight management console.
- **Secondary appliance:** Hosts the BeyondTrust event server that can manage policy distribution.

In this example model, you can deploy the event server in a variety of locations, including internet facing, if you want to support on and off-network devices.

The appliance can support up to 10,000 endpoints and additional event servers can be added to increase the capacity.

The following sections provide high-level configuration details.

Primary U-Series Appliance

Before proceeding with the setup of the primary appliance, keep the following considerations in mind:

- On a primary appliance, ensure the management console and reporting roles are enabled. In an architecture with more than one appliance, enable the management console role on only one appliance.
- When the SQL Server database resides on the primary appliance, then you must configure access to the remote database so secondary appliances can connect to the database. Set remote access on the **SQL Server Database** role.

To configure a primary appliance:

- Complete the appliance deployment and configuration wizards, taking the appropriate steps to achieve the objectives outlined above. Step-by-step instructions are located here: [Configure the BeyondTrust U-Series Appliance](#).

Event Server Appliance

A U-Series Appliance can be set up as an event server to serve policy to your estate.

Before proceeding with the setup of the event server appliance, keep the following configuration details in mind when going through the deployment and configuration wizards:

- You must activate the Event Collector role either during the configuration wizard or later in the U-Series Appliance software.
- Disable roles that are configured on the primary: **BeyondInsight Management Console**, **BeyondInsight Analysis Services**, and **Analytics and Reporting - Reporting Service**.
- When an appliance is acting as the event server, then you must set up remote database settings on the primary appliance.

To configure an appliance as an event server:

- Complete the appliance deployment and configuration wizards, taking the appropriate steps to achieve the objectives outlined above. Step-by-step instructions are located here: [Configure the BeyondTrust U-Series Appliance](#).

Configure BeyondInsight and EPM via OAuth

Starting in BeyondInsight 24.1 and Endpoint Privilege Management 24.3, configure the components to communicate via OAuth. If the BeyondInsight server is configured with a publicly trusted HTTPS certificate, this can now be accomplished without adding any certificates to the endpoint. Using OAuth simplifies attaching endpoints to BeyondInsight.

To continue using the self-signed certificate generated by the BeyondInsight server, follow the instructions in [Configure BeyondInsight and Endpoint Privilege Management](#) before proceeding with deploying OAuth. Certificates in this configuration are used only for HTTPS/TLS communication; and adding the certificate during installation is no longer required.

Installing EPM with an OAuth activation secret

Instructions to set up OAuth are provided in the BeyondInsight User Guide.



For more information, see [Configure OAuth Authentication for Agents Using Installer Activation Keys](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/configure-installer-activation-keys.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/configure-installer-activation-keys.htm>.

Configure BeyondInsight and Endpoint Privilege Management

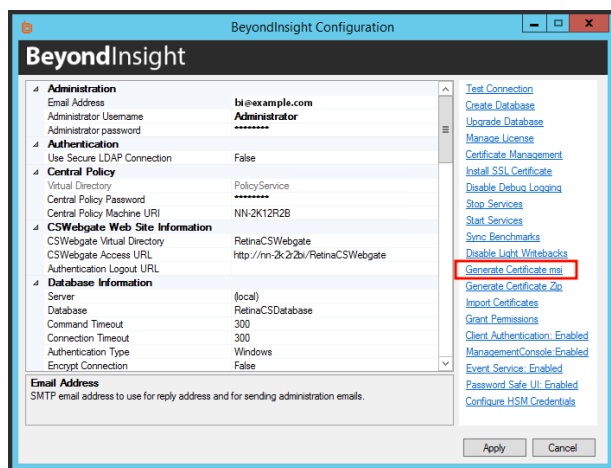
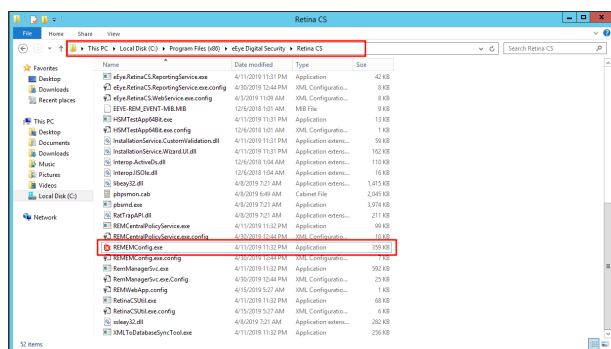
To establish communication between BeyondInsight and Endpoint Privilege Management for Windows clients:

- Generate a client certificate from BeyondInsight.
- Install the certificate on every client that must send information to BeyondInsight.

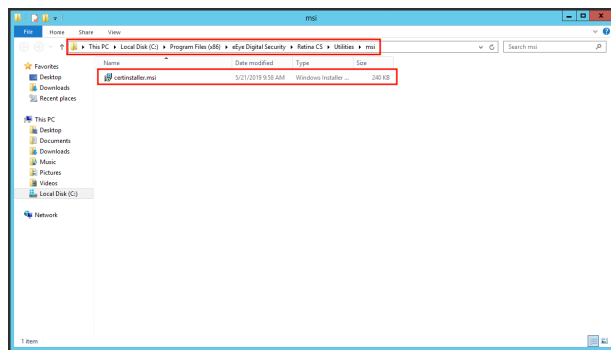
We recommend installing the BeyondInsight client certificate before installing the Endpoint Privilege Management for Windows client.

Generate Client Certificate MSI

1. On the BeyondInsight server, go to **C:\Program Files (x86)\eEye Digital Security\Retina CS**.
2. Run **REMEmConfig.exe** to open the **BeyondInsight Configuration Tool**.
3. Click the **Generate Certificate.msi** link. A command prompt opens, indicating the MSI is being generated.



4. Once the prompt closes, the MSI appears in the **C:\Program Files (x86)\eEye Digital Security\Retina CS\Utilities\msi** directory.



Deploy the Certificate MSI

After you generate the **certinstaller.msi**, you must deploy and install the MSI on each machine you want to communicate with BeyondInsight, using administrator rights. You can deploy the MSI using the following methods:

- Command prompt running as Administrator
- Group Policy
- Enterprise Software Management tool of your choice, such as SCCM

Each method is detailed below.

Use Command Prompt

1. Add a copy of the **certinstaller.msi** to the machine
2. Run **cmd.exe** as administrator
3. Run the following command: **msiexec /i certinstaller.msi**

Create a Group Policy

Use the Group Policy Management Console (GPMC) to deploy certificate packages to your client computers.

1. To deploy the certificate MSI package, copy the certificate MSI package to an accessible location.
2. Click **Start > Control Panel > Administrative Tools > Group Policy Management** to open the GPMC. If the GPMC is not already installed, it can be downloaded from www.microsoft.com/en-us/download.
3. In the GPMC, click **Forest > Domains > Mydomain > Group Policy Objects**.
4. To create a new GPO, right-click **Group Policy Objects**, and click **New**.
5. Enter a name for the GPO and click **OK**. Alternatively, you can add configurations to an existing GPO.
6. Right-click the GPO and click **Edit** to launch the Group Policy Management Editor to configure settings for the GPO.
7. In the Group Policy Management Editor, click **Computer Configuration > Policies > Software Settings**.
8. Right-click **Software Installation** and click **New > Package**.
9. Select the certificate MSI installer package, and click **Open**.
10. Select **Assigned** and click **OK**. After a brief delay, the name of the software to be installed is displayed in the **Details** pane of the Group Policy Management Editor.
 - If the name does not appear, right-click **Software Installation** and click **Refresh** until it does.
 - To modify installation settings, double-click the item name in the display pane.
 - To remove an item, right-click the item name and select **All Tasks > Remove**.

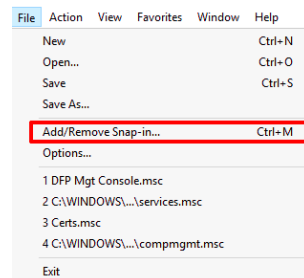
Restart each client computer to initiate the installation. This can be done manually or by using Group Policy mechanisms.

Use an Enterprise Software Management Tool (such as SCCM)

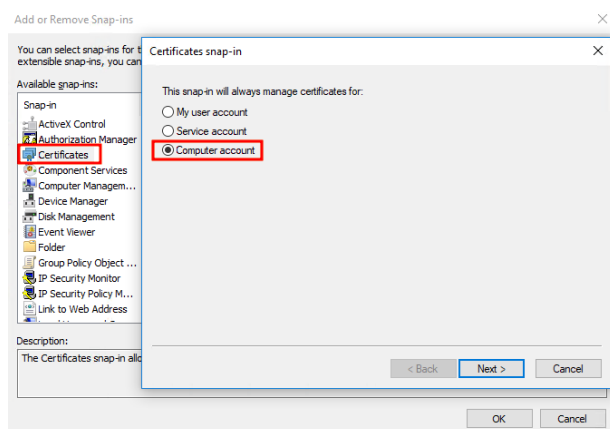
Be sure to consult the guides for the management tool you use.

After you have deployed the client certificate, confirm it is on the system, following the steps below.

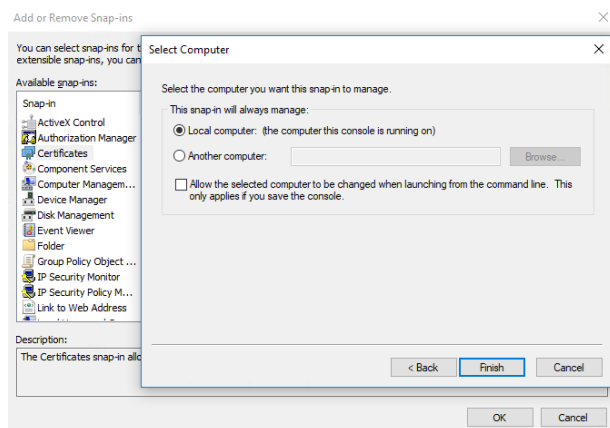
1. Run the **Microsoft Management Console (MMC)** as administrator.
2. Go to **File > Add/Remove Snap-in**.



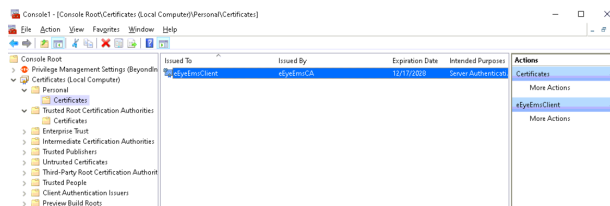
3. From the **Snap-in** menu, select **Certificates**, and click **Add >**.
4. In the **Certificates snap-in** dialog, select **Computer account**.



5. Choose **Local computer: (The computer this console is running on)**. Click **Finish**.



6. In the MMC Console, expand **Console Root > Certificates (Local Computer)**.
7. Expand both the **Personal > Certificates** directory and the **Trusted Root Certification Authorities** directory to ensure the **eEyeEmsClient** client certificate is listed.



Note: If the certificates are not present, it is possible they were incorrectly installed in the **Certificates (Current User)** store. If you find them there, delete them and uninstall **certinstaller.msi** from **Programs & Features (appwiz.cpl)** before repeating these steps.

Install Endpoint Privilege Management for Windows

For BeyondInsight integration with Endpoint Privilege Management for Windows, you must set the **BIMODE** installer variable to **1**. In the majority of cases, only the URL of your BeyondInsight Event Service must be specified. For context, example installation strings are provided below.

**Example:**

```
PrivilegeManagementForWindows_x64.exe /v"BIMODE=1  
BEYONDINSIGHTURL=https://example.com/EventService/Service.svc"
```

**Example:**

```
msiexec.exe /i PrivilegeManagementForWindows_x64.msi BIMODE=1  
BEYONDINSIGHTURL="https://example.com/EventService/Service.svc"
```

If you are using a custom certificate or workgroup, you can specify non-default values as additional install variables, as shown in the following examples.

**Example:**


```
PrivilegeManagementForWindows_x64.exe /v"BIMODE=1  
BEYONDINSIGHTURL=https://example.com/EventService/Service.svc  
BEYONDINSIGHTCERTNAME=CertExample  
BEYONDINSIGHTWORKGROUP=BeyondTrust WorkGroup"
```

**Example:**

```
msiexec.exe /i PrivilegeManagementForWindows_x64.msi BIMODE=1  
BEYONDINSIGHTURL="https://example.com/EventService/Service.svc"  
BEYONDINSIGHTCERTNAME="CertExample"  
BEYONDINSIGHTWORKGROUP="BeyondTrust WorkGroup"
```

The following table details the available installer variables and their default values:

Location	Name	Default	Installer Variable Name
HKEY_LOCAL_MACHINE\SOFTWARE\Avecto\Privilege Guard Client	BeyondInsightUrl	[Empty] - You must specify this	BEYONDINSIGHTURL
	BeyondInsightCertName	eEyeEmsClient	BEYONDINSIGHTCERTNAME
	BeyondInsightWorkgroup	BeyondTrust Workgroup	BEYONDINSIGHTWORKGROUP
	BeyondInsightHeartbeatIntervalMins	720	
	BeyondInsightPolicyIntervalMins	90	

 **Tip:** The default values of **BeyondInsightPolicyIntervalMins** and **BeyondInsightHeartbeatIntervalMins** can be shortened for testing purposes (low numbers of machines). Be aware that decreasing these values increases load on the BeyondInsight Event Service server.




IMPORTANT!



When updating the clients on an existing deployment of BeyondInsight and Endpoint Privilege Management for Windows, the registry keys from the previous install will be removed. Any previously specified variables in the install string must be restated in an upgrade.

Verify Endpoints are Registered in BeyondInsight

After deploying your Endpoint Privilege Management for Windows endpoints, ensure that BeyondInsight is receiving heartbeats and information from them. Once they check in, the endpoints are shown as entries on the **Assets** grid in BeyondInsight, as well as the Endpoint Privilege Management **Agents** grids.

BeyondInsight


Assets


 (Global)

[Endpoint Privilege Management Agents](#)
[Manage Smart Rules](#)

ASSETS

Smart Group filter






Endpoint Privilege Management C...

Last Updated filter








Last 90 days

Filter by

Create New Asset +

2 items

Asset	Domain	Operating System	Asset Type	Solution	Asset Risk	Last Updated
<input type="checkbox"/> test	domain	Windows 10 (x64)	--	  	--	Feb 11, 2022, 8:02 AM
<input type="checkbox"/> UVI	WORKGROUP	--	--	   	--	Feb 11, 2022, 8:00 AM

Use Smart Rules to Assign Policy

After you add and upload a policy to BeyondInsight from the Policy Editor (if you are using the MMC Policy Editor), log in to your BeyondInsight instance to create Smart Rules to assign policies for assets and users.



Tip: If BeyondInsight and Endpoint Privilege Management for Windows are successfully communicating, the Endpoint Privilege Management option becomes available under **Menu > Assets**.

Create a Smart Rule to Assign Policy to Assets

1. From the left menu in your BeyondInsight instance, click **Smart Rules**.
2. Click **Create Smart Rule**.
3. From the **Category** dropdown, select **Assets and Devices**.
4. Type a name and description for the Smart Rule.
5. In the **Selection Criteria** section, design a query to create a list of assets you want to assign policy to.



Tip: For this example, we can narrow down the results of our query to locate our test system, NN-1K12RBR. Choose to match **ALL** criteria and select **Asset fields > Asset Name > contains > NN-1K12RBR**.

6. From the **Actions** dropdown, select **Deploy Endpoint Privilege Management Policy**.
7. Click **Select Policies for Deployment**.
8. The Endpoint Privilege Management policies you uploaded from Endpoint Privilege Management for Windows are listed. Click **+** to add the policy, and then click **Accept Changes**.
9. Click **Create Smart Rule**.

Create New Asset Based Smart Rule

Details

Category

Assets and Devices

Name

Assign Policies to Assets

Description

Reprocessing limit

Default

Active

☒

Selection Criteria

Include items that match

ALL

of the following

Asset fields

Asset Name

contains

NN-1K12RBR

[Add another condition](#)
[Add a new group](#)

Actions

Deploy Endpoint Privilege Management Policy

SELECT POLICIES FOR DEPLOYMENT (1)

Allow assignment despite workgroup mismatches between agent and policy

☐

[Add another action](#)

CREATE SMART RULE

DISCARD



For more information about creating and organizing Smart Rules, see [Use Smart Rules to Organize Assets in the BeyondInsight User Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/smart-rules/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/smart-rules/index.htm>.

Create a Smart Rule to Assign Policy to Users

1. From the left menu in your BeyondInsight instance, click **Smart Rules**.
2. Select **Policy User** from the dropdown.
3. Click **Create Smart Rule +**.
4. From the **Category** dropdown, select **Policy Users**.
5. Type a name and description for the Smart Rule.
6. In the **Selection Criteria** section, design a directory query to create a list of users you want to assign policy to.
7. From the **Actions** dropdown, select **Deploy Endpoint Privilege Management Policy**.
8. Click **Select Policies for Deployments**.
9. The Endpoint Privilege Management policies you uploaded from Endpoint Privilege Management for Windows are listed. Click **+** to add the policy, and then click **Accept Changes**.
10. Click **Create Smart Rule**.

Create New Policy User Based Smart Rule

Details

Category
Policy Users

Name
Assign Policies to Users
Active

Description

Reprocessing limit
Default

Selection Criteria

Include Items that match ALL of the following

Directory Query

Include accounts from Directory Query

Find all Server 2008

Re-run the query every X hours 0

Discover users

Add another condition Add a new group

Actions

Deploy Endpoint Privilege Management Policy

SELECT POLICIES FOR DEPLOYMENT (1)

Add another action

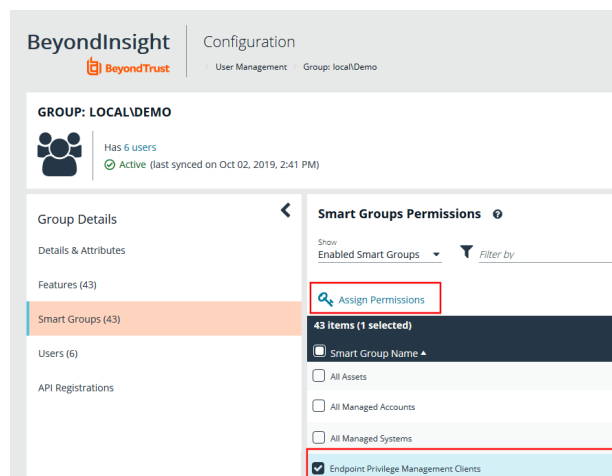
CREATE SMART RULE DISCARD

i For more information about managing policies for EPM, see [Manage EndPoint Endpoint Privilege Management Policies in the BeyondInsight User Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/epm/policies.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/epm/policies.htm>.

Grant Users Permissions to Log in to the Policy Editor

If you want to grant additional users access to log in to the Policy Editor, read and write access must be included on the Endpoint Privilege Management for Windows assets. Add this access by including permissions in the Smart Rule.

1. From the homepage in your BeyondInsight instance, click **Configuration**.
2. Under **Role Based Access**, select **User Management**.
3. Locate the group you want to edit and click the menu to the far right.
4. Select **View Group Details**.
5. In the **Group Details** pane, click **Smart Groups**.
6. In the **Smart Groups Permissions** pane, select the appropriate Smart Group.
7. Click **Assign Permissions** above the grid.
8. Select **Assign Permissions Full Control**.



Install Web Policy Editor in BeyondInsight Instance


Note:

- The WPE is compatible only with BeyondInsight 22.1 and later releases.
- If using WPE 23.4 or later version, BeyondInsight must be at least version 23.1.

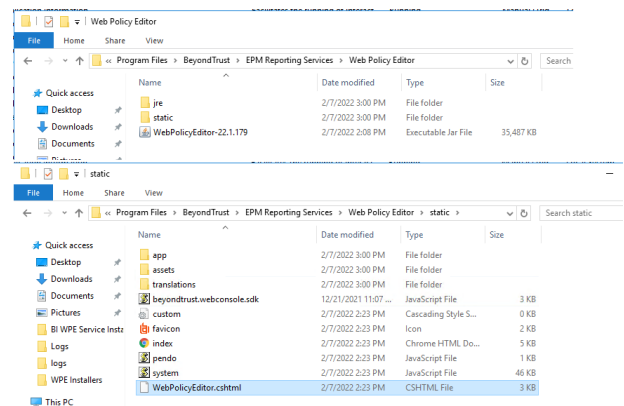
Install Endpoint Privilege Management WPE and the BeyondInsight WPE Plugin

1. Copy the WPE installer and the BeyondInsight WPE plugin MSI files to the BeyondInsight server in the same parent directory. The files are named as follows:
 - **BeyondTrust WebPolicyEditor-2x.x.xxx.msi**
 - **BeyondInsight.EPM.WebPolicyEditor.Services-2x.x.xxx.msi**
2. Run the WPE installer (**BeyondTrust WebPolicyEditor-2x.x.xxx.msi**). Check the **Destination Folder** selected is correct.
3. Run the WPE plugin installer (**BeyondInsight.EPM.WebPolicyEditor.Services-2x.x.xxx.msi**). Check the **Destination Folder** selected is correct.



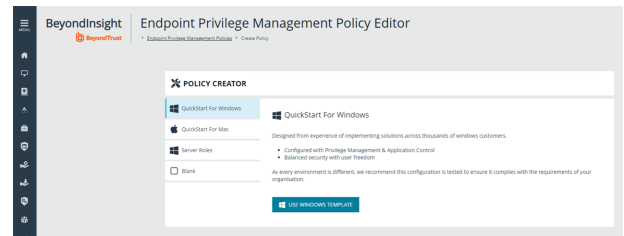
Note: The Web Policy Editor must be installed before the WPE service, as the service looks for the WPE files.

4. Verify the WPE installed successfully, as follows:
 - Navigate to the **C:\Program Files\BeyondTrust\EPM Reporting Services\Web Policy Editor** folder and verify the **WebPolicyEditor-2x.x.xxx** file is listed.
 - Navigate to the **C:\Program Files\BeyondTrust\EPM Reporting Services\Web Policy Editor\static** folder and verify the **WebPolicyEditor.cshhtml** file is listed.

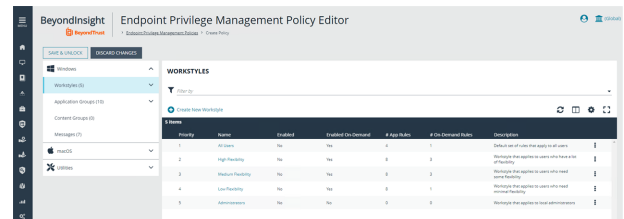


5. Verify the WPE works in BeyondInsight, as follows:
 - From the left menu in BeyondInsight, under **Endpoint Privilege Management**, click **Policies**.
 - Click **Create Policy**.

- Verify the **Policy Creator** displays.



- Click through the QuickStart options to verify the templates contain preloaded Workstyles, groups, and Messages.



Upgrade the Endpoint Endpoint Privilege Management WPE

1. Copy the latest WPE installer (**BeyondTrustWebPolicyEditor-2x.x.xxx.msi**) and the latest WPE Service, (**BeyondInsight.EPM.WebPolicyEditor.Services-2x.x.x.xxx.msi**), to the BeyondInsight server. We recommend copying to a **c:\temp** folder.
2. Stop the **BeyondTrust EPM Web Policy Editor** service.
3. Run the WPE installer (**BeyondTrustWebPolicyEditor-2x.x.xxx.msi**) on the BI server. Check the **Destination Folder** selected is correct.
4. Run the WPE Service installer (**BeyondInsight.EPM.WebPolicyEditor.Services-2x.x.x.xxx.msi**) on the BI Server. Check the **Destination Folder** selected is correct.
5. Verify the **BeyondTrust EPM Web Policy Editor** service has started.
6. In the BeyondInsight console, verify you can view policies listed on the **Endpoint Endpoint Privilege ManagementPolicies** page:
 - Click the menu for a policy, and then click **View Policy**.
 - Verify you can view the contents of the policy.



Tip: If a blank page displays when creating or viewing a policy in BeyondInsight, this may indicate the **WebPolicyEditor.cshtml** file did not update. Follow the below troubleshooting steps to confirm and resolve:

- Press **F12** or **Ctrl + Shift + I** to open the **Dev Tools** window.
- Click the **Network** tab.
- If red errors are listed for Vendor and Main with a GUID attached, you have two options to resolve:
 - Copy the **WebPolicyEditor.cshtml** file manually from **C:\Program Files\BeyondTrust\EPM Reporting Services\Web Policy Editor\static** to **C:\Program Files (x86)\eEye Digital Security\Retina CS\WebConsole\Views\Apps**.
 - Uninstall and reinstall the **BeyondTrust EPM Web Policy Editor Service**.

i For more information on working with the Web Policy Editor, see "Manage Endpoint Privilege Management Policies" in the *BeyondInsight User Guide* at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm>.

Install Endpoint Privilege Management Reporting in BeyondInsight

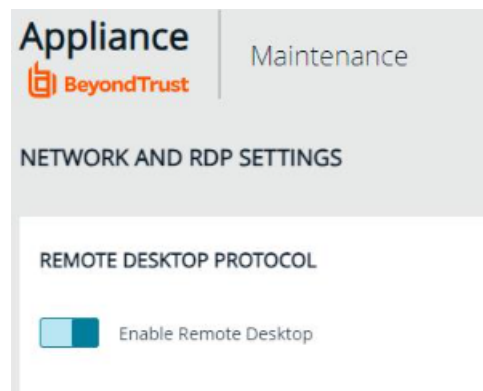
Endpoint Privilege Management Reporting (PMR) can be installed and configured to integrate with BeyondInsight (BI), allowing you to view PMR dashboards and reports using the BeyondInsight console. The below sections detail how to install the PMR database, UI, and event collector components in your BeyondInsight instance.

i Once the PMR in BI integration is installed and configured, for more information on working with the Endpoint Privilege Management Reporting in the BeyondInsight console, see "View Endpoint Privilege Management Reports" in the *BeyondInsight User Guide* at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm>.

Prerequisites

The following prerequisites must be in place before installing and configuring PMR with BI:

- The versions of BeyondInsight, PMR UI, PMR database, Event Collector and the supporting services must be at versions which are supported collectively.
 - Current version: See *BeyondTrust Product Integrations* in [BeyondInsight and Password Safe Supported Platforms](#).
 - Earlier versions: See [archived documentation](#).
- Supports up to SQL Server 2022. If installing the Endpoint Privilege Management Reporting database on the SQL Server 2022 platform, it is recommended to use the EXE installer rather than the MSI. If you prefer to use the MSI, you must ensure that Microsoft SQL Server 2012 Native Client (x64) TLS 1.2 Support is installed on your database server.
- To use the **Add To Policy** functionality from the **Endpoint Privilege Management Reporting > Events** grid in BI, the Endpoint Privilege Management Web Policy Editor version 23.4 or later must be installed and configured with BI.
 - If installed prior to installing PMR, ensure the **BeyondInsight.EPM.WebPolicyEditor.Services**, **BeyondInsight.EPM.ReportingGateway.Services**, and **BeyondInsight.EPM.EventCollector.Services** are restarted after installing Endpoint Privilege Management Reporting and Endpoint Privilege Management Web Policy Editor.
- Only SQL authentication is supported between BI and the PMR database. Windows authentication is not supported. The SQL server must be in mixed mode. To configure this in SQL Management Studio:
 - Go to **SQL server name > Properties > Security**.
 - Select **SQL Server and Windows Authentication** mode.
- Remote Desktop Protocol (RDP) must be enabled on the U-Series Appliance. This is required only during the PMR installation and can be disabled once the install is complete. To enable RDP on the appliance:
 - Go to **Maintenance > Network and RDP Settings**.
 - Click the toggle to turn on the **Enable Remote Desktop** option.





Note: To integrate PMR in versions of BeyondInsight prior to 23.1, please contact your BeyondTrust representative for assistance with installing and configuring.

Install BeyondTrust Endpoint Privilege Management Reporting Database

The **PrivilegeManagementReportingDatabase** MSI must be at least version 23.2 to support the new user interface for Endpoint Privilege Management Reporting (PMR).

1. On the server where you want to host the PMR database, run the **PrivilegeManagementReportingDatabase** EXE file as administrator, either from the folder where it is stored or from a command prompt. The PMR database can be hosted on the BI server or on an external database server.



IMPORTANT!

There is currently a requirement to install the **PrivilegeManagementReportingDatabase** executable or MSI on the BeyondInsight Management Server to see the **Endpoint Privilege Management Reports** link, and the **Endpoint Privilege Management Reporting Database Configuration** tile in BI.

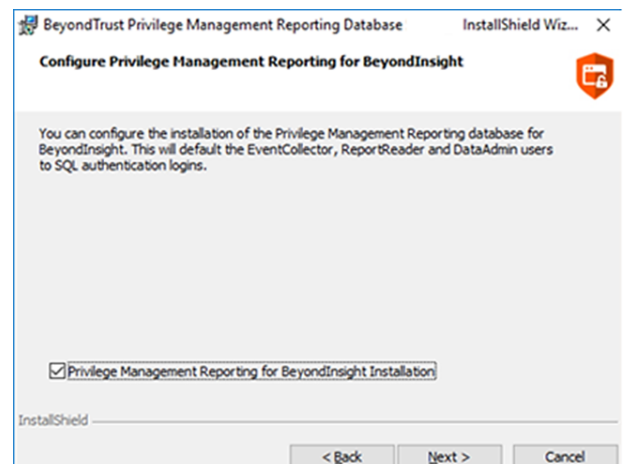
If you are hosting the PMR database on an external database server, you must install the **PrivilegeManagementReportingDatabase** twice - once on the external database server, and again on the BeyondInsight Management server. When you set the configuration for the database, you can specify the external database server here to ensure that the remote database is used for event ingestion and reporting. See ["Configure Advanced SQL and Event Collector Settings for PMR in BI Integration"](#) on page 42.

2. Check **Endpoint Privilege Management Reporting for BeyondInsight Installation** and click **Next**.

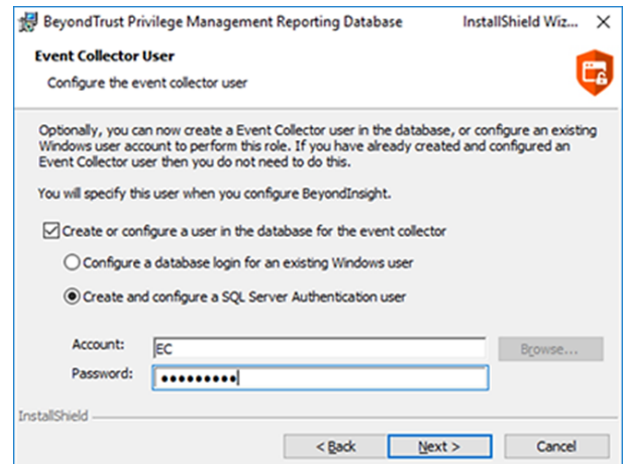
Check this box to use SQL Server authentication for the event collector, report reader, and data admin users configured in subsequent stages of the wizard.



Note: Windows authentication to the PMR database is not supported.



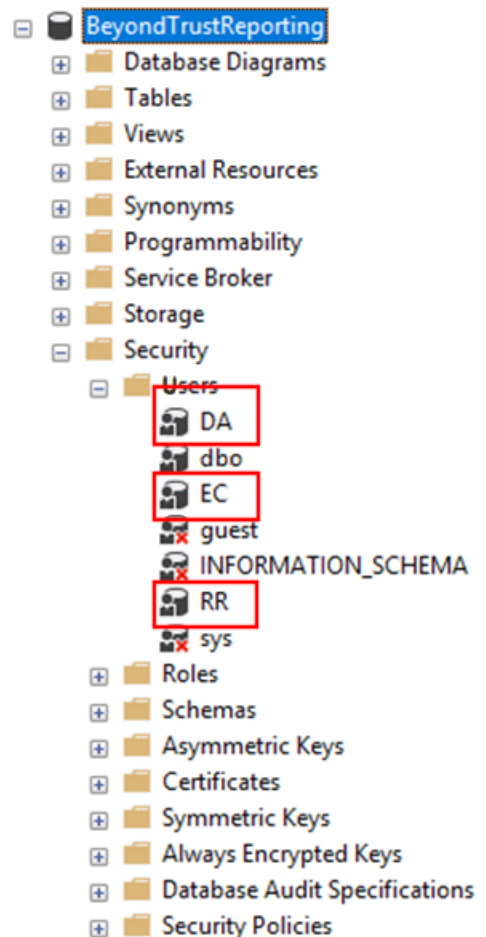
- Continue through the wizard to create the event collector, report reader, and data admin user accounts by checking the option to create or configure the user in the database and entering the SQL credentials. An example of creating the event collector user account is shown.



- Following the database installation, ensure the PMR database is created and accessible from Microsoft SQL Server Management Studio with the users created, as shown.



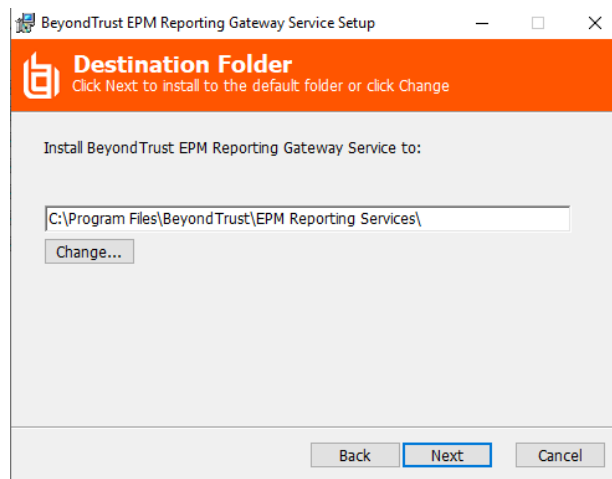
Tip: We recommend using the SQL Server Agent job to run the **CopyFromStaging** process rather than using the default Service Broker queue. To switch to using the SQL Server Agent job, execute the **Create_ER_Database_Agent.sql** script against the PMR database. This removes the Service Broker queue and creates and enables the SQL Server Agent job.



Install BeyondTrust Endpoint Privilege Management Reporting UI

As of version 23.4, PMR in BI includes a new user interface known as *PMR UI*, which is based on Angular, to replace the discontinued Unified Reporting (UR) user interface, which was based on the out-of-support AngularJS.

1. On the BI server, run the **BeyondInsight.EPM.ReportingGateway.Services** MSI file as administrator, either from the folder where it is stored or from a command prompt.
2. Keep the default destination folder. This service must be installed in its default location for the PMR in BI integration to work



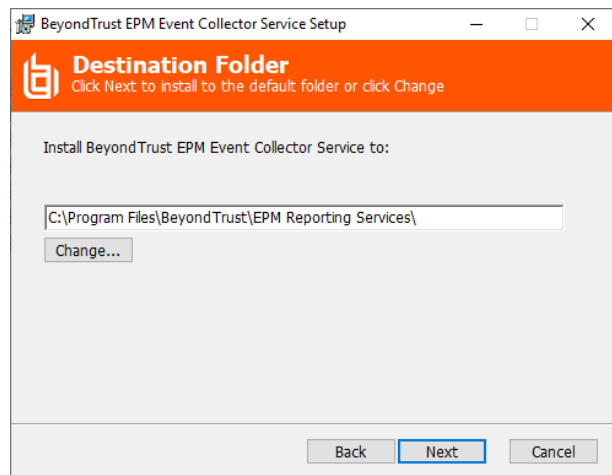
3. Run the **BeyondTrust PMR UI** MSI on the BI server. The reporting gateway service starts automatically as part of the installation.



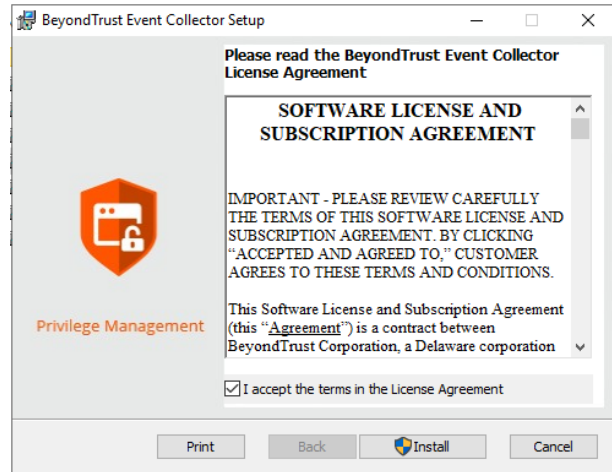
Install the BeyondTrust EPM Event Collector

1. On the BI server, run the **BeyondInsight.EPM.EventCollector.Services** MSI file as administrator, either from the folder where it is stored or from a command prompt.

- Keep the default destination folder. This service must be installed in its default location for the PMR in BI integration to work



- Run the **BeyondTrust EventCollector** MSI on the BI server. The event collector service starts automatically as part of the installation.



IMPORTANT!

If using U-Series Appliance, before continuing with configuration, disable RDP access again by going to **Maintenance > Network and RDP Settings** on the appliance and clicking the toggle to turn off the **Enable Remote Desktop** option.

It is common to configure BI with external event collector worker nodes, which are separate from the main BI management server.



For more information on configuring PMR in the BeyondInsight console and configuring optional advanced options, see:

- ["Configure Endpoint Privilege Management Reporting in BeyondInsight" on page 38](#)
- ["Configure Advanced SQL and Event Collector Settings for PMR in BI Integration" on page 42](#)

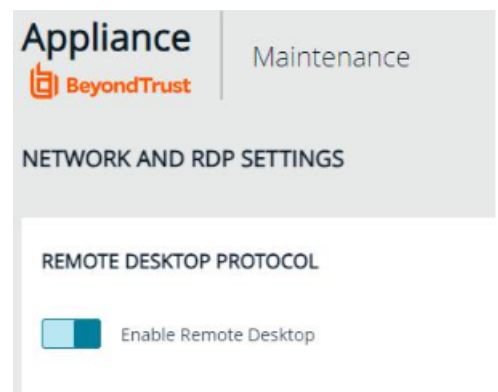
Upgrade Endpoint Privilege Management Reporting in BeyondInsight

The sections below detail how to upgrade the Endpoint Privilege Management Reporting (PMR) database, UI, and event collector components in your BeyondInsight (BI) instance to the latest releases. These steps are applicable only when BI is at version 23.1 or later, and when upgrading the PMR UI to 23.4 or later.

Prerequisites

The following prerequisites must be in place before performing the upgrade:

- The versions of BeyondInsight, PMR UI, PMR database, Event Collector and the supporting services must be at versions which are supported collectively.
 - Current version: See *BeyondTrust Product Integrations* in [BeyondInsight and Password Safe Supported Platforms](#).
 - Earlier versions: See [archived documentation](#).
- Supports up to SQL Server 2022. If installing the Endpoint Privilege Management Reporting database on the SQL Server 2022 platform, it is recommended to use the EXE installer rather than the MSI. If you prefer to use the MSI, you must ensure that Microsoft SQL Server 2012 Native Client (x64) TLS 1.2 Support is installed on your database server.
- To use the **Add To Policy** functionality from the **Endpoint Privilege Management Reporting > Events** grid in BI, the Endpoint Privilege Management Web Policy Editor version 23.4 or later must be installed and configured with BI.
 - If installed prior to installing PMR, ensure the **BeyondInsight.EPM.WebPolicyEditor.Services**, **BeyondInsight.EPM.ReportingGateway.Services**, and **BeyondInsight.EPM.EventCollector.Services** are restarted after installing Endpoint Privilege Management Reporting and Endpoint Privilege Management Web Policy Editor.
- Only SQL authentication is supported between BI and the PMR database. Windows authentication is not supported. The SQL server must be in mixed mode. To configure this in SQL Management Studio:
 - Go to **SQL server name > Properties > Security**.
 - Select **SQL Server and Windows Authentication** mode.
- Remote Desktop Protocol (RDP) must be enabled on the U-Series Appliance. This is required only during the PMR upgrade and can be disabled once the upgrade is complete. To enable RDP on the appliance:
 - Go to **Maintenance > Network and RDP Settings**.
 - Click the toggle to turn on the **Enable Remote Desktop** option.



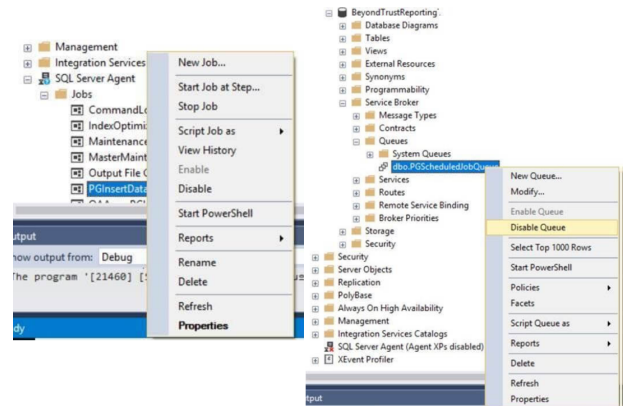
Upgrade BeyondTrust Endpoint Privilege Management Reporting Database

Not all upgrades of the PMR UI require an updated PMR database, as there might not be any database changes since the previous release of PMR UI in BI. Check the version of the installed BeyondTrust Endpoint Privilege Management Reporting database in **Windows Control Panel > Programs and Features** (or **Settings > Apps & features**). If it matches the version specified in the name of the **PrivilegeManagementReportingDatabase** MSI supplied with the latest build, you can skip this section. Otherwise, follow the steps below to upgrade the PMR database.

! IMPORTANT!

Prior to upgrading the PMR database, stop the **CopyFromStaging** process from running, using one of the below methods.

- If the **CopyFromStaging** process is being run by the SQL Server Agent job:
 - In SQL Server Management Studio, expand **SQL Server Agent**.
 - Right-click the **PGInsertData** job, and select **Disable**.
- If the **CopyFromStaging** process is being run by the Service Broker queue:
 - In SQL Server Management Studio, expand **Service Broker > Queues**.
 - Right-click **dbo.PGScheduledJobQueue**, and select **Disable Queue**.



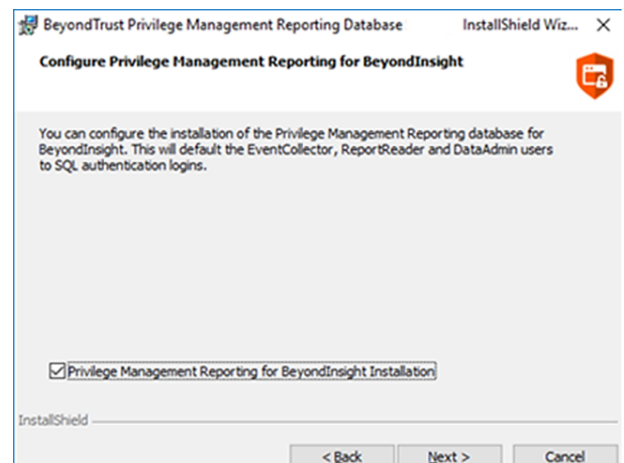
To upgrade the PMR database, follow these steps:

1. On the server that hosts the PMR database, run the **PrivilegeManagementReportingDatabase** EXE file as administrator, either from the folder where it is stored or from a command prompt.
2. On the **Database Server** step of the wizard, ensure the existing PMR database name you are upgrading is selected.
3. Check **Endpoint Privilege Management Reporting for BeyondInsight Installation** and click **Next**.

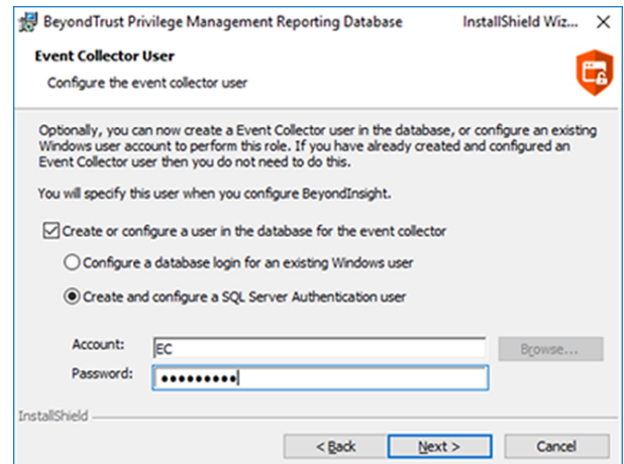
Check this box to use SQL Server authentication for the event collector, report reader, and data admin users configured in subsequent stages of the wizard.



Note: Windows authentication to the PMR database is not supported.



4. If the event collector, report reader, and data admin user accounts are already in the database, uncheck the box to create or configure the user on each of those pages in the wizard, so that new users are not created during the upgrade. If the users don't already exist, check the box to create them. An example of creating the event collector user account is shown.




IMPORTANT!

Following the database upgrade, re-enable the SQL Server Agent job or the Service Broker queue, depending on which mechanism is being used.



Tip: We recommend using the SQL Server Agent job to run the **CopyFromStaging** process rather than using the default Service Broker queue. To switch to using the SQL Server Agent job, execute the **Create_ER_Database_Agent.sql** script against the PMR database. This removes the Service Broker queue and creates and enables the SQL Server Agent job.

Upgrade BeyondTrust Endpoint Privilege Management Reporting UI

As of version 23.4, PMR in BI includes a new user interface known as **PMR UI**, which is based on Angular, to replace the discontinued Unified Reporting (UR) user interface which was based on the out-of-support AngularJS.

If upgrading from UR to PMR UI, the upgrade steps differ from those needed to upgrade one version of PMR UI to another.

To identify if UR is currently being used in BI, on the BI management server assuming that the previous version of PMR was installed in its default location, browse to **C:\Program Files\BeyondTrust\EPM Reporting Services\ReportingGateway**. If the previous UR / PMR UI installed is in a custom location, browse to the custom location instead.

- If a JAR file exists that has the name beginning with **AvectoUnifiedReporting**, this indicates UR is installed.
 - Follow these instructions: ["Option 1 - Upgrade from UR to PMR UI" on page 29.](#)
- If the JAR file starts with **PMR_UI**, this indicates PMR UI is installed.
 - Follow these instructions: ["Option 2 - Upgrade from One Version of PMR UI to Another Version" on page 33.](#)

Option 1 - Upgrade from UR to PMR UI

This section covers upgrading UR versions of PMR in BI to the latest version of PMR UI.



Note: These steps do not apply to upgrades from one version of PMR UI to another version. That type of upgrade is covered in the next section. Please see ["Upgrade Endpoint Privilege Management Reporting in BeyondInsight" on page 27.](#)

Stop Services and Back Up Folders

1. From **Windows Services**, stop the following services:
 - BeyondTrust EPM Reporting Gateway Service
 - BeyondTrust EPM Event Collector Service
2. Back up reporting services folders as follows:
 - Go to **C:\Program Files\BeyondTrust\EPM Reporting Services** (or the relevant location if a custom location was chosen for the existing UR install).
 - Rename the **ReportingGateway** folder to **ReportingGatewayUnifiedReportingBackup**.
 - Rename the **EventCollector** folder to **EventCollectorUnifiedReportingBackup**.



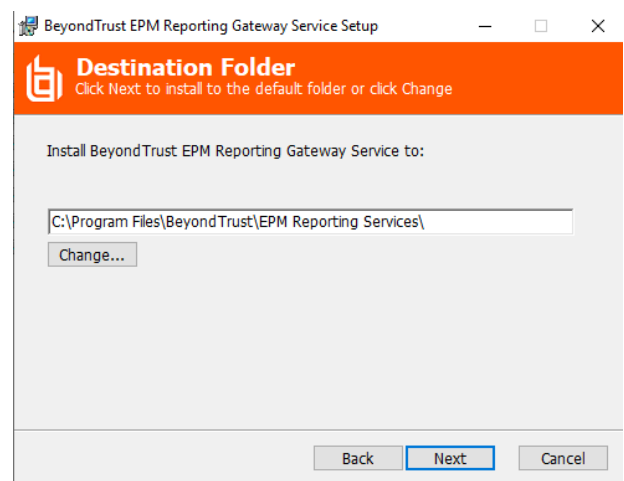
IMPORTANT!

*If a message appears informing you that the file or folder is in use even after stopping the above services, you may also need to stop the **BeyondInsight Admin API** service rename the above folders.*

These folders are renamed rather than deleted to enable rollback of the PMR UI upgrade back to UR in case of any upgrade issues, and also to retain log files. At the point where you are confident that the upgrade to PMR UI is successful, and if you are comfortable to delete the previous UR logs, you can remove these folders.

Upgrade Reporting Gateway Service

1. On the BI server, run the **BeyondInsight.EPM.ReportingGateway.Services** MSI file as administrator, either from the folder where it is stored or from a command prompt.
2. Keep the default destination folder. This service must be installed in its default location for the PMR in BI integration to work.

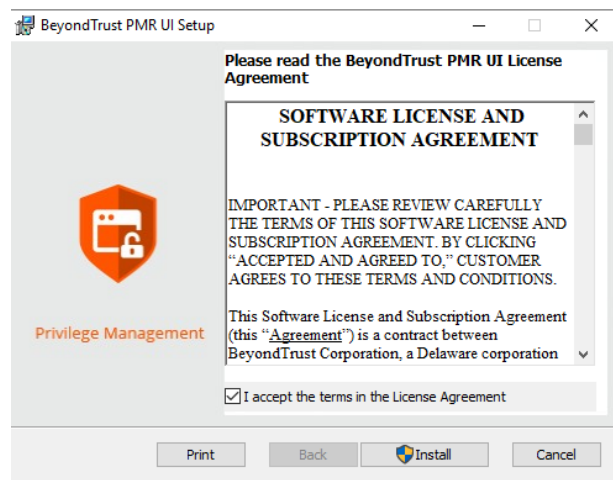


**IMPORTANT!**

*If the existing reporting gateway service is installed in a custom location, when running the latest **BeyondInsight.EPM.ReportingGateway.Services** MSI, the default install folder in the MSI is displayed as the custom location where the existing service is located. In this case, you must change the install location to **C:\Program Files\BeyondTrust\EPM Reporting Services**.*

Upgrade PMR UI

Run the **BeyondTrust PMR UI** MSI on the BI server. The upgraded reporting gateway service starts automatically as part of the installation.

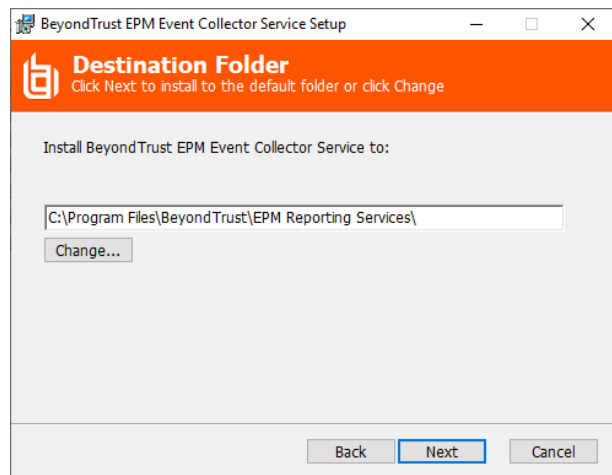


Upgrade the EPM Event Collector

Upgrade the Event Collector Services MSI

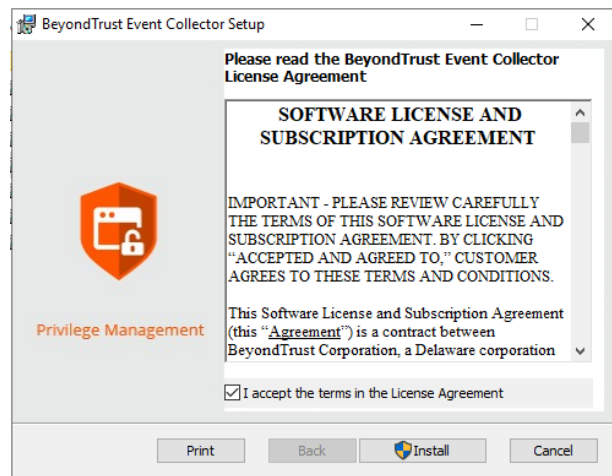
1. On the BI server, run the **BeyondInsight.EPM.EventCollector.Services** MSI file as administrator, either from the folder where it is stored or from a command prompt.

- Keep the default destination folder. This service must be installed in its default location for the PMR in BI integration to work



Install the Event Collector MSI

Run the **BeyondTrust EventCollector** MSI on the BI server. The event collector service starts automatically as part of the installation.



Verify Upgrade

To confirm the upgrade is successful:

- Reset IIS by opening a command prompt as administrator and running the **iisreset** command.
- Verify you can view PMR reports from the left navigation in BeyondInsight, under **Endpoint Endpoint Privilege Management > Reports**.

Upgrade and Configure External Event Collector Worker Nodes

It is common to configure BI with external event collector worker nodes, which are separate from the main BI management server. If you are upgrading PMR in BI using this configuration, please follow the steps below.

1. Ensure the BI event collector worker node is installed and configured.
2. Ensure all steps detailed in the above sections for upgrading PMR in BI have been followed.
3. Verify that PMR is displaying reports in BI and that it is receiving events from an endpoint that is configured to point to the BI event collector on the BI management server. This is to verify that the end-to-end process is working and that events can flow from the endpoint to the BI event collector on the BI management server, to the PMR event collector, and finally to the PMR database.
4. Ensure that the PMR database connection setting configured in the BI console is using the DNS hostname or IP address for the PMR database server, and not localhost or 127.0.0.1. Otherwise, the external event collectors are not able to communicate with the PMR database.
5. Stop the event collector service on the external event collector node to release the lock on the existing **EventCollector** folder.
6. Rename the existing **EventCollector** folder on the external event collector node to **EventCollectorUnifiedReportingBackup**. This folder is renamed rather than deleted to enable rollback of the event collector upgrade to UR's event collector, and also to retain log files.
7. Run the **BeyondInsight.EPM.EventCollector.Services** MSI on each event collector worker node.



Note: This must be installed in its default location for the PMR in BI integration to work.

8. Run the **BeyondTrust EventCollector** MSI on each external event collector worker node. The event collector service starts automatically as part of the upgrade.
9. Configure an endpoint to point to an external event collector node and raise events. Confirm they can be seen in the PMR reports.



IMPORTANT!

If using U-Series Appliance, before continuing on with configuration, disable RDP access again by going to **Maintenance > Network and RDP Settings** on the appliance and clicking the slider to turn off the **Enable Remote Desktop** option.

Option 2 - Upgrade from One Version of PMR UI to Another Version

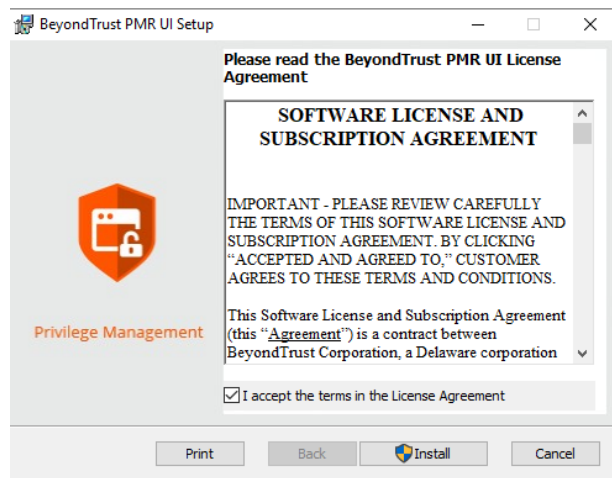
This section of the guide covers upgrades from an existing version of PMR UI to a later version of PMR UI.



Note: Stop the BeyondTrust EPM Reporting Gateway Service. This ensures that any locks on existing files are removed cleanly and that a reboot is not required.

Upgrade PMR UI

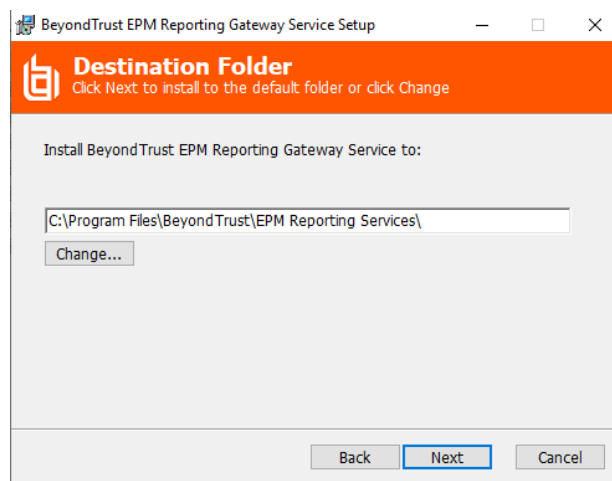
Run the **BeyondTrust PMR UI** MSI on the BI server. The upgraded Reporting Gateway service starts automatically as part of the installation.



Upgrade Reporting Gateway Service

Note: Not all upgrades require an updated reporting gateway service, because there may not have been any changes since the previous release of PMR UI in BI. Check the version of the installed reporting gateway service (BeyondTrust EPM Reporting Gateway Service) in **Windows Control Panel > Programs and Features** (or **Settings > Apps & features**). If it matches the version in the name of the **BeyondInsight.EPM.ReportingGateway.Services** MSI supplied with the latest build, you can skip this section. Otherwise, follow the steps below.

1. On the BI server, run the **BeyondInsight.EPM.ReportingGateway.Services** MSI file as administrator, either from the folder where it is stored or from a command prompt.
2. Keep the default destination folder. This service must be installed in its default location for the PMR in BI integration to work.



Upgrade the EPM Event Collector

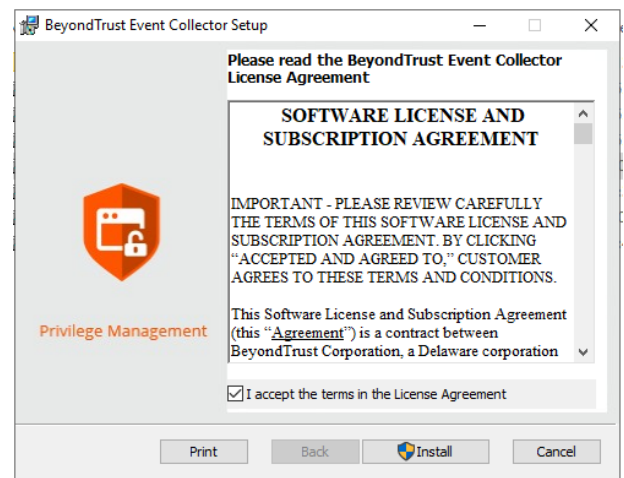
The event collector must be upgraded before the event collector services.

Upgrade the Event Collector



Note: Stop the BeyondTrust EPM Event Collector Service. This ensures that any locks on existing files are removed cleanly and that a reboot is not required.

Run the **BeyondTrust EventCollector** MSI on the BI server. The event collector service starts automatically as part of the installation.



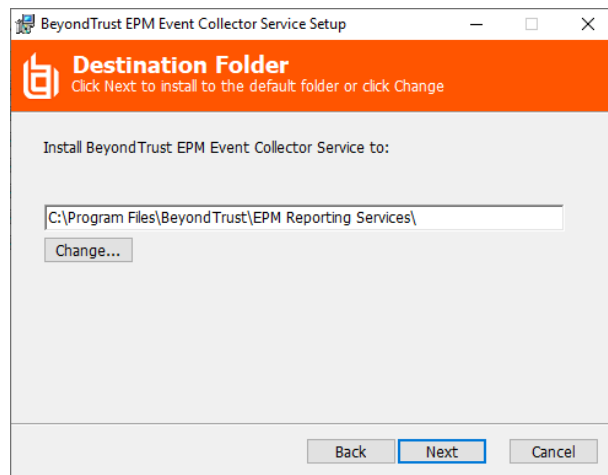
Upgrade the Event Collector Services MSI



Note: Not all upgrades require an updated event collector service, because there may not have been any changes since the previous release of PMR UI in BI. Check the version of the installed event collector service (BeyondTrust EPM Event Collector Service) in **Windows Control Panel > Programs and Features** (or **Settings > Apps & features**). If it matches the version specified in the name of the **BeyondInsight.EPM.EventCollector.Services** MSI supplied with the latest build, you can skip this section. Otherwise, follow the steps below.

1. On the BI server, run the **BeyondInsight.EPM.EventCollector.Services** MSI file as administrator, either from the folder where it is stored or from a command prompt.

- Keep the default destination folder. This service must be installed in its default location for the PMR in BI integration to work



Verify Upgrade

To confirm the upgrade is successful:

Verify you can view PMR reports from the left navigation in BeyondInsight, under **Endpoint Privilege Management > Reports**.

Upgrade and Configure External Event Collector Worker Nodes

It is common for BI to be configured with external event collector worker nodes, which are separate from the main BI management server. If you are upgrading PMR in BI using this configuration, please follow the steps below.

- Ensure the BI event collector worker node is installed and configured.
- Ensure all steps detailed in the sections above for upgrading PMR in BI have been followed.
- Verify that PMR is displaying reports in BI and that it is receiving events from an endpoint that is configured to point to the BI event collector on the BI management server. This is to verify that the end-to-end process is working and that events can flow from the endpoint to the BI event collector on the BI management server, then to the PMR event collector, and finally to the PMR database.
- Ensure that the PMR database connection setting configured in the BI console is using the DNS hostname or IP address for the PMR database server, and not localhost or 127.0.0.1. Otherwise, the external event collectors are not able to communicate with the PMR database.
- Stop the event collector service on the external event collector node to release the lock on the existing **EventCollector** folder.
- Run the **BeyondTrust EventCollector** MSI on each external event collector worker node. The event collector service starts automatically as part of the upgrade.
- Run the **BeyondInsight.EPM.EventCollector.Services** MSI on each event collector worker node.



Note: This must be installed in its default location for the PMR in BI integration to work.

- Configure an endpoint to point to an external event collector node and raise events. Confirm they can be seen in the PMR reports.

**IMPORTANT!**

*If using U-Series Appliance, before continuing on with configuration, disable RDP access again by going to **Maintenance > Network and RDP Settings** on the appliance and clicking the toggle to turn off the **Enable Remote Desktop** option.*



For more information on BI event collectors, configuring PMR in the BeyondInsight console, and configuring optional advanced options, see:

- ["Configure U-Series Appliance" on page 8](#)
- ["Configure Endpoint Privilege Management Reporting in BeyondInsight" on page 38](#)
- ["Configure Advanced SQL and Event Collector Settings for PMR in BI Integration" on page 42](#)

Configure Endpoint Privilege Management Reporting in BeyondInsight

Once the Endpoint Privilege Management Reporting components have been installed, a BeyondInsight administrator must configure the Endpoint Privilege Management Reporting database, assign permissions to users so they can access the reports, and configure the Endpoint Privilege Management Policy Editor to raise events in BeyondInsight, following the steps detailed in the sections below.

Configure Endpoint Privilege Management Reporting Database in BeyondInsight



IMPORTANT!

If you change your SQL Server port or Endpoint Privilege Management Reporting Database configuration, restart the Reporting Gateway service and Event Collector service to pick up the changes.

Named Instances

If using a named instance, the **SQL Connection Options** field must be used to provide a connection string to the PMR database. (Link to the SQL Connection Options section).

If the SQL Server named instance is listening on a dynamic port, use the instance name in the connection string without a port number because the allocated port number which SQL Server is listening on can change. The SQL Server Browser service must be running to locate the dynamic port.

Example connection string:

```
jdbc:jtds:sqlserver://SERVERNAME/BeyondTrustReporting;instance=INSTANCENAME
```

If the SQL Server named instance is listening on a static port, either the instance name can be used (with the SQL Server Browser Service running), or the port number can be supplied directly in the connection string.

Example:

```
jdbc:jtds:sqlserver://SERVERNAME:STATICPORTNUMBER/BeyondTrustReporting
```



Note: If using an external BI Event Collector it is recommended to use the Microsoft JDBC driver as specified in the "SQL Connection Options" section, using either the instance name or the port number.



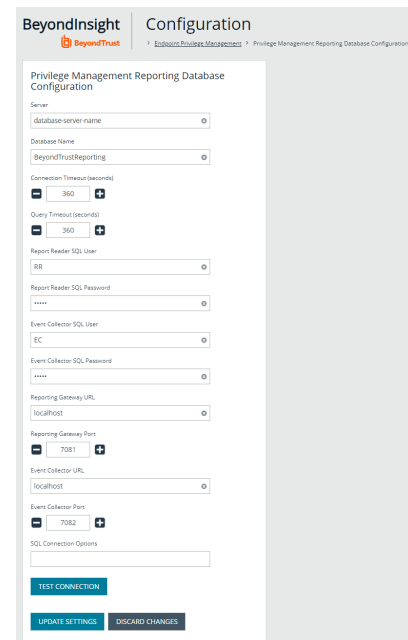
For more information about SQL Connection Options, see ["SQL Connection Options \(Including SSL Configuration\)" on page 42](#).

Follow these steps to configure the Endpoint Privilege Management Reporting database in BI:

1. Log in to the BI console and navigate to **Configuration > Endpoint Endpoint Privilege Management > Endpoint Privilege Management Reporting Database Configuration**.

2. Enter the database connection settings fields as follows:

- **Server:** Enter the hostname or IP address of the database server where the PMR database was installed.



Note: If using external event collector worker nodes, do not enter **localhost** even if the PMR database is hosted on the same server as the BI management server. PMR events will not flow through these nodes to the PMR database unless the DNS hostname or IP address is used here.

- **Database Name:** Enter the name of the PMR database specified when you ran the PMR database installer.
- **Report Reader SQL User:** Enter the username of the report reader user specified when you ran the PMR database installer.
- **Report Reader SQL Password:** Enter the password of the report reader user specified when you ran the PMR database installer.
- **Event Collector SQL User:** Enter the username of the event collector user specified when you ran the PMR database installer.
- **Event Collector SQL Password:** Enter the password of the event collector user specified when you ran the PMR database installer.
- **Reporting Gateway URL:** Enter the server name where the reporting gateway service and PMR UI were installed.

This can be set to **localhost** or **127.0.0.1**. In some instances localhost certificates can be impacted by proxies, in which case use 127.0.0.1.

- **Reporting Gateway Port:** Enter the port number on which the reporting gateway service runs PMR UI. This can be left as the default in most cases.
- **Event Collector URL:** Enter the server name where the event collector service and event collector were installed.

This can be set to **localhost** or **127.0.0.1**. In some instances localhost certificates can be impacted by proxies, in which case use 127.0.0.1.

- **Event Collector Port:** Enter the port number on which the event collector service runs event collector. This can be left as the default in most cases.
- **SQL Connection Options:** This is an advanced setting that allows custom parameters to be appended to the SQL connection string to the PMR database, or changing the default driver used for connectivity to the PMR database.

3. Click **Test Connection** to test the connection to the PMR database.

4. Click **Update Settings**.

5. Restart the following services:

- BeyondTrust EPM Event Collector Service
- BeyondTrust EPM Reporting Gateway Service
- BeyondTrust EPM Web Policy Editor Service

6. From the left navigation in the BI console, verify that **Reports** is now listed under **Endpoint Endpoint Privilege Management**.

 For more information on SQL connection options, see ["Configure Advanced SQL and Event Collector Settings for PMR in BI Integration" on page 42.](#)

Assign Permissions to Users to Access Reports in BeyondInsight

To view Endpoint Privilege Management Reporting in BI, the user must belong to a user group that has (at a minimum) the following permissions set:


- Management Console Access (Read Only permission)
- Endpoint Privilege Management - Reporting (Read Only permission)

To use the **Add to Policy** functionality in PMR, the user must belong to a user group that has (at a minimum) the following permissions set:

- Endpoint Privilege Management (Read Only permission)
- Endpoint Privilege Management - Policy Editor (Full Control permission)



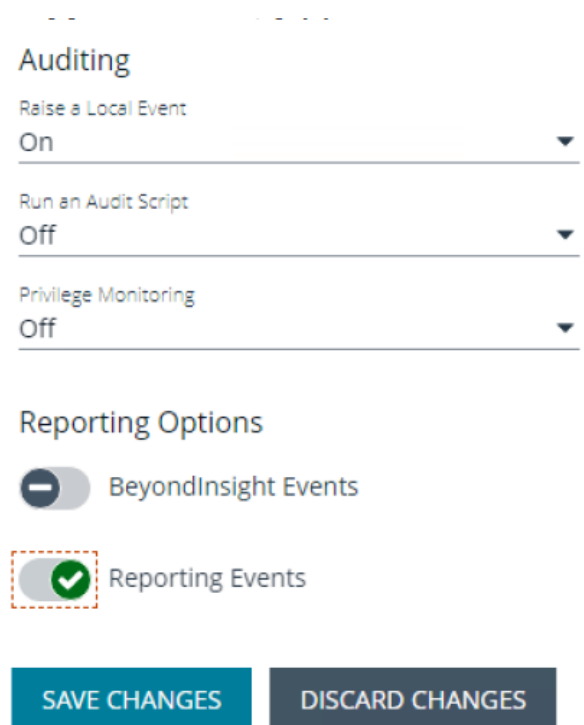
Note: If the user only has Read Only permissions, the **Add to Policy** button does not display in BI.


 For more information on how to set up users, groups, and assign feature permissions in BeyondInsight, see "Role-Based Access" in the [BeyondInsight User Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm>.

Configure Endpoint Privilege Management Policy Editor to Raise Events in BI


1. From the left navigation in the BI console, under **Endpoint Privilege Management**, click **Policies**.
2. Create a new policy or edit an existing policy:
 - To create a new policy:
 - Click **Create Policy** above the grid.
 - Enter a name for the policy and select the appropriate workgroup from the dropdown.
 - Click **Create Policy**.
 - Select a template and continue to step 3.
 - To edit an existing policy:
 - Click the vertical ellipsis for the policy.
 - Select **Edit & Lock Policy** and continue to step 3.
3. Create a workstyle or edit an existing workstyle:
 - To create a new workstyle:
 - Click **Create New Workstyle** above the grid.
 - Enter a name and description for the workstyle.

- Click the toggle to enable the workstyle.
 - Click **Create Workstyle**.
 - From the left navigation, expand **Workstyles**.
 - Expand the newly created workstyle.
 - Click **Application Rules** and continue to step 4.
 - To edit an existing workstyle:
 - From the left navigation, expand **Workstyles**.
 - Expand the desired workstyle.
 - Click **Application Rules** and continue to step 4.
4. Create or edit an application rule, and at the bottom of the **Application Rule** panel, set the following:
- Under **Auditing**, set **Raise a Local Event** to **On**.
 - Under **Reporting Options**, toggle the options to enable them. The options are:
 - **BeyondInsight Events**: Enable this option to configure endpoint clients to raise events which can be viewed from the Endpoint Endpoint Privilege Management Events grid in BI and in reports in BeyondInsight Analytics & Reporting in the **Endpoint Endpoint Privilege Management** folder.
 - **Reporting Events**: Enable this option to configure endpoint clients to raise events which can be viewed from the **Endpoint Endpoint Privilege Management Reporting** page in BI. To view these reports in BI:
 - From the left navigation, click **Menu**, and then click **Reports** under **Endpoint Endpoint Privilege Management**.



 **Note:** We recommend using the **Reporting Events** option, because PMR contains more detail in the events and provides advanced functionality such as **Add to Policy**. The **Add to Policy** feature provides a convenient way to add applications to Endpoint Endpoint Privilege Management policies. Enabling both reporting options results in a greater load on the server and additional resources may be required to handle the load.

 **Note:** You must enable reporting options for every application rule for which you want to raise events.

 For more information on how to install and configure the BeyondTrust Endpoint Privilege Management for Windows clients in your BeyondInsight instance, see ["Configure BeyondInsight and Endpoint Privilege Management" on page 11](#).

Configure Advanced SQL and Event Collector Settings for PMR in BI Integration

The below sections detail how to configure optional advanced SQL and event collector settings for your PMR in BI integration.

SQL Connection Options (Including SSL Configuration)

The **SQL Connection Options** field, available in the **Endpoint Privilege Management > Endpoint Privilege Management Reporting Database Configuration** form in BI, allows custom parameters to be appended to the SQL connection string. These can be used to configure functionality such as SSL encryption for the PMR database connection.

If the full connection string is provided in this field, these connection details are used instead of the **Server** and **Database Name** fields in the form.

By default the jTDS driver is used for connectivity to the PMR database. The jTDS connection string can be added to the SQL Connection Options field using the following format:

```
jdbc:jtds:<server_type>://<server>
[:<port>][/<database>]
[;<property>=<value>[;...]]
```

There are many optional parameters that can be appended to the jTDS connection string using the *property=value;* format. For example, to require that SSL is used for the connection using the jTDS driver, append the following to the jTDS connection string in the **SQL Connection Options** field:

```
ssl=require
```

For environments with external BI event collector worker nodes, if using SSL, we recommend using the Microsoft JDBC driver rather than the jTDS driver, because some issues have been found with the jTDS driver over external connections when using SSL.

To use the Microsoft driver, provide the connection string in the **SQL Connection Options** field in the following format:

```
jdbc:sqlserver://[serverName[\\instanceName][:portNumber]][;property=value[;property=value]
```



IMPORTANT!

*Do not include the user and password custom parameters in the SQL connection string, because these are populated from the **Report Reader SQL User** and **Report Reader SQL Password** fields.*



For more information, see the following:

- For more information on details of the optional parameters that can be added to the **SQL Connection Options** field, see [The jTDS Project Frequently Asked Questions](#).
- For more information on the connection string format and the optional parameters it supports for the JDBC driver, see



[Building the connection URL.](#)

- For more information on configuring SSL encryption for the Microsoft JDBC driver, see [Connecting with encryption.](#)

SQL Always On Availability Group Support

The PMR database supports running within a SQL Always On availability group. This prevents the **CopyFromStaging** scheduled job from running on the secondary replica in the availability group, so that it only ever runs on the primary replica.

- You must use the Microsoft JDBC driver for the SQL connection. The default jTDS driver does not work with SQL Always On.
- The SQL recovery model for the database must be set to **Full**.



IMPORTANT!

*When using the full recovery model, ensure that best practice is followed to back up the PMR database transaction log. Frequently running **CopyFromStaging** causes the transaction log to quickly use up disk space.*

- Install the PMR database on the primary replica server, and then add the database to the availability group. The database is then replicated to the secondary replica.
- Use the SQL Agent job (**PGInsertData**) to run the **CopyFromStaging** stored procedure, not the Service Broker job. The Service Broker can be unreliable restarting after failover. The Service Broker is currently the default job when installing the PMR database.
- Users are only created on the primary replica. You must create users on the secondary replica and synchronize the SIDs between the replicas. In a failover scenario, PMR loses the connection to the database if the accounts are not created on the secondary replica.

Follow the steps below to switch to using the SQL Agent job to run **CopyFromStaging**.

CopyFromStaging SQL Server Agent Configuration

To switch to the SQL Server Agent job after installing the PMR database, take the following steps:

1. Execute the **Create_ER_Database_Agent.sql** script against the PMR database on the primary replica. This removes the Service Broker queue and creates the SQL Server Agent job on the primary node.
2. Configure read-only access to the secondary replica of the Always On availability group by setting **Readable secondary** to **Yes**. This is required for the next step.
3. Execute the **Create_ER_Database_Agent.sql** script against the PMR database on the secondary replica.



Note: *Provided the script has been run on the primary replica first, it does not attempt to make any changes to the database on the secondary replica, as the removal of the Service Broker queue has already been replicated across from the primary to the secondary. Running this script only creates the SQL Server Agent job on the secondary replica. This job runs on the secondary but does not execute the **CopyFromStaging** stored procedure unless failover occurs, and this becomes the primary replica.*

4. Remove the read-only access to the secondary replica (set **Readable secondary** to **No**).
5. In the **Endpoint Privilege Management Reporting Database Configuration** form in BI, set the **Server** field to point to the PMR database in the Always On availability group, using the availability group listener address instead of the primary replica server address. The listener forwards any calls to the primary replica.



For more information on configuring read-only access to the secondary replica of the Always On availability group, see [Configure read-only access to a secondary replica of an Always On availability group](#).

Install and Configure External Event Collector Worker Nodes

1. Ensure the BI event collector worker node is installed and configured.
2. Ensure all steps detailed in the above sections for installing and configuring PMR in BI have been followed.
3. Verify that PMR is displaying reports in BI and that it is receiving events from an endpoint that is configured to point to the BI event collector on the BI management server. This is to verify that the end-to-end process is working and that events can flow from the endpoint to the BI event collector on the BI management server, then to the PMR event collector, and finally to the PMR database.
4. Ensure the PMR database connection setting configured in the BI console is using the DNS hostname or IP address for the PMR database server, and not localhost or 127.0.0.1. Otherwise, the external event collectors are not able to communicate with the PMR database.
5. Run the **BeyondInsight.EPM.EventCollector.Services** MSI on each event collector worker node.



Note: This must be installed in its default location for the PMR in BI integration to work.

6. Run the **BeyondTrust EventCollector** MSI on each external event collector worker node. The event collector service starts automatically as part of the upgrade.
7. Configure an endpoint to point to an external event collector node and raise events. Confirm they can be seen in the PMR reports.



For more information on BI Event Collectors, see ["Configure U-Series Appliance" on page 8](#).

Troubleshoot

A diagnostics tool, **EndpointUtility.exe**, is available with Endpoint Privilege Management for Windows installed files. Using the tool, you can:

- Diagnose the cause of connection problems. The tool offers actions to remedy the issue.
- Request an immediate policy update from BeyondInsight.

The tool does not require any elevated rights to run; any authenticated user on the system can use the tool.

Use the EndpointUtility.exe Tool

Arguments

Management platform argument:

/bi: BeyondInsight

Task arguments:

/c: Test connection

/p: Force policy

Test Connection

Run the following commands to send a test message to the BeyondInsight instance. The test results are displayed in the console window.

The registry settings used to connect to BeyondInsight are displayed first, followed by the result of the test message.

If Endpoint Privilege Management for Windows is installed in the default location, run the following from the command line:

```
"C:\Program Files\Avecto\Privilege Guard Client\EndpointUtility.exe" /bi /c
```

PowerShell:

```
& "C:\Program Files\Avecto\Privilege Guard Client\EndpointUtility.exe" /bi /c
```

Possible Test Connection Results

Result	Remedy
Connection Successful	NA
Defendpoint BeyondInsight Adapter cannot be contacted.	Reinstall BeyondTrust Endpoint Privilege Management with BIMODE=1 and correct parameters for; BEYONDINSIGHTURL (and optionally BEYONDINSIGHTCERTNAME and BEYONDINSIGHTWORKGROUP).

Result	Remedy
BeyondInsight Client Certificate Name could not be found.	Check the value of BEYONDINSIGHTCERTNAME in the registry and verify that the certificate is installed in and accessible from the correct certificate store
BeyondInsight Connection refused.	Check the value of BEYONDINSIGHTURL in the registry and that you have installed the correct BeyondInsight client certificate.
BeyondInsight URL not specified	Provide a value for BEYONDINSIGHTURL in the registry
BeyondInsight could not be contacted	Check the value of BEYONDINSIGHTURL in the registry, and network and firewall settings

Force Policy

Run the following commands to force a policy update on endpoints from BeyondInsight.

If Endpoint Privilege Management for Windows is installed in the default location, run the following command from the Windows command prompt:

```
"C:\Program Files\Avecto\Privilege Guard Client\EndpointUtility.exe" /bi /p
```

PowerShell:

```
& "C:\Program Files\Avecto\Privilege Guard Client\EndpointUtility.exe" /bi /p
```

Force Update Policy for End Users

End users can check and force a policy update to their computer from the system tray. Using this option reduces the time it takes to update a policy.

1. In the system tray, click the Endpoint Privilege Management icon.
2. Click **Check for Policy Update**.

One of the following notifications can appear:

- **Update Finished** to notify the user that a policy update has been applied.
- **No Updates Found** if the current policy is already up to date.
- **Unable to Check for Updates** if the computer cannot reach the management platform.

Use the Capture Config Utility

In Endpoint Privilege Management for Windows 22.3, we added the ability to run the BeyondTrust Capture Config Utility from the command line, both *locally* and *remotely*. It is initiated through **EndpointUtility.exe** (formerly **diagnosticsCli.exe**).

 **Note:** If you are running a version of Endpoint Privilege Management for Windows earlier than 22.3, follow the steps described in KB0017213, at https://beyondtrustcorp.service-now.com/kb?id=kb_article_view&sysparm_article=KB0017213&sys_kb_id=515853271b73c95c34216570604bcbaf&spa=1.

Initiate the Capture Config Utility from the Command Line

If you are running this on a *remote* machine, proceed to ["Run Remotely and Silently Using PowerShell" on page 47](#).

To initiate the utility:

1. Open PowerShell as **admin**.
2. Change directory (**cd**) to the Endpoint Privilege Management for Windows install location. By default, this is **C:\Program Files\Avecto\Privilege Guard Client** (include the 's' in your command, as below).

```
cd 'C:\Program Files\Avecto\Privilege Guard Client'
```

3. (Optional). Use the command below to create a new folder, or proceed to step 4 if you already have a folder created on the machine. Replace *<Chosen Path>* with the path you want the new folder to reside in, and replace *<Chosen Name>* with the preferred name for the folder. For example, the case reference number.

```
$output = New-Item -Path <Chosen Path> -Name <Chosen Name> -ItemType directory
```

4. Run the capture config script with the command below. Replace *<Desired .zip name>* with the preferred name for the logs, which will be exported to a ZIP file.

If you opted to use a preexisting folder (or did not use the *\$output* variable in the previous command), remove *\$output* and type the path to the existing folder, and the desired name of the log file which will be exported to a new ZIP file with that name. See the examples below.

```
.\EndpointUtility.exe /cc $output <Desired .zip name>
```

OR

```
.\EndpointUtility.exe /cc <Path to folder> <Desired .zip name>
```

Replace *<path to folder>* with the path to the existing folder, and then replace *<Desired .zip name>* with the preferred name for the log export.

5. A ZIP file will be output to the chosen location, with your specified reference or filename.

Run Remotely and Silently Using PowerShell

To produce the Config Capture on a *remote* session, use the PSSession commands as below:

1. Launch PowerShell as **admin**.
2. Run the command below (replace *<machine name>* with the name of the remote machine).

```
Enter-PSSession -ComputerName <machine name>
```

3. **cd** to the Endpoint Privilege Management for Windows install location. By default, this is **C:\Program Files\Avecto\Privilege Guard Client** (include the 's' in your command).

```
cd 'C:\Program Files\Avecto\Privilege Guard Client\'
```

- (Optional). Use the command below to create a new folder on the remote machine, or proceed to step 5 if you already have a folder created on the remote machine. Replace *<Chosen Path>* with the path you would like the new folder to reside in, and then replace *<Chosen Name>* with the preferred name for the folder. For example, the case reference number.

```
$output = New-Item -Path <Chosen Path> -Name <Chosen Name> -ItemType directory
```

- Run the capture config script with the command below. Replace *<Desired .zip name>* with the preferred name for the logs, which will be exported to a ZIP file.

If you opted to use a preexisting folder (or did not use the *\$output* variable in the previous command), remove *\$output* and type the path to the existing folder, and the desired name of the log file which will be exported to a new ZIP file with that name. See the examples below.

```
.\EndpointUtility.exe /cc $output <Desired .zip name>
```

OR

Replace *<Path to folder>* with the path to the existing folder, and then replace *<Desired .zip name>* with the preferred name for the log export.

```
.\EndpointUtility.exe /cc <Path to folder> <Desired .zip name>
```



Note: The screen PowerShell command will remain with the cursor "-" for a few minutes while the command is in progress. This is normal; do not close the window.

You will then see a success message.

- Open File Explorer and navigate to the remote directory you chose in steps 3 and 4, and then copy the ZIP folder to your machine.



IMPORTANT!

If you run the command below without first copying the logs, you must re-do this process to collect the logs again.

- (Optional). To remove the logs from the remote machine once you have copied the ZIP file, run the command below.

```
Remove-Item -Path $output -Force -Recurse
```



For more information, see [KB0016797](https://beyondtrustcorp.service-now.com/now/nav/ui/classic/params/target/kb_view.do%3Fsys_kb_id%3D895f04631bac9d586fe95287624bcb3d) at https://beyondtrustcorp.service-now.com/now/nav/ui/classic/params/target/kb_view.do%3Fsys_kb_id%3D895f04631bac9d586fe95287624bcb3d.