



BeyondTrust

Endpoint Privilege Management for Mac BeyondInsight Integration Guide

Table of Contents

Integrate Endpoint Privilege Management for Mac and BeyondInsight	4
Overview	4
Architecture	5
Prerequisites	5
Integration Workflow	8
Configure U-Series Appliance	9
Primary/Secondary Deployment Model	9
Configure BeyondInsight and Endpoint Privilege Management	11
Generate Client Certificate ZIP	11
Install the Endpoint Privilege Management for Mac Client	12
Verify Security Settings	13
Set Allow on com.beyondtrust.endpointsecurity.systemextension	13
Verify Privacy Settings	13
Verify Finder Extensions is Enabled	13
Install the BeyondInsight Adapter	14
Confirm the Endpoint is Connected	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 Endpoint Privilege Management WPE and the BeyondInsight WPE Plugin ..	19
Upgrade the Endpoint Endpoint Privilege Management WPE	21
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	27

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 the 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
Password Safe Integration	45
Prerequisites	45
Configure the BeyondInsight Adapter Settings	45
Configure Password Safe	45
Configure Off-Network Account Management	46
Supported Scenarios	46
Requirements	46
Download a Client Certificate	47
Create a Policy	47
Install Steps for macOS Endpoints	48
Onboard the Managed System in Password Safe	49
Set up Endpoint Privilege Management for Mac and Password Safe Cloud	50
Set up a New Password Safe Cloud Integration	50
Upgrade to Password Safe Cloud	52
Troubleshoot	53
Use the Diagnostics Tool	53

Integrate Endpoint Privilege Management for Mac and BeyondInsight

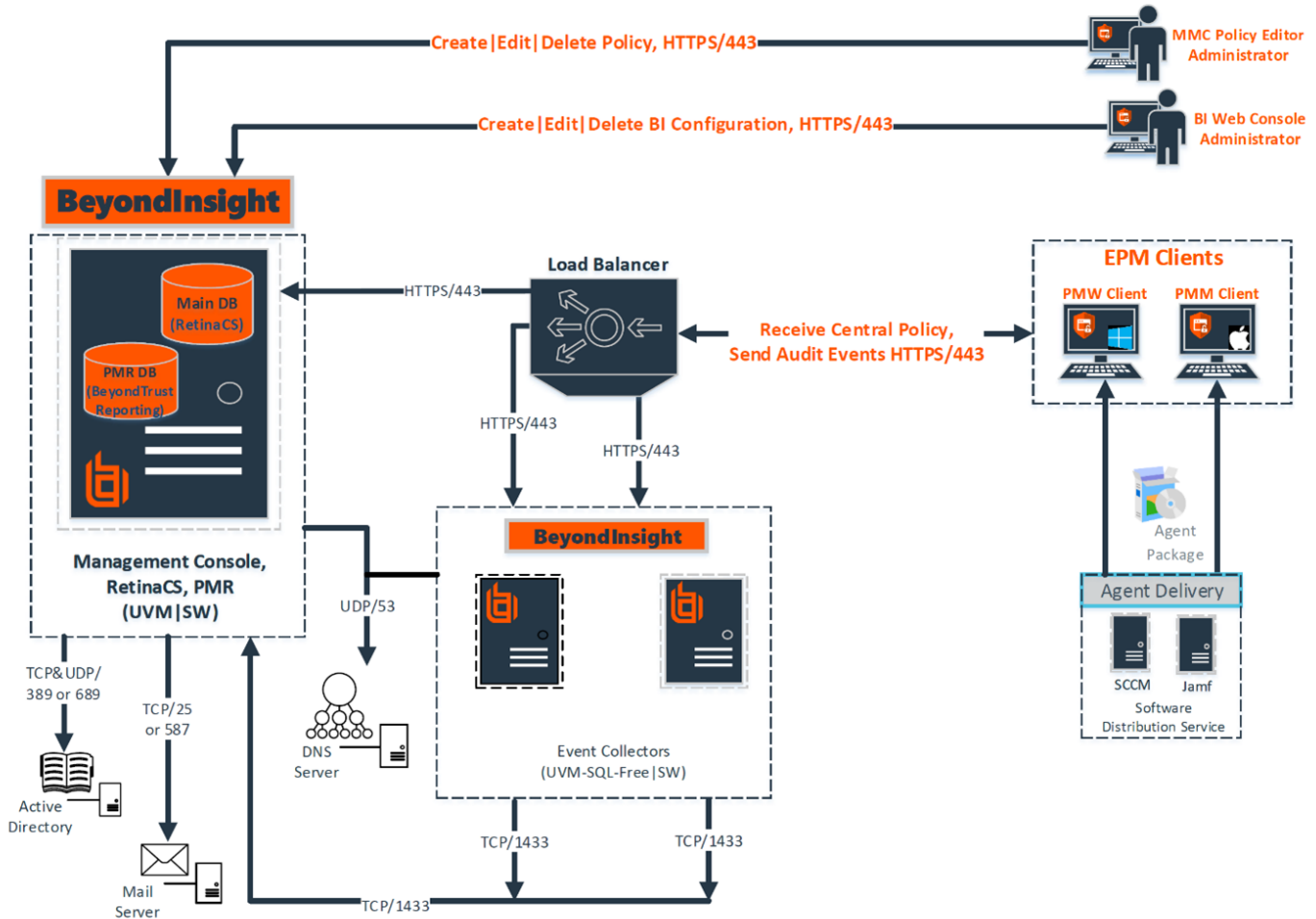
Overview

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 Mac 5.4.51.0 or later

Verify all BeyondInsight and Endpoint Privilege Management components are properly installed in your environment.



For more installation information, see:

- *BeyondInsight installation: [BeyondInsight Installation Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm>.*

- *Endpoint Privilege Management for Mac: [Mac Administration Guide](https://www.beyondtrust.com/docs/privilege-management/mac/index.htm) at <https://www.beyondtrust.com/docs/privilege-management/mac/index.htm>.*

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>

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

- *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.

- *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 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 export the BeyondInsight client certificate.
2. Use the Rapid Deployment Tool to create a redistributable settings package (.pkg file) for all endpoints accessing the BeyondInsight instance.



Note: In the Rapid Deployment Tool, use the Jamf integration to automatically distribute the settings .pkg to your endpoints if you are using Jamf for MDM with a Samba File Distribution Share.

3. Using Mobile Device Management (MDM) or your method of choice, deploy:
 - The Endpoint Privilege Management for Mac client
 - The BeyondInsight adapter
 - The .pkg file created in the Rapid Deployment Tool if you did not use the Jamf integration (step 2).
4. Verify BeyondInsight is receiving heartbeats and information from Endpoint Privilege Management for Mac endpoints.
5. Configure the policy editor to communicate with BeyondInsight and test the connection.
6. Create a policy in the editor.
7. Create a Smart Rule in BeyondInsight.
8. 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](https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/index.htm) 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](#).

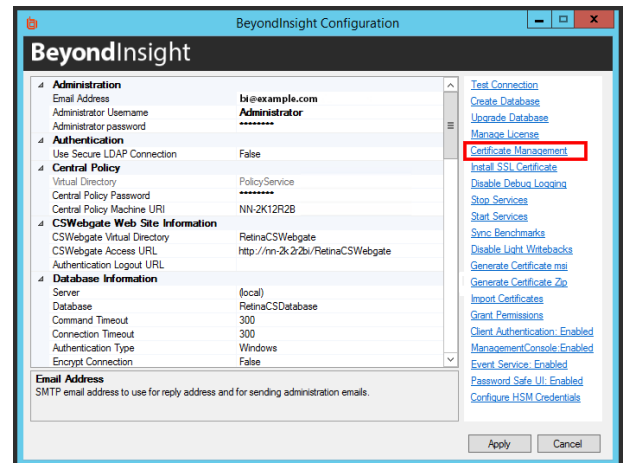
Configure BeyondInsight and Endpoint Privilege Management

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

- Generate a client certificate in BeyondInsight
- Install the certificate on every Endpoint Privilege Management for Mac client that needs to send information to BeyondInsight

Generate Client Certificate ZIP

1. On the BeyondInsight Server, go to **C:\Program Files (x86)\eEye Digital Security\Retina CS**.
2. Run **REMEMConfig.exe**, which opens the **BeyondInsight Configuration Tool**.
3. Click on the **Certificate Management** link.



4. In the **Certificate Management** dialog window, select **Export Certificate**.
5. Select **Client Certificate** as the **Certificate type**.
6. Enter a password. We recommend using the existing BeyondInsight Central Policy password.
7. Enter a file name and select **Certificate files (*.pfx)** as the file type. We recommend using the name **eEyeEmsClient.pfx**. Click **Save**.
8. Click **OK**. Click **OK** again.



Deploy the BeyondInsight Client Certificate



For more information, see the *Rapid Deployment Tool Guide* at <https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-mac-rapid-deployment-tool>.

Install the Endpoint Privilege Management for Mac Client

The client and the adapter are obtained from BeyondTrust after purchasing Endpoint Privilege Management with BeyondInsight, and may be distributed to the endpoints using the method of your choice, including Mobile Device Management (MDM), such as Jamf or AirWatch.

You can create a settings package to set the adapter's configuration on all endpoints by using the Endpoint Privilege Management for Mac Rapid Deployment Tool.



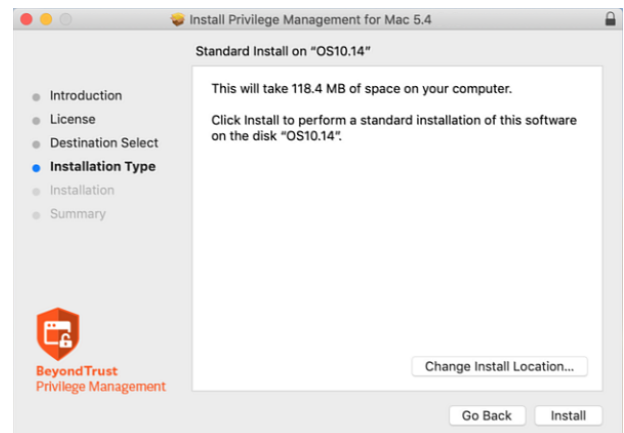
For more information, see the [Rapid Deployment Tool Guide](https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-mac-rapid-deployment-tool) at <https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-mac-rapid-deployment-tool>.

The filenames are as follows, where **x.x.x.x** represents the version:

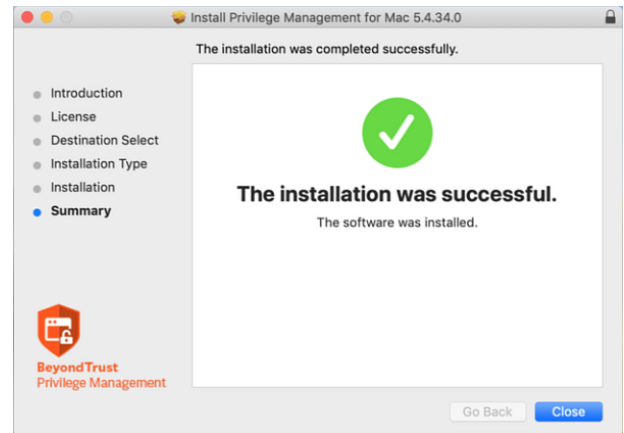
- **PrivilegeManagementForMac_x.x.x.x.pkg**
- **BIAdapter_x.x.x.x.pkg**

To install the Endpoint Privilege Management for Mac client:

1. Double-click the **PrivilegeManagementForMac_x.x.x.x.pkg** file.
2. Click **Continue** on the **Introduction** page.
3. On the **Software License Agreement** page, click **Continue** and then click **Agree** to agree to the terms and conditions.
4. (Optional) To change the installation destination, click the **Change Install Location** button. The **Destination Select** page will allow you to choose from viable installation location options. Click **Continue**.
5. Click the **Install** button on the **Installation Type** page. If prompted, enter your admin credentials to continue. Click **OK** if the **Installer.app** needs permission to modify passwords, networking, or system settings.



- The **Summary** page shows that the installation was successful. Click **Close** to complete the installation.



Verify Security Settings

Go through the following sections to ensure Endpoint Privilege Management for Mac files have correct access.

Set Allow on `com.beyondtrust.endpointsecurity.systemextension`

After the agent and adapter are installed, ensure the security on the Endpoint Privilege Management system extension is set to **Allow**.

For `com.beyondtrust.endpointsecurity.systemextension`, go to **System Preferences > Security & Privacy > General**, and then select **Allow**.

Verify Privacy Settings

The following Endpoint Privilege Management for Mac files require the privacy settings **Full Disc Access** and **Files and Folders**:

- `com.beyondtrust.interrogator`
- `PrivilegeManagement`
- `defendpointd`
- `com.beyondtrust.endpointsecurity.systemextension`

To confirm the settings:

- Go to **System Preferences > Security & Privacy > Privacy**, and then select **Full Disk Access**. Ensure the Endpoint Privilege Management files are listed.
- Select **Files and Folders** and confirm the Endpoint Privilege Management files are listed.

Verify Finder Extensions is Enabled

One way to confirm Finder Extensions is on, go to the **Applications** folder and verify the Endpoint Privilege Management shield icon is next to the applications.

Install the BeyondInsight Adapter

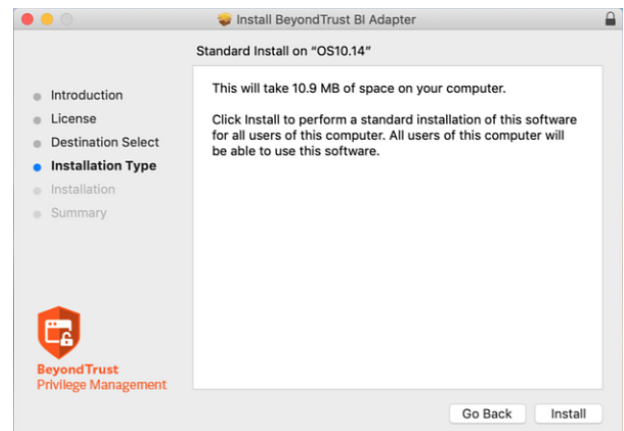
The best practice to deploy the BeyondInsight adapter is to use the Endpoint Privilege Management for Mac Rapid Deployment Tool.

However, you can choose the deployment method. Examples include: Mobile Device Management methods (such as Jamf or AirWatch), manual configuration, download from a shared resource, etc.

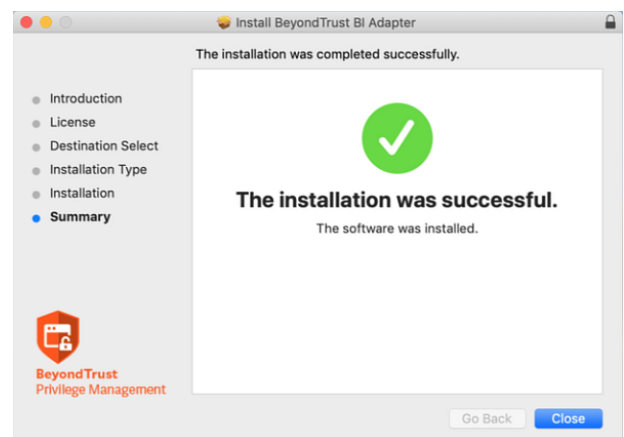


For more information, see the [Rapid Deployment Tool Guide](https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-mac-rapid-deployment-tool) at <https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-mac-rapid-deployment-tool>.

1. Double-click the **BIAdapter_x.x.x.x.pkg** file.
2. Click **Continue** on the **Introduction** page.
3. On the **Software License Agreement** page, click **Continue** and then click **Agree** to agree to the terms and conditions.
4. Click the **Install** button on the **Installation Type** page. If prompted, enter your admin credentials to continue. Click **OK** if **Installer.app** needs permission to modify passwords, networking, or system settings.



5. The **Summary** page shows that the installation was successful. Click **Close**.



Confirm the Endpoint is Connected

The Endpoint Privilege Management endpoint can check in and send events to BeyondInsight after the settings file is configured.

If you can access the machine running the BeyondInsight server, use one of the following methods to confirm the endpoint has checked in:

1. Go to **Assets > Endpoint Privilege Management** to see if the endpoint is displayed.



Note: Configure the **Activity Monitor** to show all processes, as **BIAdapter** runs as user **_defendpoint**.

2. Run the following SQL query:

```
select * from Asset_PBDInfo
select * from Asset_PBDInfoEx
```



Tip: To force a policy update for a client getting an update for the first time, you can restart the BeyondInsight Adapter. In the **Activity Monitor**, restart the **BIAdapter** process.

The default time for the policy update and for the heartbeat is six hours. These values can be changed on the BeyondInsight server, and the policy can be applied to the endpoint, but this policy is not applied until the initial 6 hour period has elapsed. Manually changing the **RCSHeartbeatInterval** and **RCSPolicyValidationInterval** values will also cause the endpoint to check in more often. Enter the values in minutes.

```
<?xml version="1.0"?>
- <Settings>
  <InstallIdentifier>12B2D6CA-208D-4777-95A9-C4AE1C38E9E4</InstallIdentifier>
  <UniqueID>1B7F5614-208D-4C73-87FA-2FAA2D332888</UniqueID>
  <Version>5.4.0</Version>
  <RCSServer/>
  <RCSCertName>eEyeEmsClient</RCSCertName>
  <RCSWorkgroupName>BeyondTrust Workgroup</RCSWorkgroupName>
  <HeartbeatReceived>0</HeartbeatReceived>
  <PolicyValidationReceived>0</PolicyValidationReceived>
  <RCSHeartbeatInterval>360</RCSHeartbeatInterval>
  <RCSPolicyValidationInterval>360</RCSPolicyValidationInterval>
  <RCSPolicyValidationIntervalVariance>30</RCSPolicyValidationIntervalVariance>
</Settings>
```

If you can access the endpoints, you can use either of the following methods to determine if they have checked in:

- Open **Console** and filter on **subsystem: com.beyondtrust.BIAdapter**. Ensure that **Info** and **Debug Messages** are on. Logs about the connection are displayed in real time. You can check when the next policy validation is scheduled and the next heartbeat request.
- Open **Activity Monitor**. The **BIAdapter** service is displayed as running.

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 Mac are successfully communicating, the Endpoint 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 Endpoint Privilege Management policies you uploaded from Endpoint Privilege Management for Mac 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 ⊟ Active

Description

Reprocessing limit
Default ⊟

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 Endpoint Privilege Management policies you uploaded from Endpoint Privilege Management for Mac 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 ⊟ ⊗

Re-run the query every X hours ⊟ ⊕

Discover users

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

Actions ⊟

Deploy Endpoint Privilege Management Policy ⊟ ⊗

SELECT POLICIES FOR DEPLOYMENT (1)

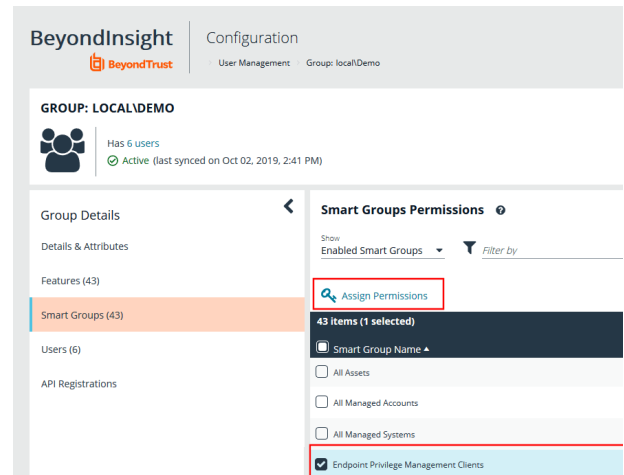
[Add another action](#)

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 Mac 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.

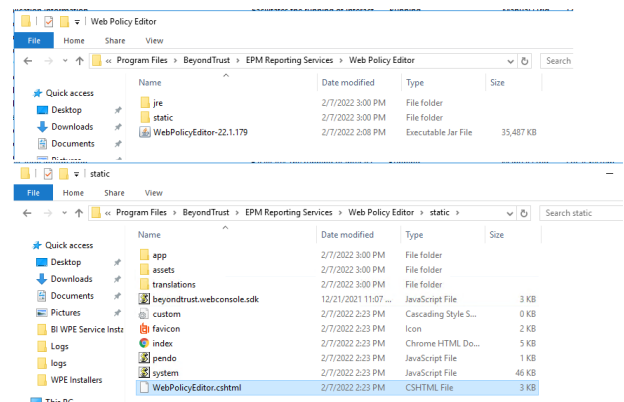
Install Endpoint Endpoint Privilege Management WPE and the BeyondInsight WPE Plugin

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 (**BeyondTrust WebPolicyEditor.Services-2x.x.xxx.msi**). Check the **Destination Folder** selected is correct.



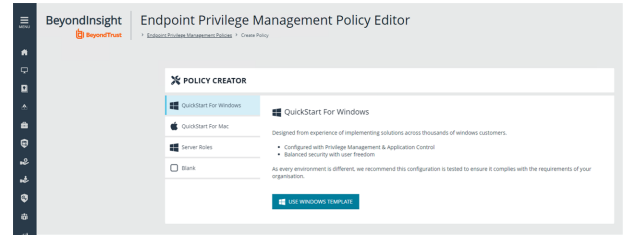
Note: The Web Policy Editor must be installed before the WPE service, as the service looks for the WPE files.

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.

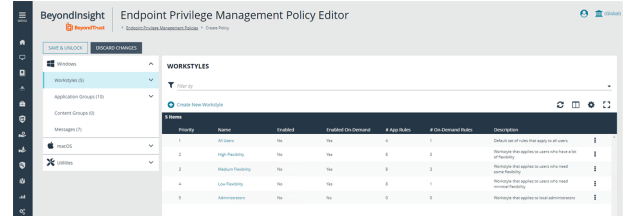


5. Verify the WPE works in BeyondInsight, as follows:
 - From the left menu in BeyondInsight, under **Endpoint Endpoint Privilege Management**, click **Policies**.
 - Click **Create Policy**.

- 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)\Eye Digital Security\Retina CS\WebConsole\Views\Apps**.
 - Uninstall and reinstall the **BeyondTrust EPM Web Policy Editor Service**.



For more information on working with the Web Policy Editor, see "Manage Endpoint Endpoint Privilege Management Policies" 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>.

Install Endpoint Privilege Management Reporting in BeyondInsight

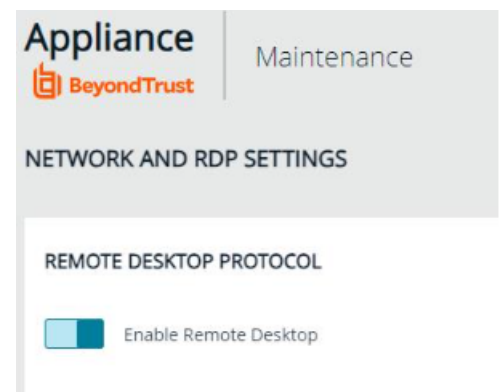
Endpoint Privilege Management Reporting (PMR) can be installed and configured to integrate with BeyondInsight (BI), allowing you to view PMR dashboards and reports using the BeyondInsight console. The below sections detail how to install the PMR database, UI, and event collector components in your BeyondInsight 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](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm) 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:

- BeyondInsight must be at minimum version of 23.1.
- 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.

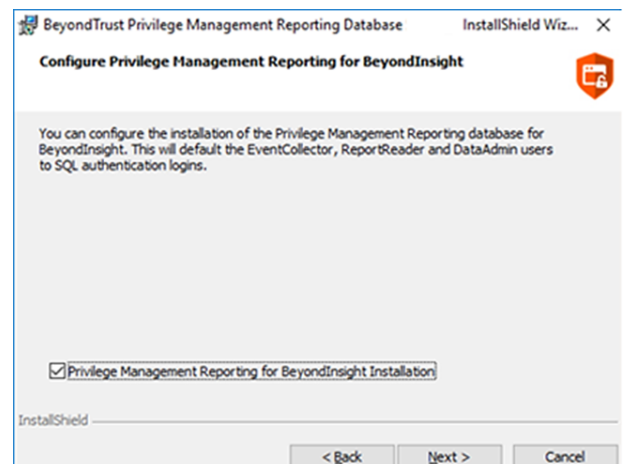
If you are hosting the PMR database on an external database server, you must install the **PrivilegeManagementReportingDatabase** twice - once on the external database server, and again on the BeyondInsight Management server. When you set the configuration for the database, you can specify the external 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**.

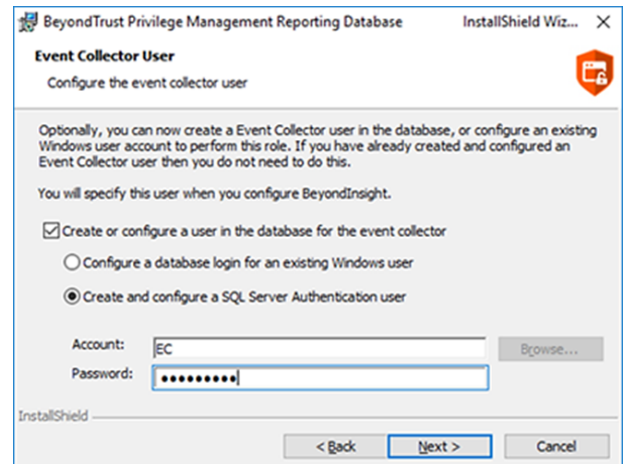
Check this box to use SQL Server authentication for the event collector, report reader, and data admin users configured in subsequent stages of the wizard.



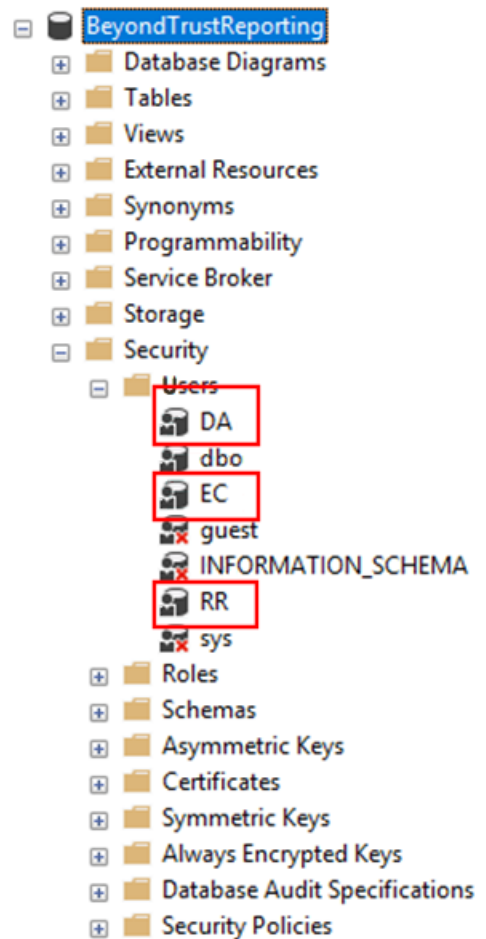
Note: Windows authentication to the PMR database is not supported.



- 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.

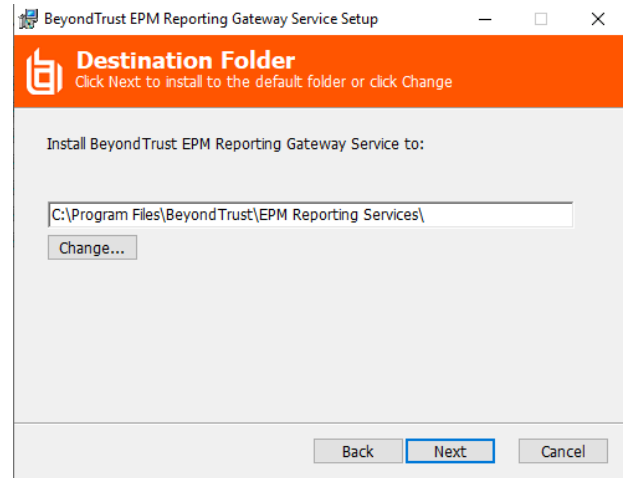


Tip: We recommend using the SQL Server Agent job to run the **CopyFromStaging** process rather than using the default Service Broker queue. To switch to using the SQL Server Agent job, execute the **Create_ER_Database_Agent.sql** script against the PMR database. This removes the Service Broker queue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

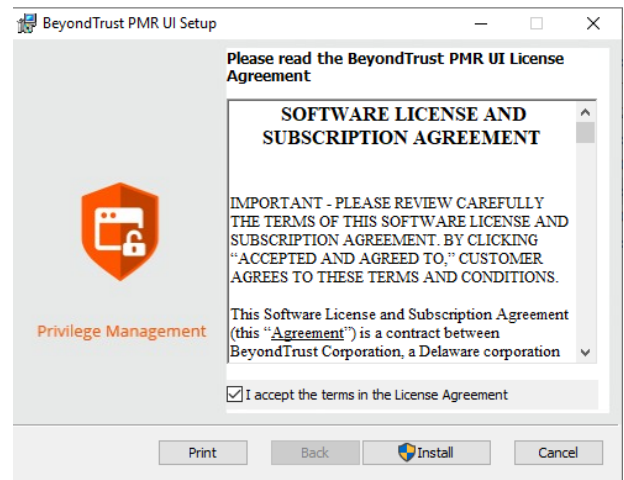
Install BeyondTrust Endpoint Privilege Management Reporting UI

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



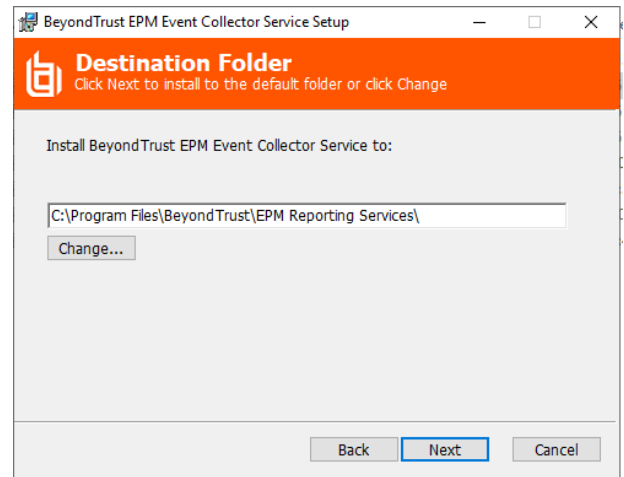
3. Run the **BeyondTrust PMR UI** MSI on the BI server. The reporting gateway service starts automatically as part of the installation.



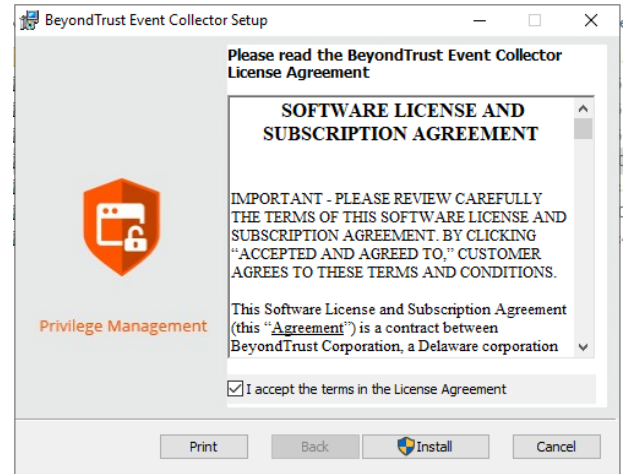
Install the BeyondTrust EPM Event Collector

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.

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 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](#)

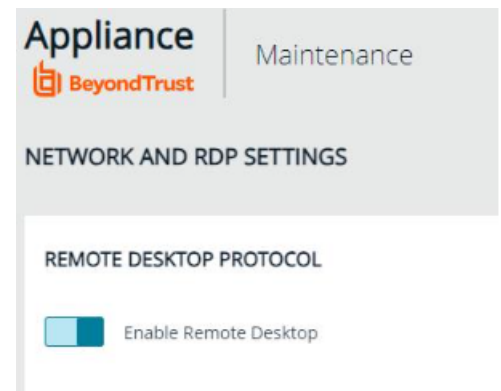
Upgrade Endpoint Privilege Management Reporting in BeyondInsight

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:

- BI must be at minimum version of 23.1.
- 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

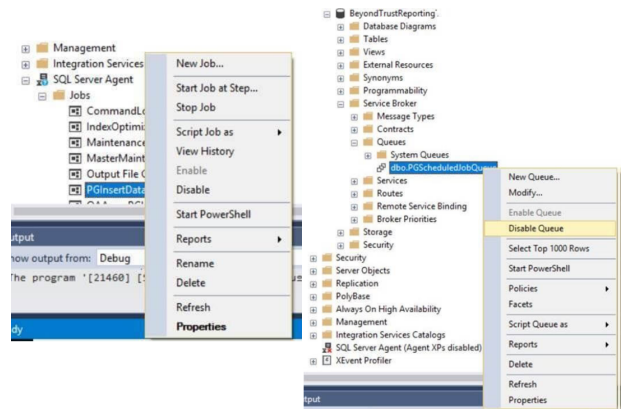
Not all upgrades of the PMR UI require an updated PMR database, as there might not be any database changes since the previous release of PMR UI in BI. Check the version of the installed BeyondTrust Endpoint Privilege Management Reporting database in **Windows**

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**.



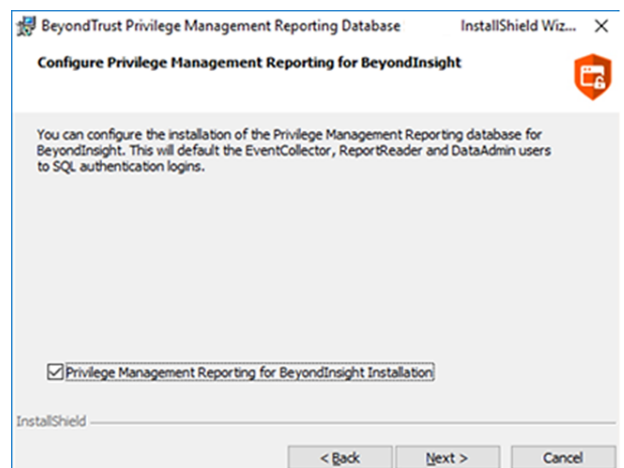
To upgrade the PMR database, follow these steps:

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**.

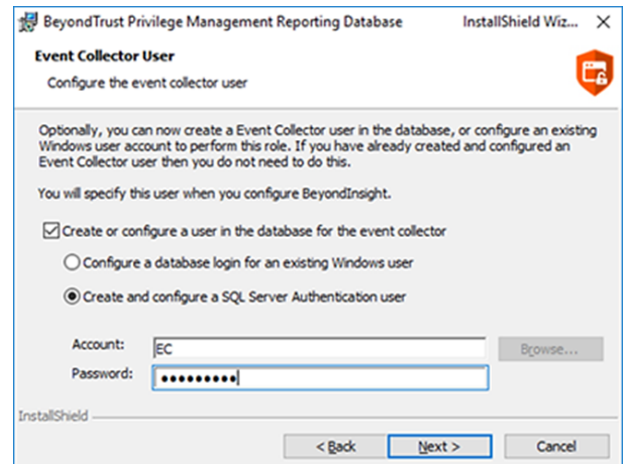
Check this box to use SQL Server authentication for the event collector, report reader, and data admin users configured in subsequent stages of the wizard.



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



- 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**.



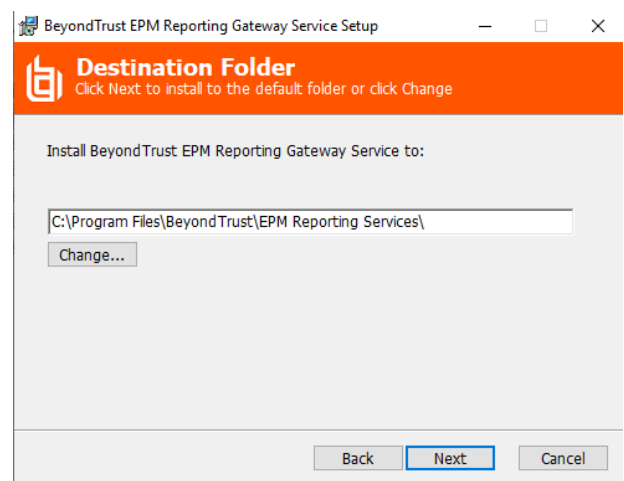
IMPORTANT!

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.

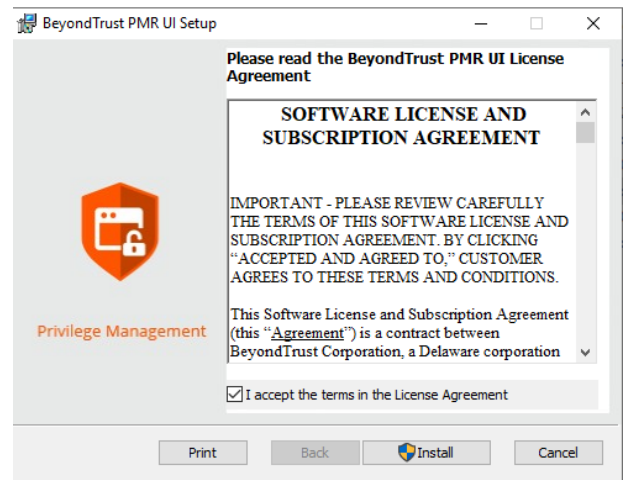


 **IMPORTANT!**

*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.

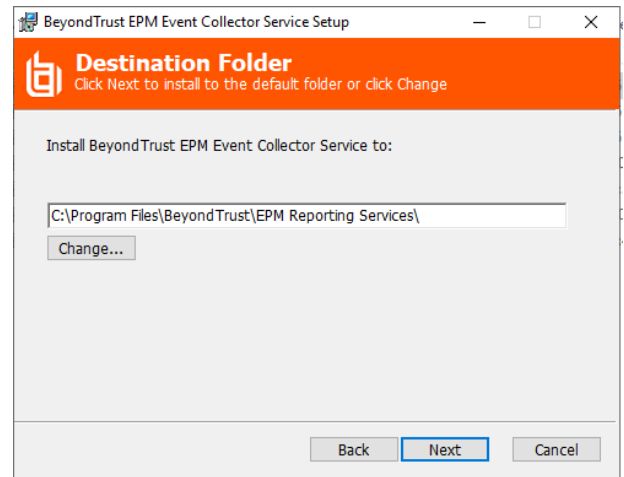


Upgrade the EPM Event Collector

Upgrade the Event Collector Services MSI

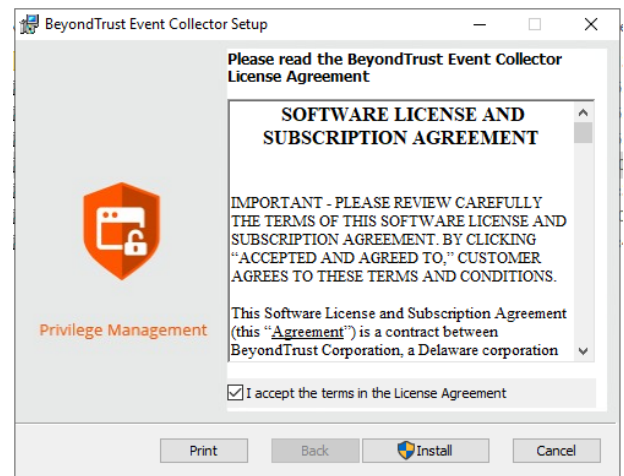
1. On the BI server, run the **BeyondInsight.EPM.EventCollector.Services** MSI file as administrator, either from the folder where it is stored or from a command prompt.

- 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

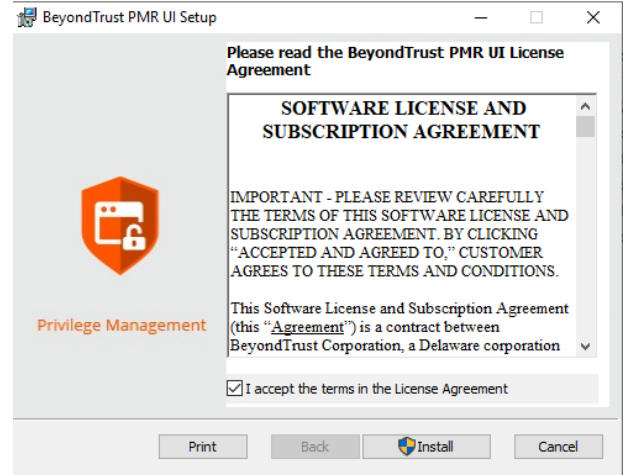
This section of the guide covers upgrades from an existing version of PMR UI to a later version of PMR UI.



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.

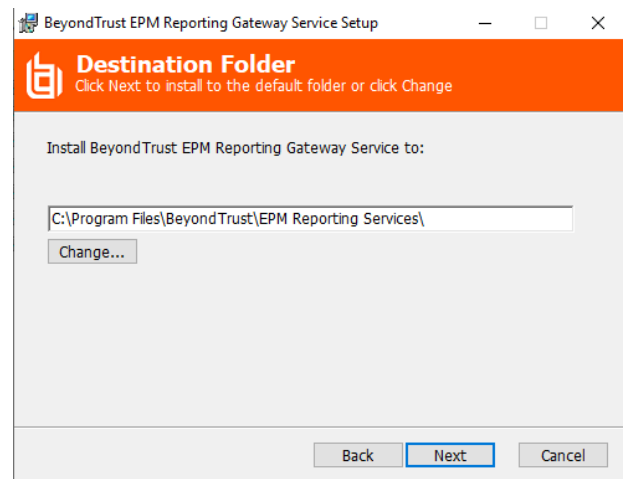


Upgrade Reporting Gateway Service



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

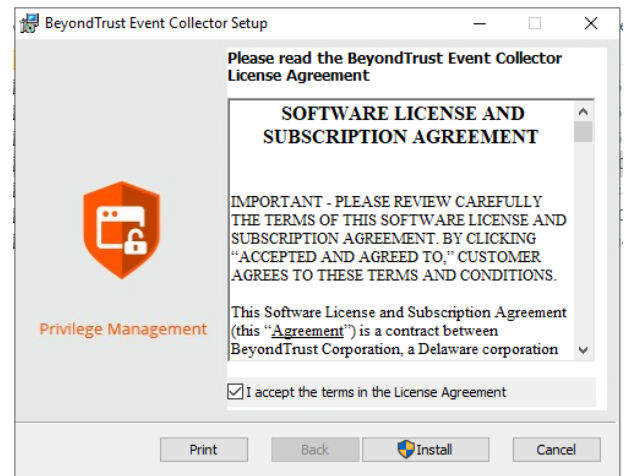
The event collector must be upgraded before the event collector services.

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.



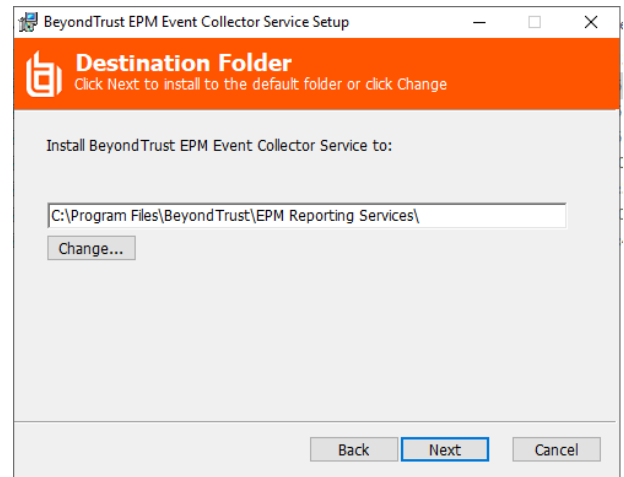
Upgrade the Event Collector Services MSI



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.

2. 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.

1. Ensure the BI event collector worker node is installed and configured.
2. Ensure all steps detailed in the sections above 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, then 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. Run the **BeyondTrust EventCollector** MSI on each external event collector worker node. The event collector service starts automatically as part of the upgrade.
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. 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 9](#)
- ["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.

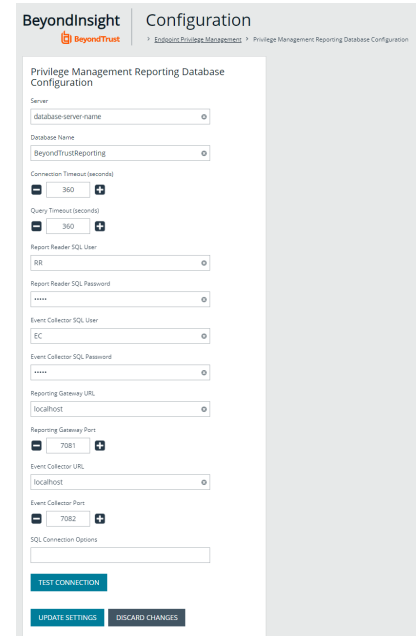



For more information, see "[SQL Connection Options \(Including SSL Configuration\)](#)" on page 42.

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)



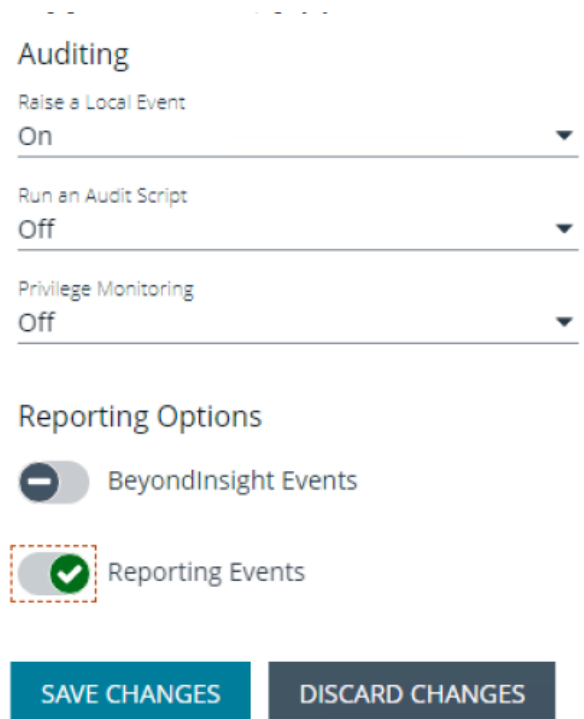
Note: If the user only has Read Only permissions, the **Add to Policy** button does not display in BI.

 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 the 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**.



Auditing

Raise a Local Event
On

Run an Audit Script
Off


Privilege Monitoring
Off

Reporting Options

BeyondInsight Events

Reporting Events

SAVE CHANGES **DISCARD CHANGES**

 **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 Endpoint Privilege Management for Mac 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.

i 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.

i For more information on BI Event Collectors, see ["Configure U-Series Appliance" on page 9](#).

Password Safe Integration

You can integrate Endpoint Privilege Management for Mac and Password Safe to rotate passwords on your macOS endpoints.

This section applies only to Password Safe on-premises.

Prerequisites

- BeyondInsight Adapter 21.2

Configure the BeyondInsight Adapter Settings

BeyondInsight Adapter installation instructions are provided earlier in the guide.

 For more information, see "[Install the BeyondInsight Adapter](#)" on page 14.

Configure the following settings in the **settings_app.xml**:

- **PasswordSafeState**: The state of the feature: **Enabled**, **Disabled**, and **Not_Configured** (case sensitive). The default is **Not_Configured**.
- **PasswordSafeHeartBeatInterval**: The time span, in minutes, the endpoint polls Password Safe checking for updated passwords. Valid values are 1 to <max unsigned 32 bit integer>. The default is 60 minutes.

You can change settings in two ways:


- Add the settings
- Send an Endpoint Privilege Management for Mac policy that contains Password Safe settings. When an asset has multiple policies, the first policy with valid settings is used. The policy's settings are written to **settings_app.xml**.

Example section of the Password Safe settings in Endpoint Privilege Management for Mac policy:

```
<Configuration>
  <!-- Omitted usual nodes -->
  <PasswordSafeLocalRotation>
    <State>Enabled</State>
    <PasswordHeartbeatInterval>60</PasswordHeartbeatInterval>
  </PasswordSafeLocalRotation>
</Configuration>
```

Configure Password Safe

The macOS endpoints must be added to Password Safe as assets.

 For more information, see [Add Assets to Password Safe in the Password Safe Administration Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/add-assets/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/add-assets/index.htm>.

Configure Off-Network Account Management

In a typical password rotation using Password Safe, the appliance or Resource Broker reaches out to the target system to trigger the password change using the functional account credentials. However, off-network clients that are not ever or not consistently accessible by a Password Safe appliance or Resource Broker cannot use this mechanism.

Using Password Safe integration settings in the Policy Editor, Endpoint Privilege Management clients can check in with Password Safe at a configured interval for password change commands, including password rotation.

The Endpoint Privilege Management client is the password agent. A functional account is not required, however a limitation in 22.1 requires a dummy functional account to be created and assigned if using a Smart Rule to onboard.

Supported Scenarios

- Password Safe Cloud/On-prem with EPM
- Password Safe Cloud/On-Prem with GPO/webserver
- Password Safe on the same server as BeyondInsight for Endpoint Privilege Management.

Requirements

- Password Safe: Endpoints require a Password Safe license.
- Endpoint Privilege Management client: Endpoint Privilege Management license not required for this use case.
- Endpoint Privilege Management policy: Required to deliver the integration settings.



IMPORTANT!

Install the Endpoint Privilege Management client on computers before you run a Password Safe discovery scan. If you run the scan first, then the computers are onboarded to Password Safe with Password Safe as the change agent with an asset ID. If you install the Endpoint Privilege Management client on the same computer later, the asset has a unique install ID. A duplicate record is created with the same asset name but different asset ID.

The following section provides information on how to set up the off-network scenario. The high-level steps are:

- Download a client certificate for authentication
- Install Endpoint Privilege Management client and adapter
- Create a policy in Endpoint Privilege Management
- Onboard the managed system in Password Safe
- Add accounts to Password Safe



For more information and detailed step-by-step instructions, see our [Knowledge Base](#) article.

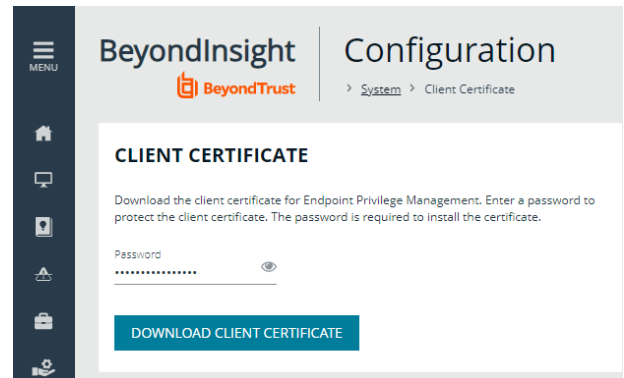
Download a Client Certificate

Communication between EPM and the BeyondInsight server are encrypted over port 443. The Endpoint Privilege Management computers need a client certificate to authenticate to BeyondInsight or Password Safe.

The certificate must be deployed to all EPM client machines and Policy Editor machines.

Download the client certificate to the Endpoint Privilege Management computer, from PS Cloud or BeyondInsight console: **Configuration > System > Client Certificate**.

- PS Cloud: The client certificate Issued to PS Cloud authentication.
- BeyondInsightU-Series Appliance: Default certificate is issued to eEyeEmsClient.



Use Wildcards to Match on Certificate Name

To improve the deployment with Password Safe, use wildcards in the *RCSCertName* (also known as the certificate name) in the **settings_app.xml** located here:

/Library/Application Support/BeyondTrust/PasswordSafe/

Use wildcards to provide a partial certificate name. For example, *Hostname.PS Cloud Authentication* can match **.PS Cloud Authentication*.

Wildcard examples that match on a certificate named *PS Cloud Authentication*:

- `<RCSCertName>*authentication</RCSCertName>` (Not case sensitive).
- `<RCSCertName>?S Cloud Authentication</RCSCertName>`
- `<RCSCertName>*Authenticatio?</RCSCertName>`

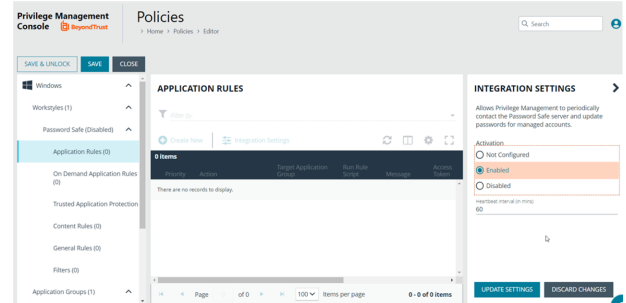
Create a Policy

You must configure integration settings in the Policy Editor.

Use the following procedure when EPM SaaS is managing the policy. If you are using the on-premises Policy Editor, see the [knowledge base](#) article for instructions.

1. Click the **Policies** menu, and then click **Create Policy**.
2. Select **Blank** on the **Policy Creator** page, and then click **Use Blank Template**.
3. Enter a name and description, and then click **Create Policy**.
4. Create a workstyle.
5. Expand the workstyle, and then click **Application Rules**.
6. Click **Integration Settings**.

7. Select **Enabled**.
8. Enter a heartbeat interval. The default value is 60 minutes. This is the time span the computer polls Password Safe unless the time is determined by Password Safe. The Endpoint Privilege Management computer checks in for missed jobs such as scheduled password rotations, forced resets, and password releases. Password rotations run at this time.



9. Click **Update Settings**.

Install Steps for macOS Endpoints

IMPORTANT!

When creating the adapter settings package in the Rapid Deployment Tool:

- Use the PS Cloud certificate when managing the macOS computer in PS Cloud.
- Use the appliance certificate when managing the macOS computer in the appliance.

To install packages for macOS integration:

1. Create settings package for EPM or BeyondInsight adapters using the Rapid Deployment Tool. Follow the steps in this guide: [Create Packages With the Rapid Deployment Tool](#)
2. Install Endpoint Privilege Management client and adapters. Install the packages in the following order:
 - EPM
 - a. **PMC Settings XX.pkg**
 - b. **PMC_Adapter_XX.pkg**
 - c. **BI Settings XX.pkg**
 - d. **BIAdapter_XX.pkg**
 - e. **Pwsclient_xx.pkg**
 - f. **PrivilegeManagementForMac.pkg**
 - BeyondInsight Appliance
 - a. **BI Settings XX.pkg**
 - b. **BIAdapter_XX.pkg**
 - c. **Pwsclient_xx.pkg**
 - d. **PrivilegeManagementForMac.pkg**

Onboard the Managed System in Password Safe

During the Endpoint Privilege Management client installation, the computer registers as an asset with the Endpoint Privilege Management solution flag set. Therefore, you can onboard the asset manually, using a Smart Rule, or the API.

The Endpoint Privilege Management client is the password agent. A functional account is not required, however a limitation in 22.1 (and earlier) requires a dummy functional account to be created and assigned if using a Smart Rule to onboard accounts.

Sample Smart Rule

Criteria

Currently the Endpoint Privilege Management identifier is hidden in PS Cloud. Other identifiers are needed to include all Endpoint Privilege Management computers in the criteria.

Action

Actions to set on the Smart Rule:

- Add to Password Safe
- Set password agent to Endpoint Privilege Management
- Select a functional account



Note: Currently a limitation prevents adding "none" for functional account even though it is not needed. Create a dummy functional account first.

Default values for the following account settings in Password Safe are applied in an Endpoint Privilege Management off-network integration and cannot be changed in this scenario:

- Change Services (Yes)
- Restart Services (No)
- Change Tasks (No)

Add the Account as a Managed Account

The Endpoint Privilege Management client only registers basic information and does not provide an account list and usually cannot be scanned due to the distributed nature. Therefore, an API script is likely required to onboard the local privileged accounts.



For more information, see *Add Assets to Password Safe in the Password Safe Administration Guide* at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/documents/ps/ps-admin.pdf>.

Set up Endpoint Privilege Management for Mac and Password Safe Cloud

Starting with the Endpoint Privilege Management for Mac 21.6 release, you can add macOS computers to Password Safe Cloud to rotate passwords on the endpoints.

This section applies to only Password Safe Cloud.

Packages in the 21.6 Release

- **BIAdapter_x.x.x.x.pkg**
- **pwsclient_x.x.x.x.pkg**: A standalone Password Safe client installer. In earlier versions, Password Safe was bundled with the BIAdapter package.
- **PrivilegeManagementForMac_x.x.x.x.pkg**

Set up a New Password Safe Cloud Integration

For new installations, the workflow is:

- Install the Endpoint Privilege Management for Mac client.
- Install the standalone Password Safe client.
- Set advanced settings for Password Safe.
- Add the computer to Password Safe as a managed asset.

Install the Endpoint Privilege Management for Mac Client

Installation instructions for the Endpoint Privilege Management for Mac are provided earlier in this guide.

i For more information, see "[Install the Endpoint Privilege Management for Mac Client](#)" on page 12.

Install the Standalone Password Safe Client

When the new Password Safe client is installed, existing BeyondInsight settings are copied to a new location (from **/Library/Application Support/BeyondTrust/Defendpoint/** to **/Library/Application Support/BeyondTrust/PasswordSafe/**) so that on-premises Password Safe installations continue to work as expected.

1. Start up the installer and go through the wizard.
2. Click **Continue** on the **Introduction** page.
3. Read through the license agreement.
4. Select the installation location.
5. Set the installation type.
6. The **Summary** page indicates the installation was successful.

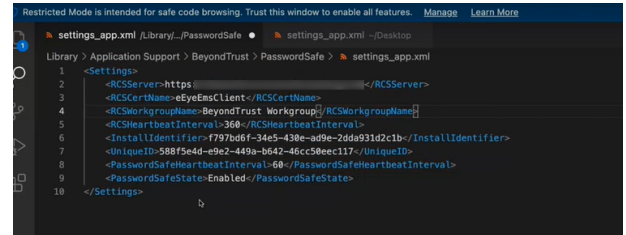
Set Advanced Settings

After the Password Safe client is successfully installed, you must manually update the **settings_app.xml** file located in the **/Library/Application Support/BeyondTrust/PasswordSafe/** directory.

In a future Rapid Deployment Tool release, support for creating an installable package with Password Safe settings will be available.

Add the following settings:

- **RCSSTServer:** The URL to the BeyondInsight server.
- **RCSSTCertificate:** The name of the BeyondInsight client certificate used to communicate with BeyondInsight.
- **RCSSTWorkgroup:** The name of the workgroup that is sent to BeyondInsight to assist when grouping assets.



After the **settings_app.xml** file is saved, the Password Safe client tries to connect to the BeyondInsight server and register. When successful, the computer can be added as a managed system.

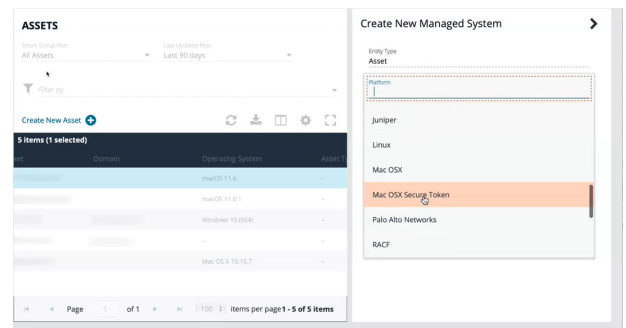
The settings can be changed in the registry.



For more information about registry settings, see *Endpoint Privilege Management for Windows Installation in Endpoint Privilege Management for Windows BeyondInsight Integration Guide* at <https://www.beyondtrust.com/docs/privilege-management/integration/pmw-beyondinsight/install.htm>.

Add the macOS Computer to Password Safe Cloud as a Managed System

When adding the computer, select **Mac OSX Secure Token** from the **Platform** list.



For complete step-by-step instructions on adding managed systems and accounts, see *Add Assets to Password Safe* at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/add-assets/index.htm>.

Upgrade to Password Safe Cloud

You can upgrade to Password Safe Cloud from Password Safe on-premises deployment.

The upgrade workflow:

- Install the Endpoint Privilege Management for Mac client.
- Install the BeyondInsight Adapter.
- Install the standalone Password Safe client.



For more information, see the following:

- ["Install the Endpoint Privilege Management for Mac Client" on page 12](#)
- ["Install the Standalone Password Safe Client" on page 50](#)

Troubleshoot

A diagnostics tool is available with installed files to help troubleshoot causes of connection issues to the BeyondInsight server. The tool does not require any elevated rights to run; any authenticated user on the system can use the tool.

Use the Diagnostics Tool

You can use the tool to check the connection to the BeyondInsight server using a terminal request or as part of an extension attribute in your MDM.

i For more information about Jamf extension attributes, see [Computer Extension Attributes](#).

Commands and Flags

Command	Description
<code>/usr/local/libexec/Avecto/BIAdapter/BIAdapter -v</code>	Reports the currently installed BeyondInsight adapter version.
<code>/usr/local/libexec/Avecto/BIAdapter/BIAdapter -e / --extension-attribute</code>	Reports any known failures or problems when attempting to contact the BeyondInsight platform. The output from using this flag is formatted to be compatible with use as an extension attribute in Jamf. When configured, the output is listed as an attribute against managed computers in Jamf.
<code>/usr/local/libexec/Avecto/BIAdapter/BIAdapter -c / --connection-test</code>	Reports the same information as above, but is more verbose and is intended to be run to gather information so that an engineer can read and more easily determine the cause of deployment problems before resorting to looking through application logs in Console.app .

Test Connection

Run the following command to test the connection to the BeyondInsight instance. The test results are displayed in the terminal window.

```
/usr/local/libexec/Avecto/BIAdapter/BIAdapter -e
```

Possible Test Connection Results

Result	Remedy
Empty response - Exit code 0	NA. The connection was successful.
BeyondInsight certificate name is empty	Check the value of RCSCertName in the settings_app.xml .

Result	Remedy
Configured certificate name not found in Keychain	Check the value of RCSCertName in the settings_app.xml and verify that the certificate is installed in and accessible in Keychain Access.
BeyondInsight connection refused.	Check the value of RCSServer in the settings_app.xml and that you have installed the correct BeyondInsight client certificate.
BeyondInsight URL not configured or empty	Provide a value for RCSServer in the settings_app.xml .
The network connection was lost	Check the value of RCSServer in the settings_app.xml , and network and firewall settings.
The request timed out	Check the value of RCSServer in the settings_app.xml , and network and firewall settings.

Configure an Extension Attribute in Jamf

You can configure an extension attribute to report the output of the BeyondInsight connection tool.

Create an extension attribute in **Jamf Settings > Computer Management > Extension Attributes** with the following configuration:

- **Data type:** String
- **Input type:** Script
- **Shell command:** `/usr/local/libexec/Avecto/BIAdapter/BIAdapter -e`

With this configured, each computer reports the status of the BeyondInsight connection as indicated in the table above.