Privilege Management for Windows
BeyondInsight Integration Guide

Table of Contents

Integrate BeyondTrust Privilege Management for Windows with BeyondInsight

Overview

Privilege Management combines privilege management and application control technology in a single lightweight agent. This scalable solution allows global organizations to eliminate admin rights across the entire business. With the integration between BeyondInsight and 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 analytics capabilities needed to effectively operate your business in a secure fashion.

Network Considerations

TCP Port 443	An event service is used to communicate between PM and BeyondInsight using port 443. Events from PM are sent to BeyondInsight using this service. Communications over this channel is secured by means of a client certificate.

This guide details how to use the BeyondInsight default client certificate (eEyeEmsClient), but you can use your own Private Key Infrastructure (PKI) if you wish.

> ℹ️ For more information, please refer to the *Use a Domain PKI for* BeyondInsight *Communication* section of the BI Installation Guide at www.beyondtrust.com/docs/beyondinsight-password-safe/bi/.

Prerequisites

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

> 📌 *Note: The reporting component is available in BeyondInsight versions 6.10 and later.*

> ℹ️ For information on integrating BeyondTrust Privilege Management for Mac with BeyondInsight, please see the Privilege Management for Mac BeyondInsight Integration Guide, at www.beyondtrust.com/docs/privilege-management/mac.htm.

Steps to Integrate Privilege Management for Windows with BeyondInsight

Once you have BeyondInsight and Endpoint Privilege Management installed in your environment, you will need to configure both instances to communicate with each other. Below is a list of high level steps needed to complete the integration.

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

Installation Information for BeyondInsight and Privilege Management for Windows

Create and Deploy the BeyondInsight Client Certificate for Privilege Management for Windows

To establish communication between BeyondInsight and Privilege Management for Windows clients, a client certificate must be generated from BeyondInsight, and installed on every client needing to transmit information to BeyondInsight. We recommend installing the BeyondInsight client certificate prior to the Privilege Management for Windows client.

> **Tip:** *You do not need to generate a client certificate if there is already a certificate for PowerBroker for Windows Endpoint Protection Platform or BeyondInsight Network Security Scanner. You can use the existing client certificate for your Privilege Management for Windows assets.*

Generate Client Certificate MSI

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 **Generate Certificate.msi** link. A command prompt opens, indicating the MSI is being generated.
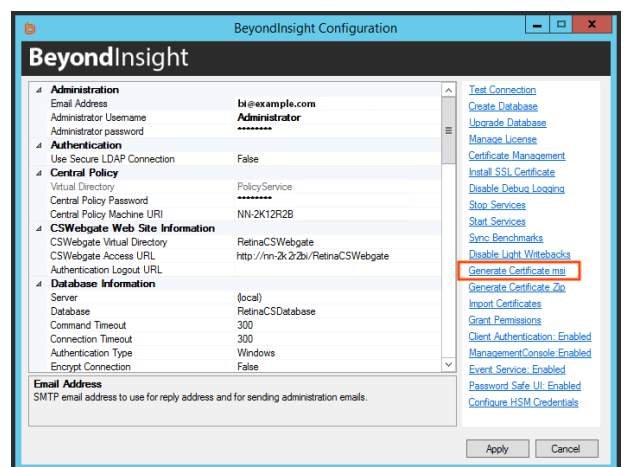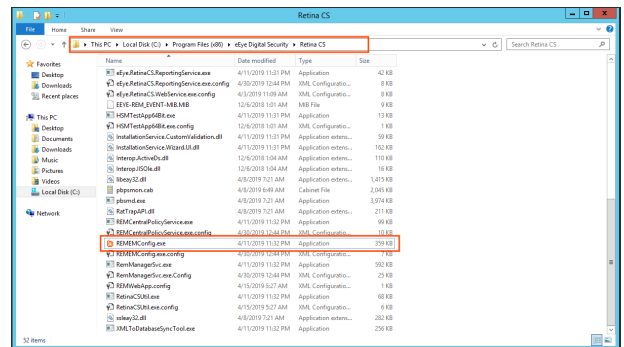
4. Once the prompt closes, the MSI appears in the **C:\Program Files (x86)\eEye Digital Security\Retina CS\Utilities\msi** directory.
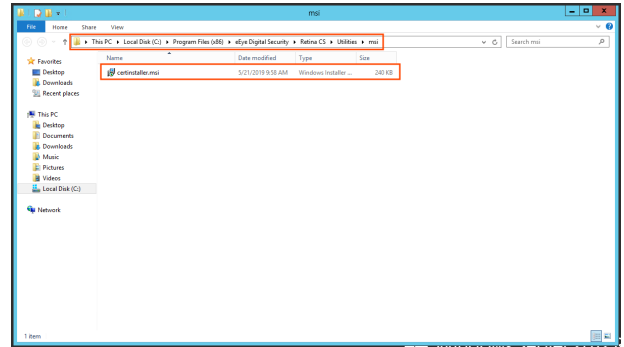
Deploy the Certificate MSI for Privilege Management for Windows

After you have generated the **certinstaller.msi** from BeyondInsight, you must deploy and install the MSI on each machine you wish to communicate with BeyondInsight, using Administrator rights. You may deploy the MSI using the following methods:

Command prompt already running as Administrator

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**

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.

**An enterprise software management tool of your choice, for example, 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.
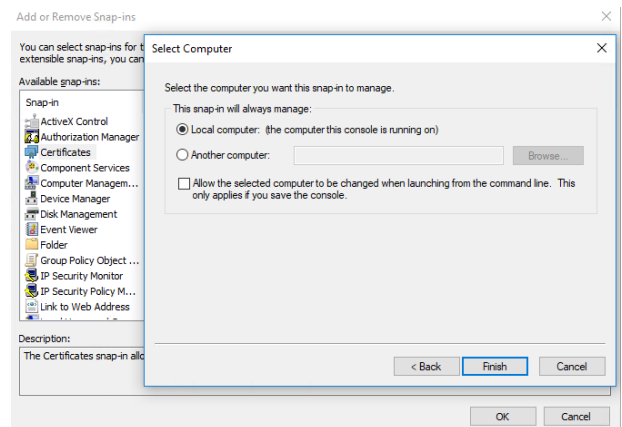
1. Run the **Microsoft Management Console** (MMC) as administrator.
2. Go to **File > Add/Remove Snap-in**.
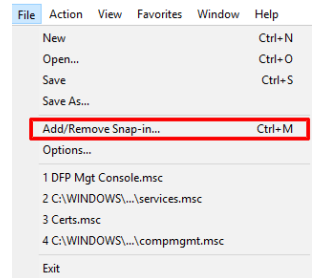
3. From the **Snap-in** menu, select **Certificates**, and click **Add >**.
4. In the **Certificates snap-in** dialog, select **Computer account**.
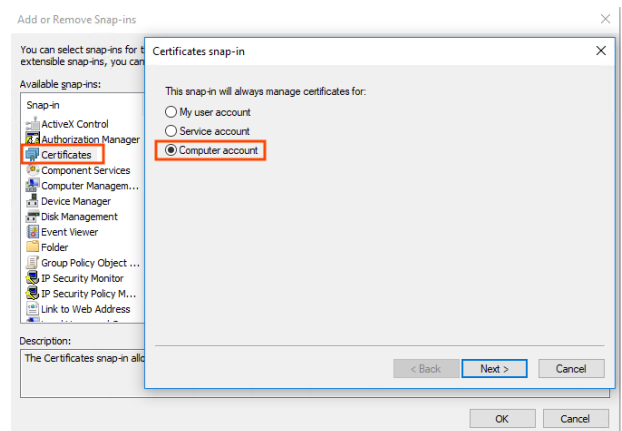
5. Choose **Local computer: (The computer this console is running on)**. Click **Finish**.

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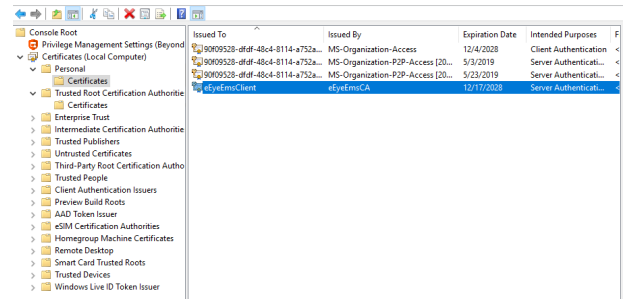
> 📌 *Note: If the certificates are not present, it is possible they were incorrectly installed in the* **Certificates (Current User)** *store. If you find them there, delete them and uninstall* **certinstaller.msi** *from* **Programs & Features (appwiz.cpl)** *before repeating these steps.*

Privilege Management for Windows Installation

For BeyondInsight integration with 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:

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

```
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.

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

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

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

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

8

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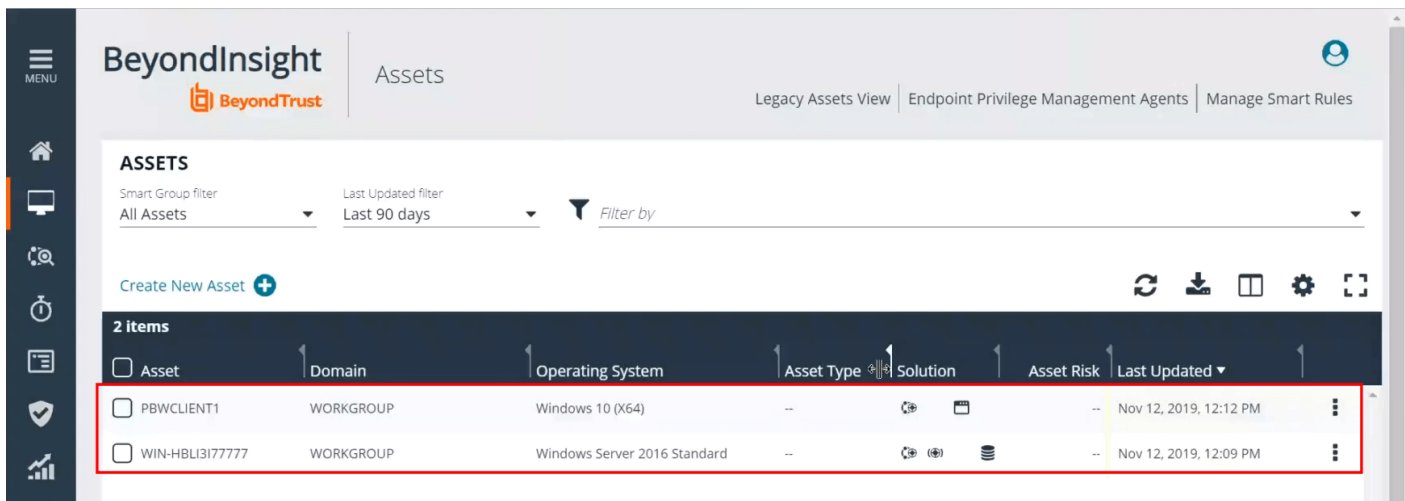
> **IMPORTANT!**
>
> When updating the clients on an existing deployment of BeyondInsight and Privilege Management for Windows, the registry keys from the previous install will be removed. Any previously-specified variables in the install string must be restated in an upgrade.

Ensure that endpoints are registered in BeyondInsight

After deploying your Privilege Management for Windows endpoints, you should 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.

# Prepare the Privilege Management Policy Editor System

Create and Deploy the BeyondInsight Client Certificate for Privilege Management Policy Editor

In BeyondInsight version 6.10, you can run the **certinstaller.msi** to deploy the certificate to your Policy Editor machines. Generating and deploying the **certinstaller.msi** is described earlier in this guide.

> ℹ️ For more information, please see "Installation Information for BeyondInsight and Privilege Management for Windows" on page 5.

In BeyondInsight version 6.9, go through the following procedure. Export the eEyeEmsClient certificate from your BeyondInsight server and import the **eEyeEmsClient.pfx** file to the Local Computer Personal certificate store on all Policy Editor machines.

1. Export the eEyeEmsClient certificates from your BeyondInsight instance using the BeyondInsight Configuration application and click **Generate Certificate Zip**.
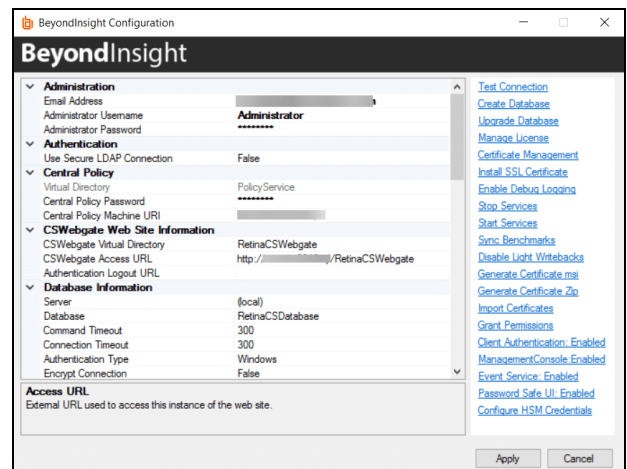

2. Choose an export directory and a password.
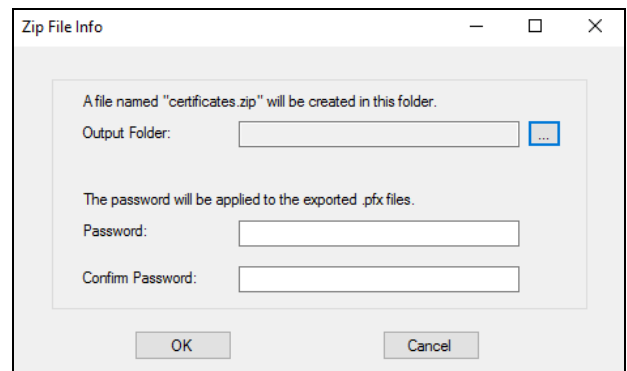
3. Log on to the Policy Editor machine as the user who is responsible for editing policy.
4. Open **Manage Computer Certificates** (**certlm.msc**).
5. Import the **eEyeEmsClient.pfx** file to the **Certificates > Local Computer (Personal)** certificate store. You need to provide the password from the previous step.
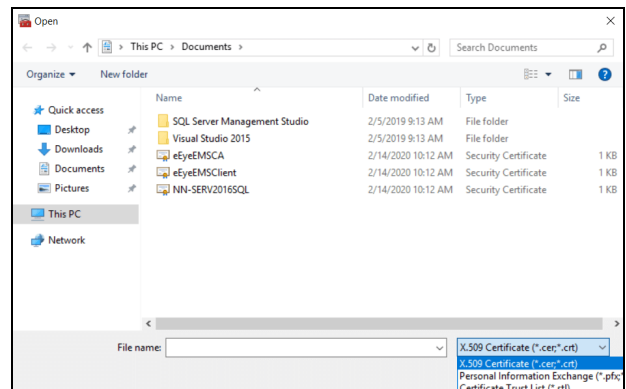
6. Right-click **Personal store** and go to **All Tasks > Import** in the context menu to start the **Certificate Import Wizard**.
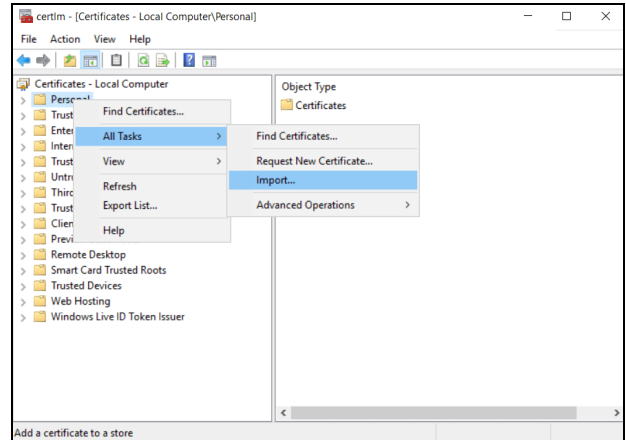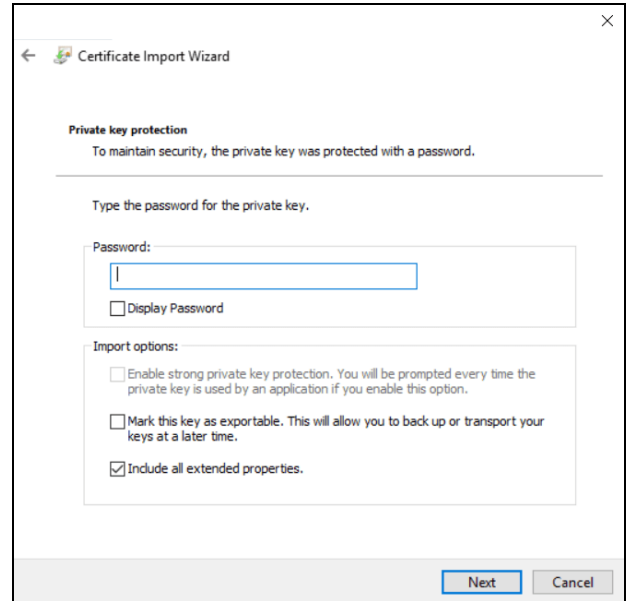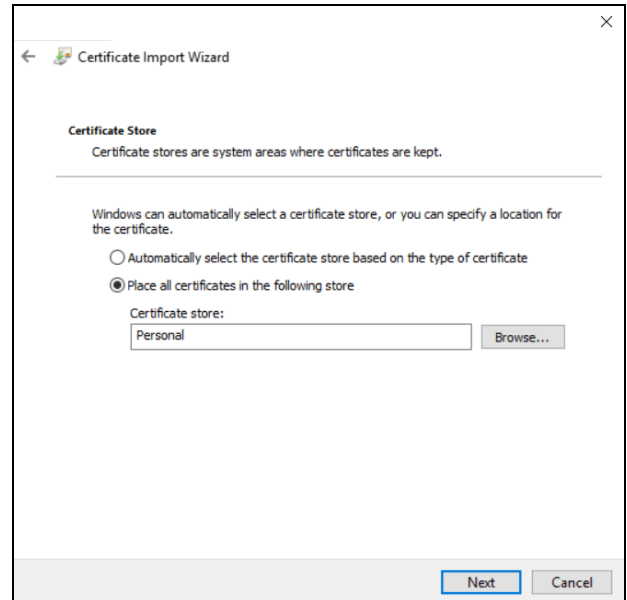

7. Click **Next**.
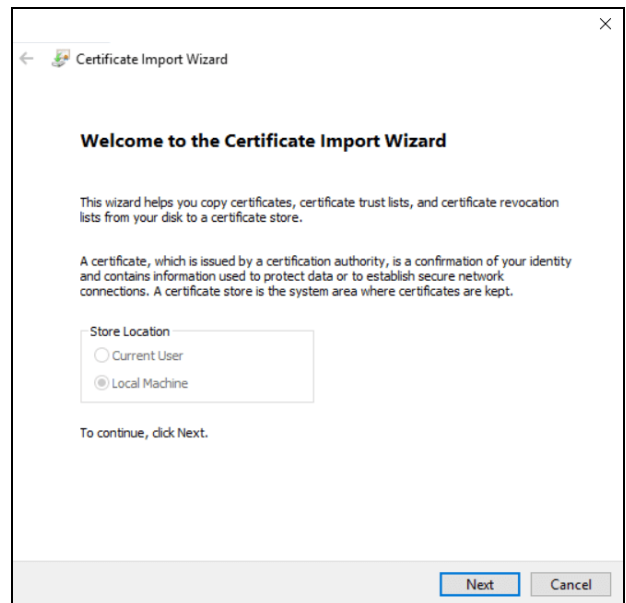
8. Click **Browse**.

9. Change the File Type to ***.pfx** and browse to the **eEyeEmsClient.pfx** file (previously exported from BeyondInsight).

10. Enter the password you chose when exporting from BeyondInsight. Leave other settings as default.

11. Import to the Personal store (default), click **Next** and then **Finish**.

12. Copy **eEyeEmsCA** from **Personal\Certificates** to **Trusted Root Certification Authorities\Certificates**.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

12

Configure the Privilege Management Policy Editor

After you deploy the client certificate to your Privilege Management Policy Editor machines, you can set up the Privilege Management Policy Editor and configure the editor to work with BeyondInsight.

1. Launch the Microsoft Management Console (**mmc.exe**) as an admin and go to **File > Add/Remove Snap-in**.
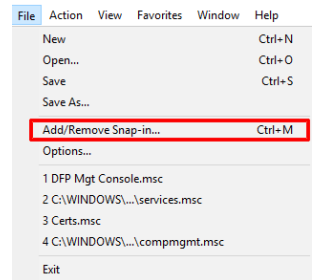
2. In the **Available snap-ins** menu, locate and select the **Privilege Management Settings (BeyondInsight)** snap-in.
3. Click **Add >**, then click **OK**. The **Privilege Management Settings (BeyondInsight**) snap-in will appear in the **Console Root** menu.
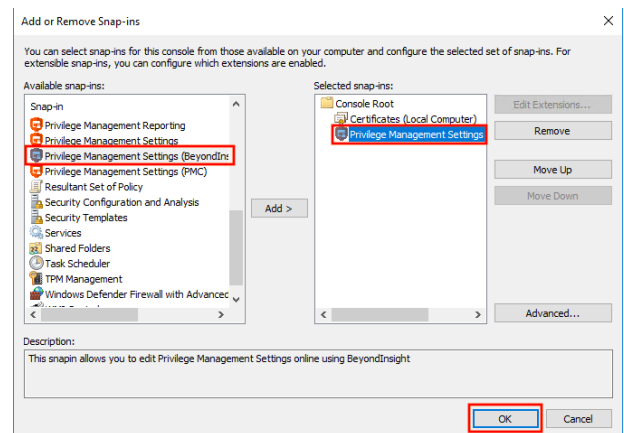
Test the Connection

Before continuing on with the remainder of the integration setup, you need to test the following:

- Test to ensure that a client certificate of the correct name is available in the certificate store.
- Test to ensure the policy editor can reach the BeyondInsight Server.

To test, click on **Remote Server Details** from the **Welcome** page. From the **BeyondInsight Server Details** dialog, enter the server details. Then click **Test** by **Certificate Name** and **BeyondInsight Server** to check each component.

> 📌 *Note: The **Certificate Name** and **Workgroup Name** fields are populated with default values.*
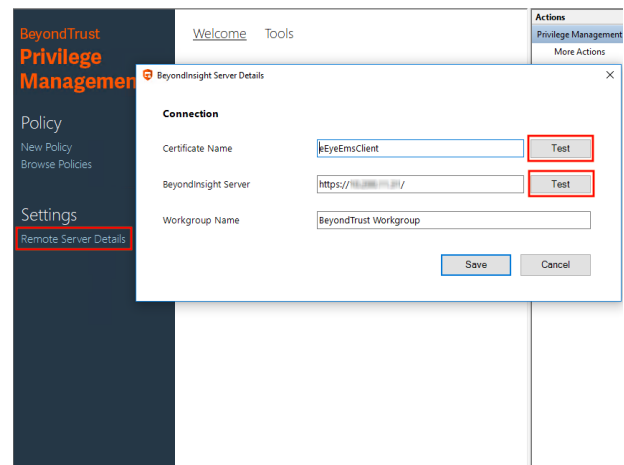
If a certificate of the correct name is found, a message appears stating *Valid certificate found in certificate store*.

<div style="border:1px solid red; display:inline-block">Valid certificate found in certificate store</div>　　[Save] [Cancel]

If the BeyondInsight Server can be reached, a message appears stating *The server was reached successfully*.

<div style="border:1px solid red; display:inline-block">The server was reached successfully</div>　　[Save] [Cancel]

When finished testing, click **Save**.

SALES: www.beyondtrust.com/contact　**SUPPORT:** www.beyondtrust.com/support　**DOCUMENTATION:** www.beyondtrust.com/docs
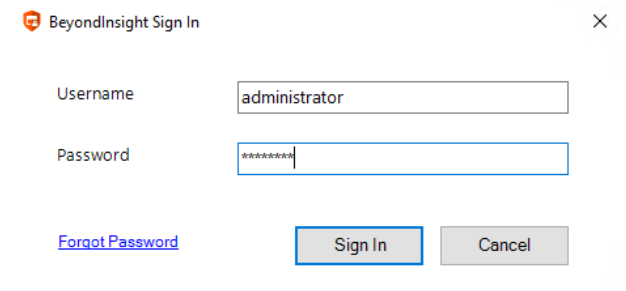
14

Create a New Policy in the Privilege Management Policy Editor

Once you have established communication between the Privilege Management Policy Editor and the BeyondInsight Server, you can create a new policy from the editor.
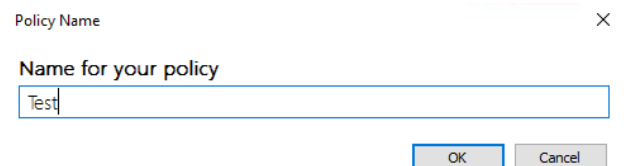
1. From the **Welcome** page, click **New Policy**.
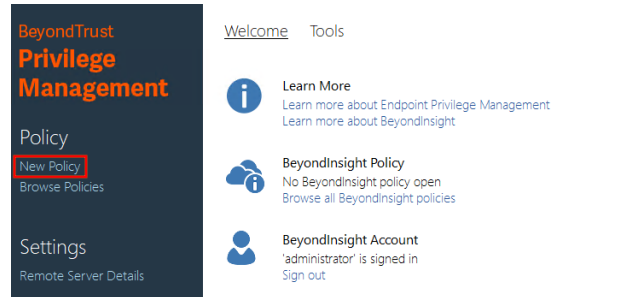
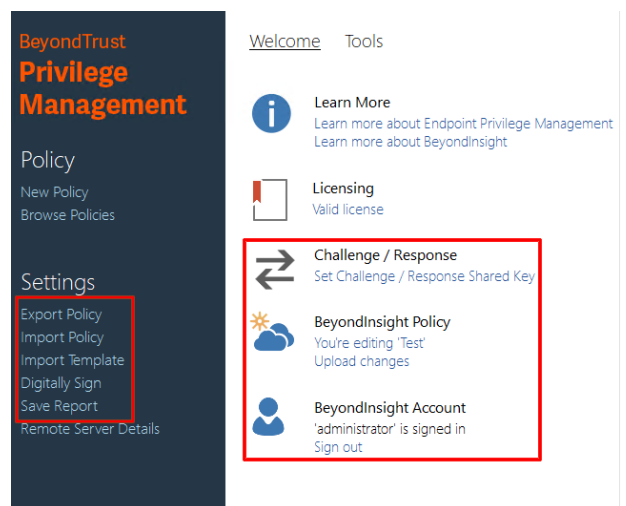2. Enter the credentials used to log into your BeyondInsight instance.

3. Type in a name for your new policy, and then click **OK**.

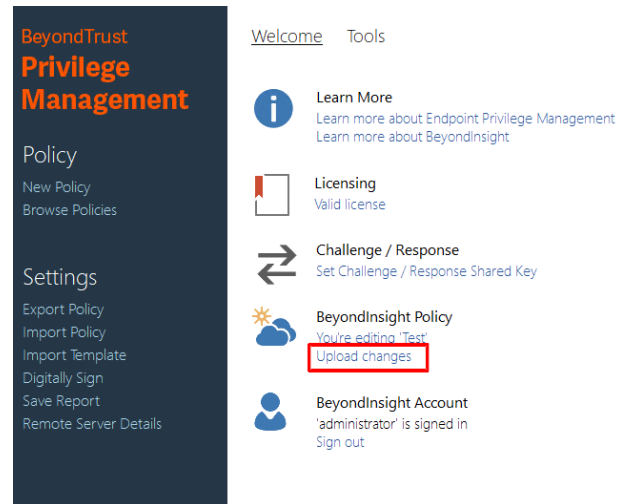The **Welcome** page will update to show more options, including:

- **Export Policy**
- **Import Policy**
- **Import Template**
- **Digitally Sign**
- **Save Report**
- **Challenge/Response**
- **BeyondInsight Policy**
- **BeyondInsight Account**

> ℹ️ For more information on policy creation and best practices, please see the [Privilege Management for Windows Administration Guide](https://www.beyondtrust.com/docs/privilege-management/windows/index.htm) at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm.

Upload Changes

Once you have created and modified your policy, you can upload your changes to BeyondInsight by clicking **Upload Changes** on the **Welcome** page.

After you have uploaded your policy to the BeyondInsight Server, you can view it in BeyondInsight Server from **Menu > Configuration > Privilege Management Policies**.

# Create a Smart Rule and Assign Policy in BeyondInsight

After you have added and uploaded your policy to BeyondInsight from the policy editor, log into your BeyondInsight instance to create Smart Rules and assign policies for assets and users.

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

Create a Smart Rule for Assets

1. In your BeyondInsight instance, click on **Assets**.

2. Click **Manage Smart Rules**.
3. Click **New**.
4. From the **Smart Rules Manager for Assets** dialog, type a name for your Smart Rule.
5. Check **Active**.
6. From the **Category** dropdown, select **Assets and Devices**.
7. Enter a description, if needed.
8. In the **Asset Selection Criteria** section, design a query to pull in the assets you wish to assign policy to.
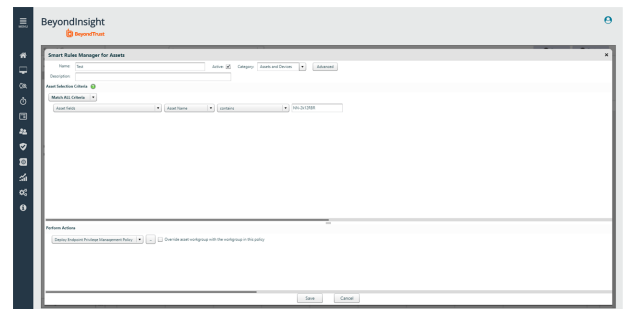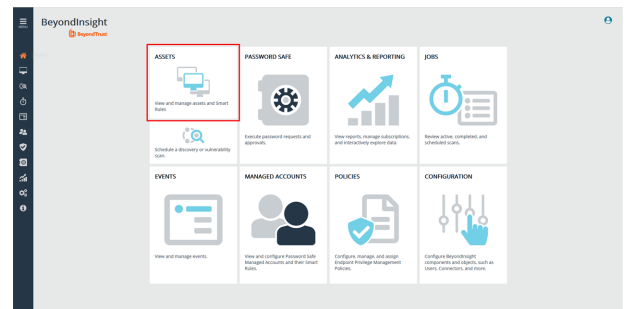
> **Tip:** *For this example, we can narrow down the results of our query to locate our test system, NN-1K12RBR. Choose **Match ALL Criteria**. Select **Asset fields > Asset Name > contains > NN-1K12RBR**.*

9. From the **Perform Actions** dropdown, select **Deploy Endpoint Privilege Management Policy**.
10. Click the **..** button.
11. Select an option from the policy you uploaded from Privilege Management for Windows .
12. Click **Save**.

> ℹ For more information about creating and organizing Smart Rules, please see *Use Smart Rules to Organize Assets* in the *BeyondInsight User Guide* at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm.

Create a Smart Rule for Users

1. In your BeyondInsight instance, click on **Policies**.

2. Click **Manage Smart Rules**.
3. Click **New**.
4. From the **Smart Rules Manager for Assets** dialog, type a name for your Smart Rule.
5. Check **Active**.
6. From the **Category** dropdown, select **Policy Users**.
7. Enter a description, if needed.
8. In the **Selection Criteria** section, design a query to pull in the users you wish to assign policy to.
9. Click the **..** button to build your query.
10. When finished, click **Save**.
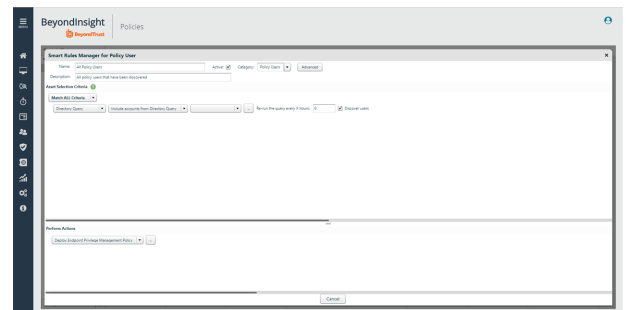11. From the dropdown, choose the query.
12. Check **Discover Users**.
13. From the **Perform Actions** section, choose your policy users and policies you wish to apply. Order policies as needed.
14. Select **Show as Group**.
15. Click **OK**.
16. Click **Save**.

> ℹ️ For more information about managing policies for EPM, please see **Manage User Policies** in the BeyondInsight User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm.

Grant Users Permissions to Log into the Policy Editor

If you would like to grant additional users access to log into the Policy Editor, read and write access needs to be included on the Privilege Management for Windows assets. This access is included by including permissions in the Smart Rule.

1. On the BeyondInsight **Home** page, click **Configuration**.
2. On the **Configuration** grid, select **Role Based Access > User Management**.
3. Locate the group you wish to edit and click the vertical ellipsis button 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.
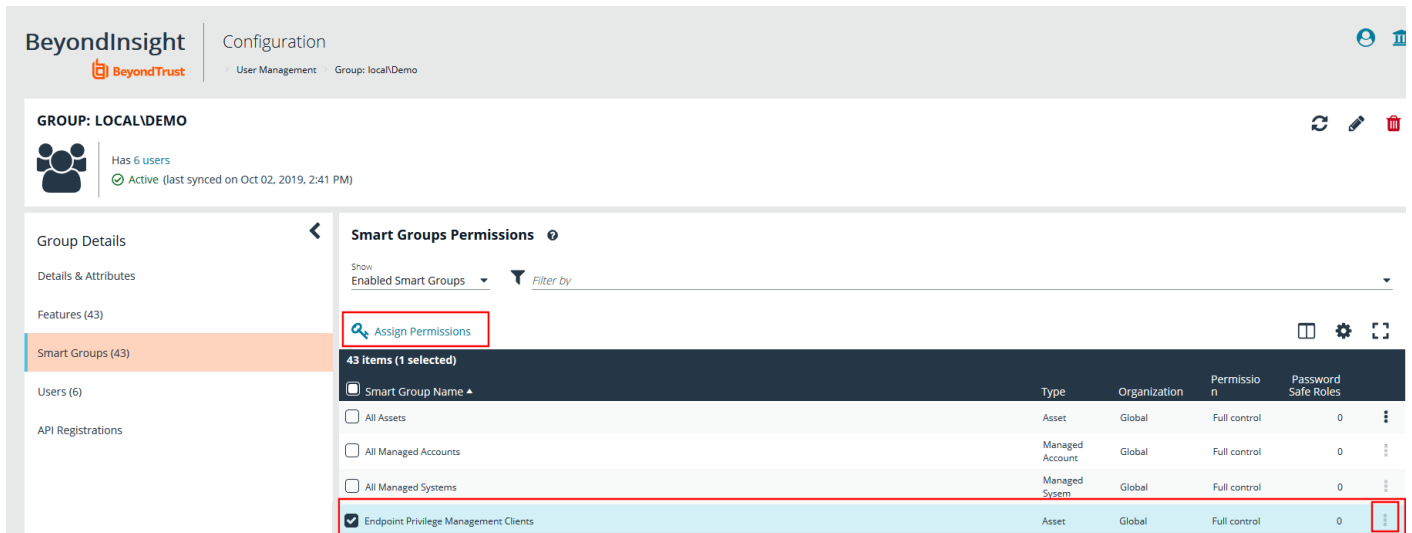
7. Click either the vertical ellipsis button to the far right or the **Assign Permissions** button at the top of the list.

8. Click **Assign Permissions Full Control**.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

19

Install and Configure Privilege Management Reporting

For assistance installing and configuring Privilege Management Reporting with BeyondInsight, please contact your BeyondTrust representative.

Password Safe Integration

In Privilege Management for Windows 5.7, features to support Password Safe integration include:

- Off-network account management: Privilege Management for Windows contacts Password Safe for password tests or password changes.
- Allow as Password Safe User: You can run an application using managed account credentials sourced from Password Safe.

Off-Network Account Management

Password Safe can change passwords on managed accounts. There are two scenarios where Password Safe can change a password:

- **On-network**: Password Safe uses a functional account (an account which has rights to change the managed accounts passwords) to manage local accounts on managed systems.
- **Off-network**: Privilege Management for Windows can periodically contact Password Safe and request tasks, such as password changes or password tests.

The following section provides information on how to set up the off-network scenario.

Prerequisites

The Privilege Management for Windows client requires the BeyondInsight client certificate to enable communication with the BeyondInsight server.

> ℹ For more information, please see "Installation Information for BeyondInsight and Privilege Management for Windows" on page 5.

Install Privilege Management for Windows Client

The Privilege Management for Windows installer includes the service **Password Safe Service**.

Privilege Management for Windows must be installed using the Password Safe mode flags, **PSMODE=1** and **BIMODE=1**, as shown:

```
PrivilegeManagementForWindows_x64.exe /v"BIMODE=1 PSMODE=1
BEYONDINSIGHTURL=https://uvm002.btrusteng.com/EventService/Service.svc"
```

Configure the Password Safe Service

> 📌 *Note: This feature is only available with the BeyondInsight management console.*

Configure the Heartbeat Interval

1. In the Policy Editor, select the **Integration Settings** node.
2. From the **Activation** list, select one of the following: **Not Configured**, **Enabled**, or **Disabled**.

3. Set the default heartbeat interval. This is the time span the endpoint polls Password Safe unless the time is determined by Password Safe. For most subsequent messages, the poll time is driven by Password Safe in the messages it sends to Privilege Management for Windows. This is because Password Safe knows when the next scheduled action must be performed.

Configure Password Safe

Managed systems and managed accounts can be added to Password Safe in the same way as an on-network scenario; manually and using Smart Rules. A discovery scan is not possible in the off-network scenario.

> ℹ️ For more information, please 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.

Limitations

Default values for the following **Account Settings** in Password Safe are applied in a Privilege Management for Windows off-network integration: **Change Services** (yes), **Restart Services** (no), and **Change Tasks** (no). The settings cannot be changed in this scenario.

Allow as Password Safe User

In Privilege Management for Windows 5.7, you can run an application using Managed Account credentials sourced from Password Safe.

Prerequisites

Endpoint

The endpoint must be set up as a managed system in Password Safe.

Communication to Password Safe relies on BeyondInsight communication channels and the appropriate client certificate. Therefore Privilege Management for Windows must be installed using the **BIMODE=1** flag:

```
PrivilegeManagementForWindows_x64.exe /v"BIMODE=1
BEYONDINSIGHTURL=https://uvm002.btrusteng.com/EventService/Service.svc"
```

Password Safe

The Password Safe account name must be a managed account associated with the managed system (endpoint).

> ℹ️ For more information, please 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 .

Configure the Application Rule

> 📌 *Note: This feature is only available with the BeyondInsight management console.*

To configure the Password Safe user in the Privilege Management for Windows client, you need to set up an application rule that includes the Password Safe user.

1. In the **Edit Rule Application** dialog box, select **Allow as Password Safe User** from the **Action** list.
2. In the **Password Safe Account Name** field, enter the name of the account exactly as configured in Password Safe. This is the Managed Account configured in Password Safe for the endpoint.

End user messaging is not available in this release.

> ℹ️ For more information about application rules, please see *Application Rules* in the Privilege Management for Windows Administration Guide at https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-windows-admin-guide.pdf.

Troubleshoot

A diagnostics tool, **DiagnosticsCli.exe**, is available with 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 DiagnosticsCli.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 Privilege Management for Windows is installed in the default location, run the following from the command line:

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

PowerShell:

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

Possible Test Connection Results

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

Result	Remedy
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 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\DiagnosticsCli.exe" /bi /p
```

PowerShell:

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