# Privilege Management for Windows BeyondInsight Integration Guide

### **Table of Contents**

Integrate BeyondTrust Privilege Management for Windows with BeyondInsight
Steps to Integrate Privilege Management for Windows with BeyondInsight 4
Installation Information for BeyondInsight and Privilege Management for Windows 5
Create and Deploy the BeyondInsight Client Certificate for Privilege Management for Windows
Generate Client Certificate MSI 5
Deploy the Certificate MSI for Privilege Management for Windows
Privilege Management for Windows Installation
Prepare the Privilege Management Policy Editor System10
Create a New Policy in the Privilege Management Policy Editor15
Create a Smart Rule and Assign Policy in BeyondInsight17
Install and Configure Privilege Management Reporting
Password Safe Integration
Off-Network Account Management21
Prerequisites
Install Privilege Management for Windows Client21
Configure the Password Safe Service21
Allow as Password Safe User
Prerequisites
Configure the Application Rule22
Troubleshoot
Use the DiagnosticsCli.exe Tool

# 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.

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

#### **Prerequisites**

1

٦.

- 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.

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

# 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**.

🔁 💿 🖌 🕇 📕 🕨	This PC + Local Disk (C) + Program Files (x86) +	eEye Digital Security	<ul> <li>Retina CS</li> </ul>		~ ¢	Search Retina CS	
* Favorites	Name	Date modified	Туре	Size			
Desktop	E eEye.RatinaCS.ReportingService.exe	4/11/2019 11:31 PM	Application	42 KB			
Downloads	P eEye.RetinaCS.ReportingService.exe.config	4/30/2019 12:44 PM	XML Configuratio	8 KB			
Recent places	D elye RetinaCS.WebService.exe.config	4/3/2019 11:09 AM	XML Configuratio	0.03			
	EEVE-REM_EVENT-MIB.MIB	12/6/2018 1:01 AM	MIB File	9 KB			
This PC	HSMTestApp64Bit.exe	4/11/2019 11:31 PM	Application	13 KB			
Besktop	P. HSMTestApp64Bit.eve.config	12/6/2018 1:01 AM	XML Configuratio	1.68			
Documents	S InstallationService.CustomValidation.dll	4/11/2019 11:31 PM	Application extens	59 KB			
Downloads	InstallationService.Wizard.ULdll	4/11/2019 11:31 PM	Application extens	162 KB			
Music	Interop ActiveDs.dll	12/6/2018 1:04 AM	Application extens	110 KB			
Pictures	Interop JISOle.dll	12/6/2018 1:04 AM	Application extens	16 KB			
Videos	Bibeay32.dll	4/8/2019 7:21 AM	Application extens	1,415 KB			
Local Disk (C:)	pbpsmon.cab	4/8/2019 6-49 AM	Cabinet File	2,045 KB			
	pbsmd.exe	4/8/2019 7:21 AM	Application	3,974 KB			
S Network	RatTrapAPLdI	4/8/2019 7:21 AM	Application extens	211 KB			
	REMCentralPolicyService.exe	4/11/2019 11:32 PM	Application	99 KB			
	REMCentralPolicyService.exe.config	4/30/2019 12:44 PM	XML Configuratio	10 KB			
	REMEMConfig.exe	4/11/2019 11:32 PM	Application	359 KB			
	9.3 REMEMConfig.exe.config	4/30/2019 12:44 PM	XML Configuratio	7 KB			
	RemManagerSvc.exe	4/11/2019 11:32 PM	Application	592 KB			
	RemManagerSvc.exe.Config	4/30/2019 12:44 PM	XML Configuratio	25 KB			
	9. REMWebApp.config	4/15/2019 5:27 AM	XML Configuratio	1 KB			
	RetinaCSUtiLexe	4/11/2019 11:32 PM	Application	68 KB			
	RetinaCSUtiLexe.config	4/15/2019 5/27 AM	XML Configuratio	6 KB			
	🔊 ssleay32.dll	4/8/2019 7:21 AM	Application extens	282 KB			

3. Click on the **Generate Certificate.msi** link. A command prompt opens, indicating the MSI is being generated.

4	Administration		^	Test Connection
	Email Address	bi@example.com		Create Database
	Administrator Username	Administrator		Upgrade Database
	Administrator password		=	
4	Authentication			Manage License
	Use Secure LDAP Connection	False		Certificate Management
4	Central Policy			Install SSL Certificate
	Virtual Directory	PolicyService		Disable Debug Logging
	Central Policy Password			Stop Services
	Central Policy Machine URI	NN-2K12R2B		
4	CSWebgate Web Site Information	n		Start Services
	CSWebgate Virtual Directory	RetinaCSWebgate		Sync Benchmarks
	CSWebgate Access URL	http://nn-2k2r2bi/RetinaCSWebgate		Disable Light Writebacks
	Authentication Logout URL			Generate Certificate msi
4	Database Information			Generate Certificate Zip
	Server	(local)		Import Certificates
	Database	RetinaCSDatabase		
	Command Timeout	300		Grant Permissions
	Connection Timeout	300		Client Authentication: Enabled
	Authentication Type	Windows		ManagementConsole:Enabled
	Encrypt Connection	False	$\sim$	Event Service: Enabled
	nail Address ITP email address to use for reply addres	ss and for sending administration emails.		Password Safe UI: Enabled Configure HSM Credentials

5

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

Point     In the K* is used bit (2) + Proper Trins bit): • dire Diputationary • Rates (2) + Datas • runi     v C)     Each run       W Facility     Data modulati Tyre     Data       Besting     Strint (2)     Data modulati Tyre     Data       Besting     Strint (2)     Strint (2)     Data modulati Tyre     Data       Besting     Strint (2)     Strint (2)     Data     Data       Besting     Strint (2)     Strint (2)     Data     Data       Besting (2)     Strint (2)     Strint (2)     Strint (2)     Data       Besting (2)     Strint (2)     Strint (2)     Strint (2)     Strint (2)	1 🕞 🔛 👳 l		msi	
Product     Non-     Date modified     Type     See       Boundarie     Unitarian (See Contraction (See Cont	File Home Shar	e View		
Description     ∰ enderwarker mei     \$177(2019) 252 8.84     Westwork includer _ 2010       Description     Benders     Description       Description     Description	🖻 🛞 – 🕈 🕌 🖬 1	Fhis PC + Local Disk (C:) + Program	Files (x86) + eEye Digital Security + Retina CS + Utilities + mai	v 🖒 Search msi .
■ Donatada	* Emorites	Name	Date modified Type Size	
Root Diverse     Decembra     Decembra	Desktop	🙀 certinstaller.msi	5/21/2019 9:58 AM Windows Installer 240 KB	
N The FC				
Derugente     Decompose     Decompose	Recent places			
© Doumits © Domitst © Main: © Rotant ■ Main () ♥ Hainest	🛤 This PC			
ii Doministi ii Maa ii Maa ii Maa ii Kaadaba (c) ii Kaadaba				
ii Maix ii Polous ii Volus ii Sourch (C) ↓ Halant				
ii Pointe iii Votee iii Lead Dav (<) iii Renork				
in Long Data (C) ∰ Marcel	Pictures			
Se Tatuest				
	Local Disk (C:)			
	🗣 Network			

### 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

BeyondTrust

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.

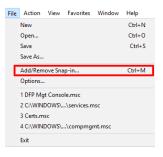
Restart each client computer to initiate the installation. This can be done manually or by using Group Policy mechanisms.

#### 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.



7

- 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.

dd or Kemove Snap-Ins	^
ou can select snap-ins for t xtensible snap-ins, you can	Certificates snap-in X
valable grap-ins: Snap-in ActiveX Control ActiveX Control ActiveX Control ActiveX Control ActiveX Control ActiveX Control Component Services Component Services Component Services Device Management Bevent Viewer Polage Polage Polage Decurity Monitor Bersecurity Monitor Device Manager Link to Web Address escription:	This snap-in will always manage certificates for: My user account Service account © Computer account
Escription: The Certificates snap-in allo	< Back Net > Cancel OK Cancel
dd or Remove Snap-ins ou can select snap-ins for t xtensible snap-ins, you can	Select Computer X
Attended snap-ins: valable gnap-ins: Snap-in ActiveX Control Authorization Manager Certificates Computer Managem. Dek Management Event Viewer Folder Group Policy Object P Security Policy M De Security Policy M Link to Web Address escription:	Select the computer you want this snap-in to manage. This snap-in will always manage:
escription: The Certificates snap-in allo	< Back Rnish Cancel
	OK Cancel

<sup>©2003-2020</sup> BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository TC: 10/13/2020 institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- In the MMC Console, expand Console Root > Certificates (Local Computer).
- 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.

Console Root	Issued To	Issued By	Expiration Date	Intended Purposes
Privilege Management Settings (Beyond	190f09528-dfdf-48c4-8114-a752a	MS-Organization-Access	12/4/2028	Client Authentication
Certificates (Local Computer)	10000000000000000000000000000000000000		5/3/2019	Server Authenticati
Personal     Certificates	10000000000000000000000000000000000000	MS-Organization-P2P-Access [20	5/23/2019	Server Authenticati
Certificates	EyeEmsClient	eEyeEmsCA	12/17/2028	Server Authenticati
Certificates				
<ul> <li>Enterprise Trust</li> </ul>				
Intermediate Certification Authoritie				
> Trusted Publishers				
> Untrusted Certificates				
> Third-Party Root Certification Autho				
> Trusted People				
Client Authentication Issuers				
> Preview Build Roots				
AAD Token Issuer				
eSIM Certification Authorities				
> Homegroup Machine Certificates				
> C Remote Desktop				
> Smart Card Trusted Roots				
> 📋 Trusted Devices				
Windows Live ID Token Issuer				

## **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:

Location	Name	Default	Installer Variable Name
	BeyondInsightUrl	[Empty] - You must specify this	BEYONDINSIGHTURL
HKEY_LOCAL_	BeyondInsightCertName	eEyeEmsClien t	BEYONDINSIGHTCERTNAME
MACHINE\SOFTWARE\Avecto\Privileg e Guard Client	BeyondInsightWorkgroup	BeyondTrust Workgroup	BEYONDINSIGHTWORKGROU P
	BeyondInsightHeartbeatIntervalMin s	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 BeyondInsightas well as the Endpoint Privilege Management **Agents** grids.

MENU	BeyondInsig	trust Assets		Legacy Assets View Endpoir	nt Privilege Managen	nent Agents	Manage		<b>O</b> ules
*	ASSETS								
<b>P</b>	Smart Group filter All Assets	Last Updated filter ▼ Last 90 days	Filter by						•
يم ڻ	Create New Asset 🕂					с.	≴ □	٥	::
•	Asset	Domain	Operating System	Asset Type 🕮 Solution	Asset Risk	Last Upda	ted 🔻		
<b>v</b>	PBWCLIENT1	WORKGROUP	Windows 10 (X64)	🕩 🖻		Nov 12, 201	9, 12:12 PM		E *
<b>:</b> ái	WIN-HBLI3I77777	WORKGROUP	Windows Server 2016 Standard	(*)		Nov 12, 201	9, 12:09 PM		:

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

# Prepare the Privilege Management Policy Editor System

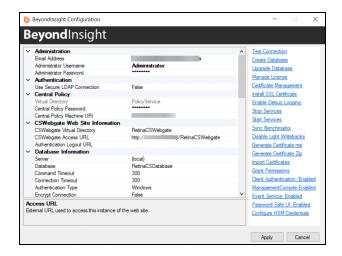
#### Create and Deploy the BeyondInsight Client Certificate for Privilege Management Policy Editor

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.

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.

Zip File Info			-	×
A file named "certificates.z	ip" will be created in th	is folder.		
Output Folder:				
The password will be appli	ed to the exported .pfx	files.		
Password:				
Confirm Password:				
Coninini Password.				
			_	
OK		Cancel		

- 3. Log on to the Policy Editor machine as the user who is responsible for editing policy.
- 4. Open Manage Computer Certificates (certIm.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.

 $\times$ 

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).

> Previ Help	
Smart Card Trusted Roots     Trusted Devices     Web Hosting     Windows Live ID Token Issuer	
	۲
Add a certificate to a store	
	×
Certificate import wizard	
Walasma ta tha Ca	atificants Invested Missard
welcome to the Ce	ertificate Import Wizard
This wizard helps you copy ce lists from your disk to a certifi	rtificates, certificate trust lists, and certificate revocation cate store.
and contains information used	oy a certification authority, is a confirmation of your identity to protect data or to establish secure network re is the system area where certificates are kept.
Store Location	
O Current User	
Local Machine	
To continue, click Next.	
	Next Cancel

Object Type

Request New Certificate. Import...

Advanced Operations

Find Certificates...

Certificates

Section - [Certificates - Local Computer/Personal]

Find Certificates.

All Tasks

View

Refresh

Help

Export List..

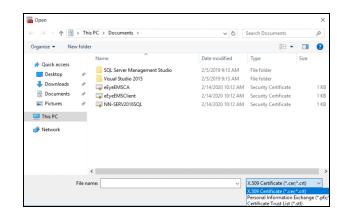
File Action View Help 🗢 🧼 🙍 📰 📋 🙆 💀 👔 📷 🗊 Certificates - Local Computer

Perso Trust

📫 Enter

Inten Trust Untri Thirc

Trust Clien



11

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

 $\sim$ 

Next Cancel

12

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.

BeyondTrust

Priv	rate key protection To maintain security, the private key was protected with a password.
	Type the password for the private key.
	Password:
	Display Password
	Import options:
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
	Include all extended properties.
	Next Can
Şe ci	Next Can
Şe C	
-	
-	ertificate Import Wizard
-	ertificate Import Wizard <b>tificate Store</b> Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for
-	ertificate Import Wizard tificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.
-	ertificate Import Wizard tificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate (a) Place all certificates in the following store Certificate store:
-	ertificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  i Place all certificates in the following store
-	ertificate Import Wizard tificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate © Place all certificates in the following store Certificate store:
-	ertificate Import Wizard tificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate © Place all certificates in the following store Certificate store:

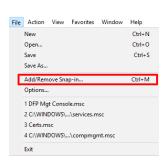
Γ

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

#### **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.

 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.
- Click Add >, then click OK. The Privilege Management Settings (BeyondInsight) snap-in will appear in the Console Root menu.

vailable snap-ins: Snap-in Privilege Management Reporting	^		s (Local Computer)	Edit Extensions
Privilege Management Settings     Privilege Management Settings (Beyo     Privilege Management Settings (PMC)		Privilege M	anagement Settings	Move Up
Resultant Set of Policy Security Configuration and Analysis Security Templates Services	Add	>	1	Move Down
3 Shared Folders Task Scheduler TPM Management				
Windows Defender Firewall with Adva	anced v	<	<b>&gt;</b>	Advanced
escription: This snapin allows you to edit Privilege Mi				

#### **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.

			Actions
	Welcome Tools		Privilege Management
Privilege			More Actions
Privilege Managemer	G BeyondInsight Server Details		×
Policy	Connection		
	Certificate Name	eEyeEmsClient	Test
	Beyondinsight Server	https://	Test
Settings	Workgroup Name	BeyondTrust Workgroup	
Remote Server Details			
		Save	Cancel

13

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

14

If a certificate of the correct name is found, a message appears stating Valid certificate found in certificate store. If the BeyondInsight Server can be reached, a message appears stating The server was reached successfully.

When finished testing, click **Save**.

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

# 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.

BeyondTrust	Welcome Tools
<b>Privilege</b> Management Policy	Learn More Learn more about Endpoint Privilege Management Learn more about Beyondinsight
New Policy Browse Policies	Beyondinsight Policy No Beyondinsight policy open Browse all Beyondinsight policies
Settings Remote Server Details	BeyondInsight Account 'administrator' is signed in Sign out
👽 Beyondlnsight Sign In	×
Username	administrator
Password	******
Forgot Password	Sign In Cancel
Policy Name	×
Name for your policy Test	
	OK Cancel
BeyondTrust <b>Privilege</b>	<u>Welcome</u> Tools
Management	Learn More Learn more about Endpoint Privilege Management Learn more about Beyondinsight
Policy New Policy Browse Policies	Licensing Valid license
Settings	Challenge / Response Set Challenge / Response Shared Key
Export Policy Import Policy Import Template	SeyondInsight Policy You're editing 'Test' Upload changes
Digitally Sign Save Report Remote Server Details	BeyondInsight Account 'administrator' is signed in Sign out

15

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:

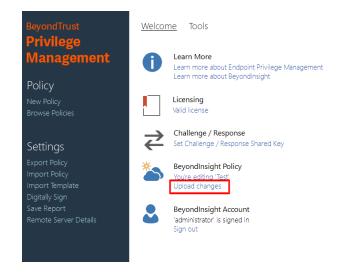
- Export Policy
- Import Policy
- Import Template
- Digitally Sign
- Save Report
- Challenge/Response
- BeyondInsight Policy
- BeyondInsight Account

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

#### **Upload Changes**

i

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



16

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.

		Annue Contraction	benefan Aar falaan falaan falaan
	Alexandra 0 Martina 1 Andra		Anat falcihar Otaria D
			Multin BLC Others
ndom To	- Marine - Transmission -		
m Actions		prison Actiona	
m Actions		prison Actiona	
m Actions		prison Actiona	
m Actions	- A second s	prison Actiona	
m Actions	- A second s	prison Actiona	
m Actions	- A second s	prison Actiona	
m Actions	- A second s	prison Actiona	
m Actions		oform Actions	
m Actions	- A second s	prison Actiona	
m Actions	- A second s	prison Actiona	
m Actions	- A second s	prison Actiona	
m Actions	- A second s	prison Actiona	
m Actions	- A second s	prison Actiona	
m Actions		prison Actiona	
m Actions		prison Actiona	
m Actions		prison Actiona	
m Actions		prison Actiona	
ann a haann Andre y Dan ann an Ann a' Ann	han han dan dan sebagai dan dari sebagai dan	Nenhebian hang dang mahan 👔 😰 📄 Dania and calipus e dan ang	
			Percent Sections Medican Medican Medican Medican and the enderson of the enderson in the ender

17

**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.

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



#### **Create a Smart Rule for Users**

1. In your BeyondInsight instance, click on Policies.



ndInsight

- 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.
- 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.

1

For more information about managing policies for EPM, please see **Manage User Policies** in the <u>BeyondInsight User</u> 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.
- 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.



BeyondInsight Configuration	Group: local\Demo					6	) 1
GROUP: LOCAL\DEMO	1 PM)				0	<b>GAN</b>	۵
Group Details	Smart Groups Permissions 🛛 🛛						
Details & Attributes	Show Enabled Smart Groups 👻 🕇 Filter by						•
Features (43)	Assign Permissions					¢	0
Smart Groups (43)	43 items (1 selected)						
Users (6)	Smart Group Name *	Туре	Organization	Permissio n	Passwor Safe Role	d s	
API Registrations	All Assets	Asset	Global	Full control		0	:
-	All Managed Accounts	Managed Account	Global	Full control		0	1
	All Managed Systems	Managed Sysem	Global	Full control		0	1
	Endpoint Privilege Management Clients	Asset	Global	Full control		0	1

- 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.

# Install and Configure Privilege Management Reporting

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

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

# **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**

٦

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

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.

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**

1

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

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.

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

23

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.

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

# 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 <b>BEYONDINSIGHTCERTNAME</b> 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 <b>BEYONDINSIGHTURL</b> in the registry and that you have installed the correct BeyondInsight client certificate.

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

25

Result	Remedy
BeyondInsight URL not specified	Provide a value for <b>BEYONDINSIGHTURL</b> in the registry
BeyondInsight could not be contacted	Check the value of <b>BEYONDINSIGHTURL</b> 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