Privilege Management Cloud Administration Guide 21.5

TC:8/11/2021

Table of Contents

Privilege Management Cloud Administration Guide

Privilege Management Console is a management platform for Privilege Management that allows you to control your computers from one central location.

This Administration Guide details the features and functionality of PMC.

> *For detailed instructions for configuring the MMC and PMC, please see "Privilege Management Console QuickStart" on page 8.*

Sign into Privilege Management Console

> ***Note:** You must have cookies enabled in your browser to use PMC. If you do not enable cookies, you will get a blank page when you attempt to navigate to PMC.*

The PMC version is displayed at the bottom of the logon page.

To log in to PMC:

1. Navigate to your PMC instance and click **Sign in**.
2. Click the appropriate email associated with your account.
3. Determine whether or not you would like to remain signed in. Click **Yes** to limit the number of times you'll be asked to sign in, or **No** to be prompted every time.

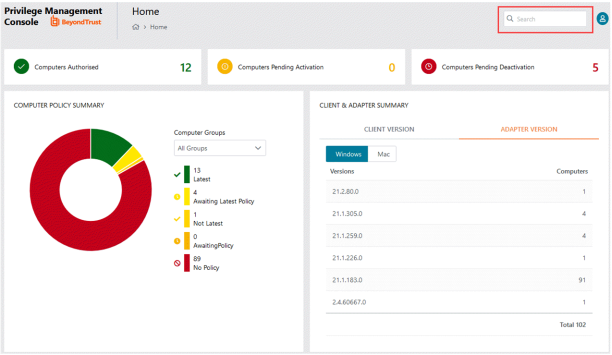
> ***Note:** To edit your time and date format, navigate to your profile by clicking the profile icon in the top right corner.*

Automatic Logout

You will be logged out of the PMC portal after 15 minutes of inactivity.

Privilege Management Console Search

Use the search box on the top right of PMC to search for various topics and features.



Computers Authorised 12

Computers Pending Activation 0

Computers Pending Deactivation 5

- 13 Latest
- 4 Awaiting Latest Policy
- 1 Not Latest
- 0 AwaitingPolicy
- 89 No Policy

Versions	Computers
21.2.80.0	1
21.1.305.0	4
21.1.259.0	4
21.1.226.0	1
21.1.183.0	91
2.4.60667.0	1
	Total 102

In PMC, you can search across:

- Groups
- Policies
- Computers
- Users

The icon adjacent to the search term indicates if it is a **Computer**, **Policy**, **Group**, or **User**, respectively.

For more information, please see the following:

- *"Privilege Management Console Groups" on page 31*
- *"Privilege Management Console Policies" on page 19*
- *"Privilege Management Console Computers" on page 26*
- *"Manage User Accounts" on page 34*

Privilege Management Console QuickStart

This section details the most likely tasks to get started with PMC, including automatically authorizing and assigning computers to groups in PMC.

After you deploy PMC, you can

- Manage policy
- Create groups and assign policy
- Assign computers to these groups

Manage Policy

There are various approaches you can take to PMC. For example, if you are new to PMC, you may want to create a group, assign it as the Default group, add all your computers to that group, and then assign the Privilege Management QuickStart policy to that group.

If you are migrating to PMC, you may want to replicate your existing groups and assign the same policy to them, before authorizing and placing your computers in those groups.

Once you have your policy, you can create groups in PMC and assign policies to those groups.

For more information, please see "Manage Policy in the MMC Snap-in" on page 23.

Create Groups and Assign Policy

Create Groups

1. Select **Computer Groups** from the sidebar menu.
2. Click **Create Group**.
3. Enter a **Group Name**. The **Description** field is optional.
4. Click **Submit**. Your group is created and appears in the grid list below.

Once the group is created, you can set it as the Default group. If set, the Default group will be selected by default when you add one or more computers to a group. To set the group as the Default group, select the desired group name, and then click **Set Default** at the top of the **Groups** grid.

Note: *The Group Name and Description can be edited at any time by clicking **Edit Group** from the **Group Details** page. Click the vertical ellipsis at the end of a group's row to expand a new menu that will take you to the **Group Details** page.*

Assign Policy

1. Select **Computer Groups** from the sidebar menu.
2. Click the vertical ellipses icon on the appropriate group's row to expand more options and select **Assign Policy to Group**.
3. Select the policy you want to assign from the dropdown and the associated revision.

***Note:** You should see a green dialog box appear in the upper corner of the console to confirm that the policy was applied successfully.*

For details on how you can control the deployment of your policy, please see "Manage Policy Deployment Settings" on page 75.

Install Privilege Management

You need to install Privilege Management for the target operating system, as well as the PMC adapter.

You can view installation package details by visiting the **Configuration** page.

The Privilege Management installation packages differ based on your operating system:

Windows

For 32-bit (x86) systems, choose the **Win 32 Bit** Download Type.

For 64-bit (x64) systems, choose the **Win 64 Bit** Download Type.

You need to install Privilege Management for Windows in silent mode with the iC3MODE switch enabled:

```
Msiexec.exe /i PrivilegeManagementForWindows_x.xxx.x.msi IC3MODE=1 /qn /norestart
```

MacOS

For MacOS computers, choose the **MacOS** Download Type.

Install the Windows Adapter

***Tip:** Setup Information is available for the Windows adapter on the **Configuration** page. On the sidebar menu, click **Configuration** to view the details.*

The PMC client adapter installers can be found in the **Configuration > Settings > Adapter Installation** folder of the PMC deployment. Use the Windows Command Prompt to install the Windows PMC Adapter.

***Note:** The adapters poll every 60 minutes.*

You must install the Privilege Management adapters using this process. You can optionally choose to automatically assign computers to groups and authorize them in one step using the **GroupID** parameter for the adapters. This is detailed in the following sections.

When Privilege Management computers are managed by the operating system, the PMC adapter is responsible for delivering policies and events between the computer and PMC servers.

If not using the **GroupID** to automatically assign and authorize computer groups, you can assign and authorize computers in PMC.

You can install and automatically authorize Windows machines to connect to PMC using the command line.

There are five parameters for the PMC Adapter:

- **TenantID**: Obtain this value from PMC. Click **Configuration** > **Adapter Installation**. Copy the Tenant ID for this script.
- **InstallationID**: Obtain this value from PMC. Click **Configuration** > **Adapter Installation**. Copy the Installation ID for this script.
- **InstallationKey**: Obtain this value from PMC. Click **Configuration** > **Adapter Installation**. Copy the Installation Key for this script.
- **ServerURI**: This is the URL for PMC. For example, **https://<customerhost>-services.pm.beyondtrust.cloud.com**, where **customerhost** is the DNS name for PMC.

> ***Note:*** *Do not include a port number or slash character on the end of the* ***ServerURI****.*
>
> *For example, neither* ***https://test.pm.beyondtrustcloud.com/*** *nor* ***https://test.pm.beyondtrustcloud.com:8080/*** *will work.*

- **GroupID**: (Optional). If supplied, this automatically authorizes the computer and assigns it to the specified group. If that group does not exist, the computer remains in the pending state. Obtain this value from PMC. Click the group you want to use. The **Group ID** is shown in the **Details** page for the script. Copy the **Group ID** for this script.

Prerequisite

.NET 4.6.2

To install adapters:

> ***Note:*** *Include the* ***GroupID*** *to automatically group and authorize the computer.*

1. Navigate to the location of the adapter installer. By default this is the **AdapterInstallers** folder.
2. Enter the command line with the required attributes and press **Enter**. The adapter installer launches. Proceed through the installation wizard as required.

> ***Example:*** *The line breaks must be removed before you run the script.*

```
msiexec.exe /i "PrivilegeManagementConsoleAdapter_x64.msi"
TENANTID="<TenantID_GUID>"
INSTALLATIONID="<InstallationID>"
INSTALLATIONKEY="<InstallationKey>"
SERVICEURI="<PMC URL>"
GROUPID="<PMC GroupID GUID>"
```

Add the following argument if you don't want the adapter service to start automatically. This option is useful when Privilege Management for Windows and the PMC adapter are being installed on an image that will be reused to create many individual computers. If the adapter is not disabled in this scenario, the PMC adapter will immediately join the PMC instance indicated.

```
SERVICE_STARTUP_TYPE=Disabled
```

You can start the **IC3Adapter** service manually later in the Services.

Example:

```
msiexec.exe /i "PrivilegeManagementConsoleAdapter_x64.msi" TENANTID="6b75f647-d3y7-4391-
9278-002af221cc3f" INSTALLATIONID="08A1CD8F-FAE4-479F-81B4-00751A55EEB8"
INSTALLATIONKEY="ABCDEFGHIJKLMNO" SERVICEURI="https://CUSTOMERHOST-
services.pm.beyondtrustcloud.com" GROUPID="e531374a-55b9-4516-g156-68f5s32f5e57"
SERVICE_STARTUP_TYPE=Disabled
```

CUSTOMERHOST *= the hostname. For example, if the hostname were* ***test****, the desired input would be:*

```
https://test-services.pm.beyondtrustcloud.com
```

For information on how to automatically assign and authorize computer groups, please see "Privilege Management Console Computers" on page 26.

Configure the Windows PMC Adapter

When the PMC Adapter communicates with the PMC portal, it uses HTTPS. If there is a proxy in place that this communication goes through, it must be configured for the PMC Adapter user account, which is separate from the logged on user account.

The computer must be configured to use proxy settings for the machine rather than the individual user. The following registry key needs to be edited to make this change:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings]
```

The Data value must read **0**. This specifies the machine (**1** specifies per user).

Name	Type	Data
ProxySettingsPerUser	REG_DWORD	0

Ensure the iC3Adapter User Has the "User Can Log on as a Service" Right

When you install the PMC Adapter, a user account called **iC3Adapter** is created. The **iC3Adapter** user is granted the right to **Log on as a Service** by the installation process. If you have a Group Policy in place that revokes this permission, ensure the **iC3Adapter** user is excluded, as it requires the **Log on as a Service** right.

For more information, please see the Microsoft Knowledgebase article Add the Log on as a service Right to an Account at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc794944(v=ws.10).

Example:

```
msiexec.exe /i "PrivilegeManagementConsoleAdapter_x64.msi" TENANTID="6b75f647-d3y7-4391-
9278-002af221cc3f" INSTALLATIONID="08A1CD8F-FAE4-479F-81B4-00751A55EEB8"
INSTALLATIONKEY="ABCDEFGHIJKLMNO" SERVICEURI="https://CUSTOMERHOST-
services.pm.beyondtrustcloud.com" GROUPID="e531374a-55b9-4516-g156-68f5s32f5e57"
SERVICE_STARTUP_TYPE=Disabled
```

CUSTOMERHOST *= the hostname. For example, if the hostname were* ***test****, the desired input would be:*

```
https://test-services.pm.beyondtrustcloud.com
```

Install the Mac Adapter

The Mac adapter can be distributed to the computers using the method of your choice, including Mobile Device Management (MDM), such as Jamf or AirWatch.

You can also use the Privilege Management for Mac Rapid Deployment Tool to install the adapter. You can download the Rapid Deployment Tool from the Configuration page.

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

Tip: *Setup Information is available for the Mac adapter on the* ***Configuration*** *page. From the sidebar menu, click the* ***Configuration*** *to view the details.*

The PMC client adapter installers can be found in the **AdapterInstallers** folder of the PMC deployment. Use the Terminal to install the Mac PMC Adapter.

Note: *The adapters poll every 60 minutes.*

You must install the PMC adapters using this process. You can optionally choose to automatically assign computers to groups and authorize them in one step, using the **GroupID** parameter for the adapters. This is detailed in the following sections.

When PMC clients are managed by the operating system, the PMC adapter is responsible for delivering policies and events between the computer and PMC servers.

If you are not using the GroupID to automatically assign and authorize computer groups, you can assign and authorize computers in PMC.

You can install and automatically authorize Mac machines to connect to PMC using the command line.

There are six parameters for the PMC Adapter:

- **TenantID** for your chosen method of authentication. This was recorded when PMC was installed.
- **InstallationID**: You get this from PMC. Click **Configuration** > **Adapter Installation**. Copy the Installation IDfor this script.
- **InstallationKey**: You get this from PMC. Click **Configuration** > **Adapter Installation**. Copy the Installation Key for this script.
- **ServiceURI**: The URL for your PMC portal.

> ***Note:*** *Do not include a port number or slash character on the end of the* ***ServerURI****.*
>
> *For example, neither* ***https://test.pm.beyondtrustcloud.com/*** *nor* ***https://test.pm.beyondtrustcloud.com:8080/*** *will work.*

- **GroupID**: (Optional). If supplied, this will auto authorize the computer and assign it to the specified group. If that group does not exist, the computer will remain in the pending state. You obtain this from PMC.
- **Cacertificateid**: (Optional). The thumbprint of your SSL certificate. If you are using an SSL certificate that is trusted by a global provider, you do not need to add this parameter. If it is not, the SSL certificate must be added to the **System** keychain (not Login). The SSL certificate must also be set to **Trusted** in the **System** keychain.

To install the private key of the SSL Certificate:

> ***Note:*** *You only need to do these steps if your SSL certificate is not issued by a trusted global provider that is preinstalled on the Mac.*

1. Obtain the .pfx portion of your SSL certificate.
2. Double-click the .pfx file to install it into the **Keychain** application on the Mac. You need to enter the password for the SSL certificate. By default the certificate will be placed in the **login** keychain folder.
3. Move the root certificate from the **login** keychain folder to the **System** folder keychain.
4. Set the root certificate to **Always Trust**.
5. Extract the thumbprint of your SSL certificate from the certificate. You need the thumbprint to install the Mac Adapter.

To install adapters:

> ***Note:*** *Include the* ***GroupID*** *to automatically group and authorize the computer.*

> ***Note:*** *Include the* ***Cacertificateid*** *if your SSL certificate is not issued by a trusted global provider.*

1. Navigate to the location of the adapter installer. By default this is the **AdapterInstallers** folder.
2. Mount the DMG and place the PMC Adapter onto the desktop.
3. Run the command line shown as in the example below from the **Terminal**.
4. Once the adapter installer launches, proceed through the installation wizard as required.

> ***Example:*** *The line breaks must be removed before you run the script.*

```
sudo /Avecto_ic3_Adapter_x_x_x/install.sh tenantid="750e85d1-c851-4d56-8c76-b9566250cf1d"
installationid="95a10760-2b96-4a0e-ab65-ed7a5e8f1649"
installationkey="VGhpcyBzZWNyZXQgaTYzIGJlZW4gQmFzZTY0IGVuY29kZWQ="
serviceuri="https://test.ic3.avecto.com" groupid="fcc4022e-12fa-4246-87w8-0de9a1483a68"
cacertificateid="b36b7345ff30aa7fb15fcd985fe2989c3e11aba7"
```

> *For more information, please see "Authorize and Assign Computers to a Group" on page 26.*

Uninstall Privilege Management for Mac

***Note:** The uninstall scripts must be run from their default locations.*

Uninstall Privilege Management

To uninstall Privilege Management locally on a Mac, run the following command:

```
sudo /usr/local/libexec/Avecto/Defendpoint/1.0/uninstall.sh
```

Uninstall the Mac Adapter

To uninstall the Mac adapter, run the following command. After running the uninstall script some related directories remain if they are not empty, such as **/Library/Application Support/Avecto/iC3Adapter**.

```
sudo /usr/local/libexec/Avecto/iC3Adapter/1.0/uninstall_ic3_adapter.sh
```

Remove the Privilege Management Policy

To remove the policy once you have uninstalled Privilege Management, run the following command:

```
sudo rm -rf /etc/defendpoint
```

***Note:** Do not remove the Privilege Management policy unless you have already uninstalled Privilege Management.*

Configure PMC to Connect to the Policy Editor

Configure PMC to allow the Privilege Management MMC snap-in to communicate with the PMC services.

1. Select **Configuration** from the sidebar menu.
2. Under **Settings**, click **MMC Snap-In Installation**.
3. Click the **Remote MMC client access** toggle to enable the feature. Generate a new GUID and enter it here. Click the Refresh button to generate a new GUID. Use the same GUID when you configure the MMC. This is the MMC Client ID in the MMC.

Once you have configured PMC, you must configure the Privilege Management MMC snap-in to communicate with it.

For more information, please see "Configure the Privilege Management MMC PMC snap-in" on page 15.

Configure the Privilege Management MMC PMC snap-in

***Tip:** Setup Information is available for the MMC snap-in on the **Configuration** page. On the sidebar menu, click **Configuration** to view the details.*

You need to install and configure the Privilege Management MMC on the machine you will use to administer PMC policy.

The installation packages differ based on your operating system:

- For 32-bit (x86) systems run **PrivilegeManagementPolicyEditor_x86.exe**.
- For 64-bit (x64) systems run **PrivilegeManagementPolicyEditor_x64.exe**.

For compatible versions, please see the Release Notes at https://www.beyondtrust.com/docs/release-notes/privilege-management/index.htm.

Add and Configure the Privilege Management PMC Snap-in

You need to use the Privilege Management MMC PMC snap-in for the Microsoft Management Console (MMC) to manage policy for computers managed by PMC.

To load the Privilege Management PMC snap-in for the MMC:

1. Run **mmc.exe** from the **Start** menu.
2. Click **File > Add/Remove Snap-in** and select **Privilege Management Settings (PMC**). Click **Add**.
3. Select the **Privilege Management Settings (PMC)** node and click **PMC Connection** under **Settings**.

***Note:** Ensure you install the **Privilege Management Settings (PMC)** snap-in, rather than the **Privilege Management Settings** snap-in.*

The next step is to configure the MMC to connect to PMC.

Setting	What to Enter
Connection	
Server URL	This is the URL for PMC with **443** in the **Port** field. This is shown on the **Finish** tab of the deployment wizard. For example, **https://<customerhost>-services.pm.beyondtrust.cloud.com**, where **customerhost** is the instance hostname for your Privilege Management Console.
Tenant ID	This can be located at **Configuration > Settings > MMC Snap-In Installation** in the PMC Portal.
Authorization Provider	

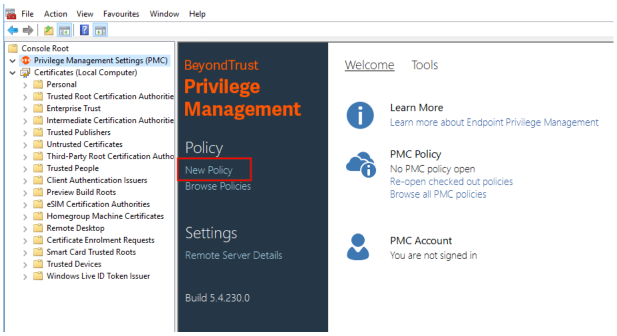
Setting	What to Enter
URL	This is the URL for PMC with **/oauth** appended to it. For example, **https://customerhost-services.pm.beyondtrust.cloud.com**, where **customerhost** is the instance hostname for your Privilege Management Console.
Identification	
MMC Client ID	This can be located at **Configuration > Settings > MMC Snap-In Installation** in the PMC Portal.
Client Return URI	Enter **http://defendpoint-mmc.com**. This string does not resolve but needs to be as stated.
Amend token resource ID	Check this box. This string needs to be **https://api.ic3.avecto.com**. This string does not resolve but needs to be as stated.

For more information, please see "Configure PMC to Connect to the Policy Editor" on page 14.

Confirm Connection to PMC

You should now confirm that you can access PMC from the Privilege Management MMC snap-in.

1. Click **New Policy** in the Privilege Management MMC snap-in.



2. Enter your credentials for PMC when prompted, and then click **Sign in**.
3. When you click **Create**, you are prompted to enter a name for your policy. When you click **PMC Policies**, you are taken to a list of policies in PMC.

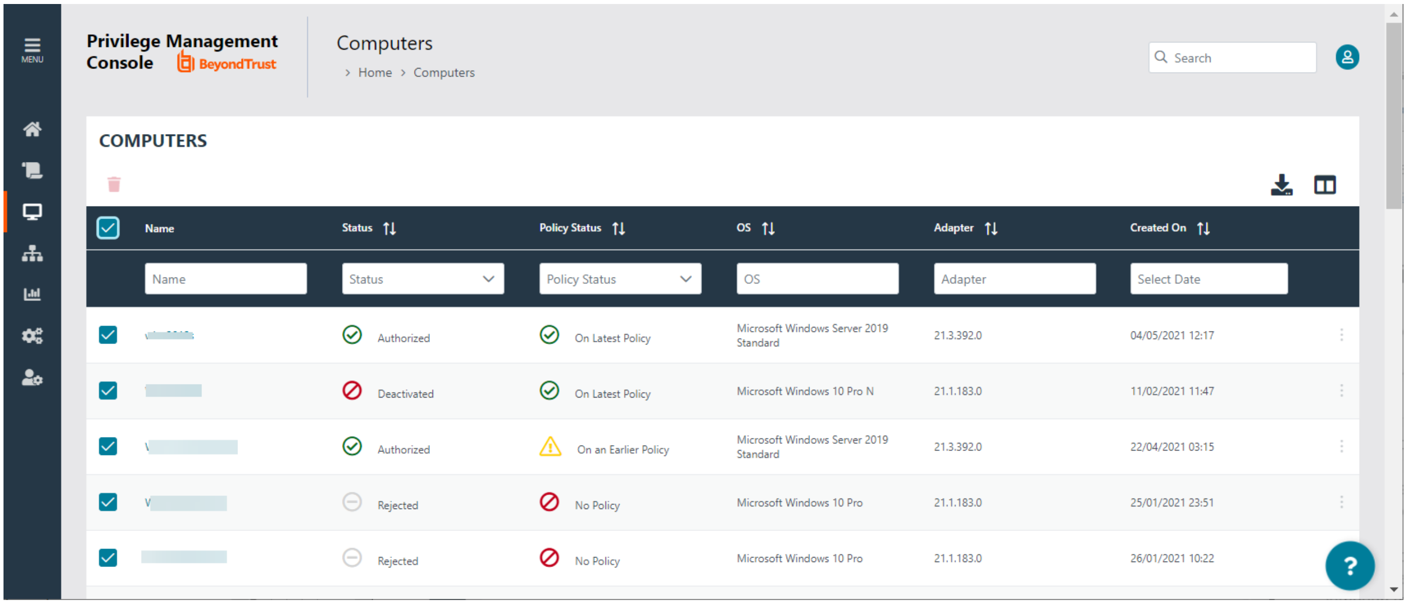
***Note:** If you receive an error connecting to PMC, ensure you have entered the correct options in both PMC and the PMC Privilege Management MMC snap-in.*

Privilege Management Console Grid Behavior

There are several grids in PMC that have similar behavior. The **Computers** grid supports the standard Windows behavior for selecting multiple rows, as you can interact with multiple computers in one action.

Select All

To select all rows, click the check mark beside the **Name** column. If you want to expand the selection, scroll to the bottom of the grid and select a value from the **items per page** list to change how many rows are displayed on each page.

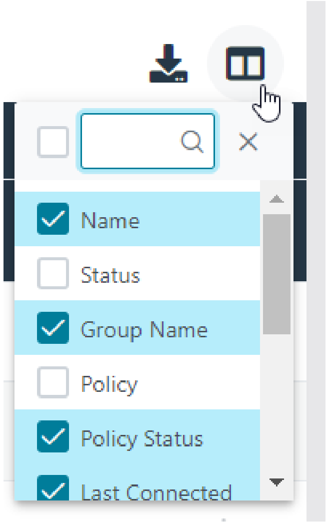


COMPUTERS

☑	Name	Status	Policy Status	OS	Adapter	Created On
	Name	Status	Policy Status	OS	Adapter	Select Date
☑	[redacted]	Authorized	On Latest Policy	Microsoft Windows Server 2019 Standard	21.3.392.0	04/05/2021 12:17
☑	[redacted]	Deactivated	On Latest Policy	Microsoft Windows 10 Pro N	21.1.183.0	11/02/2021 11:47
☑	[redacted]	Authorized	On an Earlier Policy	Microsoft Windows Server 2019 Standard	21.3.392.0	22/04/2021 03:15
☑	[redacted]	Rejected	No Policy	Microsoft Windows 10 Pro	21.1.183.0	25/01/2021 23:51
☑	[redacted]	Rejected	No Policy	Microsoft Windows 10 Pro	21.1.183.0	26/01/2021 10:22

Sort Columns

Click the column icon and select the columns you want to display.

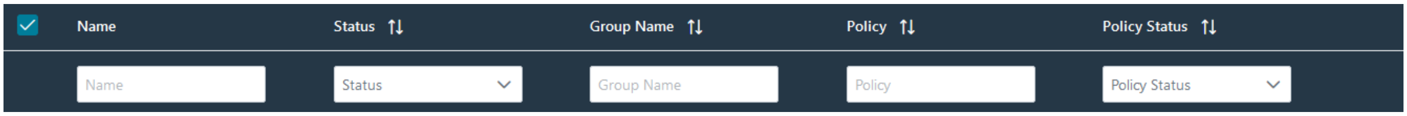


- ☑ Name
- □ Status
- ☑ Group Name
- □ Policy
- ☑ Policy Status
- ☑ Last Connected

Alternatively, you can sort columns independent of each other by clicking the column name. A column has been sorted once its name has changed in color and an up or down arrow icon appears to designate the ascending or descending sorting order.

Filter

You can filter within the grids by using the empty fields at the top of each column. If you enter a string of text in these fields, the results in the grid filter below automatically update to the records that contain that string.



☑	Name ⇅	Status ⇅	Group Name ⇅	Policy ⇅	Policy Status ⇅
	Name	Status ⌄	Group Name	Policy	Policy Status ⌄

The following grids support filtering:

- **Policies**
- **Computers**
- **Computer Groups**
- **Auditing**
- **Users**

Progress and Change Indicators

When PMC is busy performing an action, you see a spinner on the grid to indicate that it's processing.

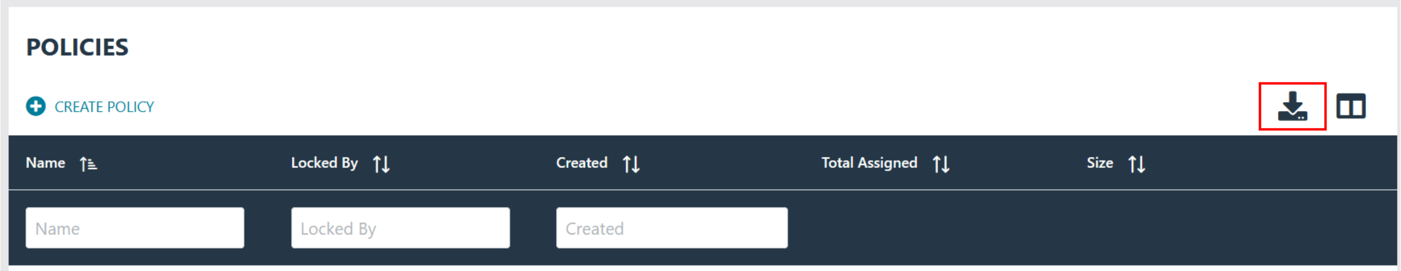
Where actions affect one or more rows, you see a green toaster notification briefly flash across the top right of the grid to indicate that PMC has processed your request.

Error Notifications

If PMC cannot complete an action successfully, it does not make any changes and you get a toaster notification on the top right, next to the search field. PMC does not process a task that it cannot action successfully. The error notification tells you that the action was not successful. You can clear the errors as required from the page that generated the error.

Export to CSV

You can export all grid data results in the currently filtered result set, not just the results which are displayed on the current page, from the **Download records to CSV** icon above the grid.

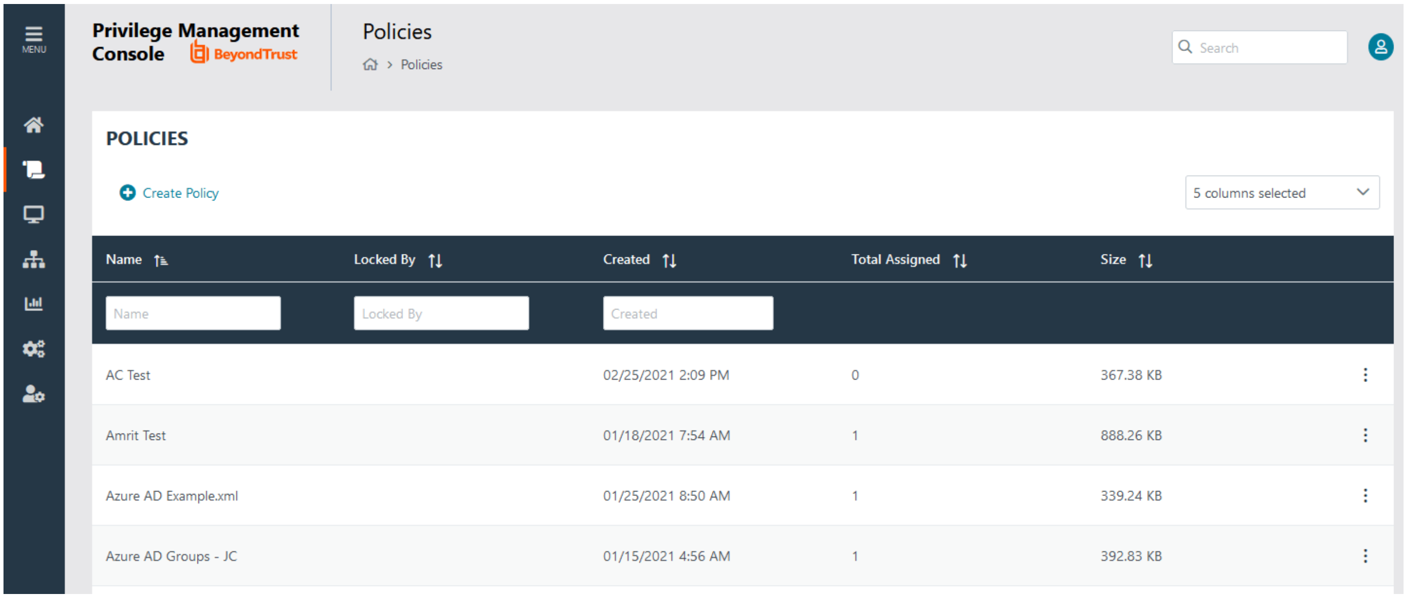


POLICIES

Name	Locked By ⇅	Created ⇅	Total Assigned ⇅	Size ⇅
Name	Locked By	Created		

Privilege Management Console Policies

The **Policies** page allows you to see and interact with the policies being deployed by PMC.



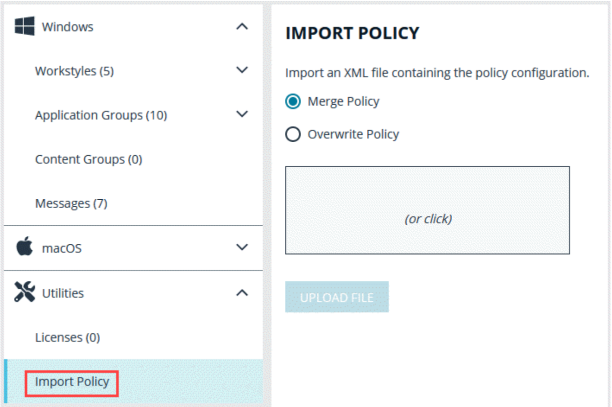
Name	Locked By	Created	Total Assigned	Size
AC Test		02/25/2021 2:09 PM	0	367.38 KB
Amrit Test		01/18/2021 7:54 AM	1	888.26 KB
Azure AD Example.xml		01/25/2021 8:50 AM	1	339.24 KB
Azure AD Groups - JC		01/15/2021 4:56 AM	1	392.83 KB

Upload a File in PMC to Create Policy

You can upload an XML policy file in PMC when you first create the policy, or make edits to the policy at a later time.

Upload XML file for a new policy:

1. Select **Policies** from the sidebar menu.
2. Click **Create Policy** at the top of the **Policies** grid.
3. Select the desired policy template and enter policy details.
4. Click **Create Policy**.
5. On the **Policies Editor**, select **Utilities** > **Import Policy**.
6. Choose either **Merge Policy** or **Overwrite Policy** and click the box to import your XML policy.
7. Click **Upload File**.



Import an XML file containing the policy configuration.

● Merge Policy

○ Overwrite Policy

Upload XML file for an existing policy:

1. Select **Policies** from the sidebar menu.
2. Click the vertical ellipsis icon beside the policy you want to edit.
3. From the dropdown menu, click **Edit**.
4. On the **Policies Editor**, select **Utilities** > **Import Policy**.
5. Choose either Merge Policy or Overwrite Policy and click the box to import your XML policy.
6. Click **Upload File**.

Upload Policy Revision

You can upload a new revision of an existing policy. Policies downloaded from PMC, modified and then reuploaded are recognized as a new revision based on a unique identifier in the XML.

Upload new revision of an existing policy:

1. Select **Policies** from the sidebar menu.
2. Click the vertical ellipsis icon beside the policy you want to edit.
3. From the dropdown menu, select **Revision History**.
4. Click **Upload Revision**. Browse to the XML file and click **Open**. The XML file is uploaded to the portal.
5. The new revision is uploaded, provided the XML validation passes. If the XML policy does not pass validation, the row is highlighted in red and the policy is not uploaded.
6. On the **Auto Assign Policy to Groups** dialog box, select the groups to update with the new policy revision.
7. Select **Apply to Groups**.

Each time the same policy is checked in, the revision of the policy is incremented.

View Policy Details

For a single policy, you can view additional details.

1. Select **Policies** from the sidebar menu.
2. Click the vertical ellipsis beside the appropriate policy and select **Policy Details** from the dropdown menu.
3. The **Details** page allows you to see additional information for the policy and what policy is currently applied to it, if any. You can click **Edit** to change these details.

Download Policy

You can download a policy from PMC in XML format if required.

To download a policy as an XML file:

1. Select **Policies** from the sidebar menu.
2. Click the vertical ellipsis beside the policy you want to edit.
3. From the dropdown menu, select **Download Latest Revision**.

> ***Note:*** *If you want to download a previous revision version, select* ***Revision History*** *from the dropdown menu.*

Edit Properties of Policy

You can edit the details for a policy.

1. Select **Policies** from the sidebar menu.
2. Click the vertical ellipsis beside the appropriate policy and select **Edit Policy** from the dropdown menu.
3. In the Policy Editor, change the properties of the policy, as needed.

4. Select **Save & Unlock**.
5. Optionally, add notes on the changes for future reference.
6. Select **Yes, auto assign latest revision to current groups**.
7. Select **Save & Unlock**.

Assign a Policy to a Group

1. Select **Computer Groups** from the sidebar menu.
2. Click the vertical ellipses icon on the appropriate group's row to expand more options and select **Assign Policy to Group**.
3. Select the policy you want to assign from the dropdown and the associated revision.

> ***Note:*** *You should see a green dialog box appear in the upper corner of the console to confirm that the policy was applied successfully.*

> *For details on how you can control the deployment of your policy, please see "Manage Policy Deployment Settings" on page 75.*

Discard Policy Draft and Undo Check Out in MMC Snap-in

If a policy is checked out using the Privilege Management MMC snap-in, you can force PMC to discard the changes and undo the checkout. You must be an Administrator or Policy Administrator.

To discard draft and undo checkout of a policy:

1. Select **Policies** from the sidebar menu.
2. Click the vertical ellipsis beside the appropriate policy and select **Revert & Discard Changes** from the dropdown menu.
3. Review the warning and click **Revert & Discard** to revert the policy changes; otherwise, click **Cancel**.

Delete a Policy

You can only delete policies if they're not assigned to any group.

To delete a policy:

1. Select **Policies** from the sidebar menu.
2. Click the vertical ellipsis beside the appropriate policy and select **Policy Details** from the dropdown menu.
3. Click **Delete** at the top of the grid.
4. You are prompted to check that you do want to perform this action. Click **Yes** to confirm and discard the policy; otherwise, click **No**.

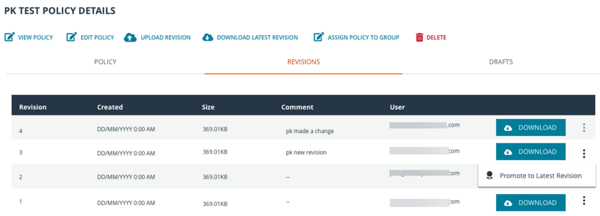
> ***Note:*** *If a policy is already assigned to a group, the **Delete** button will not be available.*

Promote a Policy

If you change a policy and you want to discard those changes, you can promote a previous version of the policy.

To promote a previous version of a policy:

1. Go to the Policy Editor.
2. Find the policy and select **Edit Policy** from the menu.
3. On the **Policy Details** page, select **Revisions**.
4. Select the menu for the policy, and then select **Promote to Latest Revision**.



PK TEST POLICY DETAILS

Revision	Created	Size	Comment	User
4	DD/MM/YYYY 0:00 AM	369.01KB	pk made a change	[redacted].com
3	DD/MM/YYYY 0:00 AM	369.01KB	pk new revision	[redacted].com
2	DD/MM/YYYY 0:00 AM	369.01KB	--	[redacted].com
1	DD/MM/YYYY 0:00 AM	369.01KB	--	[redacted].com

5. On the **Promote Policy to Latest Revision** dialog box, select **Promote to Latest**. You can add notes here for future reference.
6. If the policy is already applied to certain groups you can choose to apply the latest revision now. Select the groups to apply the policy to and select **Apply to Groups**.

Manage Policy in the MMC Snap-in

You manage policy in PMC using the Privilege Management MMC snap-in for PMC.

PMC policies can be viewed, created, drafts saved, checked out to PMC, and checked in from PMC using the Privilege Management snap-in for the MMC.

In addition, you can manually move XML policy files around by downloading them, uploading them, or uploading policy revisions.

Privilege Management Console Policy Management in the MMC

The Privilege Management MMC snap-in allows you to create, edit, check in, and check out policies to the PMC portal.

> *For information on editing Workstyle policy for Windows, please see the Windows Administration Guide at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm.*

Policy Workflow in MMC

Policies are managed on a per-revision basis in PMC. When you create or import a PMC policy in the Privilege Management MMC snap-in, you can save one or more local drafts before you check it into PMC. Revisions are not created when you are working with local drafts and PMC does not have visibility of them.

Each time you check in a policy to PMC from the MMC, a new revision is created. This allows you to revert to an older revision, if required. If you check a policy out and make changes but then change your mind, you can discard your changes and the associated checkout to cancel your original checkout and any changes.

You can check policies in and out from the Privilege Management MMC snap-in as well as create new ones.

There are six user roles for policies:

- Abort
- Create
- Delete
- Modify
- Query
- View

Only users in the Administrators or Policy Administrators group have all of the user roles.

> *For more information, please see "Assign Roles to a User Account" on page 37.*

Computer and Group Locks

Computers or groups are locked when a policy is applied. Rows are locked in the **Computers** or **Groups** grids, respectively.

After all commands are applied, the computer or group will unlock. Once the computer or group is unlocked, you can interact with the computer or group. Subsequent commands are queued by PMC as required.

Create a Policy in the MMC Snap-in

You can create a policy using the functionality in the Privilege Management MMC snap-in.

To create a policy:

1. Click **Create** in the Privilege Management MMC snap-in.
2. Enter a name for the policy and click **OK**. This creates the policy so you can now start editing it. At this stage the policy is in draft, so PMC does not have visibility of it. PMC can only see policies that you have checked in.

> *For information on editing policy for Windows computers, please see the Windows Administration Guide at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm.*

View Policies in the MMC Snap-in

You can view a list of policies that are local to the Privilege Management MMC snap-in, and whether PMC can see the state of them.

To view policies:

1. In the Privilege Management MMC snap-in, if you have a policy checked out and you want to view all policies, click **Browse Policies** in the **Start** section on the left. If you do not have a policy checked out, you can click **Browse all PMC policies** in the **PMC Policy** section.
2. You can perform additional actions such as **Save Draft**, **Check in Changes**, **Discard Draft**, and **View** from this list, depending on your user role and the state of the policy.

Check in a Policy Using the MMC Snap-in

Once you have created or imported a policy, you can check it into PMC. This will create the first revision of the policy if it's new to PMC; otherwise, it will increment the revision of the policy.

To check in a policy:

1. In the Privilege Management MMC snap-in, click **Check in your changes** in the **Policy** section.
2. Add a description of your changes and click **OK**. Your policy is now checked into PMC and is visible in the PMC portal.

Each time the same policy is checked in or uploaded to the Privilege Management MMC snap-in, the revision of the policy is incremented. New revisions of the same policy need to be manually assigned to the group; this is not done automatically.

For more information, please see "Assign a Policy to a Group" on page 21.

Check out a Policy Using the MMC Snap-in

Policies that have been checked into PMC must be checked out to be edited.

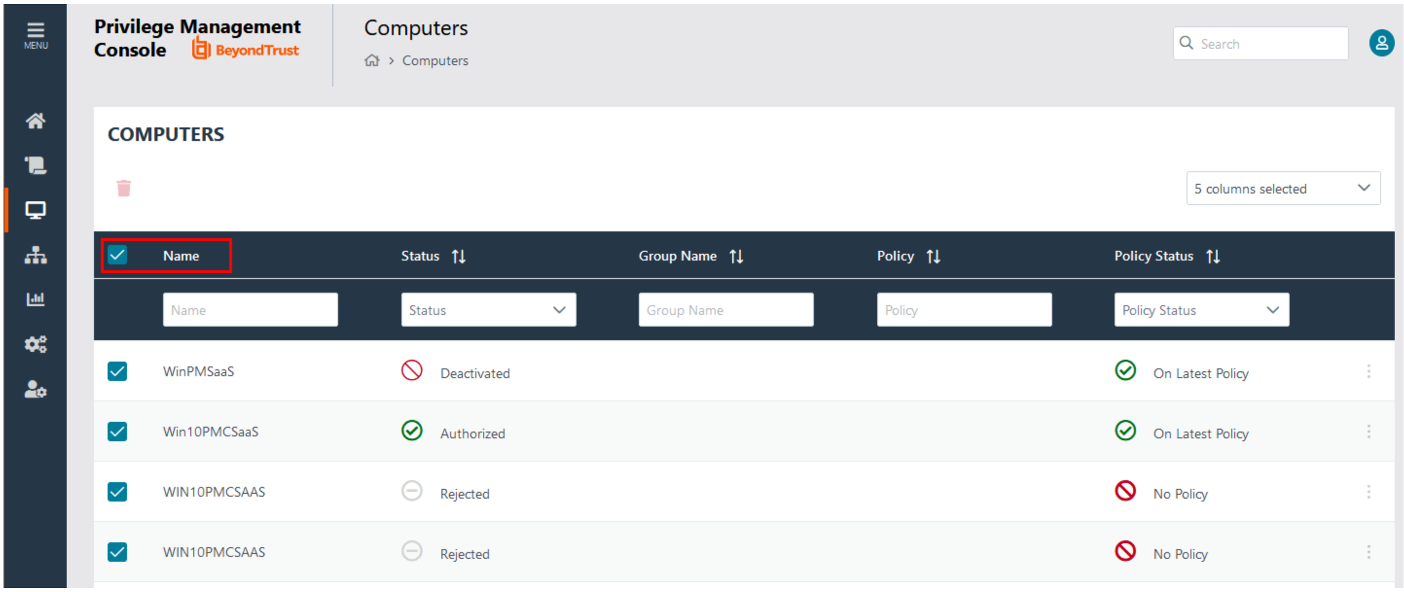
To check out a policy:

1. In the Privilege Management MMC snap-in, click **Browse all PMC policies** in the PMC **Policy** section.
2. Select your policy from the list and click **Check Out**. You can now edit the policy in the Privilege Management MMC snap-in.

Privilege Management Console Computers

The **Computers** page allows you to see and to interact with the end computers being managed by PMC.

To select all currently displayed rows, click the check mark beside the **Name** column. If you want to expand the selection, scroll down to the bottom of the grid and click the dropdown menu beside the page numbers to change how many rows are displayed on each page.



☑	Name	Status	Group Name	Policy	Policy Status
☑	WinPMSaaS	Deactivated			On Latest Policy
☑	Win10PMCSaaS	Authorized			On Latest Policy
☑	WIN10PMCSAAS	Rejected			No Policy
☑	WIN10PMCSAAS	Rejected			No Policy

Authorize and Assign Computers to a Group

You can authorize and assign computers to a group in one step, provided the computers haven't previously been authorized. If they have previously been authorized, then instead follow the steps in the link below to assign computers to a group.

You can see which endpoints have not been authorized by selecting **Pending Activation** from the top of the **Status** column.

1. Select **Computers** from the sidebar menu.
2. Click the computer(s) you want to place in a group and authorize in one step, and then select **Authorise** from the top of the grid.

> ***Note:*** *You can select multiple rows using the standard Windows functionality.*

3. Select the group you want to assign it to from the dropdown group and click **Assign**. If you haven't created any groups yet, you will see only **No Group** in the dropdown.
4. If you have a Default group, it will be selected by default, otherwise you can select the group you want to use from the dropdown menu. Click **Assign**. A toaster notification will briefly flash green at the top of the screen to indicate that PMC has processed your request.

> *For more information, please see the following:*
>
> - *For instructions on assigning computers to a group, "Assign Computers to a Group" on page 28*
> - *For information on the grids and filtering, "Privilege Management Console Grid Behavior" on page 17*

> - *For instructions on creating a group, "Privilege Management Console Groups" on page 31*

Reject Computers Not Authorized

You can reject computers not yet authorized with PMC.

Manual Deactivation

If the computer is already authorized, you can use PMC to manage deactivations manually.

> *For more information, please see "Deactivate Computers" on page 29.*

Automatic Deactivation

Alternatively, you can use PMC to manage deactivations automatically.

Rejected computers are disconnected from PMC and will no longer be able to communicate with PMC. This action can't be reversed unless you reinstall the software on the client computer.

1. Select **Computers** from the sidebar menu.
2. Click the computer you want to reject and click **Reject** from the top of the grid. You are prompted to verify that you want to continue with the rejection of the computer. Click **Reject Anyway** to proceed; otherwise, click **Cancel**.

> *For more information, please see "Computer Deactivation Settings" on page 101.*

View Details on an Computer

For a single computer you can view additional details.

1. Select **Computers** from the sidebar menu.
2. Click the vertical ellipsis icon on the row of the computer you want to view the details of and select **View Computer Details**.

The **Computer Details** screen includes additional information, including **Authorization Status**, **Deactivation Type**, **Computer Deactivated**, and **Computer Authorized** timestamps where applicable.

You can also view information about the computer, the name of the policy, and the version that is applied.

Update

You can request a computer to send its updated information by clicking **Update Computer Details**. This action gets the latest information from the computer.

1. Select **Computers** from the sidebar menu.
2. Click the vertical ellipsis icon on the row of the computer you want to update and select **Update Computer Details**.

Apply Policy

If you want to apply a policy update to a specific computer, you can do so here.

On the **Computer Details** page, click **Policy**. Click the Policy name to access the **Policy Detail** section. From here, you can edit the policy as well as upload a new revision.

For more information, please see "Privilege Management Console Policies" on page 19

Computer Logs

1. On the **Computer Details** screen, click **Logs**. This shows you a list of logs that have previously been requested. To get a new set of logs from the computer, click **Request Logs**.
2. PMC will request the logs from the computer and you can view them when this request is returned. The next time the computer connects to PMC, it will retrieve the logs.

Command Log

On the **Computer Details** screen, click **Command Log**. This shows you a list of commands that have been communicated between PMC and the computer.

Assign Computers to a Group

1. Select **Computers** from the sidebar menu.
2. Click the vertical ellipsis icon on the row of the appropriate computer.
3. From the dropdown menu, select **Edit Group**.
4. Select a group from the new dropdown menu and click **Save Group Assignment**. A toaster notification will appear and flash green to indicate that PMC has processed your request.

Note: *If you haven't created any groups yet, you will only see* ***No Group*** *in the dropdown menu.*

For more information on creating a group in PMC, please see "Create a Group" on page 31.

Clear a Computer from a Group

1. Select **Computers** from the sidebar menu.
2. Click the vertical ellipsis icon on the row of the appropriate computer.
3. From the dropdown menu, select **Edit Group**.
4. Click **Clear Group Assignment**.

Since policies are assigned to groups rather than to individual computers, if you clear a computer from a group, the policy on that computer is also cleared. The policy assignment to the wider group is not affected.

View Duplicate Computers

PMC can track duplicate computers. A duplicate is one that has the same host name as another computer but has not connected to PMC as recently. PMC does not do any additional processing to computers that are flagged as duplicates and they continue to receive policy from PMC.

Duplicate computers are hidden by default in the **Computers** grid. You can filter on duplicate computers using the grid filter and adding the column called **Total Duplicates**. In the **Total Duplicates** column, you can filter to a range of numbers.

Deduplication must be set on the **Configuration** page, on the **Policy & Computer Settings** tab.

> *For more information, please see "Computer Deduplication Settings" on page 102.*

Deactivate Computers

Computers can be automatically deactivated by PMC if you choose to enable the functionality.

You can also manually deactivate a computer that has previously been authorized by PMC.

Deactivated computers are disconnected from PMC and will no longer be able to communicate with PMC. This action can't be reversed unless you reinstall the software on the client computer.

1. Select **Computers** from the sidebar menu.
2. Click the computer you want to deactivate and click **Deactivate**. You are prompted to verify if you want to continue with the deactivation of the computer. Click **Deactivate Anyway** to proceed; otherwise, click **Cancel**.

> *For more information, please see the following:*
> - *"Computer Deactivation Settings" on page 101*
> - *If the computer hasn't been authorized, "Reject Computers Not Authorized" on page 27*

Delete Deactivated Computers

If a computer is deactivated, it can be deleted from the Privilege Management Console database.

1. Click on the row for the computer you want to delete.
2. Click **Delete** at the top of the grid.

"Update Policy on All" Option

This option is only available if you have manual deployment set in the **Policy Deployment Settings**. This allows you to manually deploy the policy to all computers. The deployment will be spread across the number of minutes you define in the **Policy Deployment Settings**.

1. Select **Computers** from the sidebar menu.
2. Select the computers you want to update, and then click **Update**. You are prompted to check you want to continue with updating the policy on all computer(s). Click **Update Policy on All** to proceed; otherwise, click **Cancel**.

For more information, please see "Policy Deployment Settings in Privilege Management Console" on page 75.

"Update Policy on Selected" Option

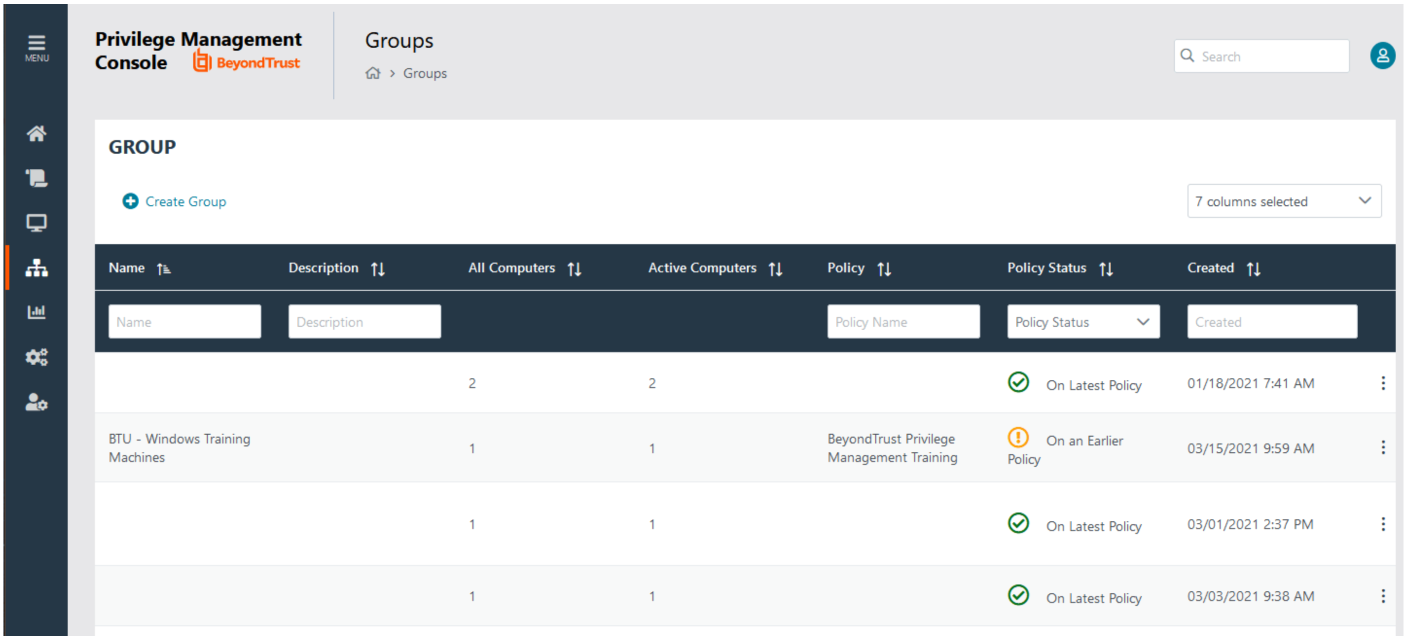
This option is only available if you have manual deployment set in the **Policy Deployment Settings**. This allows you to manually deploy to the selected computers. The deployment will be spread across the number of minutes you define in the **Policy Deployment Settings**.

1. Select **Computers** from the sidebar menu.
2. Select the computers you want to update, and then click **Update**. You are prompted to check you want to continue with updating the policy. Click **Update Policy Anyway** to proceed; otherwise, click **Cancel**.

For more information, please see "Policy Deployment Settings in Privilege Management Console" on page 75.

Privilege Management Console Groups

Groups contain one or more computers. A policy is assigned to a group.



Name	Description	All Computers	Active Computers	Policy	Policy Status	Created
		2	2		✓ On Latest Policy	01/18/2021 7:41 AM
BTU - Windows Training Machines		1	1	BeyondTrust Privilege Management Training	! On an Earlier Policy	03/15/2021 9:59 AM
		1	1		✓ On Latest Policy	03/01/2021 2:37 PM
		1	1		✓ On Latest Policy	03/03/2021 9:38 AM

You can perform the following tasks on the **Groups** page:

- Create a group
- View group details
- Edit group properties
- Set the Default Group
- Assign a policy to a group
- Delete a group

Create a Group

A group is a collection of computers to which a policy can be assigned.

1. Select **Computer Groups** from the sidebar menu.
2. Click **Create Group**.
3. Enter a **Group Name**. The **Description** field is optional.
4. Click **Submit**. Your group is created and appears in the grid list below.

Once the group is created, you can set it as the Default group. If set, the Default group will be selected by default when you add one or more computers to a group. To set the group as the Default group, select the desired group name, and then click **Set Default** at the top of the **Groups** grid.

View the Details of a Group

1. Select **Computer Groups** from the sidebar menu.
2. Click the vertical ellipses icon on the appropriate group's row to expand more options and select **View Group Details**.
3. The **Group Details** page allows you to see additional information for the group and what policy is currently applied to it, if any. You can click **Edit Group** to change these details.

> *For more information, please see "Edit Properties of a User Account" on page 36.*

Edit Properties of a Group

1. Select **Computer Groups** from the sidebar menu.
2. Click the vertical ellipsis icon on the appropriate group's row to expand more options and select **View Group Details**.
3. Select **Edit Group** at the top of the grid.
4. Change the **Group Name**, and **Description** as required, and then click **Save Group**.

Changing the details of a group, including the name, does not affect the computers that are added to the group, or the policy delivered to those computers.

Set a Default Group

1. Select **Computer Groups** from the sidebar menu.
2. Click the vertical ellipsis icon on the appropriate group's row to expand more options and select **Set Default**.
3. A prompt briefly appears and flashes green to indicate that PMC has processed your request and the new default group now has a **(default)** indicator beside its name to show the new status.

Computers being added to the system do not join the Default group if no group is specified at install time.

> *For more information, please see "Create Groups and Assign Policy" on page 8.*

Assign a Policy to a Group

Assigning a policy to a group will allow you to manage computers in that group with the policy.

1. Select **Computer Groups** from the sidebar menu.
2. Click the vertical ellipsis icon on the appropriate group's row to expand more options and select **Edit Policy Assignment**.
3. Choose the policy you want to be assigned to the group from the dropdown menu as well as which revision of the policy is needed.
4. Click **Save Policy Assignment** to assign that policy to the group. A prompt briefly appears and flashes green to indicate that PMC has processed your request.

Clear a Policy from a Group

Computers in the group will have the policy removed when you clear a policy from a group.

1. Select **Computer Groups** from the sidebar menu.
2. Click the vertical ellipsis icon on the appropriate group's row to expand more options and select **Edit Policy Assignment**.
3. Click **Clear Policy Assignment** to remove the policy from the group.
4. You are notified how many computers will be affected by the change. Click **Clear Policy Assignment** to clear the policy; otherwise click **Cancel**.

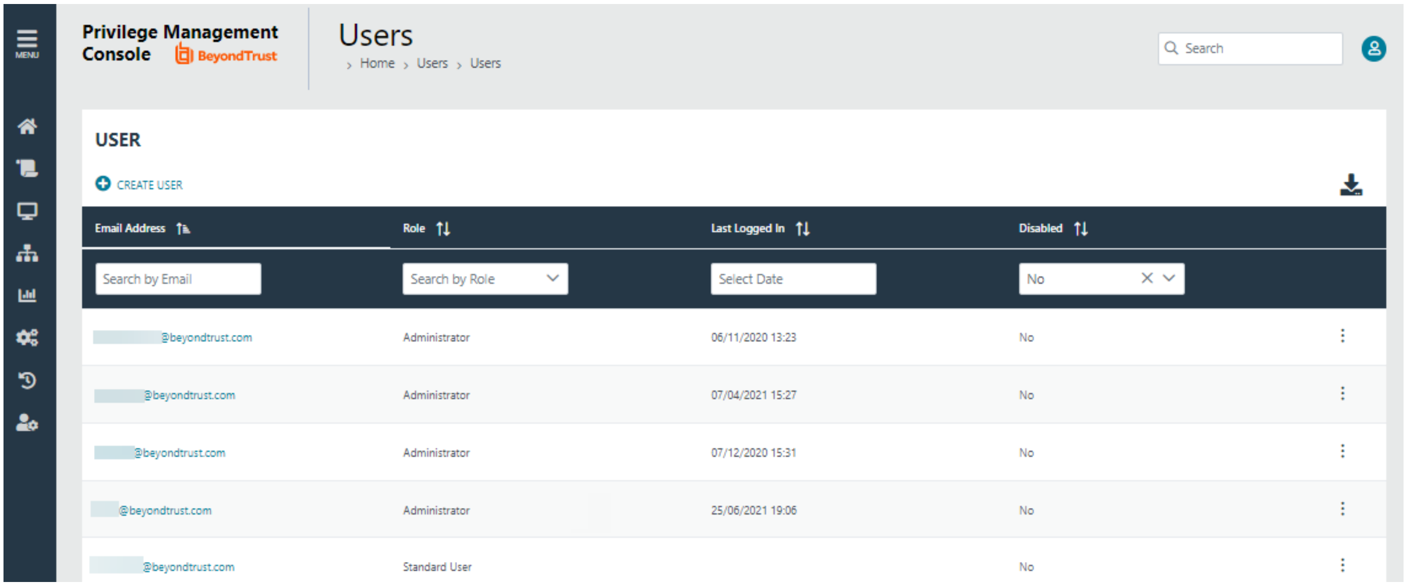
Delete a Group

You can only delete groups that do not have any computers assigned to them. Groups can be deleted if they have a policy assigned to them.

1. Select **Computer Groups** from the sidebar menu.
2. Click the vertical ellipsis icon on the appropriate group's row to expand more options and select **Delete**.
3. You are notified to confirm the decision. Click **Delete Group** to delete the group; otherwise, click **Cancel**.

Manage User Accounts

Each user in PMC must exist in your authentication provider. Each user is assigned a role which determines what actions they are allowed to perform in the PMC portal and Privilege Management MMC snap-in.



Email Address	Role	Last Logged In	Disabled
Search by Email	Search by Role	Select Date	No
[redacted]@beyondtrust.com	Administrator	06/11/2020 13:23	No
[redacted]@beyondtrust.com	Administrator	07/04/2021 15:27	No
[redacted]@beyondtrust.com	Administrator	07/12/2020 15:31	No
[redacted]@beyondtrust.com	Administrator	25/06/2021 19:06	No
[redacted]@beyondtrust.com	Standard User		No

Create a User Account in Privilege Management Console

Once the initial administrator account has been created and authorized, you can create additional user accounts in PMC with whichever roles are needed. You can also create future accounts with the **Administrator** role by following the same process outlined below.

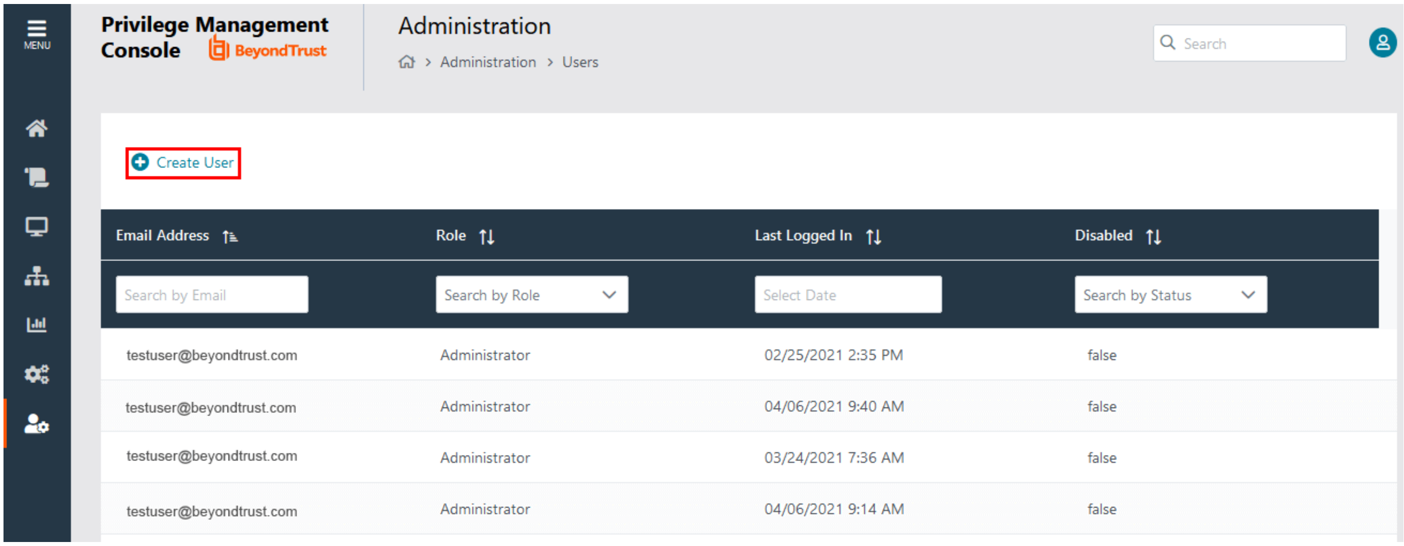
IMPORTANT!

The user needs to exist in your authorization provider before you add that user in PMC. Currently, ADFS and Azure AD are supported providers. For more information about setting up a connection to Azure AD, please see "Register an Azure Tenant" on page 117.

Create a User Account

Note: *This workflow has been tested and is supported by Azure AD. Other providers may work, but have not yet been tested.*

1. Select **Users** from the sidebar menu, and then select **User Management**.
2. Click **Create User** at the top of the grid.



Email Address	Role	Last Logged In	Disabled
Search by Email	Search by Role	Select Date	Search by Status
testuser@beyondtrust.com	Administrator	02/25/2021 2:35 PM	false
testuser@beyondtrust.com	Administrator	04/06/2021 9:40 AM	false
testuser@beyondtrust.com	Administrator	03/24/2021 7:36 AM	false
testuser@beyondtrust.com	Administrator	04/06/2021 9:14 AM	false

3. Enter your email address.

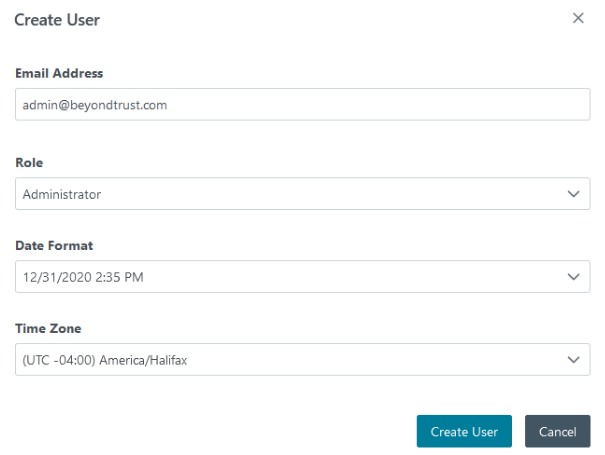
   For Active Directory Federation Services (ADFS) this must take the form:

   ```
   <username>@<ADFS Domain>.com
   ```

   For Azure AD this must take the form:

   ```
   <username>@<tenantname>.onmicrosoft.com
   ```

4. Enter the user's information into the fields in the **Create User** box that appears on the new page.
   - Enter the user's **Email Address**.
   - Select a **Role** for the new user.
   - Choose the **Time & Date** format for the new user and their appropriate **Time Zone** from the dropdown menu.
5. Click **Create User** to create your user.



Email Address: admin@beyondtrust.com

Role: Administrator

Date Format: 12/31/2020 2:35 PM

Time Zone: (UTC -04:00) America/Halifax

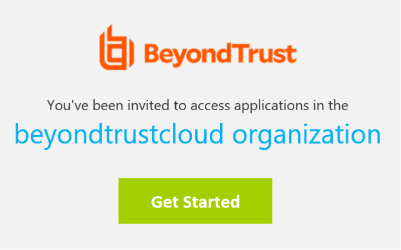
You can add a domain in the **Configuration > Domain Settings** page.

For more information, please see "Add a Domain" on page 102.

Registration and User Confirmation

Once a user account has been created in PMC, an automated email reponse should be sent to the user's email address that was provided during the creation process.

1. Navigate to your email application and look for a Microsoft Invitation that will grant you access to PMC.
2. Click the **Get Started** button in the email to be directed to the invitation landing page.
3. Review permissions and click **Accept** to continue the process.
4. Log in using your credentials.



BeyondTrust

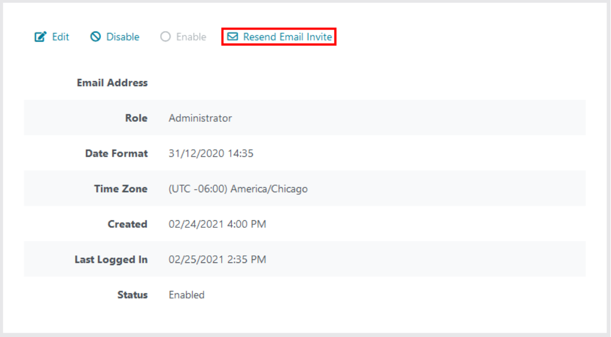
You've been invited to access applications in the
beyondtrustcloud organization

Resend User Invites

An email invitation can be resent to a user that has not accepted their invite to the PMC Portal.

1. From the **Users** page, find the corresponding user in the list of emails.
2. Click the vertical ellipsis icon to open a dropdown list of actions.
3. Select **Resend Email Invite**.

> ***Note:*** *There is no limit on how many times an invitation can be sent to a user.*



Email Address	
Role	Administrator
Date Format	31/12/2020 14:35
Time Zone	(UTC -06:00) America/Chicago
Created	02/24/2021 4:00 PM
Last Logged In	02/25/2021 2:35 PM
Status	Enabled

View Details of a User Account

1. Select **Users** from the sidebar menu, and then select **User Management**.
2. Find the appropriate user in the list and click the vertical ellipsis icon. From the dropdown menu, select **View User Details**. This section shows you the details for the user. You can also edit the details of the user here.

> *For more information, please see "Edit Properties of a User Account" on page 36.*

Edit Properties of a User Account

1. Select **Users** from the sidebar menu, and then select **User Management**.
2. Find the appropriate user in the list and click the vertical ellipsis icon. From the dropdown menu, select **View User Details**.
3. Click **Edit User**. This section allows you to edit the details for the user. You can edit details such as the account name, email address, the time and date format, as well as the time zone.
4. Click **Save User** to save your changes.

Note: *After changing either the date/time format or the time zone, be sure to log out and back in again for the changes to take effect.*

Assign Roles to a User Account

1. Select **Users** from the sidebar menu, and then click **User Management**.

Tip: *For an overview of the roles and a comparison of their access levels, click* ***User Roles****.*

2. Find the user you want to assign a new role to, and then click the vertical ellipsis icon at the end of the row. Select **View User Details**.
3. At the top of the grid, click **Edit User**.
4. Select the appropriate role for the user from the dropdown menu under **Role**.
5. Click **Save User** to save your changes.

Disable a User Account

1. Select **Users** from the sidebar menu, and then select **User Management**.
2. Find the appropriate user in the list and click the vertical ellipsis icon. From the dropdown menu, select **Disable**.
3. You are prompted to confirm if you want to disable the user. Click **Disable Anyway** to disable the user; otherwise, click **Cancel**. You can enable the user again later, if required. The row flashes green to indicate that PMC has processed your request and the user is removed from the grid if you are using the default view.

Note: *To view users that are disabled, click the dropdown menu for the* ***Disabled*** *column of the* ***Users*** *grid and select* ***Yes****.*

For more information, please see "Enable a User Account" on page 37.

Enable a User Account

Disabled users are not shown by default. To view users that are disabled, click the dropdown menu for the **Disabled** column of the **Users** grid and select **Yes**.

1. Select **Users** from the sidebar menu, and then select **User Management**.
2. Find the appropriate user in the list and click the vertical ellipsis icon. From the dropdown menu, select **Enable**.
3. The row briefly flashes green to indicate that PMC has processed your request and the user is now enabled.

User Roles

Each user in PMC has an associated user role. You can view the roles by navigating to **Users > User Roles**.

There are five user roles:

- Administrator
- Computer Administrator
- Policy administrator
- Policy editor
- Standard user

Each user role has various permissions across 11 areas:

- Computer
- Dashboard
- Enterprise reports
- Group
- Policy
- Policy draft
- Remote access settings
- Role
- Settings
- Task
- User

***Note:** Menu items and icons that appear in the left panel depend on which user role is assigned to a user. For example, the **Configuration** and **Auditing** menu options are not visible to the **Standard User** role.*

PMC displays which permissions each user role has.

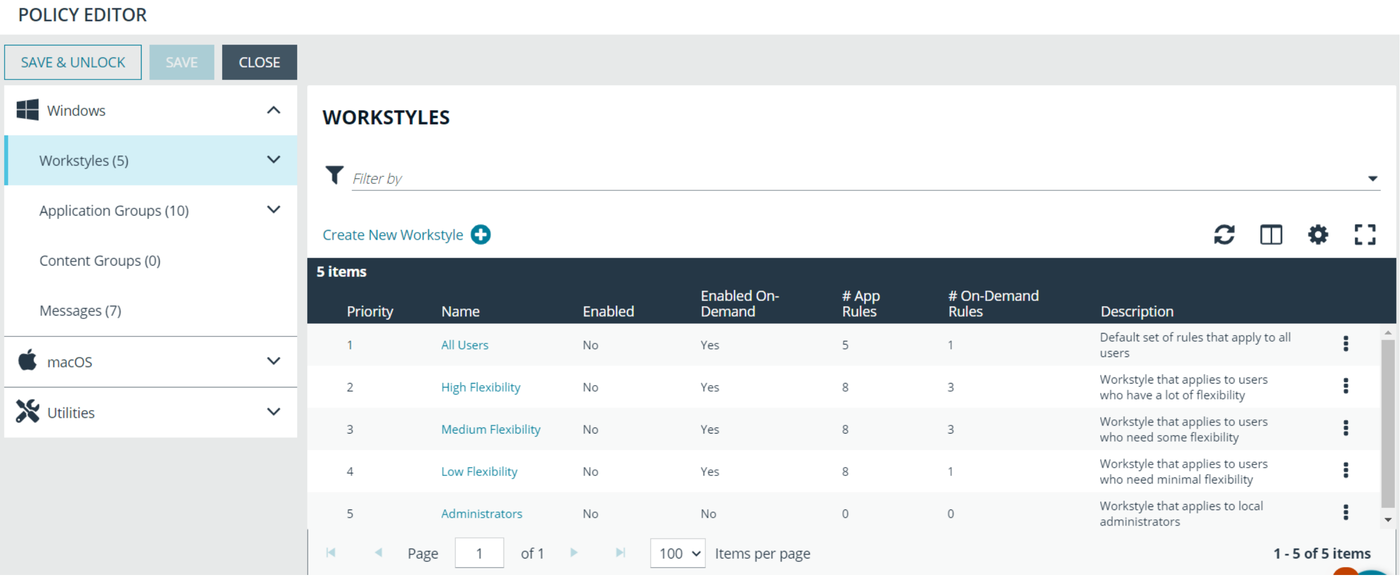
Get Started With the Policy Editor

This section provides information on getting started with the Policy Editor. Details include accessing the Policy Editor, creating a policy using QuickStart template, and editing a policy.

> ***Note:*** *You cannot edit policy in the Privilege Management Policy Editor and Privilege Management Cloud Policy Editor at the same time.*

Access the Policy Editor

1. Log in to PMC and select Policies from the sidebar menu.
2. Click a policy in the list, and then select **Edit and Lock Policy**.



Priority	Name	Enabled	Enabled On-Demand	# App Rules	# On-Demand Rules	Description
1	All Users	No	Yes	5	1	Default set of rules that apply to all users
2	High Flexibility	No	Yes	8	3	Workstyle that applies to users who have a lot of flexibility
3	Medium Flexibility	No	Yes	8	3	Workstyle that applies to users who need some flexibility
4	Low Flexibility	No	Yes	8	1	Workstyle that applies to users who need minimal flexibility
5	Administrators	No	No	0	0	Workstyle that applies to local administrators

> ***Tip:*** *For quick access to the **Workstyles Summary Page**, hover over and click the hyperlink for the appropriate Workstyle name.*

Overview of Policy Editor Components

Workstyles

Workstyles are used to assign Application Rules for a specific user, or group of users.

Application Groups

Application Groups are used by Workstyles to group applications together to apply certain Privilege Management behavior.

Content Groups

Content groups are used by Workstyles to group content together to apply certain Privilege Management behavior.

Messages

Messages are used by Workstyles to provide information to the end user when Privilege Management has applied certain behavior that you've defined and need to notify the end user.

Utilities

The Policy Editor provides some useful tools to help with managing policies, including an import policy tool and a license management tool.

Create a Policy

1. Log on to the PMC and select Policies from the sidebar menu.
2. Click **Create Policy** at the top of the grid.
3. Select one of the following:
   - **QuickStart for Windows**: A preconfigured template with Workstyles, Application Groups, messages, and Custom Tokens already configured.
   - **QuickStart for Mac**: A preconfigured template with Workstyles, Application Groups, and messages already configured.
   - **Server Roles**: The Server Roles policy contains Workstyles, Application Groups, and Content Groups to manage different server roles such as DHCP, DNS, IIS, and Print Servers.
   - **Blank**: Select to configure a policy from scratch. There are no preconfigured settings in this template.
4. Enter a name and description.
5. Click **Create Policy**.

The Policy Editor opens to the **Workstyles** page. At this point you must configure the Workstyle, Application Groups, Application Rules and other policy configuration as required for your organization.

Use the QuickStart for Windows or Mac Template

To get started quickly using the Policy Editor, create a new policy using either the **QuickStart For Windows** template, or the **Quickstart For Mac** template.

Both QuickStart templates for Windows and Mac policies contain Workstyles, Application Groups, Messages, and Custom Tokens configured with Privilege Management and Application Control. The QuickStart policy is designed from BeyondTrust's experiences of implementing the solution across thousands of customers, and is intended to balance security with user freedom. As every environment is different, we recommend you thoroughly test this configuration to ensure it complies with the requirements of your organization.

Customize the QuickStart Policy

Before deploying the QuickStart policy to your users, you need to make some company-specific customizations to the standard template.

At a minimum you need to:

- Configure the users or groups that can authorize requests that trigger messages.
- Assign users and groups to the high, medium, and low flexibility Workstyles.

- Populate the **Block - Blocklisted Apps** Application Group with any applications that you want to block for all users.
- Set your shared key so you can generate a Privilege Management Response code.

QuickStart Template Summary

This section provides information about the properties for the Windows and Mac QuickStart templates, including the Workstyles and Application Groups that comprise the template.

Workstyles

All Users

This Workstyle contains a set of default rules that apply to all standard users regardless of the level of flexibility they need.

The **All Users** Workstyle contains rules to:

- Block any applications in the **Block - Blocklisted Apps** group
- Allow Privilege Management Support tools
- Allow standard Windows functions, business applications, and applications installed through trusted deployment tools to run with admin rights (Windows QuickStart template)
- Allow standard Mac functions, business applications, and applications installed through trusted deployment tools to run with admin rights (Mac QuickStart template)
- Allow approved standard user applications to run passively

High Flexibility

This Workstyle is designed for users that require a lot of flexibility, such as developers.

The **High Flexibility** Workstyle contains rules to:

- Allow known business applications and operating system functions to run.
- Allow users to run signed applications with admin rights.
- Allow users to run unknown applications with admin rights once they confirm that the application should be elevated.
- Allow applications that are in the **Add Admin – High Flexibility** group to run with admin rights.
- Allow unknown business application and operating system functions to run on-demand.

Medium Flexibility

This Workstyle is designed for users that require some flexibility, such as sales engineers.

The **Medium Flexibility** Workstyle contains rules to:

- Allow known business applications and operating system functions to run.
- Allow users to run signed applications with admin rights once they confirm that the application should be elevated.
- Prompt users to provide a reason before they can run unknown applications with admin rights .
- Allow applications that are in the **Add Admin – Medium Flexibility** group to run with admin rights.
- Allow unknown business application and operating system functions to run on-demand.
- Restricted OS functions that require admin rights are prevented and require support interaction.

Low Flexibility

This Workstyle is designed for users that don't require much flexibility, such as helpdesk operators.

The **Low Flexibility** Workstyle contains rules to:

- Prompt users to contact support if a trusted or untrusted application requests admin rights.
- Prompt users to contact support if an unknown application tries to run.
- Allow known approved business applications and operating system functions to run (Windows only).

Administrators

This Workstyle provides visibility on the Administrator accounts in use in the estate.

The Administrators workstyle contains general rules to:

- Capture user and host information
- Block users from modifying local privileged group memberships.

Application Groups

The Application Groups that are prefixed with **(Default)** or **(Recommended)** are hidden by default and do not need to be altered.

- **Add Admin – General (Business Apps):** Contains applications that are approved for elevation for all users, regardless of their flexibility level.
- **Add Admin – General (Windows Functions):** Contains operating system functions that are approved for elevation for all users.
- **Add Admin – High Flexibility:** Contains the applications that require admin rights that should only be provided to the high flexibility users.
- **Add Admin – Low Flexibility:** Contains the applications that require admin rights that should only be provided to the low flexibility users.
- **Add Admin – Medium Flexibility:** Contains the applications that require admin rights that should only be provided to the medium flexibility users.
- **Passive - High Business Apps**
- **Passive - Medium Business Apps**
- **Passive - Low Business Apps**
- **Block - Blocklisted Apps:** This group contains applications that are blocked for all users.
- **Passive - All Users Functions & Apps:** Contains trusted applications, tasks and scripts that should execute as a standard user.
- **(Default) Any Application:** Contains all application types and is used as a catch-all for unknown applications.
- **(Default) Any Trusted & Signed UAC Prompt:** Contains signed (trusted ownership) application types that request admin rights.
- **(Default) Any UAC Prompt:** This group contains applications types that request admin rights.
- **(Default) Privilege Management Tools:** This group is used to provide access to a BeyondTrust executable that collects Privilege Management for Windows troubleshooting information.
- **(Default) Child Processes of TraceConfig.exe**
- **(Default) Signed UAC Prompt:** Contains signed (trusted ownership) application types that request admin rights.
- **(Default) Software Deployment Tool Installs:** Contains applications that can be installed by deployment tools such as System Center Configuration Manager (SCCM).
- **(Recommended) Restricted Functions:** This group contains OS applications and consoles that are used for system administration and trigger UAC when they are executed.
- **(Recommended) Restricted Functions (On Demand):** This group contains OS applications and consoles that are used for system administration.
- **(Default) Trusted Parent Processes**

Messages

The following messages are created as part of the QuickStart policy and are used by some of the Application Rules:

- **Allow Message (Authentication):** Asks the user to provide a reason and enter their password before the application runs with admin rights.
- **Allow Message (Select Reason):** Asks the user to select a reason from a dropdown menu before the application runs with admin rights.
- **Allow Message (Support Desk):** Presents the user with a challenge code and asks them to obtain authorization from the support desk. Support can either provide a response code or a designated, authorized user can enter their login details to approve the request.
- **Allow Message (Yes / No):** Asks the user to confirm that they want to proceed to run an application with admin rights.
- **Block Message:** Warns the user that an application has been blocked.
- **Block Notification:** Notifies the user that an application has been blocked and submitted for analysis.
- **Notification (Trusted):** Notifies the user that an application has been trusted.

Use the Server Role Template

The Server Roles policy contains Workstyles, Application Groups, and Content Groups to manage different server roles such as DHCP, DNS, IIS, and Print Servers.

Server Roles Template Summary

This template policy contains the following elements.

Workstyles

- Server Role - Active Directory - Template
- Server Role - DHCP - Template
- Server Role - DNS - Template
- Server Role - File Services - Template
- Server Role - Hyper V - Template
- Server Role - IIS - Template
- Server Role - Print Services - Template
- Server Role - Windows General - Template

Application Groups

- Server Role - Active Directory - Server 2008R2
- Server Role - DHCP - Server 2008R2
- Server Role - DNS - Server 2008R2
- Server Role - File Services - Server 2008R2
- Server Role - General Tasks - Server 2008R2
- Server Role - Hyper V - Server 2008R2
- Server Role - IIS - Server 2008R2
- Server Role - Print Services - Server 2008R2

Content Groups

- AD Management
- Hosts Management
- IIS Management
- Printer Management
- Public Desktop

Edit Policy

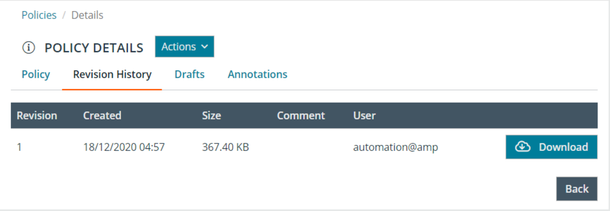
When you edit a policy, the policy is locked. Other policy administrators cannot access the policy to change the properties when the status is **Locked**.

1. Select **Policies** from the sidebar menu.
2. Find the policy in the list, and click the vertical ellipsis icon to expand another menu.
3. Select **Edit & Lock Policy**.
4. On the **Policy Editor** page, go to the policy property you want to change.
5. Click **Save** to save a draft of the policy. Clicking **Save** allows you to keep the Policy Editor open to continue changing the policy.
6. After you finish all updates to the policy, click **Save & Unlock** to save a new revision of the policy.

Policy Revisions and Drafts

You can review the history of revisions and drafts on the **Policy Details** page.

1. Click the link for the policy.
2. Click the **Revision History** tab or **Drafts** tab to view more information about the changes to the policy.



Revision	Created	Size	Comment	User	
1	18/12/2020 04:57	367.40 KB		automation@amp	Download

Unlock a Policy

A policy locked by a user can be unlocked. The policy is reverted to the previous version.

After unlocking the policy, the user account that locked the policy can no longer save or check in changes to that policy.

To unlock and discard the changes to a policy:

1. Select **Policies** from the sidebar menu.
2. Right-click the locked policy, and then click **Revert & Discard Changes**.
3. Click **Continue Anyway** to discard the draft and revert the policy version; otherwise, click **Cancel**.

Edit Policy Properties

You can change the name and description for a policy. The name and description cannot be changed if the policy is locked.

1. Select **Policies** from the sidebar menu.
2. Select the vertical ellipses menu for the policy, and then select **Edit Policy Properties**.

3. Change the properties, and then click **Edit**.

Use the Policy Editor to Manage Policy

This section provides information on editing the various components of a policy, including Workstyles, Application Rules, and Application Groups.

Workstyles

Policy Editor Workstyles are used to assign Application Groups for a specific user, or group of users.

Create a Workstyle

A Workstyle can include the following components: Application Rules, On-Demand Application Rules, Trusted Application Protection (DLL), content rules, general rules, and filters.

Trusted Application Protection (DLL), content rules, general rules are not currently available. You can use the MMC Policy Editor to manage these components.

Workstyle Summary

The **Workstyle Summary** pane provides a high-level overview of the Workstyle properties.

Create the Workstyle

1. Select **Policies** from the sidebar menu.
2. Find the row of the policy you would like to create a Workstyle for, and click the vertical ellipsis.
3. From the dropdown menu, select **Edit & Lock Policy**, or **Edit** (if the policy is already locked by you).
4. On the **Policy Editor** page, expand **Windows** > **Workstyles**.
5. Enter a name and a description. By default, the Workstyle is disabled.
6. Click **Create Workstyle**.
7. Select the Workstyle in the navigation pane to expand the properties.
8. Configure the Workstyle properties: **Application Rules**, **On-Demand Application Rules**, **Trusted Application Protection (DLL)**, **Content Rules**, **General Rules**, and **Filters**.

> ***Tip:** For quick access to the **Workstyles Summary Page**, hover over and click the hyperlink for the appropriate Workstyle name.*

Enable a Workstyle

By default, a Workstyle is disabled when initially created.

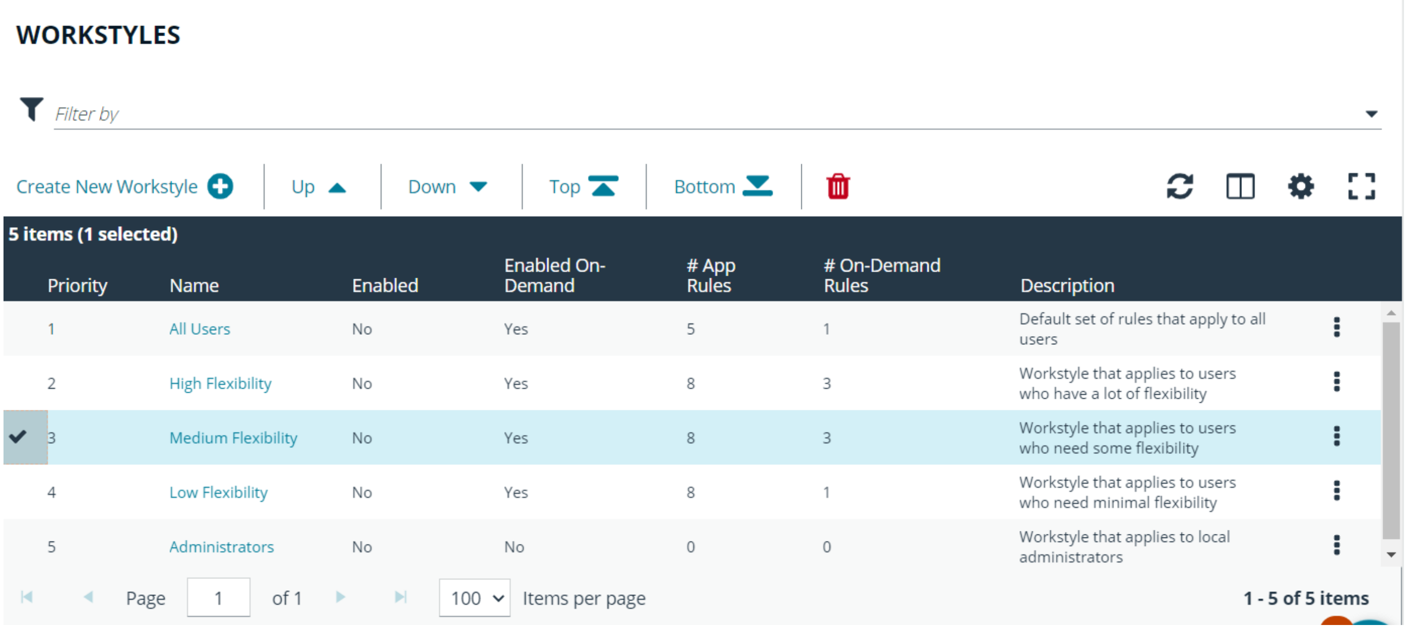
1. Go to the Policy Editor, and navigate to the Windows Workstyles.
2. Select the vertical ellipsis menu for the Workstyle, and then select **Enable**.

The Workstyle can be disabled at a later time, if required. You can disable a Workstyle when you want that Workstyle to stop processing.

Workstyle Precedence

Workstyles are evaluated in the order they are listed. When an application matches on a Workstyle, no further Workstyles are processed for that application. Ensure the order of the Workstyles is correct because it is possible for an application to match more than one Workstyle.

Select a Workstyle in the list to change the order. Changes are automatically saved.



5 items (1 selected)

	Priority	Name	Enabled	Enabled On-Demand	# App Rules	# On-Demand Rules	Description
	1	All Users	No	Yes	5	1	Default set of rules that apply to all users
	2	High Flexibility	No	Yes	8	3	Workstyle that applies to users who have a lot of flexibility
✓	3	Medium Flexibility	No	Yes	8	3	Workstyle that applies to users who need some flexibility
	4	Low Flexibility	No	Yes	8	1	Workstyle that applies to users who need minimal flexibility
	5	Administrators	No	No	0	0	Workstyle that applies to local administrators

Page 1 of 1 100 Items per page 1 - 5 of 5 items

Application Rules

Application Rules are applied to Application Groups. Application Rules can be used to enforce allow listing, monitoring, and assigning privileges to groups of applications. They are a set of rules that apply to the applications listed in the Application Group.

Create an Application Rule

1. On the **Policy Editor** page, expand **Windows**.
2. Expand the **Workstyles** node, and expand a Workstyle.
3. Click **Application Rules**, and then click **Create New**.
4. Set the following:
   - **Target Application Group**: Select an Application Group.
   - **Run Rule Script**: Assign a rule script that is run before the Application Rule triggers. Select a rule script from the list.
   - **Action**: Select **Allow** or **Block**. The action that occurs if the application in the targeted Application Group is launched by the end user.
   - **End User Message**: Select a message from the list.
   - **Access Token**: Select the type of token to pass to the target Application Group. You can select from:
     - **Passive** (no change): Doesn't make any change to the user's token. This is essentially an audit feature.

   - **Enforce User's default rights**: Removes all rights and uses the user's default token. Windows UAC always tries to add administration rights to the token being used so if the user clicked on an application that triggers UAC, the user cannot progress past the UAC prompt.
   - **Drop Admin Rights**: Removes administration rights from the user's token.
   - **Add Admin Rights**: Adds administration rights to the user's token.
 - **Raise An Event**: Off, On, Anonymous. Select if an event is raised if this Application Rule is triggered. When on, an event is sent to the local event log file. Anonymous removes user and host name from events so the user / host are not identifiable.
 - **Run an Audit Script**: Select an audit script from the list.
 - **Privilege Monitoring**: Off, On, Anonymous. Select **On** to raise a privileged monitoring event.
 - **Reporting Events**: On by default, click to turn off. When the setting is on, events are raised for viewing in PMC Reporting.

5. Click **Create Application Rule**.

Application Rule Precedence

If you add more than one Application Rule to a Workstyle, entries higher in the list have precedence. When an application matches an Application Rule, no further rules or Workstyles are processed. If an application could match more than one Workstyle or rule, then it is important that you order both your Workstyles and rules correctly.

Select an Application Rule in the list to change the order. Changes are automatically saved.

On Demand Application Rules

The **On-Demand Application Rules** node of the Workstyle allows you to create rules to launch applications with specific privileges (usually admin rights), on-demand from a right-click Windows context menu.

Windows Modern UI

If **Apply the On-Demand Application Rule to the "Run as administrator" option** is enabled and an On-Demand Application Rule is triggered, Privilege Management for Windows intercepts the **Run as administrator** option in the right-click context menu and overrides it. The labeling of the option doesn’t change in this instance. If the option is not selected, Privilege Management for Windows does not intercept the option to **Run as Administrator**.

If **Hide "Run as" and "Run as administrator" commands in the Classic Shell context menu** is selected, these options, where present, are hidden from the right-click context menu. Privilege Management for Windows does not continue process additional Application Rules.

Windows Classic Shell

If **Apply custom on-demand option to the Classic Shell context menu (this won’t affect the "Run as administrator" option)** is selected, and an On-Demand Application Rule is triggered, Privilege Management for Windows adds a new option to the right-click context menu that you configured in the **Classic Shell Context Menu Option** section, for example, **Run with Privilege Management for Windows**.

If **Hide "Run as" and "Run as administrator" commands in the Classic Shell context menu** is selected, these options, where present, are hidden from the right-click context menu. Privilege Management for Windows does not continue process additional Application Rules.

> ***Note:*** *Unlike Application Rules, the on-demand rules list only receives the assigned privileges if the user launches a relevant application using the context menu.*

To create an On-Demand Application Rule:

1. Expand **Workstyles**, and then expand a Workstyle.
2. Select **On Demand Application Rules**.
3. Select **Create New**.
4. Set the following:
   - **Target Application Group**: Select an Application Group.
   - **Run Rule Script**: Assign a rule script that is run before the Application Rule triggers. Select a rule script from the list.
   - **Action**: Select **Allow** or **Block**. The action that occurs if the application in the targeted Application Group is launched by the end user.
   - **End User Message**: Select a message from the list.
   - **Access Token**: Select the type of token to pass to the target Application Group. You can select from:
     - **Passive** (no change): Doesn't make any change to the user's token. This is essentially an audit feature.
     - **Enforce User's default rights**: Removes all rights and uses the user's default token. Windows UAC always tries to add administration rights to the token being used so if the user clicked on an application that triggers UAC, the user cannot progress past the UAC prompt.
     - **Drop Admin Rights**: Removes administration rights from the user's token.
     - **Add Admin Rights**: Adds administration rights to the user's token.
   - **Raise An Event**: Off, On, Anonymous. Select if an event is raised if this Application Rule is triggered. When on, an event is sent to the local event log file. Anonymous removes user and host name from events so the user / host are not identifiable.
   - **Run an Audit Script**: Select an audit script from the list.
   - **Privilege Monitoring**: Off, On, Anonymous. Select **On** to raise a privileged monitoring event.
   - **Reporting Events**: On by default, click to turn off. When the setting is on, events are raised for viewing in PMC Reporting.
5. Click **Create On-Demand Rule**.

General Rules

To view or edit the general rules of a Workstyle, select **Windows > Workstyles > 'Workstyle Name' > General Rules**.

The general rules include the following:

- **Collect User Information**: When enabled, raises an audit event each time a user logs on to the client machine.
- **Collect Host Information**: When enabled, raises an audit event on computer start-up or when the Privilege Management for Windows service is started.
- **Prohibit Privileged Account Management**: When enabled, blocks users from modifying local privileged group memberships. This prevents real administrators, or applications which have been granted administrative rights through Privilege Management for Windows, from adding, removing or modifying a privileged account.

  The local privileged groups that cannot be changed when this rule is enabled:

  - Built-in administrators
  - Power users
  - Account operators
  - Server operators

    - Printer operators
    - Backup operators
    - RAS servers group
    - Network configuration operators

- **Enable Windows Remote Management Connections**: When enabled, authorizes standard users who match the Workstyle to connect to a computer remotely using WinRM, which would normally require local administrator rights. This general rule supports remote PowerShell command management, and must be enabled to allow a standard user to execute PowerShell scripts or commands.

To allow remote network connections, you may be required to enable the Windows Group Policy setting access this computer from the network.

For more information, please see the following:

- *"Remote PowerShell Commands" on page 67*
- *Access this Computer from the Network on Microsoft-us/previous-versions/windows/it-pro/windows-server-2003/cc740196(v=ws.10)*

Filters

A Workstyle filter refines when a Workstyle is applied. Workstyle filters apply to Windows and macOS systems.

By default, a Workstyle applies to all users and computers who receive it. However, you can add one or more filters that restrict the application of the Workstyle:

- **Account Filter**: Restrict the Workstyle to specific users or groups of users.
- **Computer Filter**: Restrict the Workstyle to specific computers (names or IP addresses), or Remote Desktop clients.

The following conditions can be applied to a filter:

- **ALL filters must match**: The Workstyle is applied only if all filters match.
- **ANY filter can match**: The Workstyle is applied when any filter matches.

Account Filters

An account filter restricts a Workstyle to specific users or groups of users. Account filters can be created for Windows and macOS Workstyles.

You can add local or domain users and groups and Azure Active Directory groups (Windows only).

To create an account filter:

1. Expand a Workstyle, and then select **Filters**.
2. Select **Create New Filter**, and then select **Account Filter**.
3. Select the new filter in the list, and then select **Go To** from the menu.
4. Select the following to add users or groups:
    - **Add From Local/Domain AD** (Windows): Add an account name and SID details. If you are adding a group you can select from a list of known Active Directory Built-in groups. Click **Add Account**.

- **Add From Azure AD** (Windows): The Azure AD group list is populated with cached Azure AD group data. Select a group from the list, and then click **Add**. You can select more than one group at a time.
- **Add Account**: (macOS). Add the account or group details. User IDs on macOS must be values greater than 500. A value less than that might be used by a system process.

To filter account names, click inside the **Filter by** list at the top of the **Accounts** grid and select **Account Name**, **Type**, or **Value**. You can use multiple filters to help narrow down an especially lengthy list of names.

Computer Filters

A computer filter can be used to target specific computers and remote desktop clients. You can add a computer using either its host or DNS name, or by an IP address.

To restrict the Workstyle to specific computers by IP address:

1. Expand a Workstyle, and then select **Filters**.
2. Select **Create New Filter**, and then select **Computer Filter**.
3. Enter the IP address manually, in the format **123.123.123.123**. Optionally, use asterisk wildcard (*) and - for range, as shown: **127.*.0.0-99**.
4. Select **Match the remote desktop (instead of the local computer)** if the computer filter is intended to match the IP address of remote computers using remote desktop sessions.
5. Click **Add**.

To restrict the Workstyle to specific computers by host name:

1. Expand a Workstyle, and then select **Filters**.
2. Select **Create New Filter**, and then select **Computer Filter**.
3. Enter one or more host names, separated by semicolons. You can use the ***** and **?** wildcard characters in host names.
4. Select **Match the remote desktop (instead of the local computer)** if the computer filter is intended to match the IP address of remote computers using remote desktop sessions.
5. Click **Add**.

Application Groups

Application Groups are used to define logical groupings of applications.

Application Groups are assigned to Workstyles, so you must define Application Groups for all of the applications you want to assign to a Workstyle.

Show Hidden Application Groups

1. On the **Policy Editor** page, expand **Windows**.
2. Select **Application Groups**, and then select **Show Hidden**.

Create an Application Group

1. On the **Policy Editor** page, expand **Windows**.
2. Select **Application Groups**.
3. Select **Create New Application Group**.

4. Add a name and description. Click **Create Application Group**.
5. The Application Group is now displayed in the navigation pane and the grid. You are now ready to add applications to the group.

View or Edit the Properties of an Application Group

1. On the **Policy Editor** page, expand **Windows**.
2. Select **Application Groups**.
3. Select an Application Group in the list, and select **Edit** from the menu.
4. Change the properties.
5. Click **Save Changes**.

Delete

1. On the **Policy Editor** page, expand **Windows**.
2. Select **Application Groups**.
3. Select an Application Group in the list, and select **Delete** from the menu.

Duplicate

1. On the **Policy Editor** page, expand **Windows**.
2. Select **Application Groups**.
3. Select an Application Group in the list, and select **Duplicate** from the menu.
4. Select the duplicated group and change the settings, as required.

Add an Application to an Application Group

When adding an application, you can configure the following components:

- **Application Definitions**: The application definitions are the properties of an application that are used to detect the application in your environment. When the application matches on the configured criteria the rule triggers.
- **Advanced Options**: When adding the application, advanced settings on child processes and standard user rights enforcement can be configured.

For more information, please see the following:

- *"Application Definitions" on page 54*
- *"Advanced Options" on page 58*

When adding file or folder paths, you can use environment variables as part of the entry. Using environment variables is optional.

For more information, please see "Environment Variables" on page 58

You can add applications using a template. Application templates provide a way to pick from a list of known applications.

For more information, please see "Add an Application From a Template" on page 53.

The procedure for adding an application is generally the same for every application. The matching criteria varies depending on the application.

To add an application:

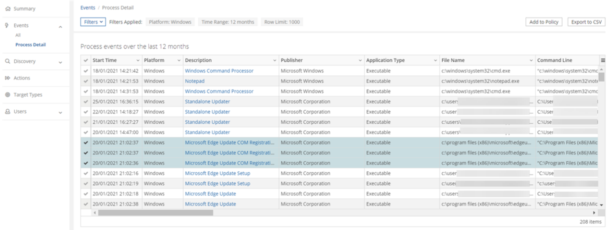
1. In the navigation pane, select the Application Group.
2. Click **Create New Application**, and then select the application type you want to add.
3. Enter a description, if required. By default, this is the name of the application you're inserting.
4. Configure the matching criteria for the application.
5. You need to configure the **Advanced Options** for the application. You can configure:
   - Allow child processes will match this application definition
   - Force standard user rights on File Open/Save common dialogs
6. Click **OK**. The application is added to the Application Group.

For more information about advanced options, please see "Advanced Options" on page 58

Add an Application From Reports

You can add an application to a policy based on events generated from a particular application type.

1. In the console, select the **Reports** tile.
2. Expand **Events** and select **All** or **Process Detail**.
3. Select events in the list and select **Add to Policy**. The Policy Editor opens.



Process events over the last 12 months

✓	Start Time	Platform	Description	Publisher	Application Type	File Name	Command Line
✓	18/01/2021 14:21:42	Windows	Windows Command Processor	Microsoft Windows	Executable	c:\windows\system32\cmd.exe	"c:\windows\system32\cmc
✓	18/01/2021 14:21:53	Windows	Notepad	Microsoft Windows	Executable	c:\windows\system32\notepad.exe	"c:\windows\system32\note
✓	18/01/2021 14:31:53	Windows	Windows Command Processor	Microsoft Windows	Executable	c:\windows\system32\cmd.exe	"c:\windows\system32\cmc
✓	25/01/2021 16:36:15	Windows	Standalone Updater	Microsoft Corporation	Executable	c:\users[redacted]...	C:\User[redacted]
✓	22/01/2021 14:18:27	Windows	Standalone Updater	Microsoft Corporation	Executable	c:\user[redacted]...	C:\User[redacted]
✓	21/01/2021 16:27:27	Windows	Standalone Updater	Microsoft Corporation	Executable	c:\users\[redacted]...	C:\Use[redacted]
✓	20/01/2021 14:47:00	Windows	Standalone Updater	Microsoft Corporation	Executable	c:\users\[redacted]...	C:\User[redacted]
✓	20/01/2021 21:02:37	Windows	Microsoft Edge Update COM Registrati...	Microsoft Corporation	Executable	c:\program files (x86)\microsoft\edgeu...	"C:\Program Files (x86)\Mic
✓	20/01/2021 21:02:37	Windows	Microsoft Edge Update COM Registrati...	Microsoft Corporation	Executable	c:\program files (x86)\microsoft\edgeu...	"C:\Program Files (x86)\Mic
✓	20/01/2021 21:02:36	Windows	Microsoft Edge Update COM Registrati...	Microsoft Corporation	Executable	c:\program files (x86)\microsoft\edgeu...	"C:\Program Files (x86)\Mic
✓	20/01/2021 21:02:16	Windows	Microsoft Edge Update Setup	Microsoft Corporation	Executable	c:\user[redacted]...	"C:\Use[redacted]
✓	20/01/2021 21:02:19	Windows	Microsoft Edge Update Setup	Microsoft Corporation	Executable	c:\user[redacted]...	"c:\users[redacted]
✓	20/01/2021 21:02:18	Windows	Microsoft Edge Update	Microsoft Corporation	Executable	c:\users[redacted]...	C:\Users[redacted]
✓	20/01/2021 21:02:38	Windows	Microsoft Edge Update	Microsoft Corporation	Executable	c:\program files (x86)\microsoft\edgeu...	"C:\Program Files (x86)\Mic

208 items

4. On the **Add Application to Policy** page, select a policy and an Application Group.
5. Select **Add and Edit**. Alternatively, select **Add and Close** here which adds the application to the Application Group and redirects you back to the report.
6. The policy opens to the **Application Groups > Applications** page where you can edit the application settings.

Add an Application From a Template

Application templates provide a way to pick from a list of known applications. A standard set of templates is provided that covers basic administrative tasks for all supported operating systems, common ActiveX controls, and software updaters.

1. On the Policy Editor page, navigate to the policy to update.
2. Go to **Application Groups > Applications**, and then select **Add From Templates**.
3. Select an application template from the list, and then click **Add**. You can select more than one template at a time.

Application Definitions

The Policy Editor must match every enabled criteria in an application definition before it will trigger a match (the rules are combined with a logical AND).

Application definitions that require a match can also be negated. To target applications that do not match the definition, select does NOT match.

Name	Description
ActiveX Codebase matches	When inserting ActiveX controls, this is enabled by default and we recommend you use this option in most circumstances. You must enter the URL to the codebase for the ActiveX control. You can choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions** Although you can enter a relative codebase name, we strongly recommend you enter the full URL to the codebase, as it is more secure.
ActiveX Version matches	If the ActiveX control you entered has a version property, then you can choose **Check Min Version** and/or **Check Max Version** and edit the respective version number fields.
App ID matches	Matches on the App ID of the COM class, which is a GUID used by Windows to set properties for a CLSID. AppIds can be used by 1 or more CLSIDs. The available operators are identical to the File or Folder Name definition.
Application Requires Elevation (UAC)	This option can be used to check if an executable requires elevated rights to run and would cause UAC (User Account Control) to trigger. This is a useful way to replace inappropriate UAC prompts with PMC end user messages to either block or prompt the user for elevation.
Application Requires Elevation (UAC)	This option can be used to check if an MSI requires elevated rights to run and would cause User Account Control (UAC) to trigger. ***Note:*** *This is supported on install only.*
BeyondTrust Zone Identifier exists	This options allows you to match on the BeyondTrust Zone Identifier tag, where present. If an Alternate Data Stream (ADS) tag is applied by the browser, we also apply a BeyondTrust Zone Identifier tag to the file. The BeyondTrust Zone Identifier tag can be used as matching criteria if required.
CLSID matches	This option allows you to match the class ID of the ActiveX control or COM class, which is a unique GUID stored in the registry.
COM Display Name matches	If the class you entered has a Display Name, then it will automatically be extracted and you can choose to match on this property. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a regular expression. The available operators are identical to File or Folder Name definition.

Name	Description
Command Line matches	If the filename is not specific enough, you can match the command line, by checking this option and entering the command line to match. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a regular expression. The available operators are identical to File or Folder Name definition. PowerShell removes double quotes from command strings prior to transmitting to the target. Therefore, we do not recommend that Command Line definitions include double quotes, as they will fail to match the command.
Controlling Process matches	This option allows you to target content based on the process (application) that will be used to open the content file. The application must be added to an Application Group. You can also define whether any parent of the application will match the definition.
Drive matches	This option can be used to check the type of disk drive where the file is located. Choose from one of the following options: • **Fixed disk:** Any drive that is identified as being an internal hard disk. • **Network:** Any drive that is identified as a network share. • **RAM disk:** Any drive that is identified as a RAM drive. • **Any Removable Drive or Media:** If you want to target any removable drive or media, but are unsure of the specific drive type, choose this option which will match any of the removable media types below. Alternatively, if you want to target a specific type, choose from one of the following removable media types: ◦ **Removable Media:** Any drive that is identified as removable media. ◦ **USB:** Any drive that is identified as a disk connected by USB. ◦ **CD/DVD:** Any drive that is identified as a CD or DVD drive. ◦ **eSATA Drive:** Any drive that is identified as a disk connected by eSATA.
File or Folder Name matches	Applications are validated by matching the file or folder name. You can choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions** *For more information, please see "Regular Expression Syntax" on page 115.* Although you can enter relative file names, we strongly recommend you enter the full path to a file or the COM server. Environment variables are also supported. We do not recommend you use the definition File or Folder Name **does NOT Match** in isolation for executable types, as it will result in matching every application, including hosted types, such as installer packages, scripts, batch files, registry files, management consoles, and Control Panel applets. When creating blocking rules for applications or content, and the **File or Folder Name** is used as matching criteria against paths which exist on network shares, this should be done using the UNC network path and not by the mapped drive letter.

Name	Description
File Hash (SHA-1 Fingerprint) matches	If a reference file was entered, then a SHA-1 hash of the PowerShell script will be generated. This definition ensures the contents or the script file (which can normally be edited by any user) remain unchanged, as changing a single character in the script will cause the SHA-1 Hash to change.
File Version matches	If the file, service executable, or COM server you entered has a File Version property, then it will automatically be extracted and you can choose Check Min Version and/or Check Max Version, and edit the respective version number fields.
Parent Process matches	This option can be used to check if an application's parent process matches a specific Application Group. You must create an Application Group for this purpose or specify an existing Application Group in the Parent Process group. Setting match all parents in tree to True will traverse the complete parent/child hierarchy for the application, looking for any matching parent process, whereas setting this option to False will only check the application's direct parent process.
Product Code matches	If the file you entered has a Product Code, then it will automatically be extracted and you can choose to check this code.
Product Description matches	If the file you entered has a Product Description property, then it will automatically be extracted, and you can choose to match on this property. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (? and *) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Product Name matches	If the file, COM server, or service executable you entered has a Product Name property, then it will automatically be extracted and you can choose to match on this property. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (? and *) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Product Version matches	If the file, COM server, or service executable you entered has a Product Version property, then it will automatically be extracted and you can choose Check Min Version and/or Check Max Version and edit the respective version number fields.
Publisher matches	Check for the existence of a valid publisher. If you browsed for an application, then the certificate subject name will automatically be retrieved, if the application is signed. For Windows system files, the Windows security catalog is searched, and if a match is found, the certificate for the security catalog is retrieved. Publisher checks are supported on Executables, Control Panel Applets, Installer Packages, Windows Scripts, and PowerShell Scripts. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Service Actions match	Define the actions which are allowed. Choose from: • **Service Stop:** Grants permission to stop the service. • **Service Start:** Grants permission to start the service. • **Service Pause / Resume:** Grants permission to pause and resume the service. • **Service Configure:** Grants permission to edit the properties of the service.
Service Display Name matches	Matches on the name of the Windows service, for example, **W32Time**. You may choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match**

Name	Description
	- **Starts With** - **Ends With** - **Contains** - **Regular Expressions**
Service Name matches	Matches on the name of the Windows service, for example, **W32Time**. You may choose to match based on the following options (wildcard characters **?** and ***** may be used): - **Exact Match** - **Starts With** - **Ends With** - **Contains** - **Regular Expressions**
Source URL matches	If an application was downloaded using a web browser, this option can be used to check where the application or installer was originally downloaded from. The application is tracked by Privilege Management for Windows at the point it is downloaded, so that if a user decided to run the application or installer at a later date, the source URL can still be verified. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Trusted Ownership matches	This option can be used to check if an application's file is owned by a trusted owner (the trusted owner accounts are SYSTEM, Administrators, or Trusted Installer).
Upgrade Code matches	If the file you entered has an **Upgrade Code**, then it will automatically be extracted and you can choose to check this code.
Windows Store Application Version	Matches on the version of the Windows Store application, for example, **16.4.4204.712**. You can choose **Check Min Version** and/or **Check Max Version** and edit the respective version number fields.
Windows Store Package Name	Matches on the name of the Windows Store Application, for example, **microsoft.microsoftskydrive**. You can choose to match based on the following options (wildcard characters **?** and ***** may be used): - **Exact Match** - **Starts With** - **Ends With** - **Contains** - **Regular Expressions**
Windows Store Publisher	Matches on the publisher name of the Windows Store Application, for example, **Microsoft Corporation**. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a Regular Expression. The other available operators are: - **Exact Match** - **Starts With** - **Ends With**

Name	Description
	- **Contains** - **Regular Expressions** The **Browse File** and **Browse Apps** options can only be used if configuring PMC settings from a Windows 8 client.

Environment Variables

You can use the following environment variables in file path and command line application definitions.

System Variables

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES(x86)%
- %COMMONPROGRAMFILES%
- %PROGRAMDATA%
- %PROGRAMFILES(x86)%
- %PROGRAMFILES%
- %SYSTEMROOT%
- %SYSTEMDRIVE%

User Variables

- %APPDATA%
- %USERPROFILE%
- %HOMEPATH%
- %HOMESHARE%
- %LOCALAPPDATA%
- %LOGONSERVER%

To use any of the environment variables above, enter the variable, including the % characters, into a file path or command line. PMC will expand the environment variable prior to attempting a file path or command line match.

Advanced Options

Allow child processes will match this application definition

If selected, then any child processes that are launched from this application (or its children) will also match this rule. The rules are still processed in order, so it's still possible for a child process to match a higher precedence rule (or Workstyle) first. Therefore, this option will prevent a child process from matching a lower precedence rule. It should also be noted that if an application is launched by an on-demand rule and this option is selected, then its children will be processed against the on-demand rules, and not the Application Rules. If this option is not selected, then the children will be processed against the Application Rules in the normal way. You can further refine this option by restricting the child processes to a specific Application Group. The default is to match <**Any Application**>, which will match any child process.

***Note:** If you want to exclude specific processes from matching this rule, then click **...match...** to toggle the rule to **...does not match...**.*

***Note:** Child processes are evaluated in the context that the parent executed. For example, if the parent executed through on-demand shell elevation, then PMC will first attempt to match On-Demand Application Rules for any children of the executed application.*

Force standard user rights on File Open/Save common dialogs

If the application allows a user to open or save files using the common Windows open or save dialog box, then selecting this option ensures the user does not have admin privileges within these dialog boxes. These dialog boxes have Explorer-like features, and allow a user to rename, delete, or overwrite files. If an application is running with elevated rights and this option is disabled, the open/save dialog boxes will allow a user to replace protected system files.

Where present, this option is selected by default to ensure PMC forces these dialog boxes to run with the user's standard rights, to prevent the user from tampering with protected system files.

When enabled, this option also prevents processes launched from within these dialog boxes from inheriting the rights of an elevated application.

Application Details

This section provides details about the properties that can be configured on the application.

In some cases, additional information to configure the application is provided.

ActiveX Control

Unlike other application types, PMC only manages the privileges for the installation of ActiveX controls. ActiveX controls usually require administrative rights to install, but once installed, they run with the standard privileges of the web browser.

Matching critieria:

- ActiveX Codebase matches
- CLSID matches
- ActiveX Version matches

Batch Files

Matching criteria

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1 Fingerprint) matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches

- Source URL matches
- BeyondTrust Zone Identifier exists

COM Classes

COM elevations are a form of elevation which are typically initiated from Explorer, when an integrated task requires administrator rights. Explorer uses COM to launch the task with admin rights, without having to elevate Explorer. Every COM class has a unique identifier, called a CLSID, that is used to launch the task.

COM tasks usually trigger a Windows UAC prompt because they need administrative privileges to proceed. PMC allows you to target specific COM CLSIDs and assign privileges to the task without granting full administration rights to the user. COM based UAC prompts can also be targeted and replaced with custom messaging, where COM classes can be allowlisted and/or audited.

COM classes are hosted by a COM server DLL or EXE, so COM classes can be validated from properties of the hosting COM server. You can configure:

Matching criteria:

- File or Folder Name matches
- Drive matches
- File Hash (SHA-1 Fingerprint) matches
- Product Name matches
- Publisher matches
- CLSID matches
- App ID matches
- COM Display Name matches
- Product Description matches
- Product Version matches
- File Version matches
- Trusted Ownership matches
- Application Requires Elevation (UAC): Match if **Application Requires Elevation (User Account Control)** is always enabled, as COM classes require UAC to elevate
- Source URL matches

Control Panel Applet

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1 Fingerprint) matches
- Product Name matches
- Publisher matches
- Product Description matches
- Product Version matches
- File Version matches

- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Executables

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1 Fingerprint) matches
- Product Name matches
- Publisher matches
- Product Description matches
- Product Version matches
- File Version matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Installer Package

PMC allows standard users to install and uninstall Windows Installer packages that normally require local admin rights. The following package types are supported:

- Microsoft Software Installers (MSI)
- Microsoft Software Updates (MSU)
- Microsoft Software Patches (MSP)

When a Windows Installer package is added to an Application Group, and assigned to an Application Rule or On-Demand Application Rule, the action will be applied to both the installation of the file, and also uninstallation when using **Add/Remove Programs** or **Programs and Features**.

> ***Note:*** *The publisher property of an MSx file may sometimes differ to the publisher property once installed in* ***Programs and Features****. We therefore recommend applications targeted using the* ***Match Publisher*** *validation rule are tested for both installation and uninstallation, prior to deployment, using the PMC Activity Viewer.*

Installer packages typically create child processes as part of the overall installation process. Therefore, we recommend when elevating MSI, MSU, or MSP packages, that the advanced option **Allow child processes will match this application definition** is enabled.

***Note:** If you want to apply more granular control over installer packages and their child processes, use the **Child Process** validation rule to allowlist or blocklist those processes that will or will not inherit privileges from the parent software installation.*

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1 Fingerprint) matches
- Product Name matches
- Publisher matches
- Product Version matches
- Product Code matches
- Upgrade Code matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Insert Privilege Management Policy Editor Snap-ins

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1 Fingerprint) matches
- Publisher matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Management Console

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1 Fingerprint) matches

- Publisher matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

PowerShell Scripts

Privilege Management for Windows allows you to target specific PowerShell scripts and assign privileges to the script without granting local administration rights to the user. Scripts can also be blocked if they are not authorized or allowlisted.

> ***Note:** PowerShell scripts that contain only a single line are interpreted and matched as a PowerShell command, and will not match a PowerShell script definition. We recommend PowerShell scripts contain at least two lines of commands to ensure they are correctly matched as a PowerShell script. This cannot be achieved by adding a comment to the script.*

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1 Fingerprint) matches
- Publisher matches
- Trusted Ownership matches
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Example PowerShell Configurations

Create New Configuration, Save to Local File

```
# Import both Defendpoint cmdlet module
Import-Module 'C:\Program Files\Avecto\Privilege Guard
Client\PowerShell\Avecto.Defendpoint.Cmdlets\Avecto.Defendpoint.Cmdlets.dll'
# Create a new variable containing a new Defendpoint Configuration Object
$PGConfig = New-Object Avecto.Defendpoint.Settings.Configuration


## Add License ##
# Create a new license object
$PGLicence = New-Object Avecto.Defendpoint.Settings.License
# Define license value
$PGLicence.Code = "5461E0D0-DE30-F282-7D67-A7C6-B011-2200"
# Add the License object to the local PG Config file
$PGConfig.Licenses.Add($PGLicence)
```

```
## Add Application Group ##
# Create an Application Group object
$AppGroup = new-object Avecto.Defendpoint.Settings.ApplicationGroup
# Define the value of the Application Group name
$AppGroup.name = "New App Group"
# Add the Application Group object to the local PG Config file
$PGConfig.ApplicationGroups.Add($AppGroup)

## Add Application ##
# Create an application object
$PGApplication = new-object Avecto.Defendpoint.Settings.Application $PGConfig
# Use the Get-DefendpointFileInformation to target Windows Calculator
$PGApplication = Get-DefendpointFileInformation -Path C:\windows\system32\calc.exe
# Add the application to the Application group
$PGConfig.ApplicationGroups[0].Applications.AddRange($PGApplication)

## Add Message ##
# Create a new message object
$PGMessage = New-Object Avecto.Defendpoint.Settings.message $PGConfig
#Define the message Name, Description and OK action and the type of message
$PGMessage.Name = "Elevation Prompt"
$PGMessage.Description = "An elevation message"
$PGMessage.OKAction = [Avecto.Defendpoint.Settings.Message+ActionType]::Proceed
$PGMessage.Notification = 0
# Define whether the message is displayed on a secure desktop
$PGMessage.ShowOnIsolatedDesktop = 1
# Define How the message contains
$PGMessage.HeaderType = [Avecto.Defendpoint.Settings.message+MsgHeaderType]::Default
$PGMessage.HideHeaderMessage = 0
$PGMessage.ShowLineOne = 1
$PGMessage.ShowLineTwo = 1
$PGMessage.ShowLineThree = 1
$PGMessage.ShowReferLink = 0
$PGMessage.ShowCancel = 1
$PGMessage.ShowCRInfoTip = 0
# Define whether a reason settings
$PGMessage.Reason = [Avecto.Defendpoint.Settings.message+ReasonType]::None
$PGMessage.CacheUserReasons = 0
# Define authorization settings
$PGMessage.PasswordCheck =
Avecto.Defendpoint.Settings.message+AuthenticationPolicy]::None
$PGMessage.AuthenticationType = [Avecto.Defendpoint.Settings.message+MsgAuthenticationType]::Any
$PGMessage.RunAsAuthUser = 0
# Define Message strings
$PGMessage.MessageStrings.Caption = "This is an elevation message"
$PGMessage.MessageStrings.Header = "This is an elevation message header"
$PGMessage.MessageStrings.Body = "This is an elevation message body"
$PGMessage.MessageStrings.ReferURL = "http:\\www.bbc.co.uk"
$PGMessage.MessageStrings.ReferText = "This is an elevation message refer"
$PGMessage.MessageStrings.ProgramName = "This is a test Program Name"
$PGMessage.MessageStrings.ProgramPublisher = "This is a test Program Publisher"
$PGMessage.MessageStrings.PublisherUnknown = "This is a test Publisher Unknown"
$PGMessage.MessageStrings.ProgramPath = "This is a test Path"
$PGMessage.MessageStrings.ProgramPublisherNotVerifiedAppend = "This is a test verification
```

```
failure"
$PGMessage.MessageStrings.RequestReason = "This is a test Request Reason"
$PGMessage.MessageStrings.ReasonError = "This is a test Reason Error"
$PGMessage.MessageStrings.Username = "This is a test Username"
$PGMessage.MessageStrings.Password = "This is a test Password"
$PGMessage.MessageStrings.Domain = "This is a test Domain"
$PGMessage.MessageStrings.InvalidCredentials = "This is a test Invalid Creds"
$PGMessage.MessageStrings.OKButton = "OK"
$PGMessage.MessageStrings.CancelButton = "Cancel"
# Add the PG Message to the PG Configuration
$PGConfig.Messages.Add($PGMessage)

## Add custom Token ##
# Create a new custom Token object
$PGToken = New-Object Avecto.Defendpoint.Settings.Token
# Define the Custom Token settings
$PGToken.Name = "Custom Token 1"
$PGToken.Description = "Custom Token 1"
$PGToken.ClearInheritedPrivileges = 0
$PGToken.SetAdminOwner = 1
$PGToken.EnableAntiTamper = 0
$PGToken.IntegrityLevel = Avecto.Defendpoint.Settings.Token+IntegrityLevelType]::High
# Add the Custom Token to the PG Configuration
$PGConfig.Tokens.Add($PGToken)

## Add Policy ##
# Create new policy object
$PGPolicy = new-object Avecto.Defendpoint.Settings.Policy $PGConfig
# Define policy details
$PGPolicy.Disabled = 0
$PGPolicy.Name = "Policy 1"
$PGPolicy.Description = "Policy 1"
# Add the policy to the PG Configurations
$PGConfig.Policies.Add($PGPolicy)

## Add Policy Rule ##
# Create a new policy rule
$PGPolicyRule = New-Object Avecto.Defendpoint.Settings.ApplicationAssignment PGConfig
# Define the Application rule settings
$PGPolicyRule.ApplicationGroup = $PGConfig.ApplicationGroups[0]
$PGPolicyRule.BlockExecution = 0
$PGPolicyRule.ShowMessage = 1
$PGPolicyRule.Message = $PGConfig.Messages[0]
$PGPolicyRule.TokenType = [Avecto.Defendpoint.Settings.Assignment+TokenTypeType]::AddAdmin
$PGPolicyRule.Audit = [Avecto.Defendpoint.Settings.Assignment+AuditType]::On
$PGPolicyRule.PrivilegeMonitoring = [Avecto.Defendpoint.Settings.Assignment+AuditType]::Off
$PGPolicyRule.ForwardEPO = 0
$PGConfig.Policies[0].ApplicationAssignments.Add($PGPolicyRule)

## Set the Defendpoint configuration to a local file and prompt for user confirmation ##
Set-DefendpointSettings -SettingsObject $PGConfig -Localfile -Confirm
```

Open Local User Policy, Modify then Save

```
# Import the Defendpoint cmdlet module
Import-Module 'C:\Program Files\Avecto\Privilege Guard
Client\PowerShell\Avecto.Defendpoint.Cmdlets\Avecto.Defendpoint.Cmdlets.dll'
# Get the local file policy Defendpoint Settings
$PGConfig = Get-DefendpointSettings -LocalFile
# Disable a policy
$PGPolicy = $PGConfig.Policies[0]
$PGPolicy.Disabled = 1
$PGConfig.Policies[0] = $PGPolicy
# Remove the PG License
$TargetLicense = $PGConfig.Licenses[0]
$PGConfig.Licenses.Remove($TargetLicense)
# Update an existing application definition to match on Filehash
$UpdateApp = $PGConfig.ApplicationGroups[0].Applications[0]
$UpdateApp.CheckFileHash = 1
$PGConfig.ApplicationGroups[0].Applications[0] = $UpdateApp
# Set the Defendpoint configuration to the local file policy and prompt for user confirmation
Set-DefendpointSettings -SettingsObject $PGConfig -LocalFile -Confirm
```

Open Local Configuration and Save to Domain GPO

```
# Import the Defendpoint cmdlet module
Import-Module 'C:\Program Files\Avecto\Privilege Guard
Client\PowerShell\Avecto.Defendpoint.Cmdlets\Avecto.Defendpoint.Cmdlets.dll'
# get the local Defendpoint configuration and set this to the domain computer policy, ensuring
the user is prompted to confirm the change
Get-DefendpointSettings -LocalFile | Set-DefendpointSettings -Domain -LDAP "LDAP://My.Domain/CN=
{GUID},CN=Policies,CN=System,DC=My,DC=domain" -Confirm
```

Registry Settings

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1 Fingerprint) matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Remote PowerShell Commands

PMC provides an additional level of granularity for management of remote PowerShell cmdlets to ensure you can execute these commands without local administrator privileges on the target computer.

```
Get-service -Name *time* | restart-Service –PassThru
```

PMC allows you to target specific command strings and assign privileges to the command without granting local admin rights to the user. Commands can also be blocked if they are not authorized or allowlisted. All remote PowerShell commands are fully audited for visibility.

To allow standard users to connect to a remote computer with Windows Remote Management, or WinRM (a privilege normally reserved for local administrator accounts), it is necessary to enable the General rule **Enable Windows Remote Management Connections**. This rule grants standard users, who match the Workstyle, the ability to connect using WinRM, and can be targeted to specific users, groups of users, or computers using Workstyle filters.

1. Select the Application Group you want to add the application to.
2. Right-click and select **Insert Application > Remote PowerShell Command**.
3. You can leave the **Select reference script file** blank to match on all applications of this files, type in a specific name or path manually, or click **Browse Cmdlets**.This lists the PowerShell cmdlets for the version of PowerShell that you installed. If the cmdlet you want to use is not listed because the target version of PowerShell is different, you can manually enter it.
4. Enter a description, if required. By default, this is the name of the application you're inserting.
5. You need to configure the matching criteria for the PowerShell command. You can configure:
    - Command Line matches: PowerShell removes double quotes from the Command Line before it is sent to the target. **Command Line** definitions that include double quotes are not matched by PMC for remote PowerShell commands.

> *For more information, please see "Application Definitions" on page 54.*

6. Click **OK**. The application is added to the Application Group.

> *If you want to manage remote PowerShell scripts instead of a single cmdlet, please see "Insert Remote PowerShell Scripts" on page 67*

Messaging

PMC end user messaging includes limited support for remote PowerShell sessions; block messages can be assigned to Workstyle rules, which block remote PowerShell scripts and commands. If a block message is assigned to a Workstyle, which blocks a script or command, then the body message text of an assigned message will be displayed in the remote console session as an error.

Insert Remote PowerShell Scripts

From within a remote PowerShell session, a script (.PS1) can be executed from a remote computer against a target computer. Normally this requires local administrator privileges on the target computer, with little control over the scripts that are executed, or the actions that the script performs. For example:

```
Invoke-Command -ComputerName RemoteServer -FilePath c:\script.ps1 -Credential xxx
```

You can target specific PowerShell scripts remotely and assign privileges to the script without granting local administration rights to the user. Scripts can also be blocked if they are not authorized or allowlisted. All remote PowerShell scripts executed are fully audited for visibility.

> ***Note:*** *You must use the* ***Invoke-Command*** *cmdlet to run remote PowerShell scripts. PMC cannot target PowerShell scripts that are executed from a remote PowerShell session. Remote PowerShell scripts must be matched by either a SHA-1 File Hash or a Publisher (if the script has been digitally signed).*

You can elevate individual PowerShell scripts and commands which are executed from a remote machine. This eliminates the need for users to be logged on with an account which has local admin rights on the target computer. Instead, elevated privileges are assigned to specific commands and scripts which are defined in Application Groups, and applied by a Workstyle.

PowerShell scripts and commands can be allowlisted to block the use of unauthorized scripts, commands, and cmdlets. Granular auditing of all remote PowerShell activity provides an accurate audit trail of remote activity.

PowerShell definitions for scripts and commands are treated as separate application types, which allows you to differentiate between predefined scripts authorized by IT, and session-based ad hoc commands.

To allow standard users to connect to a remote computer with Windows Remote Management, or WinRM (a privilege normally reserved for local administrator accounts), it is necessary to enable the General rule **Enable Windows Remote Management Connections**. This rule grants standard users who match the PMCWorkstyle the ability to connect using WinRM, and can be targeted to specific users, groups of users, or computers using Workstyle filters.

Matching criteria:

- File Hash (SHA-1 Fingerprint) matches
- Publisher matches

You can leave the **Select reference script file** blank to match on all applications of this files, type in a specific name or path manually, or click **Browse File**.

> ***Note:*** *Remote PowerShell scripts that contain only a single line will be interpreted and matched as a Remote PowerShell Command, and will fail to match a PowerShell script definition. We therefore recommend PowerShell scripts contain at least two lines of commands to ensure they are correctly matched as a script. This cannot be achieved by adding a comment to the script.*

Messaging

PMC end user messaging includes limited support for remote PowerShell sessions; block messages can be assigned to Workstyle rules which block remote PowerShell scripts and commands. If a block message is assigned to a Workstyle which blocks a script or command, then the body message text of an assigned message will be displayed in the remote console session as an error.

Uninstaller (MSI or EXE)

PMC allows standard users to uninstall Microsoft Software Installers (MSIs) and executables (EXEs) that would normally require local admin rights.

When the **Uninstaller** application type is added to an Application Group and assigned to an Application Rule in the policy, the end user can uninstall applications using **Programs and Features** or, in Windows 10, **Apps and Features**.

The **Uninstaller** application type allows you to uninstall an EXE or MSI when it is associated with an Application Rule. As the process of uninstalling a file requires admin rights, you need to ensure when you target the Application Group in the Application Rules you set the access token to **Add Admin Rights**.

Note: *The **Uninstaller** type must be associated with an Application Rule. It does not apply to On-Demand Application Rules.*

You cannot use the **Uninstaller** application type to uninstall the BeyondTrust or the BeyondTrustPMC Adapter using , irrespective of your user rights. The anti-tamper mechanism built into PMC prevents users from uninstalling PMC, and the uninstall will fail with an error message.

Note: *If a user attempts to use PMC to modify the installation of PMC, for example, uninstall it, and they do not have an anti-tamper token applied, the default behavior for the user is used. For example, if Windows UAC is configured, the associated Windows prompt will be displayed.*

If you want to allow users to uninstall either BeyondTrust's or the BeyondTrust PMC Adapter, you can do this by either:

- Logging in as a full administrator
- Elevating the **Programs and Features** control panel (or other controlling application) using a **Custom** Access Token that has anti-tamper disabled.

Upgrade Considerations

Any pre 5.7 Uninstaller Application Groups which matched all uninstallations will be automatically upgraded when loaded by the Policy Editor to File or Folder Name matches *. These will be honored by Privilege Management for Windows.

Pre 5.7 versions of Privilege Management for Windows will no longer match the upgraded rules, the behavior will be that of the native operating system in these cases.

If you do not want the native operating system behavior for uninstallers; please ensure that your clients are upgraded to the latest version before you deploy any policy which contains upgraded Uninstaller rules.

1. Select the Application Group you want to add the uninstaller to.
2. Right-click and select **Insert Application** > **Uninstaller**.
3. Enter a description, if required. By default, this is the name of the application you're inserting.
4. Click **Browse File** to select an uninstaller file and populate the available matching criteria for the selected uninstaller file.
5. Configure the matching criteria for the executable. You can configure:
   - **File or Folder Name matches**
   - **Upgrade Code matches**
   - **Product Name matches**
   - **Publisher matches**

Windows Services

The Windows service type allows individual service operations to be allowlisted, so that standard users are able to start, stop, and configure services without the need to elevate tools such as the Service Control Manager.

Matching criteria:

- **File or Folder Name matches**
- **Command Line matches**
- **Drive matches**
- **File Hash (SHA-1 Fingerprint) matches**

- **Product Name matches**
- **Publisher matches**
- **Product Description matches**
- **Product Version matches**
- **File Version matches**
- **Service Name matches**
- **Service Display Name matches**
- **Service Actions match**

Windows Store Applications

The **Windows Store** application type allows the installation and execution of Windows Store applications on Windows 8 and later to be allowlisted, so that users are prevented from installing or using unknown or unauthorized applications within the Windows Store.

> ***Note:*** *PMC can only be used to block Windows Store Applications. When you use PMC to block a Windows Store Application and assign a PMC block message to the Application Rule, the native Windows block message overrides the PMC block message, meaning it is not displayed. Event number 116 is still triggered if you have events set up in your Application Rule.*

Windows Scripts

Matching criteria:

- **File or Folder Name matches**
- **Command Line matches**
- **Drive matches**
- **File Hash (SHA-1 Fingerprint) matches**
- **Publisher matches**
- **Trusted Ownership matches**
- **Application Requires Elevation (UAC)**
- **Parent Process matches**
- **Source URL matches**
- **BeyondTrust Zone Identifier exists**

Messages

You can define two types of end user messages:

- **Messages**: Messages take focus when they're displayed to the user.
- **Notifications**: (Windows only). Message notifications appear on the user's task bar. A notifications is displayed as a toast notification.

Messages and Notifications are displayed when a user’s action triggers a rule (application/on-demand or content rule). Rules can be triggered by an application *launch* or *block*, or when content is modified.

Messages provide an effective way of alerting the user before an action is performed, for example, before elevating an application or allowing content to be modified, or advising that an application launch or content modification is blocked.

Messages give the user information about the application or content, the action taken, and can be used to request information from the user.

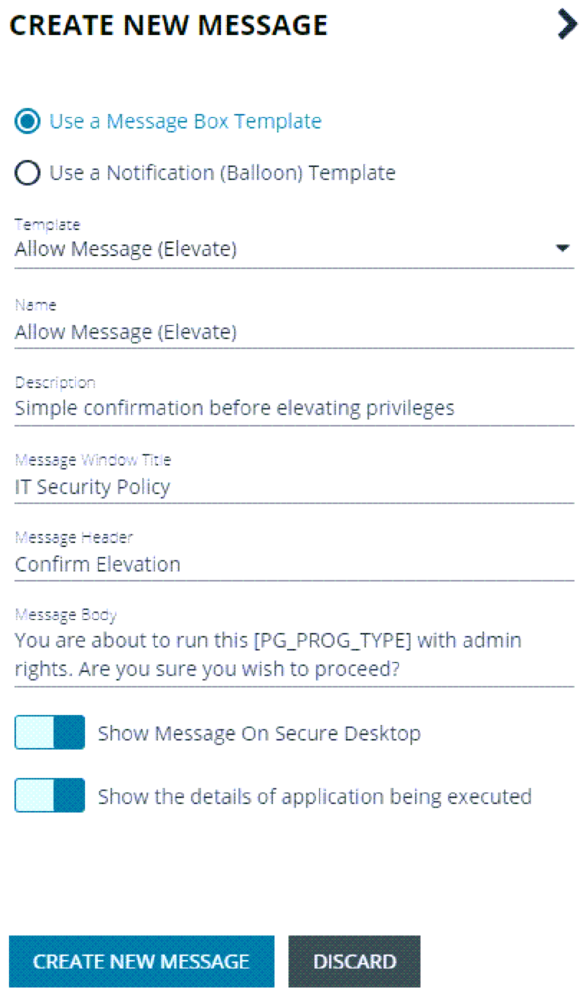
Messages are assigned to Application Rules. A message displays different properties, depending on the targets it is assigned to.

Create a Message

Message templates vary between Windows and macOS.

1. In the Policy Editor, go to **Messages**.
2. Click **Create New Message**.
3. Select a message type: message box or notification. Message types do not apply to macOS messages.
4. Select a message template from the list.
5. Enter a name and description. The default name is the name of the template.
6. Enter the title that displays in the title bar of the window. (Windows only)
7. Enter text for the message header and body.
8. Select **Show Message On Secure Desktop** to show the message on the secure desktop. (Windows only).
9. Turn off **Show the details of application being executed** to hide the details from being displayed. This option is enabled by default. (Windows only).
10. Click **Create New Message**.

You can edit or delete messages at any time.


CREATE NEW MESSAGE

● Use a Message Box Template

○ Use a Notification (Balloon) Template

Template: Allow Message (Elevate)

Name: Allow Message (Elevate)

Description: Simple confirmation before elevating privileges

Message Window Title: IT Security Policy

Message Header: Confirm Elevation

Message Body: You are about to run this [PG_PROG_TYPE] with admin rights. Are you sure you wish to proceed?

Show Message On Secure Desktop

Show the details of application being executed

Customize a Message

There are attributes of a message that you can choose to use when configuring messaging:

- General message features such as header and title information.
- User Reason settings when you want your end users to provide a reason before proceeding.
- Challenge/Response Authorization where a user must enter a response code before proceeding.

Select the **Edit** menu for a message template to customize the message properties.

Message Options

Configure the following settings:

- **Show Message On Secure Desktop**: (Windows only). Select to show the message on the secure desktop. We recommend this if the message is being used to confirm the elevation of a process, for enhanced security.
- **Title Text**: (Windows only). Add text that appears in the title bar of the dialog box.
- **Header Type**: Select the type of header: **Default**, **Error**, **None**, **Warning**, **Question**.
- **Header Background Type**: Select **Solid** or **Custom Image**. If you select **Custom Image**, you must select an image from the **Select Image** list. If you select **Solid**, select a header background color.
- **Show Header Text**: Select if you want to display header text.
- **Header Text**: Add text that displays next to the header type icon.
- **Header Text Color**: Select the color for the header text.
- **Body Text**: Add additional information for the end user.
- **Refer URL Text**: (Windows only). Update text for existing link on the message. In some cases, you might want to provide a website with more information for your end users. The URL appears below the body text.

You can configure the following settings for notifications (Windows only): **Title Text** and **Body Text**.

Add User Reason Properties

To configure the user reason details, select User Reason and set the following:

- **User Reason Type**: Select **Textbox** or **Drop-down**. When you select **Drop-down**, the **User Reason List** is displayed further below. Add reason text that the end user selects as part of the authorization process.
- **Remember User Reason (per application)**: Select to enable. Reasons are stored per-user in the registry.
- **Reason Text**: When using **Textbox** as **User Reason Type**, add the text that displays above the box. When using **Drop-down** add text to display above the drop-down to explain to the user what is expected.
- **Reason Error Message Text**: The text displayed to the end user if the end user clicks **Yes** and doesn't enter a reason.
- **Drop-down List Prompt Text**: The text that displays in the **User Reason** list area.

Add Challenge/Response Authorization

There are two parts to setting up Challenge/Response Authorization:

- **Set a shared key**: The Challenge/Response Key must be set to use Challenge/Response Authorization in your messages. The key is encrypted. The key is required by the Challenge/Response generator to generate response codes. The only way to change the shared key is by setting a new one.
- **Add the authorization type to a message**: When configuring your message, configure the Challenge/Response settings.

The Challenge/Response feature is a global setting and can be configured for Windows and macOS messages. Challenge/Response Authorization only applies to Allow message types.

To add a shared key:

1. In the Policy Editor, go to **Messages**.
2. Select **Challenge/Response Keys**.
3. Enter a key value and enter again to confirm.
4. Click **Set Key**.

To configure Challenge/Response Authorization:

1. In the Policy Editor, go to **Messages**.
2. Select a message template or select an existing message.
3. Select **Challenge / Response Authorization** to activate the feature.
4. Set the following:
   - **Header text**:The text that introduces the challenge/response authorization.
   - **Hint text**: The text that is in the response code field for challenge/response messages.
   - **Authorization period (per application)**: Set this option to determine the length of time a successfully returned challenge code is active for.
   - **Suppress messages once authorized** (Windows only): If the **Authorization period** is not set to **One Use Only**, the **Suppress messages once authorized** option is enabled and configurable.
   - **Show Information Tip** (Windows only): Select to add helpful information for the end user.
   - **Information Tip Text**: Add text that appears above the challenge and response code fields. In Windows, this only appears if the **Show Information Tip** option above is selected.
   - **Error Message Text**: Add text to display to the end user if they enter an incorrect response code.
   - **Maximum Attempts**: Select from **Unlimited** and **Three Attempts**.
   - **Maximum Attempts Exceeded Message Text**: The message is only displayed when **Three Attempts** is selected. Add text to display to the end user if they exceed the allowed number of challenge/response attempts.

Policy Editor Utilities

Policy Editor Licensing

Privilege Management for Windows requires a valid license code to be entered in the Privilege Management Policy Editor. If more than one policy is applied to a computer, you need at least one valid license code for one of those policies.

For example, you could add the Privilege Management for Windows license to a Privilege Management policy that is applied to all managed endpoints, even if it doesn't have any Workstyles. This ensures all endpoints receive a valid license if they have Privilege Management for Windows installed. If you are unsure, then we recommend you add a valid license when you create the Privilege Management policy.

To add a license:

1. In the console, select **Policies** from the sidebar menu.
2. Find the row of the policy, and click the vertical ellipsis. Click **Edit & Lock Policy** from the dropdown menu.
3. Expand the **Utilities** node.
4. Click the **Licenses** node.
5. Click **Add**.
6. Enter the license key, and then click **Add License**.

Import Policy

Privilege Management policies can be imported to and exported from Group Policy as XML files, in a format common to other editions of Privilege Management, such as the Privilege Management ePO Extension. Policies can be migrated and shared between different deployment mechanisms.

1. In the Policy Editor, expand **Utilities**.
2. Select **Import Policy**.
3. Select one of the following:
   - **Merge Policy**
   - **Overwrite Policy**: If you select to overwrite, you can optionally select **Export Existing Policy** to save a copy before overwriting the policy.
4. Drop the file onto the box or click inside the box to navigate to the file.
5. Click **Upload File**.

Policy Deployment Settings in Privilege Management Console

You can choose to deploy policy to your computers automatically or manually.

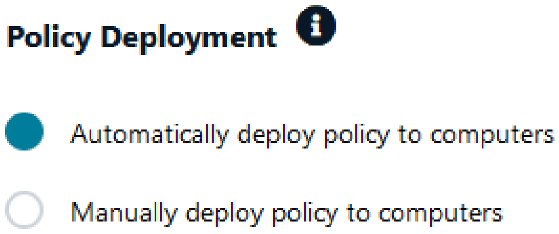
***Note:** It is highly recommended that you automatically deploy policy to computers.*

Manage Policy Deployment Settings

Go to **Configuration** > **Policy & Computer Settings** to choose to deploy the policy automatically or manually to your computers.

If you select automatic deployment, you do not need to do anything else to deploy a policy that is assigned to a group containing computers.

If you select manual deployment, there are two additional options when you interact with one or more computers in the **Computers** grid. These settings allow you to deploy to the selected computers or all computers.



Policy Deployment

● Automatically deploy policy to computers

○ Manually deploy policy to computers

Force Update Policy for End Users

End users are able to force a policy update to their computer from the system tray. This feature allows the end-user to request a new policy from their desktop, thus significantly reducing the time it takes to update a policy.

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

A notification appears with **Update Finished** to notify the user that a policy update has been applied to the client.

A notification appears with **No Updates Found** if the current policy is already up to date.

A notification appears with **Unable to Check for Updates** if the computer is unable to reach the management platform.

***Note:** The Force Update Policy feature is not currently available for macOS.*

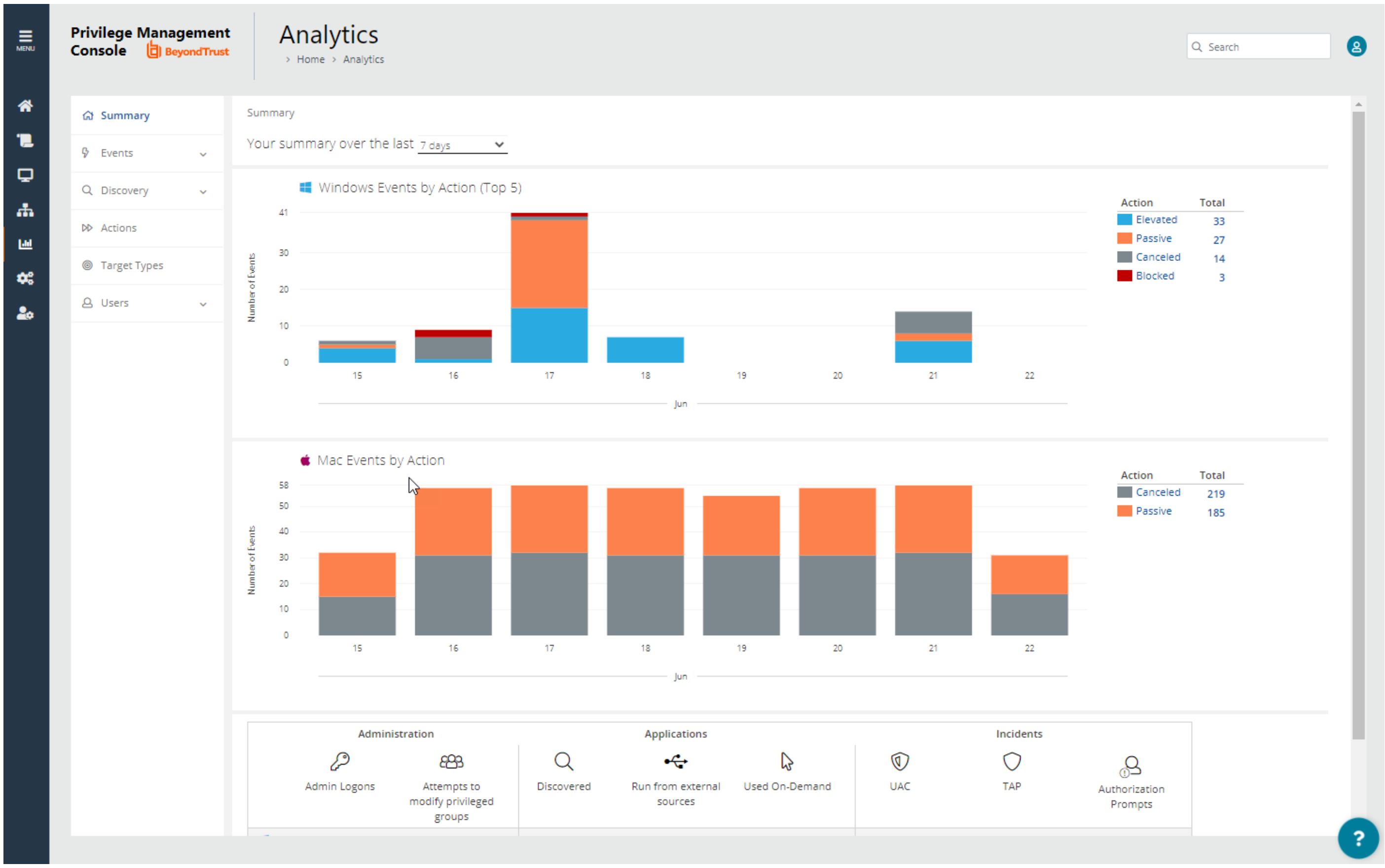
Privilege Management Console Analytics

Use analytics to review detailed activity information for computers in your Privilege Management Console environment. Areas covered include:

- Summary of data collected
- Events
- Discovery
- Actions
- Target types
- Users

Summary Reports in Privilege Management Console

The bar charts on the **Summary** dashboard summarize the most important activity that has occurred in the time period defined by the quick filter. The legends to the right of the bar charts display totals for the shown activities. Click on the legend or on a chart to show details of an action type. The **Administration**, **Applications**, and **Incidents** tables provide additional information to help inform Workstyle development or to show anomalous user behavior in your organization.



Your summary over the last 7 days

Action	Total
Elevated	33
Passive	27
Canceled	14
Blocked	3

Action	Total
Canceled	219
Passive	185

The **Summary** dashboard includes the following tables:

Table	Description
Applications discovered	The total number of newly discovered **Applications** split by the type of user rights required: • Admin rights required • Standard rights required **Discovered** applications are shown in the **Applications** table. Click the number next to the OS icon to show details.
Admin logons, by users, on endpoints	Summarizes the number of admin logons, how many users carried them out, and how many endpoints were used. **Admin Logons** are shown in the **Administration** table. Click the number next to the OS icon to show details.
Applications run from external sources	The number of applications that were run from external sources. Applications **Run from external sources** are shown in the **Applications** table. Click the number next to the OS icon to show details.
Trusted Application Protection	The number of Trusted Application (TAP) incidents, how many users, and how many endpoints were affected. **TAP** events are shown in the **Incidents** table. Click the number next to the OS icon to show details.
Attempts to modify privileged groups	The number of blocked attempts to modify privileged groups. **Attempts to modify privileged groups** are shown in the **Administration** table. Click the number next to the OS icon to show details.
UAC matches	The number of applications that triggered User Account Control (UAC). **UAC** events are shown in the **Incidents** table. Click the number next to the OS icon to show details.

Discovery Reports in Privilege Management Console

This report displays information about applications that have been discovered by the Reporting database for the first time. An application is first discovered when an event is received by the Reporting database.

This dashboard displays the following charts:

Chart	Information
Applications first reported over the last x months (number)	Grouped by: • Admin Rights Detected • Admin Rights Not Detected
Types of newly discovered applications	Grouped by: • Admin Rights Detected • Admin Rights Not Detected

Chart	Information
New applications with admin rights detected (top 10 of <number>)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Matched**, **Application Description**, and **Publisher** filters applied.
New applications with admin rights not detected (top 10 of <number>)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Matched**, **Application Description**, and **Publisher** filters applied.
New applications with admin rights detected (by type)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Admin Rights** and **Application Type** filters applied.
New applications with admin rights not detected (by type)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Admin Rights** and **Application Type** filters applied.

"Discovery by Path" Report

The table displays all distinct applications installed in certain locations that are discovered during the specified time frame.

- **User Profiles:** /Users?%
- **Applications:** /Applications/%, /usr/%
- **Operating System Areas:** /System/%, /bin/%, /sbin/%

> ***Note:*** *The paths can be changed using the filter panel.*

The following columns are available for the Windows **Discovery By Path** table:

- **Path:** The Path category that the application was installed in. You can click the **+** icon to expand the row and see each application.
- **# Users:** The number of users.
- **Median # processes / user:** The median number of processes per user.
- **# Hosts:** The number of hosts.
- **# Processes:** The number of processes.
- **# Applications:** The number of applications.
- **Date first reported:** The date the application was first entered in the database.
- **Date first executed:** The first known date the application was executed.

Some of these columns allow you to drill down to additional information:

- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table and lists the events received in the time period for the selected application.

The following quick filters are available:

- **Platform**
- **Time First Reported**
- **Time First Executed**
- **Path**

"Discovery by Publisher" Report

The table displays the discovered applications grouped by publisher. Where there is more than one application per publisher, click **+** to expand the entry to examine each application.

The following columns are available for the Windows **Discovery By Publisher** table:

- **Publisher**: The publisher of the applications.
- **Description**: The description of the application.
- **Name**: The product name of the application.
- **Type**: The type of application.
- **Version**: The version number of a specific application.
- **# Users**: The number of users.
- **Median # processes / user**: The median number of processes per user.
- **# Hosts**: The number of hosts.
- **# Processes**: The number of processes.
- **# Applications**: The number of applications.
- **Date first reported**: The date the application was first entered in the database.
- **Date first executed**: The first known date the application was executed.
- **Name**: The product name. This is hidden by default but you can select it from the **Actions** > **Choose Columns** menu.

Some of these columns allow you to drill down to additional information:

- **"i" icon**: Opens the **Applications report** for that application.
- **# Users**: Displays a list of users the application events came from.
- **# Hosts**: Displays a list of hosts the application events came from.
- **# Processes**: Displays the **Events All** table and lists the events received in the time period for the selected application.

The following quick filters are available:

- **Platform**
- **Time First Reported**
- **Time First Executed**
- **Path**
- **Source**
- **Admin Rights**
- **Ownership**
- **Rule Match Type**

"Discovery by Type" Report

The table displays applications filtered by type. When there is more than one application per type, click **+** to expand the entry to see each application.

The following columns are available for the **Discovery By Type** table:

- **Type**: The type of application
- **# Users**: The number of users
- **Median # processes / user**: The median number of processes per user
- **# Hosts**: The number of hosts
- **# Processes**: The number of processes
- **Applications**: The number of applications
- **Date first reported**: The date the application was first entered in the database
- **Date first executed**: The first known date the application was executed

Some of these allow you to drill down to additional information:

- **"i" icon**: Opens the **Target Types** > **Applications report** which is filtered to that application
- **# Users**: Displays a list of users the application events came from
- **# Hosts**: Displays a list of hosts the application events came from
- **# Processes**: Displays the **Events All** table and lists the events received in the time period for the selected application

The following quick filters are available:

- **Platform**
- **Time First Reported**
- **Time First Executed**
- **Path**

"Discovery Requiring Elevation" Report

The table displays the applications that were elevated or required admin rights.

The following columns are available for the **Discovery Requiring Elevation** table:

- **Description**: The description of the application
- **Publisher**: The publisher of the application
- **Name**: The product name of the application
- **Type**: The type of application
- **Elevate Method**: The type of method used to elevate the application: **All**, **Admin account used**, **Auto-elevated**, or **on-demand**
- **Version**: The version number of a specific application
- **# Users**: The number of users
- **Median # processes / user**: The median number of processes per user
- **# Hosts**: The number of hosts
- **# Processes**: The number of processes

- **Date first reported**: The date the application was first entered in the database
- **Date first executed**: The first known date the application was executed

Some of these allow you to drill down to additional information:

- **"i" icon**: Opens the **Target Types** > **Applications report** filtered to that application.
- **# Users**: Displays a list of users the application events came from.
- **# Hosts**: Displays a list of hosts the application events came from.
- **# Processes**: Displays the **Events All** table and lists the events received in the time period for the selected application.
- **Elevate Method**: Displays the **Events All** table with an extra **Elevate Method** column.

The following quick filters are available:

- **Platform**
- **Time First Reported**
- **Time First Executed**
- **Elevate Method**
- **Path**
- **Source**
- **Challenge / Response**
- **Matched**

"Discovery from External Sources" Report

This table displays all applications that have originated from an external source, such as the internet or an external drive.

You can click on the link in the **Description** column to see more detailed information on the application, including the actions over the last 30 days split by the type of token, the top 10 users, the top 10 hosts, the run method, and the portion of those discoveries where admin rights were detected.

The following columns are available for the **Discovery By Publisher** table:

- **Description:** The description of a specific application
- **Publisher:** The publisher of the applications
- **Name:** The product name of a specific application
- **Type:** The type of application
- **Source:** The source of the application
- **Version:** The version number of a specific application
- **# Users:** The number of users
- **Median # processes/user:** The median number of processes per user
- **# Hosts:** The number of hosts
- **# Processes:** The number of processes
- **Date first reported:** The date when the application was first entered into the database
- **Date first executed:** The first known date that the application was executed

New applications from external sources first reported over the last <time period>

This table groups the applications by type. You can click the plus icon to expand the path to show each individual application. You can view additional information about the application, their type, version, and the number of users using them. You can click the description to see in depth information about the application.

"Discovery All" Report

This table lists all applications discovered in the time period, grouped by the application description. If multiple versions of the same application exist, they are grouped on the same line. These can be expanded by clicking on the plus (**+**) symbol in the **Version** column.

The following columns are available for the Windows **Discovery By Publisher** table:

- **Description:** The description of a specific application
- **Publisher:** The publisher of the applications
- **Name:** The product name of a specific application
- **Type:** The type of application
- **Version:** The version number of a specific application
- **# Users:** The number of users
- **Median # processes/user:** The median number of processes per user
- **# Hosts:** The number of hosts
- **# Processes:** The number of processes
- **Date first reported:** The date when the application was first entered into the database
- **Date first executed:** The first known date that the application was executed

You can click on the link in the **Description** column to see more detailed information on the application, including the actions over the last 30 days split by the type of token, the top 10 users, the top 10 hosts, the run method, and the portion of those discoveries where admin rights was detected.

Actions Reports in Privilege Management Console

The following reports are available for actions:

- **Actions Elevated**
- **Actions Blocked**
- **Actions Passive**
- **Actions Canceled**
- **Actions Custom**
- **Actions Drop Admin Rights**

"Actions Elevated" Report

The **Actions Elevated** report breaks down the elevated application activity by target type.

This dashboard displays the following charts:

Chart	Information
Elevated activity over the last <time period>	The number of targets that were elevated for each time segment split by the type of action. Clicking on the chart takes you to the **Target Types > All** report with the **Action**, **Target Type**, **Range Start Time**, and **Range End Time** filters applied.
Distinct elevated target count by target type	The number of targets that were elevated for the complete time period split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action** and **Target Type** filters applied.
Top 10 elevated targets	The top ten targets that were elevated for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Actions Blocked" Report

The **Actions Blocked** dashboard breaks down the blocked application activity by target type.

This dashboard displays the following charts:

Chart	Information
Blocked activity action over the last <time period>	The number of targets that were blocked for each time segment split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action**, **Target Type**, **Range Start Time**, and **Range End Time** filters applied.
Distinct blocked action target count by target type	The number of targets that were blocked for the complete time period split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action** and **Target Type** filters applied.
Top 10 blocked action targets	The top ten targets that were blocked for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Actions Passive" Report

The **Actions Passive** dashboard breaks down the passive application activity by target type.

This dashboard displays the following charts:

Chart	Information
Passive action activity over the last <time period>	The number of targets where a passive token was used for each time segment split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action**, **Target Type**, **Range Start Time**, and **Range End Time** filters applied.
Distinct passive activity action target count by target type	The number of targets where a passive token was used for the complete time period split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action** and **Target Type** filters applied.
Top 10 passive action targets	The top ten targets where a passive token was used for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Actions Canceled" Report

The **Actions Canceled** dashboard breaks down the canceled application activity by target type.

This dashboard displays the following charts:

Chart	Information
Canceled activity action over the last <time period>	The number of targets that were canceled for each time segment split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action**, **Target Type**, **Range Start Time**, and **Range End Time** filters applied.
Distinct canceled action target count by target type	The number of targets that were canceled for the complete time period split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action** and **Target Type** filters applied.
Top 10 canceled action targets	The top ten targets that were canceled for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Actions Custom" Report

The **Actions Custom** report breaks down the custom application activity by the type of action.

This dashboard displays the following charts:

Chart	Information
Custom action activity over the last <time period>	The number of targets where a Custom Token was used for each time segment split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action**, **Target Type**, **Range Start Time**, and **Range End Time** filters applied.
Distinct custom action target count by target type	The number of targets where a Custom Token was used for the complete time period split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action** and **Target Type** filters applied.
Top 10 custom action targets	The top ten targets where a Custom Token was used for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

"Actions Drop Admin Rights" Report

The **Actions Drop Admin Rights** dashboard breaks down the drop admin application activity by target type.

This dashboard displays the following charts:

Chart	Information
Drop admin rights action activity over the last <time period>	The number of targets where a drop admin rights token was used for each time segment split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action**, **Target Type**, **Range Start Time**, and **Range End Time** filters applied.
Distinct drop admin rights action target count by target type	The number of targets where a drop admin rights token was used for the complete time period split by the type of action. Click the chart to go to the **Target Types > All** report with the **Action** and **Target Type** filters applied.
Top 10 targets drop admin rights action targets	The top ten targets where a drop admin rights token was used for the time period. Click the chart to go to the **Events > All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

Target Types

This table lists all applications active in the time period, grouped by the application description ordered by user count descending.

The following columns are available for the Windows **Discovery All** table:

- **Description:** The description of a specific application
- **Platform:** The platform that the events came from
- **Publisher:** The publisher of a specific application
- **Product Name:** The product name of a specific application

- **Application Type:** The type of application
- **Product Version:** The version number of a specific application
- **# Process Count:** The number of processes
- **# User Count:** The number of users
- **# Host Count:** The number of hosts

You can click **Description** to view additional information about the target, its actions over the time period, the top 10 users, top 10 hosts, the type of run method, and whether admin rights were detected.

Users Reports in Privilege Management Console

There are three reports for users:

- **User Experience Report**
- **Users Privileged Logons**
- **Users Privileged Account Management**

User Experience Report

The **User Experience** report shows you how many users have interacted with PMC events, and is broken down over the specified time frame.

This dashboard displays the following charts:

Chart	Information
User experience over the last <time period>	A chart showing the number of times users canceled a message, were presented a challenge, were blocked from launching an activity, or were allowed to use an application using on-demand privileges. Click the chart to see users who encountered each event type. Click a user to see user activity over the time period set by the filter. On the resulting user activity page, click the number in the **Applications Used** row to navigate to the **Target Types > All** page.
Message distribution	This table shows you the average number of *Allow* messages and *Block* messages users receive per day. Click the chart to see users who encountered each event type. Click a user to see user activity over the time period set by the filter. On the resulting user activity page, click the number in the **Applications Used** row to navigate to the **Target Types > All** page.
Messages per action type	A chart showing how many times prompts and notifications were allowed or blocked, as well as the number of notifications presented. Click a number in the **Allowed** or **Blocked** row to see detailed information about each event of that message type.

Users Privileged Logons Report

The **Privileged Logon** report shows you how many accounts with standard user rights, power user rights, and administrator rights have generated logon events broken down over the specified time frame.

This dashboard displays the following charts:

Chart	Information
Privileged logons over the last <time period>	A chart and table showing the number of logons by the different account types over time. Click the chart for more information about each privileged logon with the **Range Start Time**, **Range End Time**, **Show Administrator Logons**, and **Show Standard User Logons** filters applied.
Administrators, Power Users, and Standard Users table	This table shows you the number of logon events made by administrators, power users, and standard users, as well as how many users logged in.
Logons by account privileged	A chart showing the total number of logons, broken down by logon privilege. Click the chart for more information about the user logons for the time period with the **Show Administrator Logons**, **Show Standard User Logons**, and **Show PowerUser Logons** filters applied.
Logons by account type	A chart showing the total number of logons, broken down by domain accounts and local accounts. Click the chart for more information about the user logons for the time period with the **Account Authority**, **Show Administrator Logons**, **Show Standard User Logons**, and **Show PowerUser Logons** filters applied.
Top 10 logons by chassis type	A chart showing the total number of logons, broken down by the top 10 chassis types. Click the chart for more information about the user logons for the time period with the **Show Administrator Logons**, **Show Standard User Logons**, and **Show PowerUser Logons** filters applied.
Top 10 logons by operating system	A chart showing the total number of logons, broken down the top 10 host operating systems. Click the chart for more information about the user logons for the time period with the **Show Administrator Logons**, **Show Standard User Logons**, **OS**, and **Show PowerUser Logons** filters applied.
Top 10 accounts with admin rights	A chart showing the top 10 accounts with admin rights that have logged into the most host machines. Click the chart for more information about the user logons for the time period with the **Show Administrator Logons**, **Show Standard User Logons**, **User Name**, and **Show PowerUser Logons** filters applied.
Top 10 hosts with admin rights	A chart showing the top 10 host machines that have been logged onto by the most users with admin rights. Click the chart for more information about the user logons for the time period with the **Host Name**, **Show Administrator Logons**, **Show Standard User Logons**, and **Show PowerUser Logons** filters applied.

Users Privileged Account Management Report

The **Privileged Account Management** report shows any blocked attempts to modify privileged accounts over the specified time interval.

Chart	Description
Privileged Account Management over the last <time period>	A chart breaking down the privileged account management events and the number of events.
Activity table	A table showing the number of **Users blocked**, **Hosts blocked**, **Applications blocked**, and the **Total number of block events** within the specified time frame.
By Privileged Group	The same data grouped by type of account. Click the account type to go to detailed information about the account and hosts with the **Group Name** filter applied.
By application	A chart showing the privileged account modification activity that was blocked, broken down by the description of the application used. Click the chart to go to a more detailed view of that privileged account management activity for that application with the **Application Description** filter applied.
Top 10 users attempting account modifications	A chart showing the top 10 users who attempted modifications. Click the chart to go to a more detailed view of the privileged account management account modifications with the **Application User Name** filter applied.
Top 10 hosts attempting account modifications	A chart showing the top 10 hosts attempting privileged account modifications. Click the chart to go to a more detailed view of that privileged account management account modifications with the **Host Name** filter applied.

Events Reports in Privilege Management Console

This report shows information about the different types of events that have been raised over the specified time period. It also shows the time elapsed since a host raised an event.

Chart	Description
Events over the last <time period>	A column chart showing the number of the different event types, broken down by the time period. Clicking the chart takes you to the **Events > All** report with the **Event Category**, **Range Start Time**, and **Range End Time** filters applied.
Event Types	A chart showing how many events have been received, broken down by the event type. Clicking the chart takes you to the **Events > All** report with the **Event Number** filter applied.
By Category	A chart breaking down the events received, split by category. Clicking the chart takes you to the **Events > All** report with the **Event Category** filter applied.
Time since last endpoint event	A chart showing the number of computers in each time group since the last event category. Clicking the chart takes you to more detailed information about the host.

Event Types

Privilege Management sends events to the local Application event log, depending on the audit and privilege monitoring settings within the Privilege Management policy.

The following events are logged by Privilege Management:

Event ID	Description
0	Service Control Success
1	Service Error
2	Service Warning
100	Process has started with admin rights added to token.
101	Process has been started from the shell context menu with admin rights added to token.
103	Process has started with admin rights dropped from token.
104	Process has been started from the shell context menu with admin rights dropped from token.
106	Process has started with no change to the access token (passive mode).
107	Process has been started from the shell context menu with no change to the access token (passive mode).
109	Process has started with user’s default rights enforced.
110	Process has started from the shell context menu with user’s default rights enforced.
112	Process requires elevated rights to run.
113	Process has started with Custom Token applied.
114	Process has started from the shell context menu with user’s Custom Token applied.
116	Process execution was blocked.
118	Process started in the context of the authorizing user.
119	Process started from the shell menu in the context of the authorizing user.
120	Process execution was canceled by the user.
130	A Mac application bundle was installed.
131	A Mac application bundle was deleted.
150	Privilege Management handled service control start action.
151	Privilege Management handled service control stop action.
152	Privilege Management handled service control pause/resume action.
153	Privilege Management handled service control configuration action.
154	Privilege Management blocked a service control start action.
155	Privilege Management blocked a service control stop action.
156	Privilege Management blocked a service control pause/resume action.
157	Privilege Management blocked a service control configuration action.
158	Privilege Management service control action run in the context of the authorizing user.
159	Privilege Management service control start action canceled.
160	Privilege Management service control stop action canceled.
161	Privilege Management service control pause/resume action canceled.
162	Privilege Management service control configuration action canceled.
198	Privileged group modification blocked.
199	Process execution was blocked, the maximum number of challenge / response failures was exceeded.
Configuration Events	
10	License Error

Event ID	Description
200	Config Config Load Success
201	Config Config Load Warning
202	Config Config Load Error
210	Config Config Download Success
211	Config Config Download Error
User / Computer Events	
300	User User Logon
400	Service Privilege Management Service Start
401	Service Privilege Management Service Stop
Content Events	
600	Process Content Has Been Opened (Updated Add Admin)
601	Process Content Has Been Updated (Updated Custom)
602	Process Content Access Drop Admin (Updated Drop Admin)
603	Process Content Access Was Cancelled By The User (Updated Passive)
604	Process Content Access Was Enforced With Default Rights (Updated Default)
605	Process Content Access Was Blocked
606	Process Content Access Was Cancelled
607	Process Content Access Was Sandboxed
650	Process URL Browse
706	Process Passive Audit DLL
716	Process Block DLL
720	Process Cancel DLL Audit

Each process event contains the following information:

- Command line for the process
- Process ID for the process (if applicable)
- Parent process ID of the process
- Workstyle that applied
- Application Group that contained the process
- End user reason (if applicable)
- Custom access token (if applicable)
- File hash
- Certificate (if applicable)

"Events All" Report

A search history is automatically saved when you select filters on the **Events / All** page.

You can select a previous search item and clear filters associated with that search. A new search item is then automatically saved to the list of previous searches.

The search history is retained between your sessions. The list can include up to 10 search items.

The following columns are available for the Windows **Events** > **All** table:

- **Event Time:** The time of the event
- **Reputation:** Indicates the results of the reputation scan analysis.
- **Platform:** The platform that the event came from
- **Description:** The description of the event
- **User Name:** The user name of the user who triggered the event
- **Host Name:** The host name where the event was triggered
- **Event Type:** The type of event
- **Workstyle:** The Workstyle containing the rule that triggered the event
- **Event Category:** The category of the event
- **Elevation Method:** The method of elevation

You can click some of the column data to review additional information on that event.

"Process Detail" Report

This report gives details about a specific process control event. Only processes that match rules in Workstyles are displayed.

There is an **Advanced** view available with this report, which is available from the **Filters** dropdown. The **Advanced** view shows you the full set of columns available in the database.

- **Start Time:** The start time of the event
- **Platform:** The platform that the events came from
- **Description:** The description of a specific application
- **Publisher:** The publisher of a specific application
- **Application Type:** The type of application
- **File Name:** The name of the file, where applicable
- **Command Line:** The command line path of the file, if applicable
- **Product Name:** The product name, where applicable
- **Trusted Application Name:** The name of the trusted application
- **Trusted Application Version:** The version of the trusted application
- **Product Version:** The version of the product of applicable
- **Group Policy Object:** The Group Policy object, if applicable
- **Workstyle:** The Workstyle containing the rule that triggered the event
- **Message:** Any message associated with the event
- **Action:** Any action associated with the event
- **Application Group:** The Application Group that the application that triggered the event belongs to
- **PID:** The operating system process identifier
- **Parent PID:** The operating system process identifier of the parent process
- **Parent Process File Name:** The name of the parent process

- **Shell/Auto:** Whether the process was launched using the shell **Run with Privilege Management** option or by normal means (opening an application)
- **UAC Triggered:** Whether or not Windows UAC was triggered
- **Admin Rights Detected:** Whether or not admin rights was detected
- **User Name:** The user name that triggered the event
- **Host Name:** The host name where the event was triggered
- **Rule Script File Name:** The name of the Rule Script (Power Rule) that ran
- **Rule Script Affected Rule:** True when the Rule Script (Power Rule) changed one or more of the default Privilege Management for Windows rules
- **User Reason:** The reason given by the user, if applicable
- **COM Display Name:** The display name of the COM, if applicable
- **Source URL:** The source URL, if applicable

Privilege Management Console Report Filters

Filters and advanced filters are available from the **Filters** dropdown.

The reports retrieve data and sort it using Javascript. If the volume of data exceeds the row limit, you may get misleading results due to this restriction.

Name	Description
Action	This filter allows you to filter by a type of action.
	• All • Elevated • Blocked • Passive • Sandboxed • Custom • Drop Admin Rights • Enforce Default Rights • Canceled • Allowed
Activity ID	Each activity type in Privilege Management has a unique ID. This is generated in the database as required.
Admin Required	This allows you to filter on whether admin rights were required, not required, or both.
	Filter options: • **All** • **True** • **False**

Name	Description
Authorization Required	This allows you to filter on whether authorization was required, not required, or both.
	Filter options: - **All** - **True** - **False**
Admin Rights	Allows you to filter by the admin rights token.
	Filter options: - **All** - **Detected** - **Not Detected**
Application Description	A text field that allows you to filter on the application description.
Application Group	A text field that allows you to filter on the Application Group. You can obtain the Application Group from the policy editor.
Application Hash	This field is used by Reporting. You do not need to edit it.
Application Type	A text field that allows you to filter on the application type. You can obtain the application type from the policy editor.
Authorizing User Name	The name of the user that authorized the message.
Browse Destination URL	The destination URL of the sandbox.
Challenge/Response	Allows you to filter by challenge/response events. For example, you can filter the application that required elevation on those applications that were launched following a completed challenge/response message.
	Filter options: - **All** - **Only C/R**
Client IPV4	This field is used by Reporting. You do not need to edit it.
Client Name	This field is used by Reporting. You do not need to edit it.
COM Application ID	This field is used by Reporting. You do not need to edit it.
COM Display Name	This field is used by Reporting. You do not need to edit it.
COM CLSID	This field is used by Reporting. You do not need to edit it.
Command Line	A text field that allows you to filter on the command line.

Name	Description
Date Field	This allows you to filter by the time the event was first generated, discovered, or executed.
	Filter options: • **Time Generated** This is the time that the event was generated. One application can have multiple events. Each event has a **Time Generated** attribute. • **Time App First Discovered** This is the time that the first event for a single application was entered into the database. This can be delayed if the user is working offline. • **Time App First Executed** This is the first known execution time of events for that application.
Device Type	The type of device that the application file was stored on.
	Filter options: • **Any** • **Removeable Media** • **USB Drive** • **Fixed Drive** • **Network Drive** • **CDROM Drive** • **RAM Drive** • **eSATA Drive** • **Any Removeable Drive or Media**
Distinct Application ID	This field is used by Reporting. You do not need to edit it.
Elevate Method	Allows you to filter by the elevation method used.
	Filter options: • **All** • **Admin account used** • **Auto-elevated** • **On-demand**

Name	Description
Event Category	This filter allows you to filter by the category of the event.
	Filter options: • **All** • **Process** • **Content** • **DLL Control** • **URL Control** • **Privileged Account Protection** • **Agent Start** • **User Logon** • **Services**
Event Number	This field is used by Reporting. You do not need to edit it. The number assigned to the event type.
File Owner	The owner of the file.
File Version	You can filter on the file version in the **Advanced View** of the **Process Detail** report.
GPO Name	You can filter on the Group Policy Object (GPO) name in some of the advanced reports, such as **Process Detail**.
Host Name	This field allows you to filter by the name of the computer the event came from.
Ignore Admin Required Events	This field is used by Reporting. You do not need to edit it.
Just Discovery Events	This field is used by Reporting. You do not need to edit it.
Matched	Allows you to filter on the type of matching.
	Filter options: • **All** • **Matched as child** • **Matched directly**
Message Name	The name of the message that was used.
Message Type	The type of message that was used:
	Filter options: • **Any** • **Prompt** • **Notification** • **None**

Name	Description
Ownership	Allows you to group by the type of owner.
	Filter options: - **All** - **Trusted owner** - **Untrusted owner**
Parent PID	The operating system process identifier of the parent process.
Parent Process File Name	The file name of the parent process.
Path	Allows you to filter by the path. For example, to filter on applications that were launched from the System path.
	Filter options: - **All** - **System** - **Program Files** - **User Profiles**
PID	The operating system process identifier.
Platform	Filters by the type of operating system.
	- **Windows** Filters by endpoints running a Windows operating system. - **macOS** Filters by endpoints running a Mac operating system.
Process Unique ID	The unique identification of the process.
Product Code	This field is used by Reporting. You do not need to edit it.
Product Name	The product name of the application.
Product Version	The product version of the application.
Program Files Path	Sets the Program Files path used by the **Discovery > Path** report.
Publisher	The publisher of the application.
Range End Time	The end time of the range being displayed.
Range Start Time	The start time of the range being displayed.
Row Limit	The maximum number of rows to be retrieved from the database.
Rule Script Affected Rule	True when the Rule Script (Power Rule) changed one or more of the default Privilege Management rules; otherwise, false.
Rule Script File Name	The Rule Script (Power Rule) file name on disk, if applicable.
Rule Script Name	The name of the assigned Rule Script (Power Rule).
Rule Script Output	The output of the Rule Script (Power Rule).
Rule Script Publisher	The publisher of the Rule Script (Power Rule).

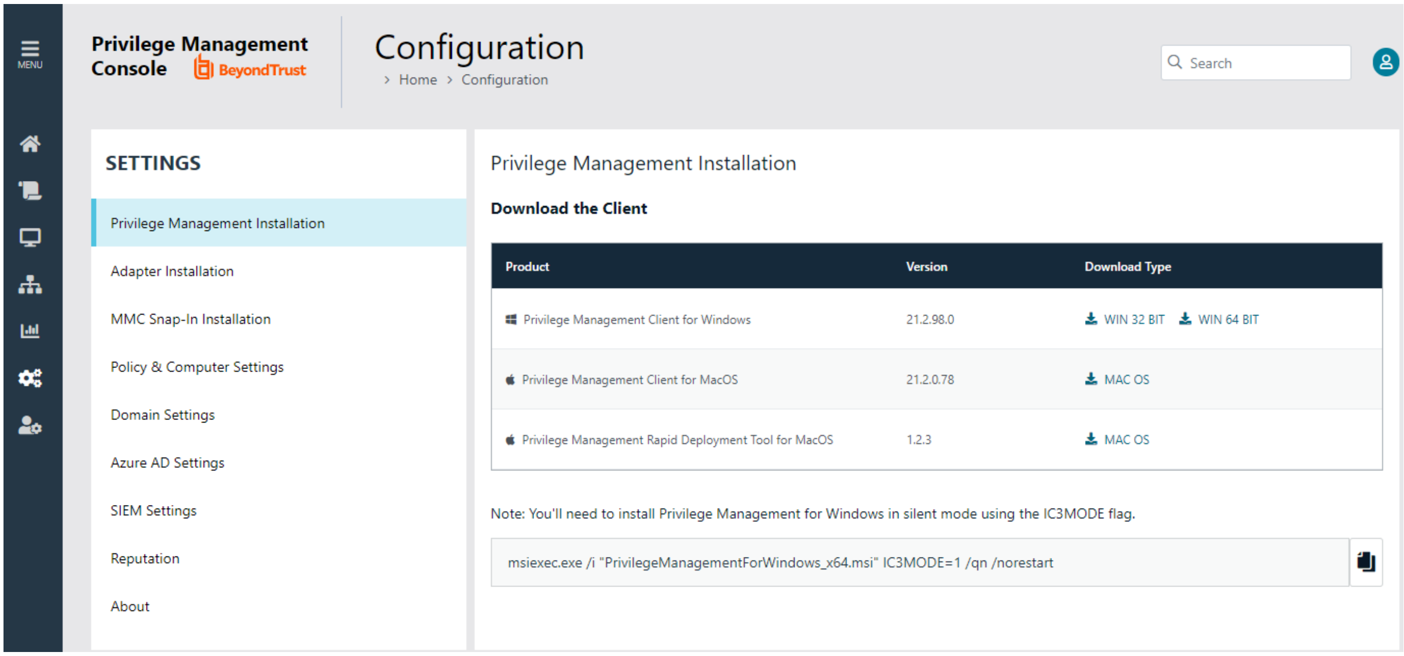
Name	Description
Rule Script Result	The result of the Rule Script (Power Rule). This can be: - *<None>* - *Script ran successfully* - *[Exception Message]* - *Script timeout exceeded: <X> seconds* - *Script execution canceled* - *Set Rule Properties failed validation: <reason>* - *Script execution skipped: Challenge Response Authenticated* - *Script executed previously for the parent process: Matched as a child process so cached result applied* - *Script execution skipped: <app type> not supported* - *Script execution skipped: PRInterface module failed signature check* - *Set RunAs Properties failed validation: <reason>*
Rule Script Status	The status of the Rule Script (Power Rule). This can be: - **<None>** - **Success** - **Timeout** - **Exception** - **Skipped** - **ValidationFailure**
Rule Script Version	The version of the assigned Rule Script (Power Rule).
Rule Match Type	Rule Match Type: - **Any** - **Direct match** - **Matched on parent**
Sandbox	The sandboxed setting.
	Filter options: - **Not Set** - **Any Sandbox** - **Not Sandboxed**
Shell or Auto	Whether the process was launched using the shell **Run with Privilege Management** option or by normal means (opening an application):
	Filter options: - **Any** - **Shell** - **Auto**

Name	Description
Show Discovery Events	Whether or not you want to show Discovery events. An event is a Discovery event if it's been inserted into the database in the filtered time period.
Source	The media source of the application. For example, whether the application was downloaded from the Internet or removable media.
	Filter options: • **All** • **Downloaded over the internet** • **Removable media** • **Any external source**
System Path	Sets the system path.
Target Description	This field allows you to filter by the target description.
Target Type	This filter allows you to filter by a type of target. For example, you can filter by the applications that have been canceled across your time range in the **Actions > Canceled** report.
	Filter options: • **All** • **Applications** • **Services** • **COM** • **Remote PowerShell** • **ActiveX** • **URL** • **DLL** • **Content**
Time First Executed	This is the time range over which the application was first executed.
	Filter options: • **24 Hours** • **7 Days** • **30 Days** • **6 Months** • **12 Months**
Time First Reported	This is the time range filtered by the date the application was first entered into the database.
	Filter options: • **24 Hours** • **7 Days** • **30 Days** • **6 Months** • **12 Months**

Name	Description
Time Range	This is the time range over which the actions are displayed.
	Filter options: • **24 Hours** • **7 Days** • **30 Days** • **6 Months** • **12 Months**
Token Type	The type of Privilege Management token that was applied to the trusted application protection event.
	Filter options: • **All** • **Blocked** • **Passive** • **Canceled**
Trusted Application Name	The trusted application that triggered the event.
Trusted Application Version	The trusted application version number.
Trusted File Owner	Whether the file owner of the target file is considered trusted. To be a trusted owner, the user must be in one of the following Windows groups: **TrustedInstaller**, **System**, or **Administrator**.
UAC Triggered	Whether or not Windows UAC was triggered.
	Filter option: • **Not Set** • **Triggered UAC** • **Did not trigger UAC**
Uninstall Action	The type of uninstall action.
	Filter options: • **Any** • **Change/Modify** • **Repair** • **Uninstall**
Upgrade Code	This field is used by Reporting. You do not need to edit it.
User Name	The user name of the user who triggered the event.
User Profiles Path	Sets the **User Profiles** path.
Workstyle	A dropdown of Workstyles in use.
Workstyle Name	The name of the Workstyle that contains the rule that matched the application.
Zone Identifier	The BeyondTrust Zone Identifier. This tag will persist to allow you to filter on it even if the ADS tag applied by the browser is removed.

Privilege Management Console Configuration

The **Configuration** page contains a variety of settings to help with automation and easy installation.



Download the Client

Product	Version	Download Type
Privilege Management Client for Windows	21.2.98.0	WIN 32 BIT WIN 64 BIT
Privilege Management Client for MacOS	21.2.0.78	MAC OS
Privilege Management Rapid Deployment Tool for MacOS	1.2.3	MAC OS

Note: You'll need to install Privilege Management for Windows in silent mode using the IC3MODE flag.

```
msiexec.exe /i "PrivilegeManagementForWindows_x64.msi" IC3MODE=1 /qn /norestart
```

The **Configuration** menu contains the following areas:

- Privilege Management Installation
- Adapter Installation
- MMC Snap-In Installation
- Policy & Computer Settings
- Domain Settings
- Azure AD Settings
- SIEM Settings
- Reputation Settings

For more information, please see the following:

- *"Privilege Management Console QuickStart" on page 8*
- *"Install the Windows Adapter" on page 9*
- *"Install the Mac Adapter" on page 12*
- *"Configure the Privilege Management MMC PMC snap-in" on page 15*
- *"Policy Deployment Settings in Privilege Management Console" on page 75*

Policy and Computer Settings

The **Policy and Computer Settings** section is where you can manage automatic policy deployment, computer deactivation, and computer deduplication.

Policy Deployment

On this page, you can choose to automatically deploy a policy to computers, or manually deploy a policy to computers.

To turn on automatic policy deployment:

1. Select **Configuration** from the sidebar menu.
2. Under **Settings**, click **Policy & Computer Settings**.
3. Click the **Automatically deploy policy to computers** radio button.

For more information, please see "Policy Deployment Settings in Privilege Management Console" on page 75

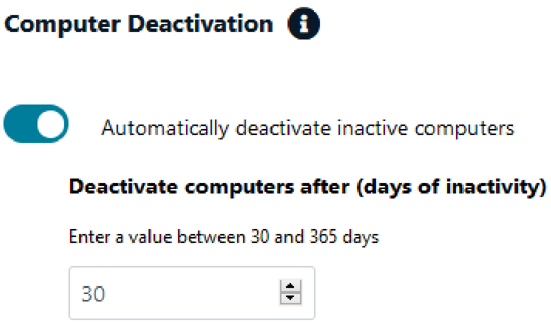
Computer Deactivation Settings

This page allows you to choose whether you want to deactivate computers that have not contacted PMC for a number of days that you define, when you enable the functionality. For example, a computer might not have contacted PMC if it's a duplicate.

The task to deactivate computers runs every day at 02:30 server time on the node where the job service is running. The deactivation job is audited in the **Activity Log**. You can filter by deactivated computers in the **Computers** grid.

To set auto deactivation on computers, select **Automatically deactivate inactive computers**. Enter the number of days that pass before the computer will be deactivated.

Deactivated computers are disconnected from PMC and are no longer able to communicate with PMC. This action can't be reversed unless you reinstall the software on the client computer.



Computer Deactivation

Automatically deactivate inactive computers

Deactivate computers after (days of inactivity)

Enter a value between 30 and 365 days

30

With the release of PMC version 20.1, auto deactivate functionality is turned off by default, for both upgrades and new installations. If you want to turn on auto deactivate functionality, use the **Computer Deactivation** setting. The functionality remains unchanged.

You can also manually deactivate computers.

For more information, please see the following:

- *"View Duplicate Computers" on page 29*
- *"Deactivate Computers" on page 29*

> ***Note:** You can view a list of deactivated computers from the **Computers** grid by filtering by the **Deactivated** status.*

Computer Deduplication Settings

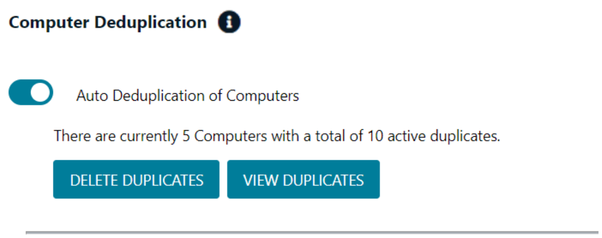
A computer duplicate is one that has the same host name as another computer but has not connected to the Privilege Management Console as recently. Auto deduplication is turned off by default.

To turn on deduplication:

1. Select **Configuration** from the sidebar menu.
2. Under **Settings**, click **Policy & Computer Settings**.
3. Click the **Auto Deduplication of Computers** toggle. The deduplication job runs nightly and detects duplicate computers.
4. Click **Save Changes**.

When deduplication is turned on and duplicate computers are detected, the status is provided on this page.

- Click **View Duplicates** to display the computers on the **Computers** page filtered by **Total Duplicates**.
- Click **Delete Duplicates** to remove any duplicates detected. The computers are no longer displayed on the **Computers** page.



Computer Deduplication

Auto Deduplication of Computers

There are currently 5 Computers with a total of 10 active duplicates.

Add a Domain

An email address is entered when a user account is created in PMC. Email notifications are sent for PMC user registration and confirmation.

> **IMPORTANT!**
>
> *It is a security best practice to restrict the domains where PMC communications can be sent.*

One domain always exists on the **Domain Settings** page. The first domain is created when the application is deployed for the first time for the customer.

Any additional domains added must exist in your authentication provider (ADFS or Azure AD) before you can add it here. If you add another domain, you can add an Administrator account associated with that domain.

> ***Note:** Only a user assigned to the Administrator role can add a domain.*

To add a domain:

1. Navigate to **Configuration > Domain Settings**.
2. Click **Add Domain**.

Note: *A valid domain must contain at least 2 segments and be at least 3 characters long.*

3. Type the domain name, and then click **Add Domain**.

At any time after a domain is created, click the **x** to remove it. A toast notification indicates the domain is successfully removed.

There must always be at least one domain in the list.

Configure SIEM Settings

Configure SIEM settings in PMC to send audit event data to an accessible S3 bucket. Events include computer, activity, and authorization request. Events are sent to the same S3 bucket in the selected format (CEF or ECS).

You must configure the S3 bucket details before you can configure the SIEM integration in PMC. In AWS, set up the bucket and access to the bucket. This includes:

- Create a bucket. When creating the bucket be sure to note the bucket name and region. You need to enter the information when configuring the settings in PMC.
- Create an access policy. When creating the access policy, the permissions required for the integration include: **PutObject**, **ListAllMyBuckets**, **GetBucketAcl**, and **GetBucketLocation**.
- Add a user. When attaching a user to a policy, be sure to select **Programmatic access** as the access type and **Attach existing policies directly** as the permission type. Copy the Access ID and secret access key to a file; you need to enter the details when configuring the settings in PMC.

For more information, please see the following AWS documentation:

- *Create your first S3 bucket at https://docs.aws.amazon.com/AmazonS3/latest/userguide/creating-bucket.html*
- *Creating IAM policies at https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create.html*
- *Creating an IAM user in your AWS account at https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html*

Configure Your SIEM Tool in PMC

1. Select **Configuration**, and then select **SIEM Settings**.
2. Select **Enable SIEM Integration** to turn on the feature.
3. Enter the details for your storage site:
   - **Access Key ID**: Enter the value created when you added the user.
   - **Secret Access Key**: Enter the value created when you added the user.
   - **Bucket**: Enter the name of the S3 bucket.
   - **Region**: Select or search for the name of the region where your storage bucket resides.
   - **SIEM Format**: Select a message format to export data to an AWS S3 bucket: **CEF - Common Event Format** or **ECS - Elastic Common Schema**.
4. Select **Server-Side Encryption** to encrypt files sent to the S3 bucket using the default AWS encryption key.
5. Click **Validate Settings** to test the connection to your storage site.
6. Click **Save Settings**.

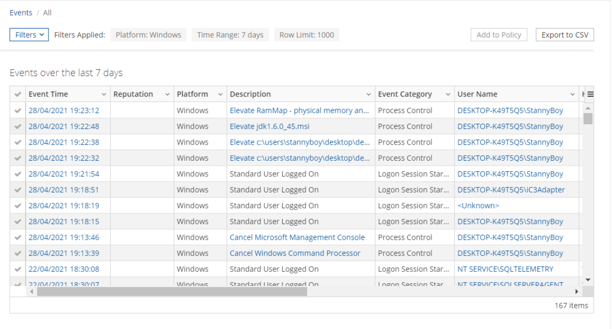
If you no longer want the SIEM integration active, click **Enable SIEM Integration** to turn the feature off.

Events are queued and sent in batches in one minute intervals. This is not configurable. A folder is created where the batches will be saved. You can open and download the batch file, which stores the event data in JSON format.

Set Up Reputation Integration

Using VirusTotal, PMC can provide scan analysis information based on application hash. The analytics gathered can help an organization determine whether an application is suspicious or malicious.

View results of the reputation findings on the **Events > All** reporting page. The Reputation column displays only when reputation is configured here.



Events / All

Filters Applied: Platform: Windows | Time Range: 7 days | Row Limit: 1000

Events over the last 7 days

Event Time	Reputation	Platform	Description	Event Category	User Name
28/04/2021 19:23:12		Windows	Elevate RamMap - physical memory an...	Process Control	DESKTOP-K49T5Q5\StannyBoy
28/04/2021 19:22:48		Windows	Elevate jdk1.6.0_45.msi	Process Control	DESKTOP-K49T5Q5\StannyBoy
28/04/2021 19:22:38		Windows	Elevate c:\users\stannyboy\desktop\de...	Process Control	DESKTOP-K49T5Q5\StannyBoy
28/04/2021 19:22:32		Windows	Elevate c:\users\stannyboy\desktop\de...	Process Control	DESKTOP-K49T5Q5\StannyBoy
28/04/2021 19:21:54		Windows	Standard User Logged On	Logon Session Star...	DESKTOP-K49T5Q5\StannyBoy
28/04/2021 19:18:51		Windows	Standard User Logged On	Logon Session Star...	DESKTOP-K49T5Q5\iC3Adapter
28/04/2021 19:18:19		Windows	Standard User Logged On	Logon Session Star...	<Unknown>
28/04/2021 19:18:15		Windows	Standard User Logged On	Logon Session Star...	DESKTOP-K49T5Q5\StannyBoy
28/04/2021 19:13:46		Windows	Cancel Microsoft Management Console	Process Control	DESKTOP-K49T5Q5\StannyBoy
28/04/2021 19:13:39		Windows	Cancel Windows Command Processor	Process Control	DESKTOP-K49T5Q5\StannyBoy
22/04/2021 18:30:08		Windows	Standard User Logged On	Logon Session Star...	NT SERVICE\SQLTELEMETRY
22/04/2021 18:30:07		Windows	Standard User Logged On	Logon Session Star...	NT SERVICE\SQLSERVERAGENT

167 items

Set Up Reputation

1. Go to **Configuration > Reputation**.
2. Select **Enable VirusTotal Reputation Integration**.
3. Integrating with VirusTotal requires an API key. If you do not already have a key, click **Get Virus Total API Key**.
4. Copy the key, and then click **Check API** to confirm the key is valid.
5. Click **Save**.

Update Reputation

1. Go to **Analytics < Events > All**.
2. Select multiple events by clicking the check marks beside each row.
3. Click **Update Application** at the top of the Analytics grid.

***Note:** Filter event categories with Filters at the top of the grid. Click Filters, then select the desired event category from the Event Category dropdown.*

***Tip:** Click the Reputation column to sort data in ascending or descending order.*

Activity Auditing

The **Activity Auditing** page provides detailed auditing information on user, group, and policy actions. Some of the audited information includes:

- User logon details
- Modify settings
- Set duplicate agents
- Assign role to users
- Modify user
- Resend user invite
- Disable user
- Create group
- Abort open policy draft
- Create user

A **Summary** column highlights the changes on an audited activity.

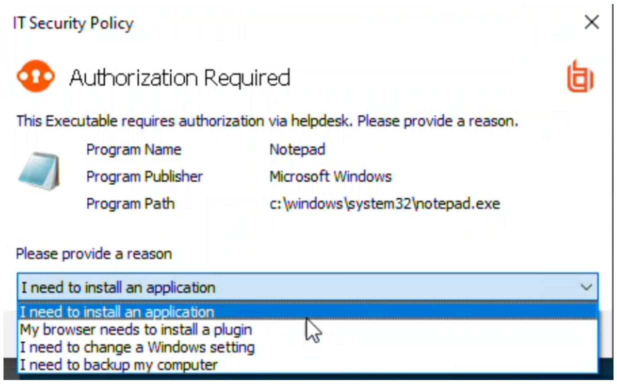
Audited activities include the user who initiated the action and timestamps on when the activity started and ended. Activity details can be viewed for each item.

Access **Activity Auditing** page from the **Auditing** main menu.

ServiceNow User Request Integration

Integrate Privilege Management with ServiceNow to manage user requests. In a typical Privilege Management scenario, the end user tries to launch an application that requires elevated privileges or falls outside of existing policy rules. With this integration, the user sends a request to run the application from PM Cloud to their existing ServiceNow instance as a ticket.

The screen capture shown here is an example of how the messages appear for the end user in a ServiceNow integration. Similar to other application rules in Privilege Management, the user can select from a list of reasons for the request, or use free form text.



IT Security Policy

Authorization Required

This Executable requires authorization via helpdesk. Please provide a reason.

Program Name	Notepad
Program Publisher	Microsoft Windows
Program Path	c:\windows\system32\notepad.exe

Please provide a reason

I need to install an application

- I need to install an application
- My browser needs to install a plugin
- I need to change a Windows setting
- I need to backup my computer

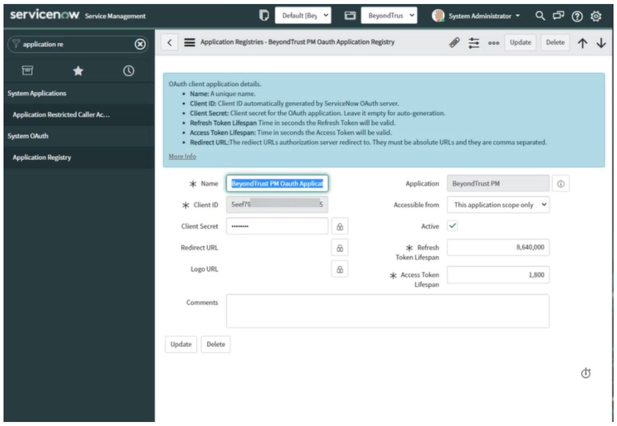
Configuration includes:

- Register Privilege Management as an OAuth client in ServiceNow.
- Create a user account in ServiceNow.
- Configure the connection details to PMC in ServiceNow.
- Activate and create a connection to ServiceNow in PMC.
- Create an application rule in the Policy Editor and apply messages to the rule that are specific to ServiceNow authorization.

Create an OAuth Client for PMC

PMC must be added as an OAuth client in ServiceNow.

1. In ServiceNow, go to **Application Registry**.
2. Configure the settings as shown. The Client ID which is automatically generated is required when setting up the connection in PMC.



Application Registries - BeyondTrust PM Oauth Application Registry

OAuth client application details.

- **Name:** A unique name.
- **Client ID:** Client ID automatically generated by ServiceNow OAuth server.
- **Client Secret:** Client secret for the OAuth application. Leave it empty for auto-generation.
- **Refresh Token Lifespan** Time in seconds the Refresh Token will be valid.
- **Access Token Lifespan:** Time in seconds the Access Token will be valid.
- **Redirect URL:**The rediect URLs authorization server redirect to. They must be absolute URLs and they are comma separated.

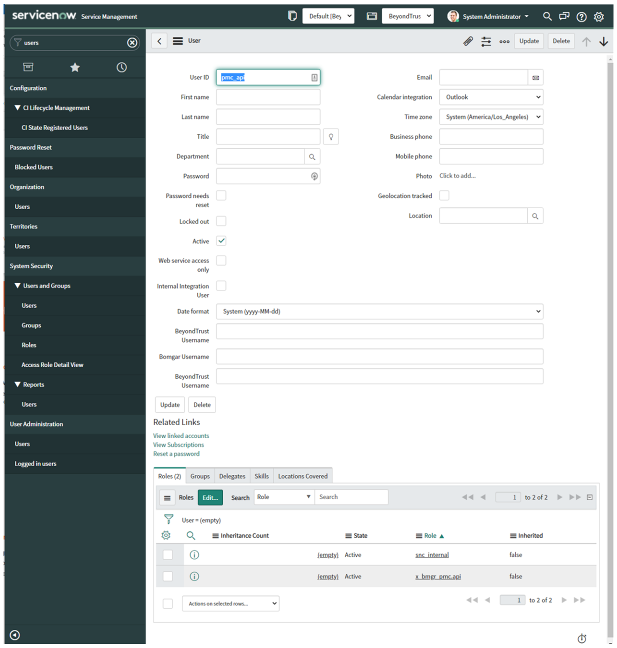
More Info

* Name	BeyondTrust PM Oauth Applicat	Application	BeyondTrust PM
* Client ID	5eef79[redacted]5	Accessible from	This application scope only
Client Secret	••••••••	Active	✓
Redirect URL		* Refresh Token Lifespan	8,640,000
Logo URL		* Access Token Lifespan	1,800
Comments			

Create a User Account in ServiceNow

When setting up the user account, the **x_bmgr_pmc.api** role is required.

1. Go to **User Administration > Users**.
2. Enter the user account information. The user account is required as part of the configuration in PMC.



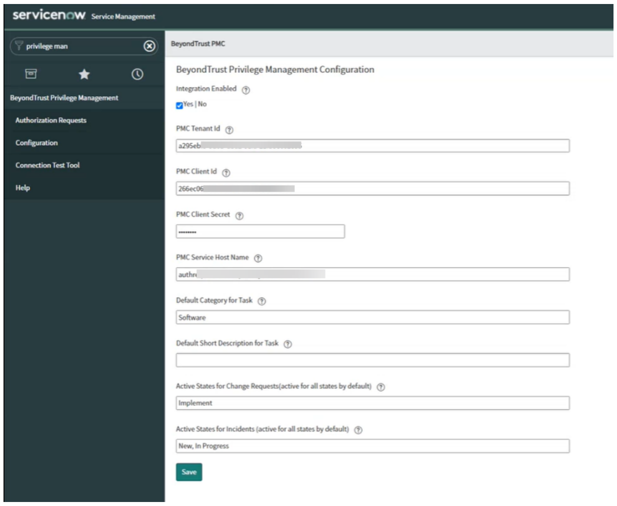
User ID	pmc_api	Email	
First name		Calendar integration	Outlook
Last name		Time zone	System (America/Los_Angeles)
Title		Business phone	
Department		Mobile phone	
Password		Photo	Click to add...
Password needs reset	□	Geolocation tracked	□
Locked out	□	Location	
Active	☑		
Web service access only	□		
Internal Integration User	□		
Date format	System (yyyy-MM-dd)		
BeyondTrust Username			
Bomgar Username			
BeyondTrust Username			

User = (empty)

Inheritance Count	State	Role ▲	Inherited
(empty)	Active	snc_internal	false
(empty)	Active	x_bmgr_pmc.api	false

Configure the Connection to PMC in ServiceNow

1. Go to **Configuration**.
2. Select **Yes** to turn on the integration to PMC.
3. Configure the settings as shown.



BeyondTrust Privilege Management Configuration

Integration Enabled
☑ Yes | No

PMC Tenant Id
a295eb[redacted]

PMC Client Id
266ec06[redacted]

PMC Client Secret
••••••••

PMC Service Host Name
authr[redacted]

Default Category for Task
Software

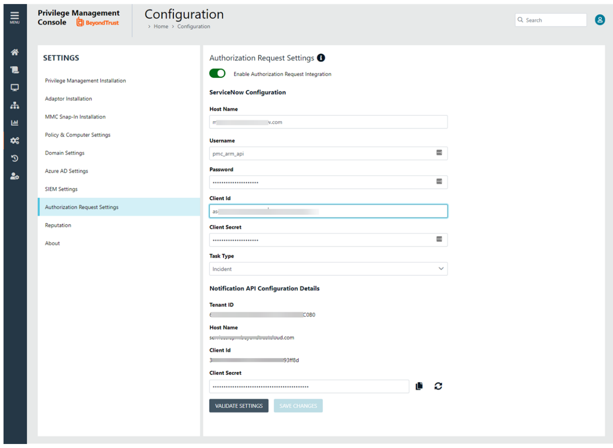
Default Short Description for Task

Active States for Change Requests(active for all states by default)
Implement

Active States for Incidents (active for all states by default)
New, In Progress

Configure the ServiceNow Integration in PMC

1. Go to **Configuration > Authorization Request Settings**.
2. Select **Enable Authorization Request Integration** to activate the integration.
3. Configure the following:
    - **Host name**: The host name provided on the **Configuration** page in ServiceNow.
    - **User name**, **Password**: Enter the user account information you created in ServiceNow.
    - **Client ID**: The ID generated in ServiceNow available on the **Configuration** page.
    - **Client Secret**: The secret created on the Configuration page in ServiceNow.
    - **Task Type**: Select a type from the list: **Incident** or **Change Request**.
4. Click **Validate Settings** to confirm the connection.



Authorization Request Settings

Enable Authorization Request Integration

ServiceNow Configuration

Host Name: m[redacted]v.com

Username: pmc_arm_api

Password: ••••••••••••••••••••

Client Id: as[redacted]

Client Secret: ••••••••••••••••••••

Task Type: Incident

Notification API Configuration Details

Tenant ID: 6[redacted]C0B0

Host Name: se[redacted]ud.com

Client Id: 3[redacted]93ff8d

Client Secret: ••

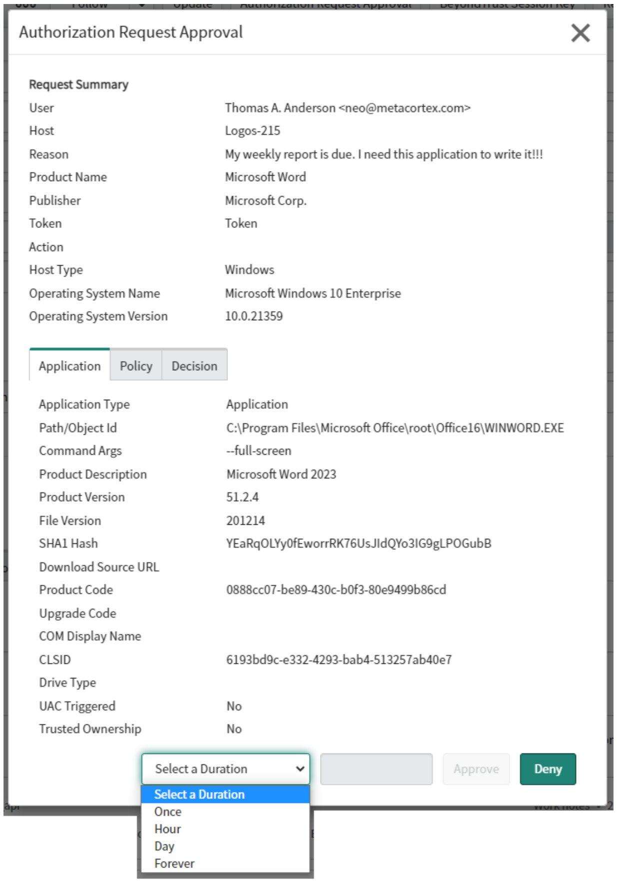
Restrict Access to Applications

In the ServiceNow authorization request workflow, you can restrict access to application requests. On an approved request, Help Desk can set a time limit in the ServiceNow ticket. The time limit is the length of time the user can use the application before the approval automatically expires.

Duration can be selected on the **Application**, **Policy**, or **Decision** tab.

Access time limit can be one of the following:

- **Once**: Permits access to the application only one time.
- **Hour**: Enter the number of hours the user will be permitted access, between 1 and 24.
- **Day**: Enter a day between 1 and 31.
- **Forever**: Access to the application never expires.


Authorization Request Approval

Request Summary

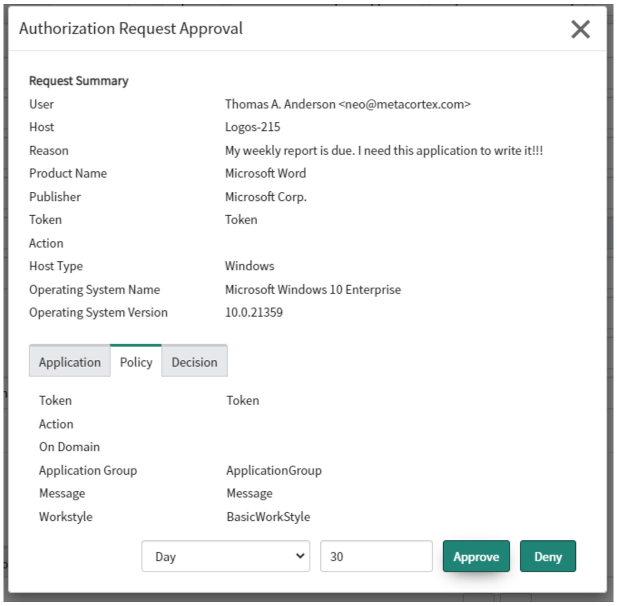
User	Thomas A. Anderson <neo@metacortex.com>
Host	Logos-215
Reason	My weekly report is due. I need this application to write it!!!
Product Name	Microsoft Word
Publisher	Microsoft Corp.
Token	Token
Action	
Host Type	Windows
Operating System Name	Microsoft Windows 10 Enterprise
Operating System Version	10.0.21359

Application Type	Application
Path/Object Id	C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
Command Args	--full-screen
Product Description	Microsoft Word 2023
Product Version	51.2.4
File Version	201214
SHA1 Hash	YEaRqOLYy0fEworrRK76UsJldQYo3lG9gLPOGubB
Download Source URL	
Product Code	0888cc07-be89-430c-b0f3-80e9499b86cd
Upgrade Code	
COM Display Name	
CLSID	6193bd9c-e332-4293-bab4-513257ab40e7
Drive Type	
UAC Triggered	No
Trusted Ownership	No

Select **Approve** after the duration is selected.

After the time expires, the user can no longer access that application. The user must go through the request workflow again with the Help Desk personnel approving and selecting a duration time for access.

Duration settings are included in the authorization auditing.


Authorization Request Approval

Request Summary

User	Thomas A. Anderson <neo@metacortex.com>
Host	Logos-215
Reason	My weekly report is due. I need this application to write it!!!
Product Name	Microsoft Word
Publisher	Microsoft Corp.
Token	Token
Action	
Host Type	Windows
Operating System Name	Microsoft Windows 10 Enterprise
Operating System Version	10.0.21359

Token	Token
Action	
On Domain	
Application Group	ApplicationGroup
Message	Message
Workstyle	BasicWorkStyle

Day | 30

User Request Configuration

Users generate requests when they attempt to access blocked applications from an endpoint through the Privilege Management Client. If configured correctly, PM Cloud transfers the requests to ServiceNow where the technician further manages the application.

> *For more information, please see "ServiceNow User Request Integration" on page 106.*

Configure the user request message content, along with other policy rules and applications, in the PMC *Web Policy Editor*.

Access Policy Editor

1. Log in to PMC and select Policies from the sidebar menu.
2. Click a policy in the list, and then select **Edit and Lock Policy**.

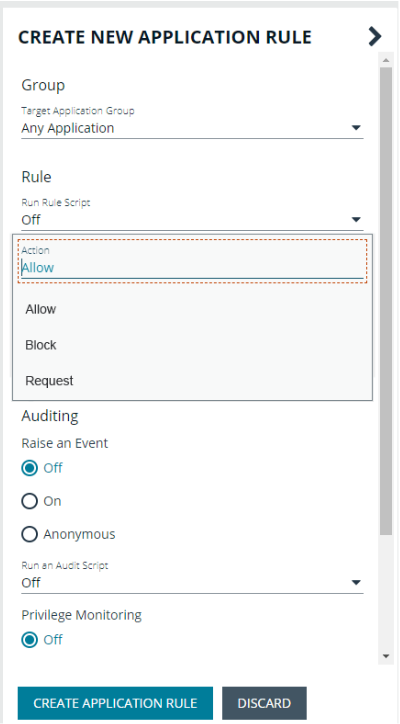
> *For more information, please see "Get Started With the Policy Editor" on page 39.*

Create User Request Rule

1. Select **Workstyles > (Workstyle Name) > Application Rules**.
2. Click **Create New** at the top of the Application Rules grid.
3. Enter the new rule information in the available fields.
4. Go to the **Rule** section and select the dropdown for the **Action** field. Choose **Request**.

> ***Note:*** *If a message box has not already been created, you will need to create one before the Request option is available.*

> ***Tip:*** *If you would like to prompt the group to request permission for all applications, select Any Application under the Target Application Group dropdown.*



CREATE NEW APPLICATION RULE

Group

Target Application Group: Any Application

Rule

Run Rule Script: Off

Action: Allow

Auditing

Raise an Event

● Off

○ On

○ Anonymous

Run an Audit Script: Off

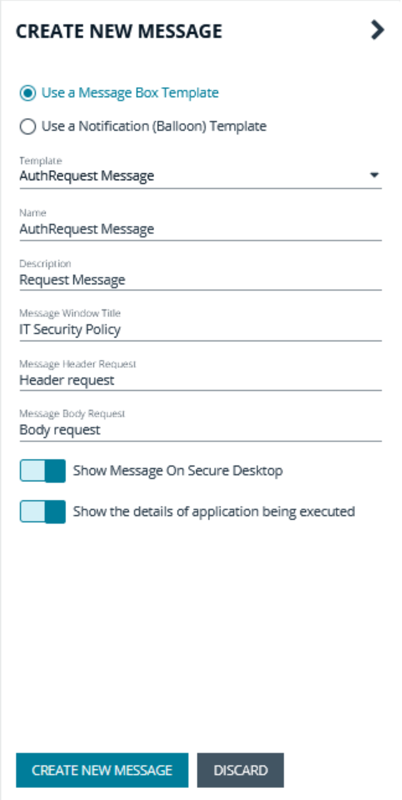
Privilege Monitoring

● Off

Create User Request Message

In the Policy Editor, go to **Messages > Create New Message**. Configure the following settings:

- Template
- Name
- Description
- Message Window Title
- Message Header Request
- Message Body Request



CREATE NEW MESSAGE

● Use a Message Box Template
○ Use a Notification (Balloon) Template

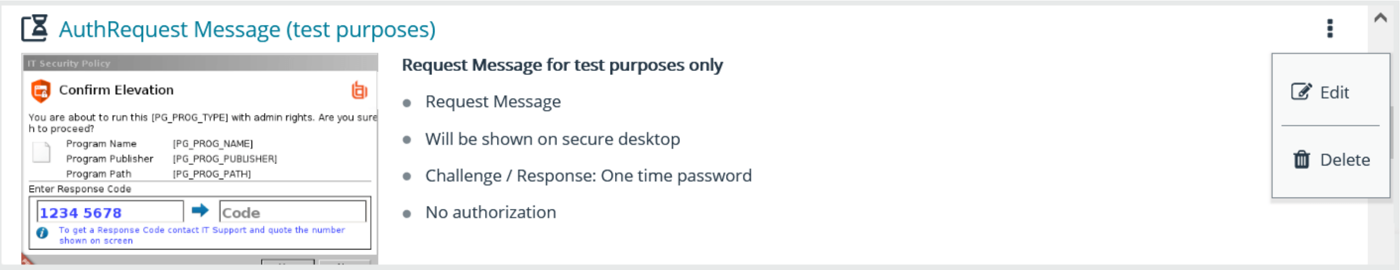
Template: AuthRequest Message
Name: AuthRequest Message
Description: Request Message
Message Window Title: IT Security Policy
Message Header Request: Header request
Message Body Request: Body request

Show Message On Secure Desktop
Show the details of application being executed

For more information, please see "Messages" on page 70.

Once a message has been created, you can find further customization in **Message Options**. Click the vertical ellipsis beside the message that was created and select **Edit** to reveal additional options:

- Title Text
- Header Type
- Header Background Type
- Select Image
- Header Request Text
- Header Pending Text
- Header Approved Text
- Header Denied Text
- Header Text Color
- Body Request Text
- Body Pending Text
- Body Approved Text
- Body Denied Text
- Refer URL Text
- Request Button Text



AuthRequest Message (test purposes)

IT Security Policy

Confirm Elevation

You are about to run this [PG_PROG_TYPE] with admin rights. Are you sure
h to proceed?

Program Name [PG_PROG_NAME]
Program Publisher [PG_PROG_PUBLISHER]
Program Path [PG_PROG_PATH]

Enter Response Code

1234 5678 → Code

To get a Response Code contact IT Support and quote the number shown on screen

Request Message for test purposes only

- Request Message
- Will be shown on secure desktop
- Challenge / Response: One time password
- No authorization

ServiceNow Authorization Requests Auditing

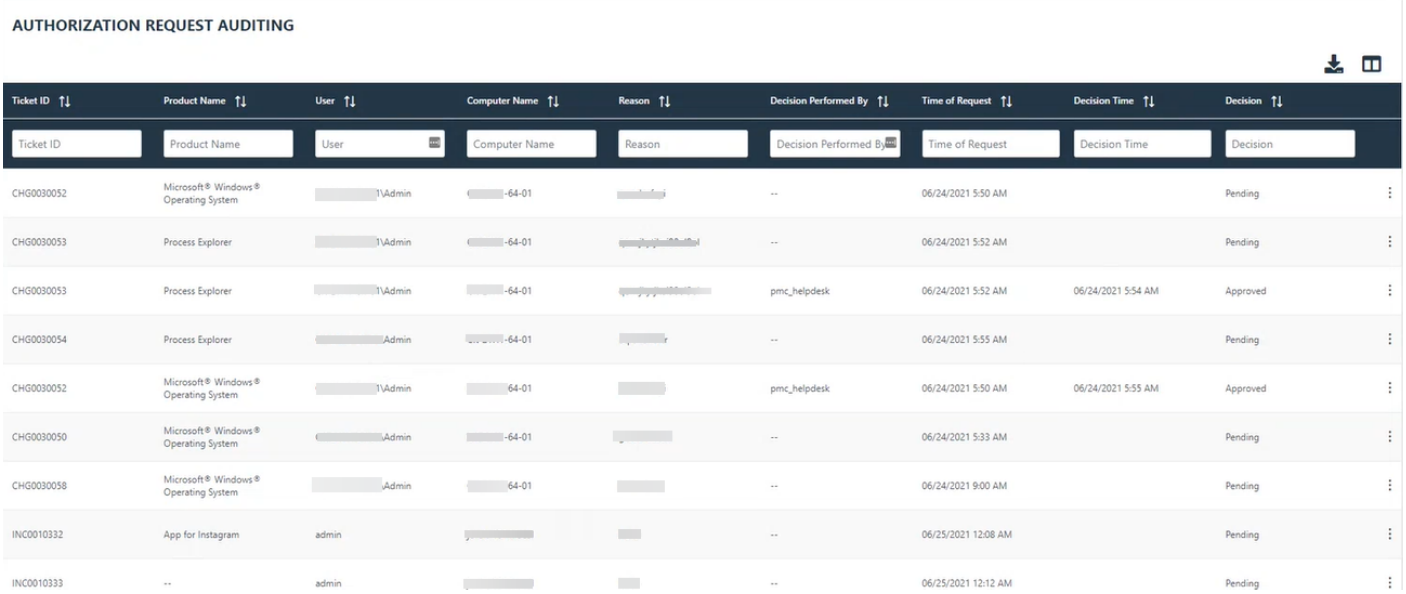
ServiceNow user authorization requests are audited for troubleshooting and logging purposes.

Select the **Auditing** menu to access the **Authorization Request Auditing** tile.

> ***Note:*** *You only see the **Authorization Request Auditing** tile if authorization request management is set up on the **Configuration > Authorization Request Settings** page.*

Some of the key elements captured in the audit include:

- **User**: The user requesting authorization.
- **Time of Request**: The time the ticket is created.
- **Decision Performed By**: The ServiceNow user approving or denying the action.
- **Decision Time**: The time approval or denial occurs.
- **Decision Duration**: The time allotted for the authorized request.
- **Decision Start Time**: The time the decision duration started.



AUTHORIZATION REQUEST AUDITING

Ticket ID	Product Name	User	Computer Name	Reason	Decision Performed By	Time of Request	Decision Time	Decision
CHG0030052	Microsoft® Windows® Operating System	[redacted]1\Admin	[redacted]-64-01	[redacted]	--	06/24/2021 5:50 AM		Pending
CHG0030053	Process Explorer	[redacted]1\Admin	[redacted]-64-01	[redacted]	--	06/24/2021 5:52 AM		Pending
CHG0030053	Process Explorer	[redacted]1\Admin	[redacted]-64-01	[redacted]	pmc_helpdesk	06/24/2021 5:52 AM	06/24/2021 5:54 AM	Approved
CHG0030054	Process Explorer	[redacted]Admin	[redacted]-64-01	[redacted]	--	06/24/2021 5:55 AM		Pending
CHG0030052	Microsoft® Windows® Operating System	[redacted]1\Admin	[redacted]64-01	[redacted]	pmc_helpdesk	06/24/2021 5:50 AM	06/24/2021 5:55 AM	Approved
CHG0030050	Microsoft® Windows® Operating System	[redacted]Admin	[redacted]-64-01	[redacted]	--	06/24/2021 5:33 AM		Pending
CHG0030058	Microsoft® Windows® Operating System	[redacted]Admin	[redacted]64-01	[redacted]	--	06/24/2021 9:00 AM		Pending
INC0010332	App for Instagram	admin	[redacted]	[redacted]	--	06/25/2021 12:08 AM		Pending
INC0010333	--	admin	[redacted]	[redacted]	--	06/25/2021 12:12 AM		Pending

Web Policy Editor: Additional Guidance

Power Rules

A Power Rule is a PowerShell based framework that lets you change the outcome of an Application Rule, based on the outcome of a PowerShell script.

Instead of a fixed Default Rule that can either be set to Allow, Elevate, Audit, or Block for the applications in the targeted Application Group, a Power Rule lets you determine your own outcome based on any scenario you can build into a PowerShell script.

Any existing Default Rule within a Workstyle can be updated to a Power Rule by setting the action to a Power Rule script, and importing the PowerShell script you want to use. PMC provides a PowerShell module with an interface to collect information about the user, application, and policy. The module can then send a resulting action back to PMC to apply.

The Power Rules module also provides a variety of message options that allow you to collect additional information to support your PowerShell script logic and provide updates to the user as to the status, progress, or outcome of your rule. The messages that are supported include:

- Authentication message
- Business Justification message
- Information message
- Pass code message
- Vaulted credential message
- Asynchronous progress dialog for long running tasks

Power Rules is a highly flexible feature with unlimited potential. If you can do it in PowerShell, you can do it in a Power Rule. Here are some example use cases for Power Rules:

- Environmental Factors: Collecting additional information about the application, user, computer, or network status to influence whether an application should be allowed to run, or run with elevated privileges.
- Service Management: Automatically submitting tickets to IT Service Management solutions, and determining the outcome of a service ticket.
- File Reputation: Performing additional checks on an application by looking up the file hash in an application store, reputation service, or a vulnerability database.
- Privileged Access Management: Checking out credentials from a password safe or vault, and passing them back to Privilege Management to run the application in that context.

For information on creating your own Power Rule, please see the Core Scripting Guide, at www.beyondtrust.com/docs/privilege-management/windows.htm.

Windows Workstyle Parameters

The Privilege Management for Windows settings include a number of features allowing customization of text and strings used for end user messaging and auditing. If you want to include properties relating to the settings applied, the application being used, the user, or the installation of Privilege Management for Windows, then parameters may be used which are replaced with the value of the variable at runtime.

Parameters are identified as any string surrounded by brackets (**[ ]**), and if detected, the Privilege Management client attempts to expand the parameter. If successful, the parameter is replaced with the expanded property. If unsuccessful, the parameter remains part of the string. The table below shows a summary of all available parameters and where they are supported.

Parameter	Description
[PG_AGENT_VERSION]	The version of Privilege Management for Windows
[PG_APP_DEF]	The name of the Application Rule that matched the application
[PG_APP_GROUP]	The name of the Application Group that contained a matching Application Rule
[PG_AUTH_METHODS]	Lists the authentication and/or authorization methods used to allow the requested action to proceed
[PG_AUTH_USER_DOMAIN]	The domain of the designated user who authorized the application
[PG_AUTH_USER_NAME]	The account name of the designated user who authorized the application
[PG_COM_APPID]	The APPID of the COM component being run
[PG_COM_CLSID]	The CLSID of the COM component being run
[PG_COM_NAME]	The name of the COM component being run
[PG_COMPUTER_DOMAIN]	The name of the domain that the host computer is a member of
[PG_COMPUTER_NAME]	The NetBIOS name of the host computer
[PG_DOWNLOAD_URL]	The full URL from which an application was downloaded
[PG_DOWNLOAD_URL_DOMAIN]	The domain from which an application was downloaded
[PG_EVENT_TIME]	The date and time that the policy matched
[PG_EXEC_TYPE]	The type of execution method: Application Rule or shell rule
[PG_GPO_DISPLAY_NAME]	The display name of the GPO (Group Policy Object)
[PG_GPO_NAME]	The name of the GPO that contained the matching policy
[PG_GPO_VERSION]	The version number of the GPO that contained the matching policy
[PG_IDP_AUTH_USER_NAME]	The value given by the Identify Provider as the user who successfully authenticated to allow the requested action to proceed. Maps to the OIDC "email" scope.
[PG_MESSAGE_NAME]	The name of the custom message that was applied
[PG_POLICY_NAME]	The name of the policy
[PG_PROG_CLASSID]	The ClassID of the ActiveX control
[PG_PROG_CMD_LINE]	The command line of the application being run
[PG_PROG_DRIVE_TYPE]	The type of drive where application is being executed
[PG_PROG_FILE_VERSION]	The file version of the application being run
[PG_PROG_HASH]	The SHA-1 hash of the application being run
[PG_PROG_NAME]	The program name of the application
[PG_PROG_PARENT_NAME]	The file name of the parent application
[PG_PROG_PARENT_PID]	The process identifier of the parent of the application
[PG_PROG_PATH]	The full path of the application file
[PG_PROG_PID]	The process identifier of the application
[PG_PROG_PROD_VERSION]	The product version of the application being run
[PG_PROG_PUBLISHER]	The publisher of the application

Parameter	Description
[PG_PROG_TYPE]	The type of application being run
[PG_PROG_URL]	The URL of the ActiveX control
[PG_STORE_PACKAGE_NAME]	The package name of the Windows Store App
[PG_STORE_PUBLISHER]	The package publisher of the Windows Store app
[PG_STORE_VERSION]	The package version of the Windows Store app
[PG_TOKEN_NAME]	The name of the built-in token or Custom Token that was applied
[PG_USER_DISPLAY_NAME]	The display name of the user
[PG_USER_DOMAIN]	The name of the domain that the user is a member of
[PG_USER_NAME]	The account name of the user
[PG_WORKSTYLE_NAME]	The name of the Workstyle

Regular Expression Syntax

Use regular expression syntax to control applications at a granular level. The Policy Editor uses the ATL regular expression library **CAtlRegExp**. Below is a summary of the regular expression syntax used by this library.

Metacharacter	Meaning	Example
Any character except [\^$.|?*+()	All characters except the listed special characters match a single instance of themselves. To match one of these listed characters use a backslash escape character (see below).	**abc** matches **abc**
\ (backslash)	Escape character: interpret the next character literally.	**a\+b** matches **a+b**
. (dot)	Matches any single character.	**a.b** matches **aab**, **abb** or **acb**, etc.
[ ]	Indicates a character class. Matches any character inside the brackets (for example, **[abc]** matches **a**, **b**, and **c**).	**[abc]** matches **a**, **b**, or **c**
^ (caret)	If this metacharacter occurs at the start of a character class, it negates the character class. A negated character class matches any character except those inside the brackets (for example, **[^abc]** matches all characters except **a**, **b**, and **c**). If **^** is at the beginning of the regular expression, it matches the beginning of the input (for example, **^[abc]** will only match input that begins with **a**, **b**, or **c**).	**[^abc]** matches all characters except **a**, **b**, and **c**
- (minus character)	In a character class, indicates a range of characters (for example, **[0-9]** matches any of the digits **0** through **9**).	**[0-9]** matches any of the digits **0** through **9**
?	Indicates that the preceding expression is optional: it matches once or not at all (for example, **[0-9][0-9]?** matches **2** and **12**).	**ab?c** matches **ac** or **abc**
+	Indicates that the preceding expression matches one or more times (for example, **[0-9]+** matches **1**, **13**, **999**, and so on).	**ab+c** matches **abc** and **abbc**, **abbbc**, etc.
* (asterisk)	Indicates that the preceding expression matches zero or more times	**ab*c** matches **ac** and **abc**, **abbc**, etc.
| (vertical pipe)	Alternation operator: separates two expressions, exactly one of which matches.	**a|b** matches **a** or **b**

Metacharacter	Meaning	Example
??, +?, *?	Non-greedy versions of **?**, **+**, and *****. These match as little as possible, unlike the greedy versions which match as much as possible. Example: given the input **<abc><def>**, **<.*?>** matches **<abc>** while **<.*>** matches **<abc><def>**.	Given the input **<abc><def>**, **<.*?>** matches **<abc>** while **<.*>** matches **<abc><def>**.
( )	Grouping operator. Example: **(\d+,)*\d+** matches a list of numbers separated by commas, such as **1** or **1,23,456**.	**(One)|(Two)** matches **One** or **Two**
{ }	Indicates a match group. The actual text in the input that matches the expression inside the braces can be retrieved through the **CAtlREMatchContext** object.	
\	Escape character: interpret the next character literally. For example, **[0-9]+** matches one or more digits, but **[0-9]\+** matches a digit followed by a plus character. Also used for abbreviations, such as **\a** for any alphanumeric character; see table below. If \ is followed by a number n, it matches the nth match group (starting from 0). Example: <{.*?}>.*?</\0> matches "<head>Contents</head>". Note that in C++ string literals, two backslashes must be used: "\\+", "\\a", "<{.*?}>.*?</\\0>".	**<{.*?}>.*?</\0>** matches **<head>Contents</head>**
$	At the end of a regular expression, this character matches the end of the input. Example: **[0-9]$** matches a digit at the end of the input.	**[0-9]$** matches a digit at the end of the input
|	Alternation operator: separates two expressions, exactly one of which matches. For example, **T|the** matches **The** or **the**.	**T|the** matches The or **the**
!	Negation operator: the expression following **!** does not match the input. Example: **a!b** matches **a** not followed by **b**.	**a!b** matches **a** not followed by **b**

Register an Azure Tenant

For PMC to query Azure AD groups, a communication channel between PMC and Azure AD must exist.

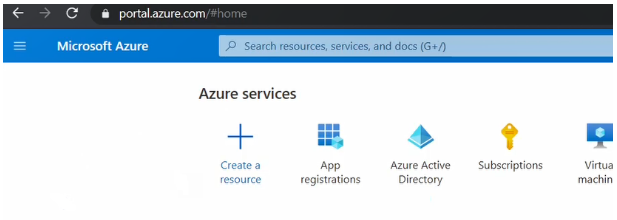
There are two key steps to create a channel:

- Create an app registration in Azure and grant the appropriate permissions. You must also set up an authentication method.
- Configure PMC with the app registration.

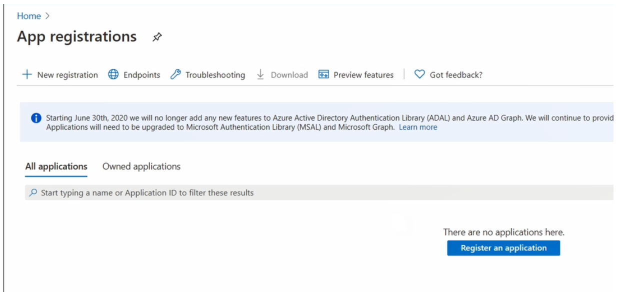
This section details the steps to register an Azure tenant.

Register a Tenant

1. Go to https://portal.azure.com.
2. Select the directory that contains the Azure AD you want to register with PMC.
3. Search for the **App registrations** service and select it.



4. Click **New registration**.

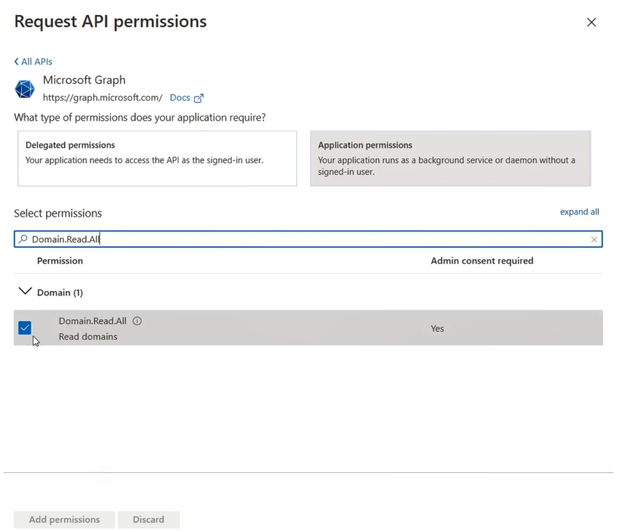


Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provid Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

There are no applications here.

5. Give the registration a name. For example, **PM Cloud Registration**.
6. Select the **Supported account types** you require for your business needs.
7. Ignore the setting **Redirect URI**.
8. Click **Register an application**.
9. Go to **Manage > API Permissions** and click **Add a permission**.
10. Click **Microsoft Graph**, and then **Application permissions**.

11. Add the following permissions. Search by name, and then select the permission when it displays.
    - **Domain.Read.All**
    - **Group.Read.All**
    - **User.Read.All**



What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

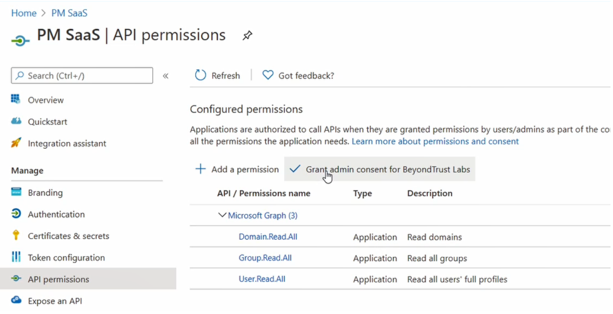
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Domain.Read.All

	Permission	Admin consent required
	Domain (1)	
☑	Domain.Read.All Read domains	Yes

12. After all 3 permissions are selected, click **Add permissions**.
13. Finally, you must grant the permissions. Click **Grant admin consent for (*Directory Name*)**.



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the co all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description
Microsoft Graph (3)		
Domain.Read.All	Application	Read domains
Group.Read.All	Application	Read all groups
User.Read.All	Application	Read all users' full profiles

Configure Authentication

You need to choose an authentication method to create a trust relationship between PMC and Azure. There are two authentication methods available:

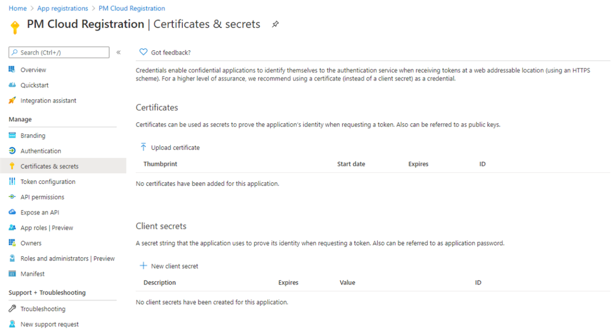
- Certificate authentication
- Client-secret authentication

Use Certificate Authentication

1. In the PMC console, select **Configuration** > **Azure AD Settings**.
2. Click **Download Certificate**.
3. Go to the Azure app registrations portal, and then select **Certificates & secrets**.
4. Click **Upload certificate**.

Use Clients-Secret Authentication

1. In the Azure app registrations portal, select **Certificates & secrets**.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	ID

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

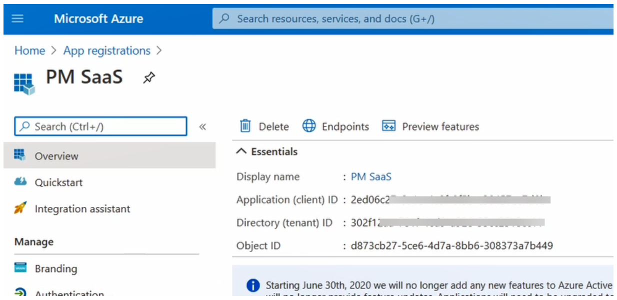
Description	Expires	Value	ID

No client secrets have been created for this application.

2. Select **Client-Secret Authentication**.
3. Click **New Client Secret**.
4. Select an appropriate expiry time, and click **Add**.
5. Copy the value to your clipboard.
6. Go to the PMC console, select **Administration > Access Settings > Azure AD Settings**.
7. Paste the client secret value into the **Application Client Secret** box.
8. Click **Save Changes**.

Client and Tenant IDs

Go to the **Overview** node and note the **Application (client) ID** and the **Directory (tenant) ID**. These are used in the PMC administration console.



Display name : PM SaaS

Application (client) ID : 2ed06c2[redacted]

Directory (tenant) ID : 302f1[redacted]

Object ID : d873cb27-5ce6-4d7a-8bb6-308373a7b449

Starting June 30th, 2020 we will no longer add any new features to Azure Active

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs 119

©2003-2021 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 institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority. TC: 8/11/2021