BeyondTrust

Privilege Management Cloud 22.5 Administration Guide

TC:7/18/2022

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 11.*

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.

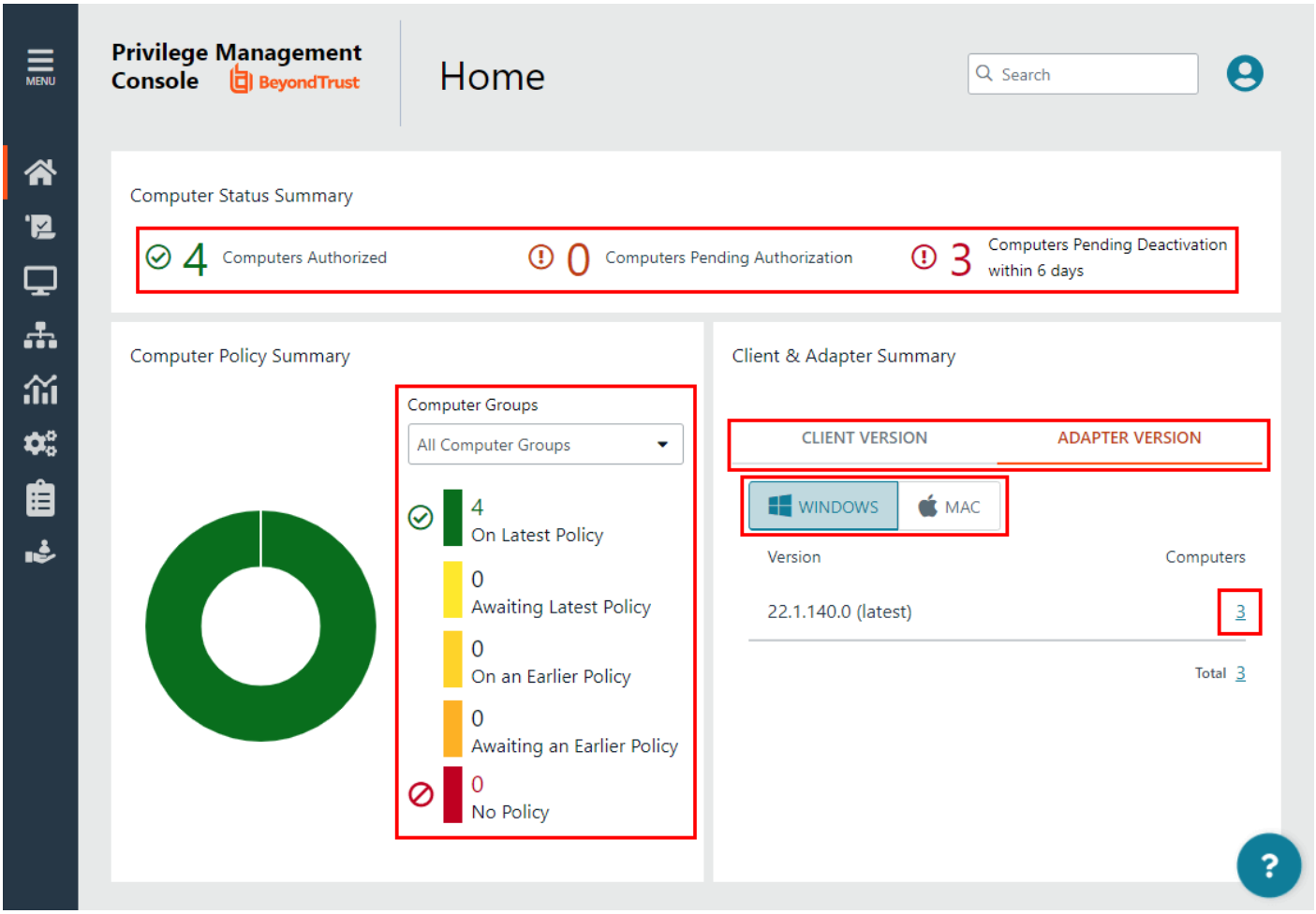
To log in to PMC:

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 will 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.*

PMC Console Home Page

The Privilege Management Console **Home** page serves as a dashboard offering **Computer Status**, **Computer Policy**, and **Client & Adapter** summary information.



Computer Status Summary

At the top, in the **Computer Status Summary** section, you can see the count for computers authorized, pending authorization, and pending deactivation. Click any one of these to go the **Computers** page, where the grid displays a filtered list based on your selection.

Computer Policy Summary

At the left, in the **Computer Policy Summary** section, graphics display all computer groups by policy assignment. Use the dropdown list to narrow your search to a specific group.

Client & Adapter Summary

At the right, in the **Client & Adapter Summary** section, you can select the following:

- Client or Adapter version
- Windows or MAC version

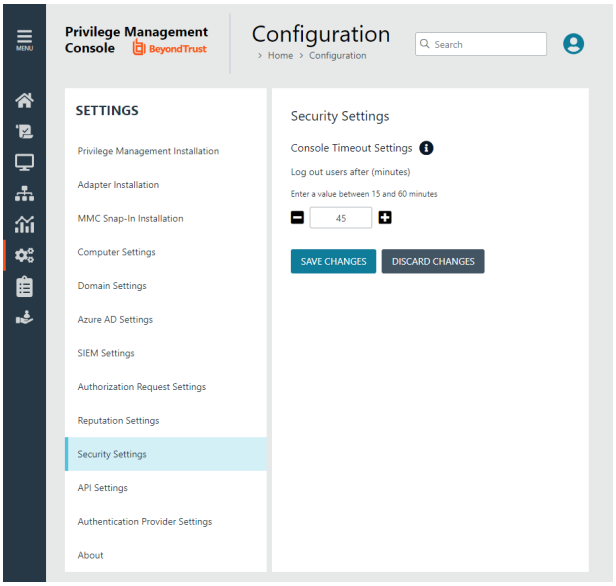
The list below displays which client/adapter version is used and by how many computers. Click any one of the computer numbers to go to the **Computers** page, where the grid displays a filtered list based on your selection.

Console Timeout Settings

You can set how long users can be in a PMC session before they are automatically logged out for a period of inactivity.

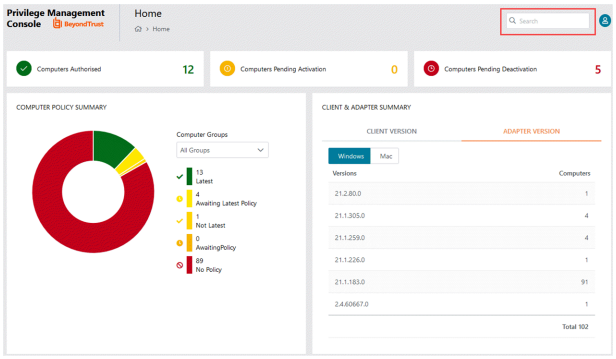
To set the **Console Timeout Settings**:

1. On the sidebar menu, select **Configuration**
2. Under **Settings**, select **Security Settings**.
3. In the **Security Settings** pane, enter a value between 15 and 60 minutes.
4. Click **Save Changes**.



Privilege Management Console Search

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



In PMC, you can search across:

- Computer Groups
- Policies
- Computers
- Users

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

For more information, please see the following:

- *"Privilege Management Console Computer Groups" on page 35*
- *"Policies" on page 24*
- *"Privilege Management Console Computers" on page 30*
- *"Manage User Accounts" on page 38*

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.

For more information, please see "Manage Policy in the MMC Snap-in" on page 28.

Create Groups and Assign Policy

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

Create Groups

1. On the sidebar menu, select **Computer Groups**.
2. Click **Create Group**.
3. Enter a **Group Name**. The **Description** field is optional.
4. Click **Create Group**. 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:** At any time, you can edit the Group Name and Description by clicking the vertical ellipsis menu icon at the end of a group's row, and then selecting **Edit Group**.*

Assign Policy

1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to assign, click the vertical ellipsis icon, and then select **Assign Policy to a Group**.
3. In the **Assign Policy to a Group** panel, use the dropdown list to select the revision for the policy you want to assign, and then select the group.
4. Click **Assign Policy**.

Note: *You should see a green dialog box appear at the bottom middle of the console to confirm that the policy was applied successfully.*

Install Privilege Management

Requirements

For more information about the installation requirements, please see Privilege Management Release Notes at https://www.beyondtrust.com/docs/release-notes/privilege-management/index.htm.

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 5 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.*

- **UserAccount** (Optional): Use **LocalSystem** as the user account name when installing the Windows adapter. The default account for installing the adapter is **iC3Adapter**.
- **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>"
USERACCOUNT=LocalSystem
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"
USERACCOUNT=LocalSystem 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 30.

Upgrade the Windows Adapter

To upgrade to a full system-level DPAPI adapter:

1. Upgrade to the 22.1 adapter, where the adapter continues to run as the IC3 user, but at the system level.
2. Upgrade from 22.1 to a later version of the adapter allows the adapter to run as any system-level user, like LocalSystem.

***Note:** For a new adapter install, starting in version 22.1, this 2-step process is not required.*

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. On the sidebar menu, click **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 5 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 ID for 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.
3. Run the command line as in the example shown below from the **Terminal** with your substituted values.
4. Once the adapter installer launches, proceed through the installation wizard as required.

Example:

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

For more information, please see "Authorize and Assign Computers to a Group" on page 31.

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** on 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 18.

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.

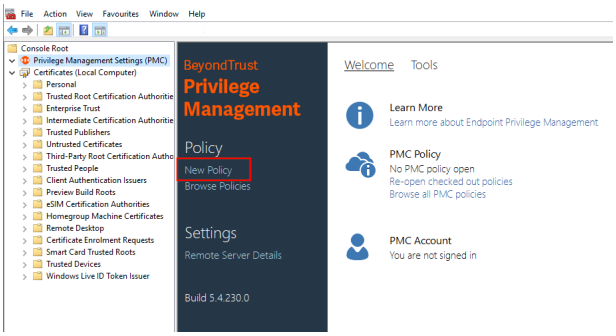
Setting	What to Enter
Connection	
Server URL	This is the URL for PMC with **443** in the **Port** field. This is shown on the **Finish** tab of the deployment wizard. For example, **https://<customerhost>-services.pm.beyondtrust.cloud.com**, where **customerhost** is the instance hostname for your Privilege Management Console.
Tenant ID	This can be located at **Configuration > Settings > MMC Snap-In Installation** in the PMC Portal.
Authorization Provider	
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 17.

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. For example, you can use filtering options to reduce the number of items displayed in the grid.

Access Details Page or Panel

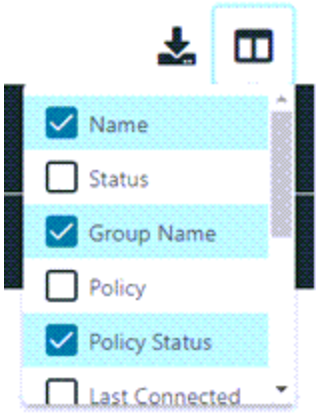
From the main page for **Computers**, **Computer Groups**, **Activity Auditing**, and **Users**, you can click the item in the first column to access a **Details** page or panel.

Click the following for access:

- Computer Name (Computers)
- Computer Group Name (Computer Groups)
- Entity (Activity Auditing)
- Email Address (Users)

Select Columns to Display

At the right, click the **Columns** icon, and then select the columns you want to display.

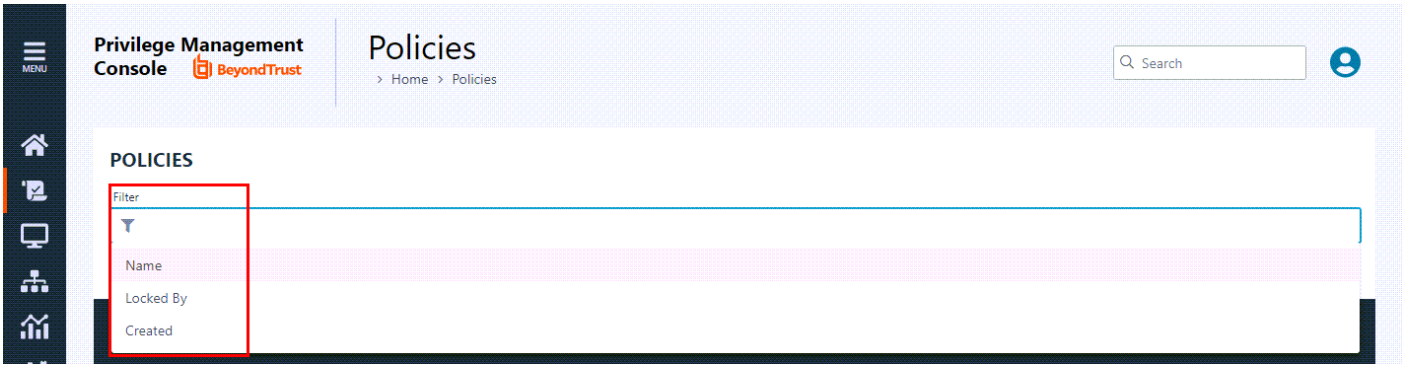


Sort Columns

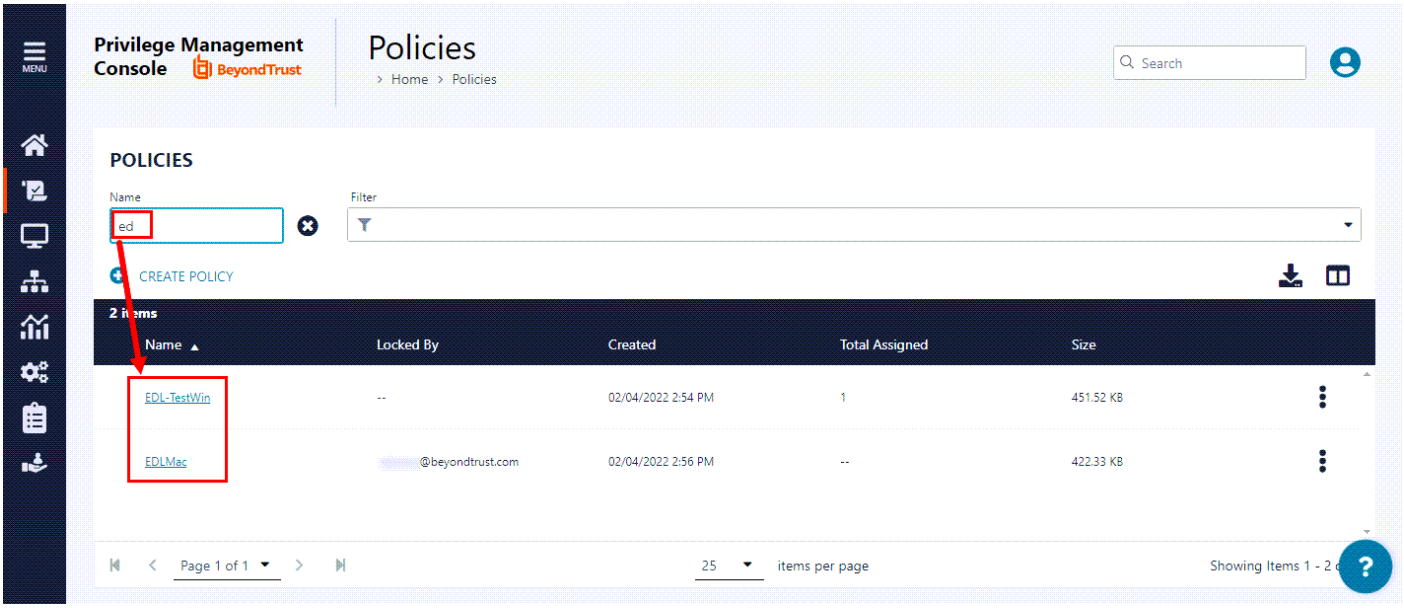
You can sort columns independent of each other by clicking the column name. An **Up** or **Down** arrow icon appears to designate the *ascending* or *descending* sorting order.

Filter

Use the filter tool to filter within the grids. click in the filter field, and then from the list, select a filtering option.



When you enter a string of text in the field, the results in the grid filter below automatically update to the records that contain that string.



To remove a filter, at the right of the filter, click the **X** icon.

The following grids support filtering:

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

> ***Tip:*** *You can use multiple filters in your search. After your initial filter is applied, click in the* ***Filter*** *field again, and select an additional filter item to use. For example, you can filter policies by name, and then by date created.*

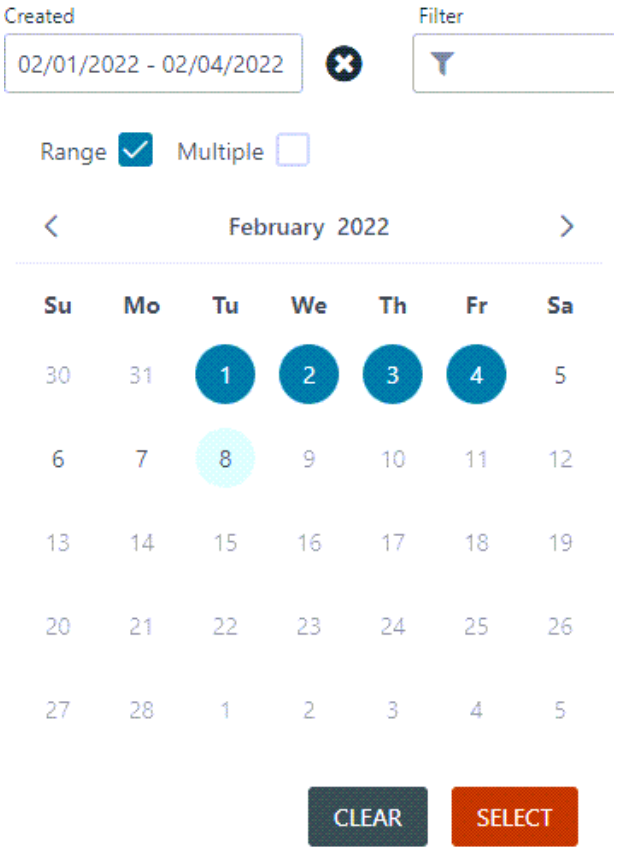
Filter Using the Date Picker

PMC has a **date picker** that you can use to filter in the grids. For example, you can use it to select a range of dates within which computers or computer groups were created.

To use the date picker:

1. On the **Policies**, **Computers**, **Computer Groups**, **Activity Auditing**, or **Users** page, click in the **Filter** field above the grid. The filter options list appears.
2. Select an option that requires a date, such as **Created**. The date picker appears.
3. You have three options for filtering:
    - Select a single date.
    - Check the **Range** box, and then select a beginning and end date for the range.
    - Check the **Multiple** box, and then select multiple, specific dates.
4. To apply the filter, click **Select**. The grid displays a list according to your criteria.

To further reduce the list returned, you can modify the dates or add one or more additional filters.



Progress and Change Indicators

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

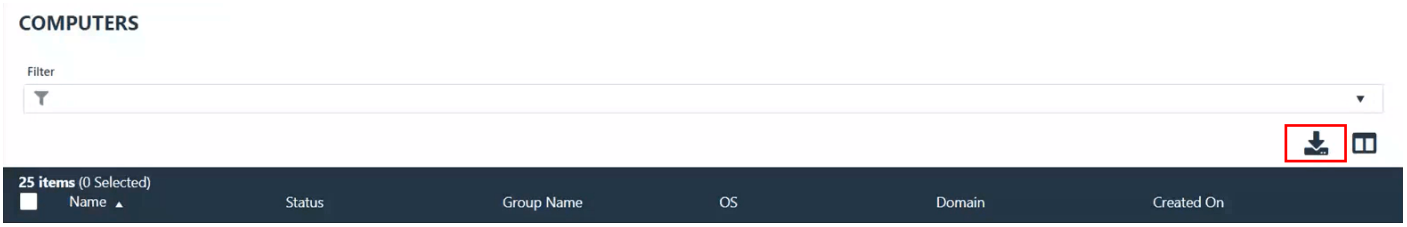
Where actions affect one or more rows, you see a green toaster notification briefly flash across the top right of the grid to indicate that PMC has processed your request.

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

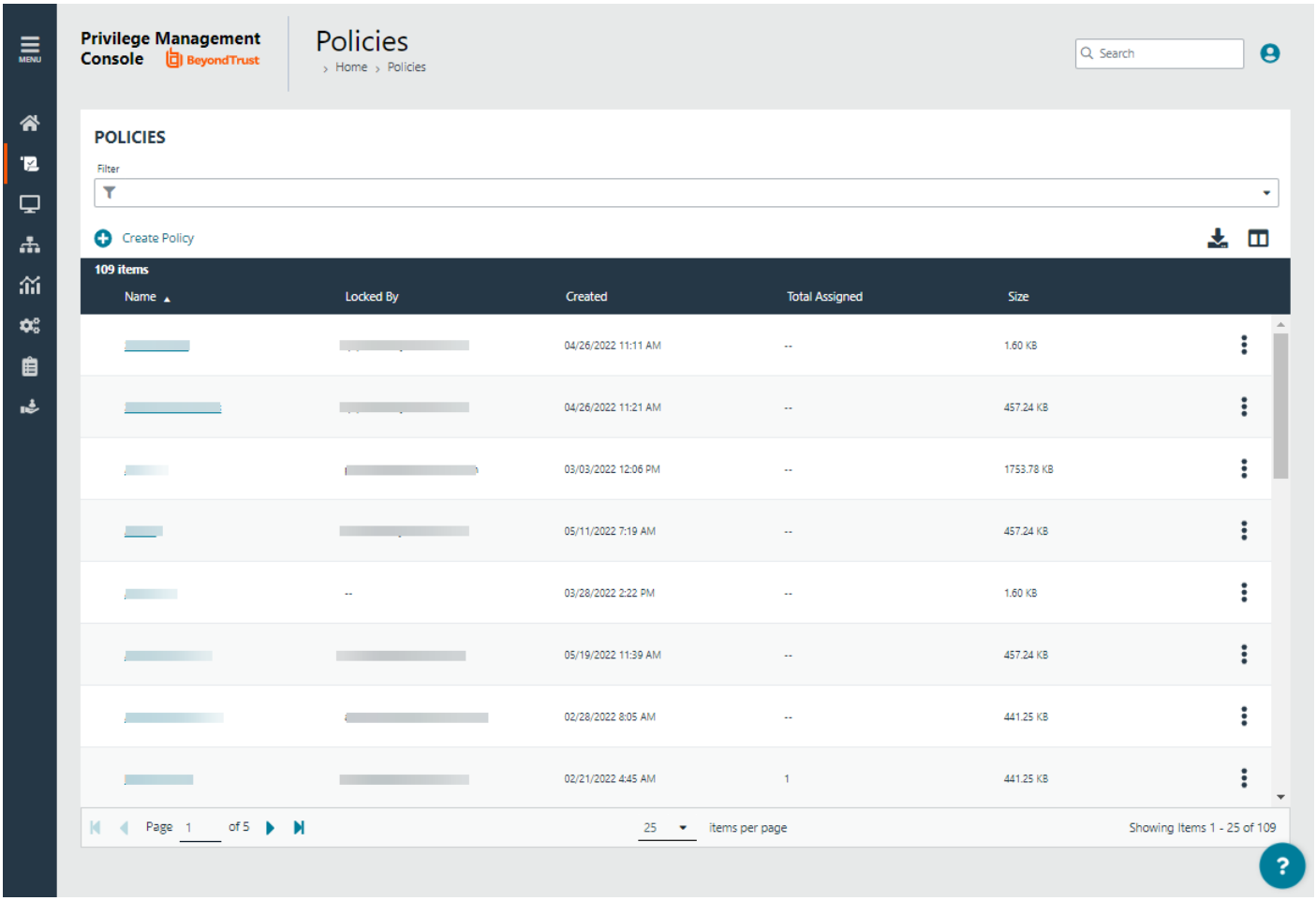
You can export all grid data results in the currently filtered result set, not just the results which are displayed on the current page, from the **Download records to CSV** icon above the grid.



Policies

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

To access the **Policies** page, on the sidebar menu, select **Policies**.

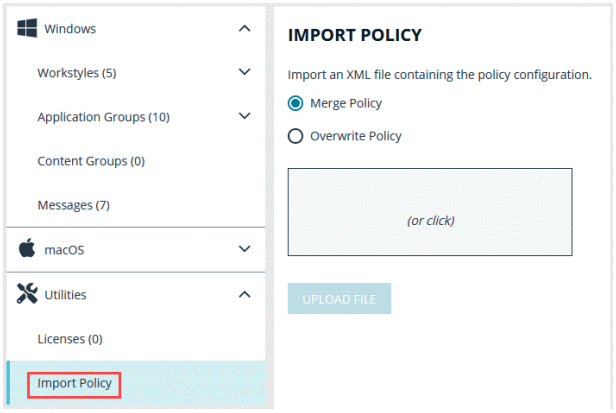


Upload a File in PMC to Create Policy

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.

To upload an XML file for a *new* policy:

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



To upload an XML file for an *existing* policy:

1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to edit, click the vertical ellipsis icon, and then select **Edit Policy**.
3. Select **Utilities > Import Policy**.
4. Choose either **Merge Policy** or **Overwrite Policy** and click the box to import your XML policy. You can also drop the file to upload in the box.
5. 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.

To upload a new revision of an existing policy:

1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to edit, click the vertical ellipsis icon, and then select **Revision History**.
3. Click **Upload Revision**. Browse to the XML file and click **Open**. The XML file is uploaded to the portal.
4. 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.
5. On the **Auto Assign Policy to Groups** dialog box, select the groups to update with the new policy revision.
6. Select **Apply to Groups**.

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

View Policy

You can view the contents of a policy in *read-only* mode.

To view a policy:

1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to view, click the vertical ellipsis icon, and then select **View Policy**. You can also just click on the policy name.
3. When done viewing the policy information, in the Read Only box at the top center of the page, click the **Policy List** link to return to the **Policies** page.
4. If you want to edit a policy, proceed as described in "Edit a Policy" on page 48.

Download Latest Policy Revision

You can download the latest revision of a policy from PMC in XML format if required.

To download the latest policy revision as an XML file:

1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to edit, click the vertical ellipsis icon, and select **Download Latest Revision**.

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

Assign a Policy to a Group

1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to assign, click the vertical ellipsis icon, and then select **Assign Policy to a Group**.
3. In the **Assign Policy to a Group** panel, use the dropdown list to select the revision for the policy you want to assign, and then select the group.
4. Click **Assign Policy**.

> ***Note:*** *You should see a green dialog box appear at the bottom middle of the console to confirm that the policy was applied successfully.*

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:

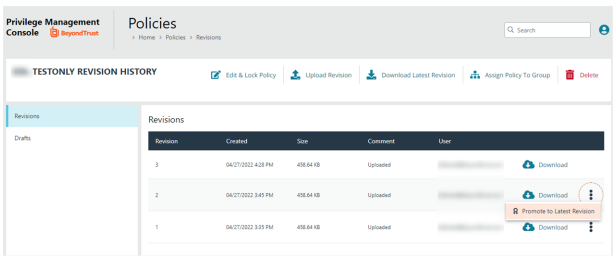
1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to edit, click the vertical ellipsis icon, and then select **Revert & Discard Changes**.
3. Review the warning and click **Revert & Discard** to revert the policy changes; otherwise, click **Cancel**.

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. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to edit, click the vertical ellipsis icon, and then select **Revision History**.
3. On the left, make sure the **Revisions** option is selected.
4. At the right of the policy you want to edit, click the vertical ellipsis icon, and then select **Promote to Latest Revision**.



5. On the **Promote Policy to Latest Revision** dialog box, you can add notes for future reference.
6. If the policy is already applied to certain groups, you can choose to apply the latest revision now by checking the **Yes, auto assign latest revision to group(s)** box.
7. Click **Promote to Latest**.

Delete a Policy

You can only delete policies if they are unlocked.

> ***Note:*** *If a policy is locked, the* ***Delete*** *button is not available for use. The policy must be unlocked first.*

To delete an *unassigned* policy:

1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to delete, click the vertical ellipsis icon, and then select **Delete**.
3. You are prompted to check that you do want to perform this action. To confirm and discard the policy, click **Delete Policy**; otherwise, click **Cancel**.

To delete an *assigned* policy:

1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to delete, click the vertical ellipsis icon, and then select **Delete**.
3. The **Policy Deletion Warning** dialog box appears, indicating that this policy is assigned to one or more groups. You have two options:
    a. Select a different policy and revision to assign to the group(s), and then click **Confirm**.
    b. Click **Confirm** without assigning any policy. The group or groups are no longer policy controlled.

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 41.*

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 26.*

Check out a Policy Using the MMC Snap-in

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

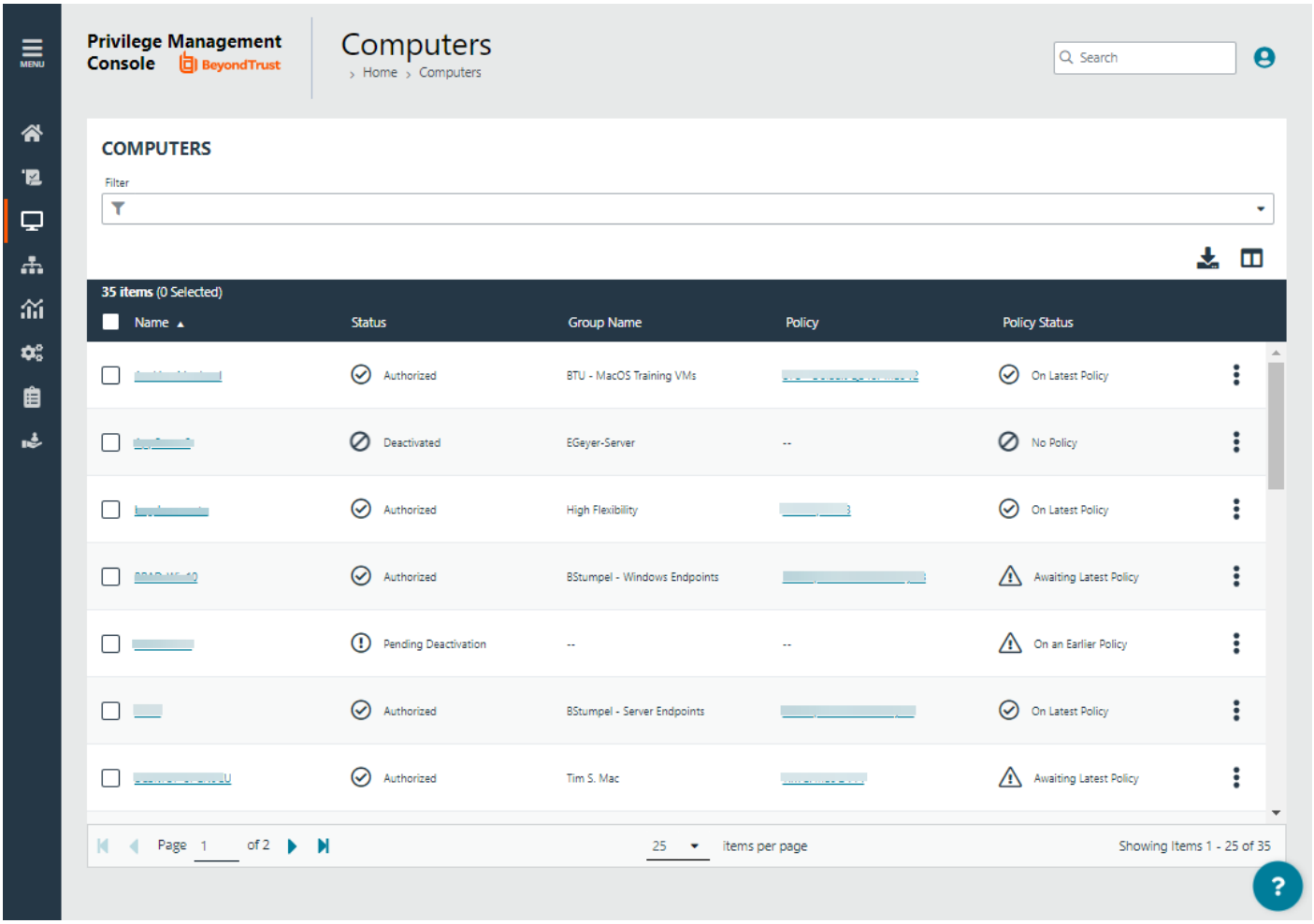
To check out a policy:

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.

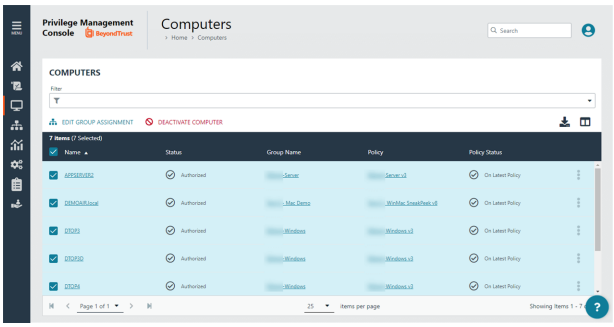
To access the **Computers** page, on the sidebar menu, select **Computers**.



Select Computer Rows

The **Computers** grid supports the standard Windows behavior for selecting multiple rows, because you can interact with multiple computers in one action. You can select one row, multiple rows, or all rows.

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



- To select multiple rows, check the box beside each of the computer names in the grid.
- To select a single row, find the row using the filtering options or scroll to find it. Check the box beside the computer name in the grid.

Authorize and Assign Computers to a Group

You can authorize and assign computers to a group in one step, provided the computers have not 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. On the sidebar menu, click **Computers**.
2. Click the computer(s) you want to place in a group and authorize in one step, and then select **Authorize** from the top of the grid.

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

3. From the group dropdown list, select the group you want to assign it to, and then click **Assign**. If you have not 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 list. Click **Assign**. A notification will briefly flash green at the bottom 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 33*
> - *For information on the grids and filtering,* *"Privilege Management Console Grid Behavior" on page 20*
> - *For instructions on creating a group,* *"Privilege Management Console Computer Groups" on page 35*

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 34.

Automatic Deactivation

Alternatively, you can use PMC to manage deactivations automatically.

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

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

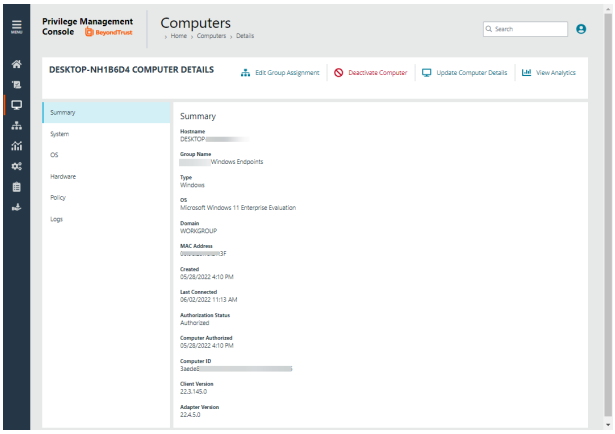
For more information, please see "Computer Deactivation Settings" on page 117.

View Computer Details

For a single computer you can view additional details.

1. On the sidebar menu, click **Computers**.
2. To the right of the computer you want to view, click the vertical ellipsis icon, and then select **View Computer Details**.

The **Computer Details** screen displays the **Summary** information for that computer. In the left panel, you can also select to view **System**, **OS**, **Hardware**, **Policy**, and **Logs** information for the computer.



View Computer Analytics

A link on the **View Computer Details** page opens a host report that provides analytics on the computer activity and includes:

- Applications that have been run
- Running processes
- Users accessing the computer
- Logon activity

To view computer analytics:

1. On the sidebar menu, click **Computers**.
2. To the right of the computer you want to view, click the vertical ellipsis icon, and then select **View Computer Details**.
3. Select **View Analytics**.

The host report can also be accessed from the **Events > All** report.

Update Computer Details

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. On the sidebar menu, click **Computers**.
2. To the right of the computer you want to view, click the vertical ellipsis icon, and then 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, in the left panel, select **Policy**. Click the policy name to access the **Policy Details** section. From here, you can edit the policy as well as upload a new revision.

For more information, please see "Policies" on page 24.

Computer Logs

1. On the **Computer Details** page, in the left panel, select **Logs**. This shows you a list of logs that have previously been requested.
2. To get a new set of logs from the computer, click **Request Logs**. PMC requests 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.
3. To download a log file, at the right of a log entry, click **Download**.

Command Logs

On the **Computer Details** page, in the left panel, select **Logs**, and then click the **Command Log** tab. This shows you a list of commands that have been communicated between PMC and the computer.

Assign Computers to a Group

1. On the sidebar menu, click **Computers**.
2. To the right of the computer you want to edit, click the vertical ellipsis icon, and then select **Edit Group Assignment**.
3. From the dropdown list, select a group, and then click **Save Group Assignment**. A notification will appear and flash green to indicate that PMC has processed your request.

***Note:** If you have not created any groups yet, you will only see **No Group** in the dropdown list.*

For more information on creating a group in PMC, please see "Create a Group" on page 36.

Clear a Computer from a Group

1. On the sidebar menu, select **Computers**.
2. At the right of the computer you want to remove from a group, click the vertical ellipsis icon, and then select **Edit Group Assignment**.
3. 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 **Computer Settings** tab.

For more information, please see "Computer Deduplication Settings" on page 118.

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

1. On the sidebar menu, click **Computers**.
2. To the right of the computer you want to deactivate, click the vertical ellipsis icon, and then select **Deactivate Computer**. You are prompted to verify if you want to continue with the deactivation of the computer. To proceed, click **Deactivate Computer**; otherwise, click **Cancel**.

For more information, please see the following:

- *"Computer Deactivation Settings" on page 117*
- *If the computer has not been authorized, "Reject Computers Not Authorized" on page 31*

Delete Deactivated Computers

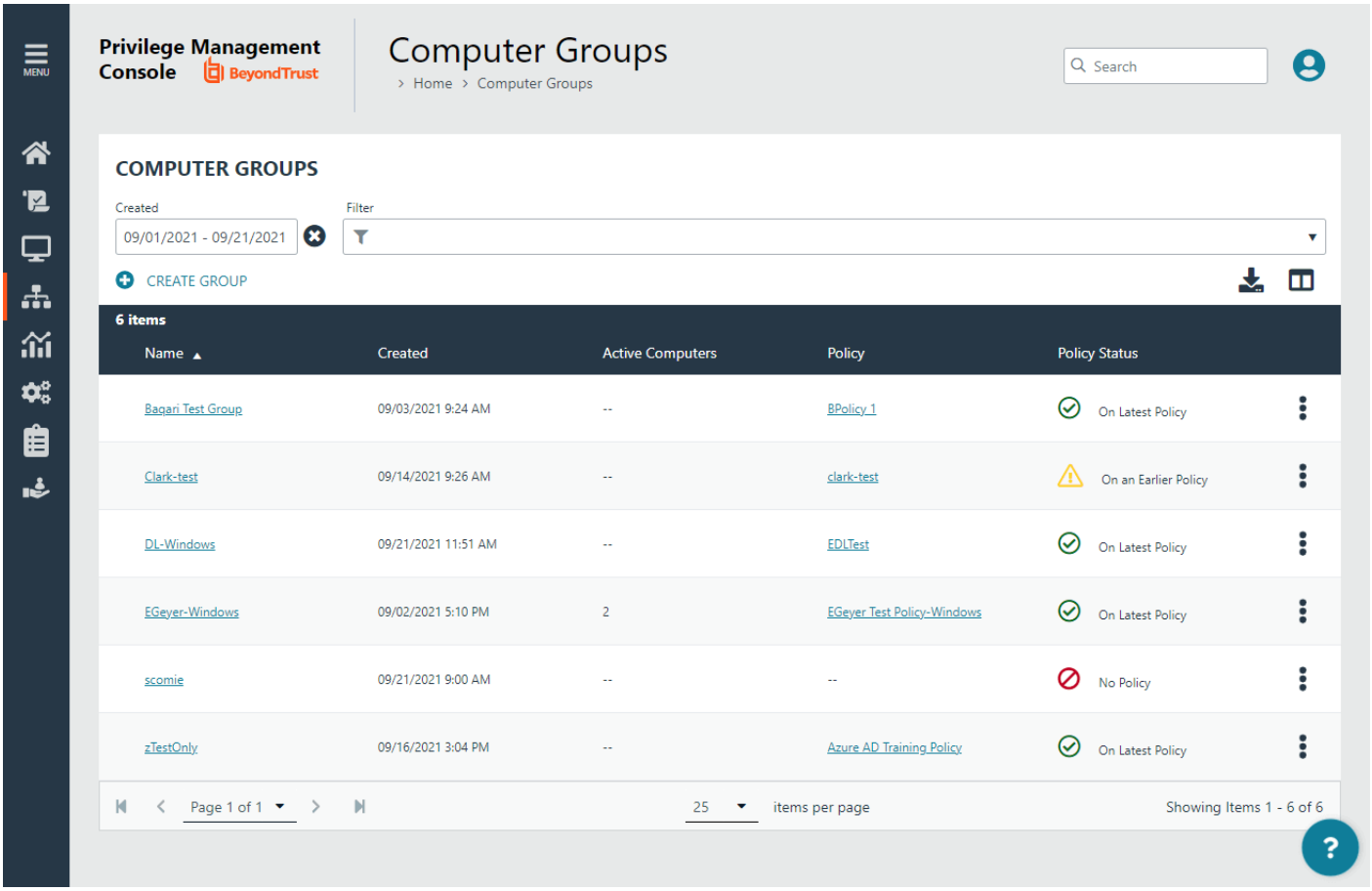
If a computer is deactivated, it can be deleted from the Privilege Management Console database.

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

Privilege Management Console Computer Groups

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

To access the **Computer Groups** page, on the sidebar menu, select **Computer Groups**.



You can perform the following tasks on the **Computer 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.

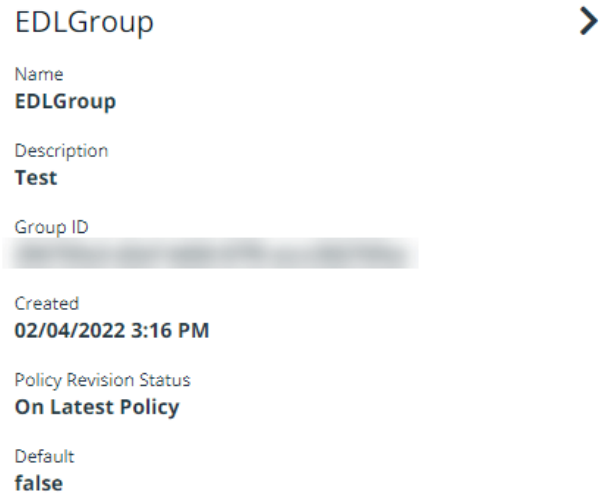
1. On the sidebar menu, select **Computer Groups**.
2. Click **Create Group**.
3. Enter a **Group Name**. The **Description** field is optional.
4. Click **Create Group**. Your group is created and appears in the grid list below.

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 Group Details

1. On the sidebar menu, select **Computer Groups**.
2. At the right of the group you want to view, click the vertical ellipsis icon, and then select **View Group Details**. You can also click the name of the group in the grid to access the panel.
3. The **Group Details** panel 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 User Account Properties" on page 40.



Edit Group Properties

1. On the sidebar menu, select **Computer Groups**.
2. At the right of the group you want to edit, click the vertical ellipsis icon, and then select **Edit Group**.
3. 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. On the sidebar menu, select **Computer Groups**.
2. At the right of the group you want to set as default, click the vertical ellipsis icon, and then select **Set as 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 11.

Assign a Policy to a Group

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

1. On the sidebar menu, select **Computer Groups**.
2. At the right of the group you want to assign a policy to, click the vertical ellipsis icon, and then select **Edit Policy Assignment**.
3. In the **Edit Policy Assignment** panel, use the dropdown list to select the policy you want to assign, and then select which revision to use.
4. Click **Save Policy Assignment**. 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. On the sidebar menu, select **Computer Groups**.
2. At the right of the group you want to edit, click the vertical ellipsis icon, and then select **Edit Policy Assignment**.
3. To remove the policy from the group, click **Clear Policy Assignment**.
4. You are notified how many computers will be affected by the change. To clear the policy assignment, click **Clear Policy Assignment**.

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.

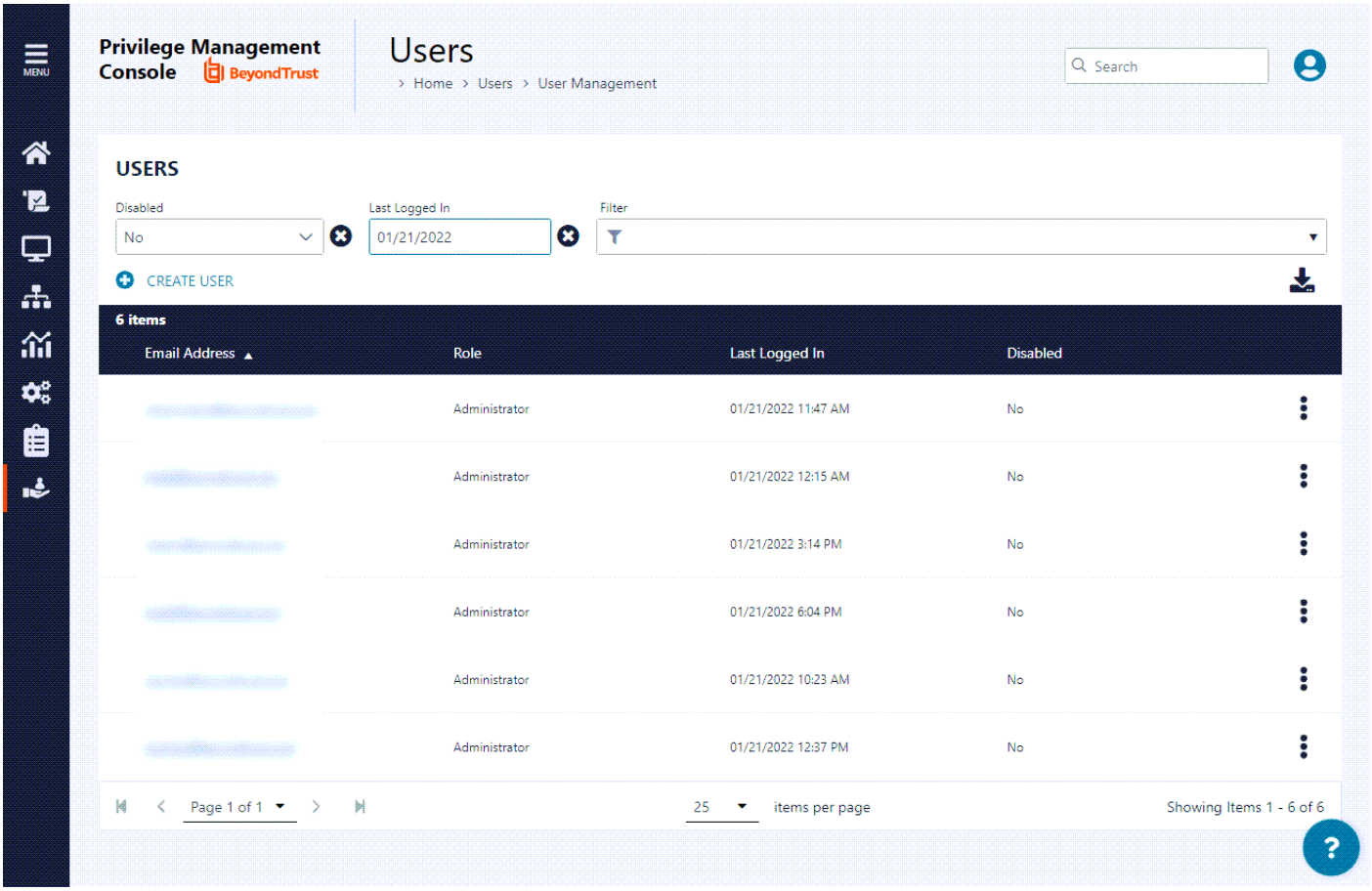
1. On the sidebar menu, select **Computer Groups**.
2. At the right of the group you want to delete, click the vertical ellipsis icon, and then select **Delete**.
3. You are prompted to confirm the decision. To delete the group, click **Delete Group.**

Manage User Accounts

The **Users** page allows you to see and to interact with the users being managed by PMC.

To access the **Users** page, on the sidebar menu, select **Users**, and then select **User Management**.

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.



Create a User Account in PMC

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.

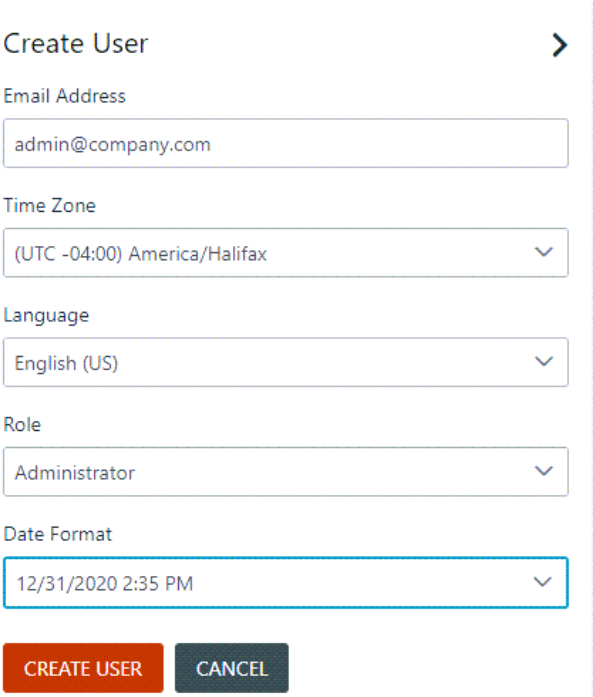
IMPORTANT!

The user needs to exist in your authorization provider before you add that user in PMC. Currently, Azure B2B and OpenID Connect are supported providers.

For more information about setting up a connection to Azure B2B, see "Register an Azure Tenant" on page 146.
If you choose to configure OpenID Connect, see "Configure OpenID Connect" on page 124.

To create a user account:

1. On the sidebar menu, select **Users**, and then select **User Management**.
2. At the top left of the grid, click **Create User**.
3. In the **Create User** panel on the right:
    - Enter the user's **Email Address**.
    - Select their appropriate **Time Zone**.
    - Select their **Language**.
    - Select a **Role** for the new user.
    - Choose the **Time & Date** format.
4. Click **Create User**.



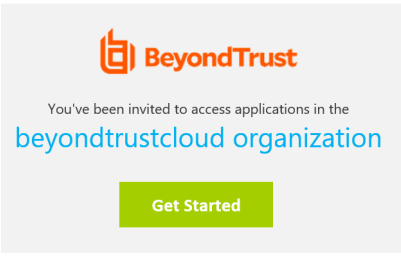
You can add a domain in the **Configuration > Domain Settings** page.

For more information, please see "Add a Domain" on page 118.

Registration and User Confirmation

Once a user account has been created in PMC, an automated email response 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.



Resend User Invites

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

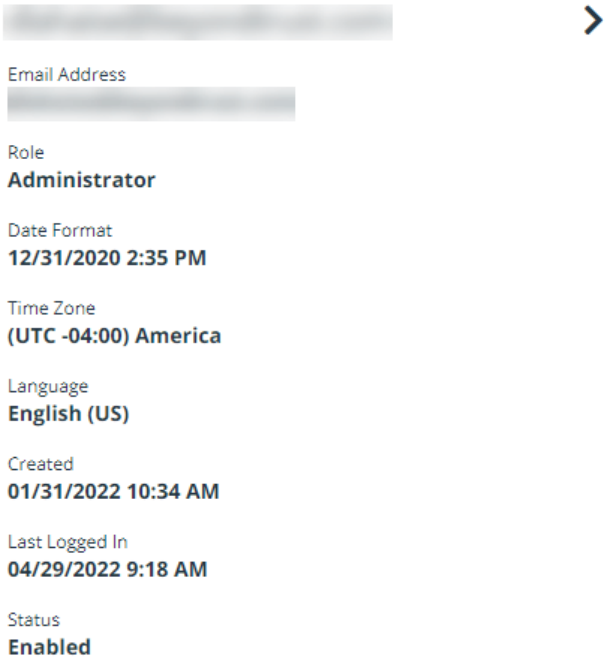
1. On the **Users** page, at the right of the user row to whom you want to resend the email invite to, click the vertical ellipsis icon, and then select **Resend Email Invite**.

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

View User Account Details

1. On the sidebar menu, select **Users**, and then select **User Management**.
2. At the right of the user you want to view, click the vertical ellipsis icon, and then select **View User Details**. You can also click the email address of the user in the grid to access the panel.. 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 User Account Properties" on page 40.*



Edit User Account Properties

1. On the sidebar menu, select **Users**, and then select **User Management**.
2. At the right of the user you want to edit, click the vertical ellipsis icon, and then select **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.
3. 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. On the sidebar menu, select **Users**, and then **User Management**.

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

2. At the right of the user you want to assign a role to, click the vertical ellipsis icon, and then select **Edit User**. You can also click the email address of the user in the grid to access the panel.
3. In the **Edit User** panel, click the **Role** dropdown list, and then select the appropriate role.
4. Click **Save User** to save your changes.

Disable a User Account

1. On the sidebar menu, select **Users**, and then select **User Management**.
2. At the right of the user account you want to disable, click the vertical ellipsis icon, and then select **Disable**.
3. You are prompted to confirm if you want to disable the user. To disable the user, click **Disable 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, use the* ***Disabled*** *filter option and select* ***Yes*** *for filtering.*

For more information, please see "Enable a User Account" on page 41.

Enable a User Account

1. On the sidebar menu, select **Users**, and then select **User Management**.
2. By default, disabled users are not shown. To view users that are disabled, at the top left, click the dropdown menu for the **Disabled** filter and select **Yes**.
3. At the right of the user account you want to enable, click the vertical ellipsis icon, and then select **Enable**.
4. 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.

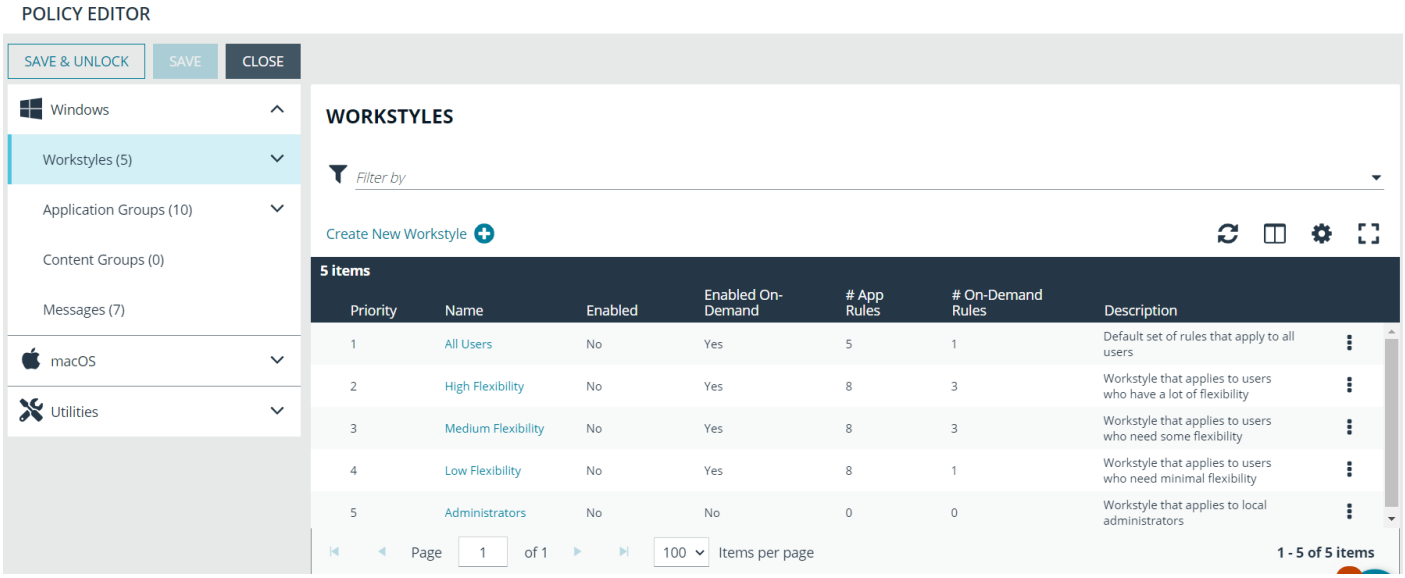
Get Started With the Policy Editor

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** on the sidebar menu.
2. Click a policy in the list, and then select **Edit and Lock Policy**.



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 have 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** on 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 application 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 a 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. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to edit, click the vertical ellipsis icon, and then select **Edit & Lock Policy** (or **Edit Policy**, if the policy is unlocked). You can also just click on the policy name.
3. On the **Policy Editor** page, go to the policy property you want to change, and edit as needed.
4. Click **Save** to save a draft of the policy. Clicking **Save** allows you to keep the Policy Editor open to continue editing the policy.
5. After you finish all updates to the policy, click **Save & Unlock** to save a new revision of the policy.
6. (Optional). On the **Save and Unlock** dialog box, you can enter **Annotation notes** about the policy changes.
7. Click **Save Policy**.

Policy Revisions and Drafts

You can review the history of revisions and drafts on the policy **Revision History** page.

1. At the right of the policy you want to edit, click the vertical ellipsis icon, and then select **Revision History**. You can also just click on the policy name.
2. On the left, click the **Revisions** or **Drafts** option to view more information about the changes to the policy.

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:

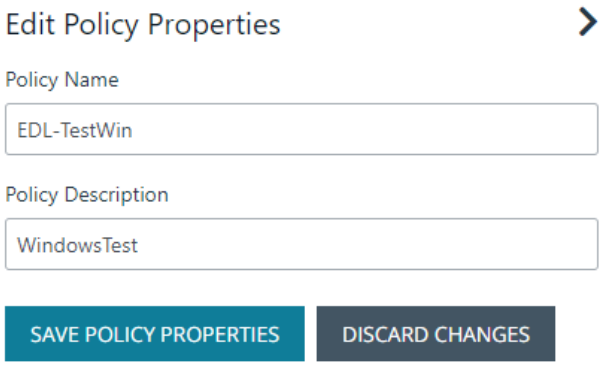
1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to unlock, click the vertical ellipsis icon, and then select **Revert & Discard Changes**.
3. Click **Revert & Discard** to discard the draft and revert the policy version; otherwise, click **Cancel**.

Edit Policy Properties

You can change the name and description for a policy.

> ***Note:*** *You can only edit the policy properties when the policy is* ***unlocked*** *(except if you are the one who locked the policy). When a policy is locked, the* ***Edit Policy Properties*** *fields are not available.*

1. On the sidebar menu, select **Policies**.
2. At the right of the policy you want to view, click the vertical ellipsis icon, and then select **Policy Properties**.
3. The **Edit Policy Properties** panel allows you to change the policy name and description.



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, content rules, general rules, and filters.

Content 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** on the sidebar menu.
2. Find the row of the policy you would like to create a Workstyle for, and then 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. Click **Create New Workstyle**.
6. Enter a name and a description. By default, the Workstyle is disabled.
7. Click **Create Workstyle**.
8. Select the Workstyle in the navigation pane to expand the properties.
9. Configure the Workstyle properties: **Application Rules**, **On-Demand Application Rules**, **Trusted Application Protection**, **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.

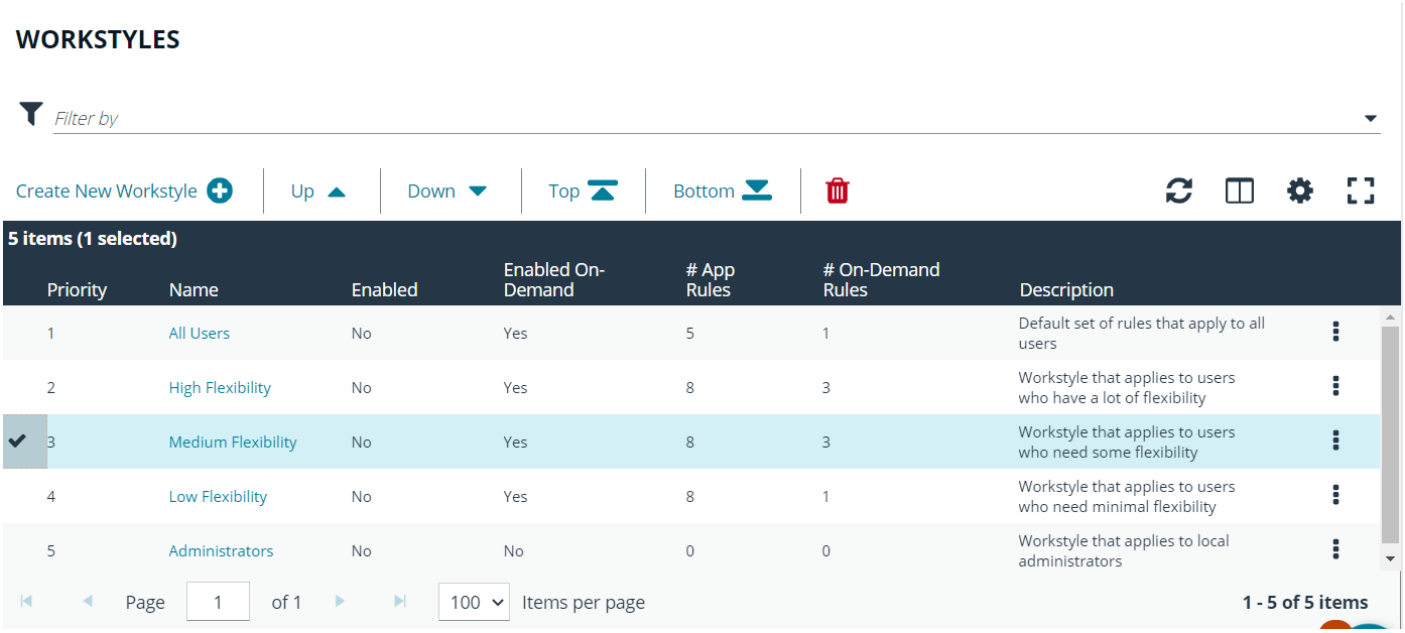
1. Go to the Policy Editor, and then navigate to the Windows Workstyles.
2. Select the vertical ellipsis menu for the Workstyle, and then select **Enable**.

The Workstyle can be disabled later, 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.



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 then expand a Workstyle.
3. Click **Application Rules**, and then click **Create New**.
4. Set the following:
    - **Target Application Group**: Select an Application Group.
    - **Action**: Select **Allow**, **Allow as Password Safe User**, **Block**, or **Request**. The action that occurs if the application in the targeted Application Group is launched by the end user.
    - **Password Safe Account Name**: Enter the Managed Account name configured in Password Safe for the computer.
    - **Run Rule Script**: Assign a rule script that is run before the Application Rule triggers. Select a rule script from the list.
    - **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 Full Admin (Required for installers)** : Standard Windows Admin token containing all Admin privileges.
  - **Add Basic Admin Rights**: Gives greater control over the privileges granted when targeting rules at actions. This *excludes* the following privileges: **SeDebugPrivilege**, **SeLoadDriverPrivilege**.
  - **Privilege Management Support Token**: Applies Add Full Admin privileges with tamper protection removed.
- **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 does not 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 will not 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.
    - **Action**: Select **Allow**, **Allow as Password Safe User**, **Block**, or **Request**. The action that occurs if the application in the targeted Application Group is launched by the end user.
    - **Password Safe Account Name**: Enter the Managed Account name configured in Password Safe for the computer.
    - **Run Rule Script**: Assign a rule script that is run before the Application Rule triggers. Select a rule script from the list.
    - **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 Full Admin (Required for installers)** : Standard Windows Admin token containing all Admin privileges.
        - **Add Basic Admin Rights**: Gives greater control over the privileges granted when targeting rules at actions. This *excludes* the following privileges: **SeDebugPrivilege**, **SeLoadDriverPrivilege**.
        - **Privilege Management Support Token**: Applies Add Full Admin privileges with tamper protection removed.
    - **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.
1. Click **Create On-Demand Rule**.

Integrate BeyondTrust Password Safe

Password Safe users can be included in an Application Rule or On-Demand Application Rule to help manage access to applications.

Password Safe must already be installed and configured.

> *For more information, please see the Password Safe Integration Guide at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm.*

Use the following procedure to set up the integration to Password Safe. After this initial setup is complete, you can edit the Application Rule or On-Demand Application Rule to allow Password Safe users.

1. On the **Policy Editor** page, expand **Windows**.
2. Expand the **Workstyles** node, and then expand a Workstyle.
3. Click **Application Rules** or **On Demand Application Rules**, and then click **Integration Settings**.
4. From the **Activation** list, select one of the following: **Not Configured**, **Enabled**, or **Disabled**.
5. Set a heartbeat interval. This is the time span the computer polls Password Safe unless the time is determined by Password Safe. For most subsequent messages, the poll time is driven by Password Safe in the messages it sends to Privilege Management for Windows. This is because Password Safe knows when the next scheduled action must be performed.
6. Click **Update Settings**.

Trusted Application Protection Rules

Privilege Management for Windows can dynamically evaluate DLLs for trusted applications for each Workstyle.

Unless a DLL has a trusted publisher and a trusted owner, it is not allowed to run within the Trusted Application Protection (TAP) application.

- **Trusted Publisher:** A trusted publisher must be signed. In addition, the publisher certificate must be valid, in date, and not revoked.
- **Trusted Owner:** A trusted owner is any owner that is in the default Windows groups **Administrators**, **SystemUser** or **TrustedInstaller**.

TAP rules affect the following applications:

- Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Publisher, Adobe Reader 11 and earlier, Adobe Reader DC, Microsoft Outlook, Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Microsoft Edge

You can turn on monitoring for TAP applications in any Workstyle.

To create a TAP rule:

1. Expand **Workstyles**, and then expand a Workstyle.
2. Select **Trusted Application Protection**.
3. In the **Rule** section, set the following:
    - **Trusted Application Protection**: From the list select **Enabled**, **Disabled**, or **Not Configured**. The first Workstyle evaluated that has TAP set to **Enabled** or **Disabled** is matched by Privilege Management for Windows, meaning subsequent Workstyles are not evaluated by Privilege Management for Windows.
    - **Action**: Select from **Passive (No Change)** or **Block**. The selected action is applied when the DLL in the TAP application tries to run.
    - **End User Message**: Select if a message is displayed to the user when the DLL tries to run (regardless of if it is allowed to run). We recommend using messages if you are blocking a DLL from running, so the end user has some feedback.
4. In the **Auditing** section, select **On** or **Anonymous**. This setting determines if an event is raised when the TAP application tries to run a DLL. When auditing is on, the event is sent to the local event log file. Anonymous removes user and host name from events so the user and host details are not identifiable.
5. In the **Reporting Options** sections, select **Reporting Events** to capture events.
6. Click the **Configure Exclusions** link to add DLLs to exclude from the TAP applications rule. These are DLLs that have either an untrusted owner or an untrusted publisher, but you still want to be allowed to run with TAP enabled in the Workstyle. This list of DLLs is not validated. If the DLL name listed is not matched by the client, then nothing is excluded.

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 to access this computer from the network.

For more information, please see the following:

- *"Remote PowerShell Commands" on page 72*
- *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.

Computer filters can be configured on Windows and macOS computers.

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. (Windows only) 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. (Windows only) 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 the applications you want to assign to a Workstyle.

Show Hidden Application Groups

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

Search Application Groups

You can search for applications that are already a part of an Application Group. Using the search, you can:

- Drill into an application and edit the properties.
- Drill into the Application Group to see the applications that are part of the group.

To search application groups:

1. On the **Policy Editor** page, expand **Windows** or **macOS**.
2. Select **Application Groups**, and then select **Search**.
3. Optionally, select filters from the list to narrow the search results.

Create an Application Group

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

Delete an Application Group

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

Duplicate an Application Group

1. On the **Policy Editor** page, expand **Windows** or **macOS**.
2. Select **Application Groups**.
3. Select an Application Group in the list, and then 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.

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

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

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 are 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, please see the following:

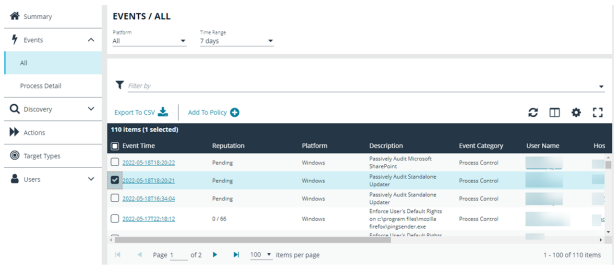
- *"Application Definitions" on page 59*
- *"Advanced Options" on page 64*
- *"Environment Variables" on page 63*
- *"Add an Application From a Template" on page 59*

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 **Analytics** from the menu.
2. Expand **Events** and select **All** or **Process Detail**.

3. Select an event in the list and select **Add to Policy**. The Policy Editor opens.



4. On the **Add Applications 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 criterion 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 on the App ID of the COM class, which is a GUID used by Windows to set properties for a CLSID. AppIds

Name	Description
matches	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 option 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.
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.

Name	Description
	◦ **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 144.* 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.
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. While SHA-1 is supported, SHA-256 is recommended.
File Hash (SHA-256) matches	Set the SHA-256 file hash on an application. The SHA-256 hash is supported on all appropriate applications, both Windows and macOS operating systems. On the Windows operating system, you can select either **match** or **does NOT match**. The **does NOT match** setting is not available on macOS. We recommend using SHA-256 rather than SHA-1.
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 then 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

Name	Description
	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** • **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

Name	Description
	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** • **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 is 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 criteria:

- 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) matches
- File Hash (SHA-256) 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) matches

- File Hash (SHA-256) 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) matches
- File Hash (SHA-256) 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) matches
- File Hash (SHA-256) 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) matches
- File Hash (SHA-256) 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) matches
- File Hash (SHA-256) 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) matches
- File Hash (SHA-256) 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) matches
- File Hash (SHA-256) 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) matches
- File Hash (SHA-256) 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 are 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.
6. Click **OK**. The application is added to the Application Group.

For more information, please see:

- *"Application Definitions" on page 59 for more about command line matching.*
- *To manage remote PowerShell scripts instead of a single cmdlet, please see "Insert Remote PowerShell Scripts" on page 73.*

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) matches
- File Hash (SHA-256) 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 Full Admin**.

> ***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 are 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) matches
- File Hash (SHA-256) 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) matches
- File Hash (SHA-256) 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 are 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.

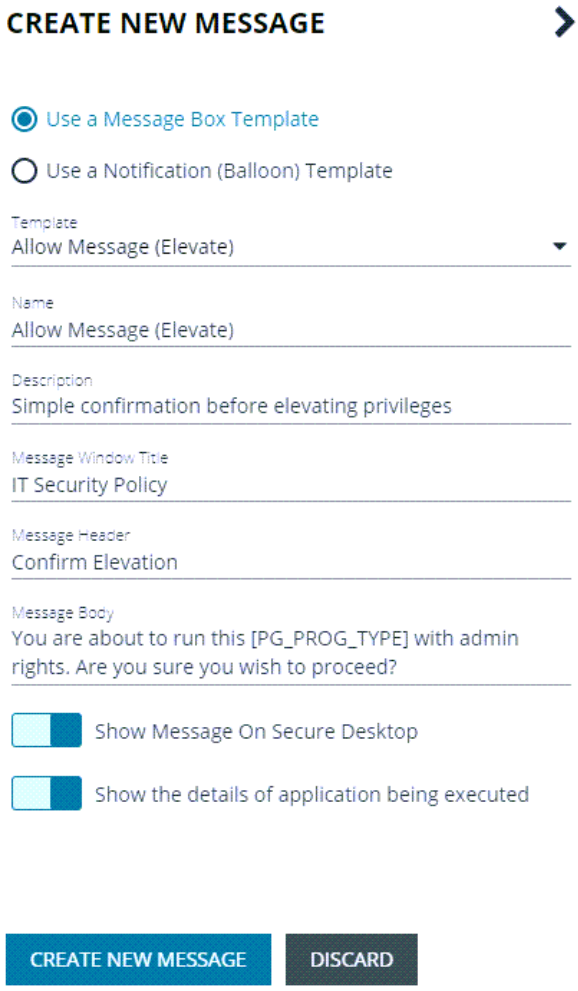
Messages are assigned to Application Rules. A message displays different properties, depending on the targets it is assigned to.

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.



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.
- User authorization where a user must provide password, smart card, or both types of authentication information.
- Multifactor authentication where an Identity Provider is configured.

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

Set up Message Header and Body Options

Configure the following settings:

Header Options

- **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.

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

Additional header message design properties are available when using the **User Request Message** template. You can customize the text for the interactive prompts displayed during the request workflow, such as request text, pending text, and approval text.

Body Options

- **Body Text**: Add additional information for the end user.
- **Message Mode**: From the list, select **Automatic** or **Custom**. You can decide what information you want to display on the message. By default, all rows are on and will be displayed as part of the message. The **Automatic** default values are:
    - **Show Line One:** The *Program Name* or the *Content Name*.
    - **Show Line Two:** The *Program Publisher* or the *Content Owner*.
    - **Show Line Three:** The *Program Path* or the *Content Program*.
- **Show Reference Hyperlink**: (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.
- **Publisher**: Enter a publisher name and information to display if the verification for the publisher fails.
- **Buttons**: Customize the labels for the **OK** and **Cancel** buttons.

Additional body message design properties are available when using the **User Request Message** template. You can customize the text for the interactive prompts displayed during the request workflow, such as request text, pending text, and approval text.

Email Settings

Email settings can be configured when using the block message template.

To access email settings, you must first create the message then edit the properties for the message.

Configure the following:

- **Mail To**: Email address to send the request to (separate multiple email addresses with semicolons).
- **Subject**: Subject line for the email request.

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.

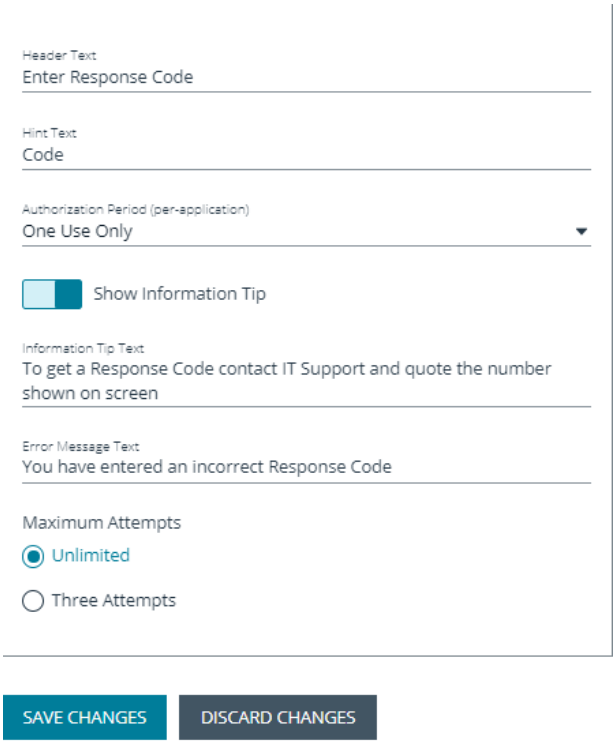
The Challenge/Response feature is a global setting and can be configured for Windows and macOS messages. Challenge/Response Authorization only applies to Allow message types.

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. Create a message following the steps provided earlier. If this is an existing message, select **Edit** from the menu.
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.
        - **One use Only**: A new challenge code is presented to the user on every attempt to run the application.
        - **Entire Session** (Windows only): A new challenge code is presented to the user on the first attempt to run the application. After a valid response code is entered, the user is not presented with a new challenge code for subsequent uses of that application until they next log on.
        - **Forever**: A new challenge code is presented to the user on the first attempt to run the application. After a valid response code is entered, the user is not presented with a new challenge code again.
        - **As defined by helpdesk** (Windows only): A new challenge code is presented to the user on the first attempt to run the application. If this option is selected, the responsibility of selecting the authorization period is delegated to the helpdesk user at the time of generating the response code. The helpdesk user can select one of the three above authorization periods. After a valid response code is entered, the user does not receive a new challenge code for the duration of time specified by the helpdesks.



- **Suppress messages once authorized** (Windows only): Select to suppress messages. This setting is not shown when set to **One Use Only**.
- **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.

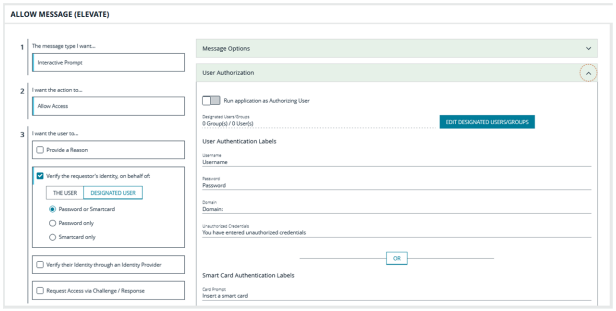
- **Maximum Attempts**: Select from **Unlimited** and **Three Attempts**.
- **Maximum Attempts Exceeded Message Text**: The message is only displayed when **Three Attempts** is selected. Add text to display to the end user if they exceed the allowed number of challenge/response attempts.

Add User Authorization

When using a message to allow access to an application, you can enforce strict access to network resources using the authorization settings. When configured, users are required to enter credentials to proceed. The credential can be a password, smart card, or both.

User authorization settings can be configured on both Windows and macOS messages.

1. Select the message where you want to add user authorization as part of the access workflow.
2. Select **Verify the requestor's identity, on behalf of:**.
3. Choose either **The User** or **Designated User**. If you select **Designated User**, see the following procedure for details on adding users and groups.
4. Select the authorization method: **Password or Smartcard**, **Password only**, or **Smartcard only**.
5. Click **User Authorization** to expand and customize labels and descriptions. The available fields will change depending on which method of authorization is selected, as noted here:



   - **The User**: When selected, enter the password. Optionally, customize the message that displays to users when the credentials are not approved.
   - **Designated User**: When selected, click the **Edit Designated Users/Groups** to add the authorized users.
     - After the groups are added, enter the user name, password, and domain.
     - (Optional). Select **Run application as Authorizing User**. When selected, the application runs in the context of the authenticating user. When not selected, the application runs in the context of the logged on user.
     - (Optional). Customize the message that displays to users when the credentials are not approved.
   - **Smart Card**: When smart card authorization is included, you can optionally customize the messages that display to the user.

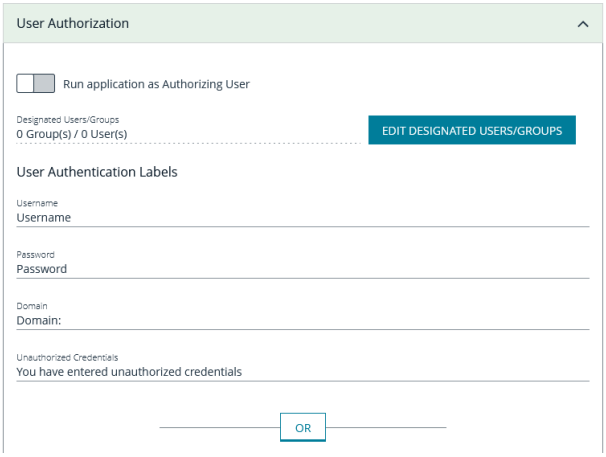
> ***Note:*** *At this time, you must fill out all of the fields under* ***User Authorization*** *to confirm your changes.*

Edit Designated Users

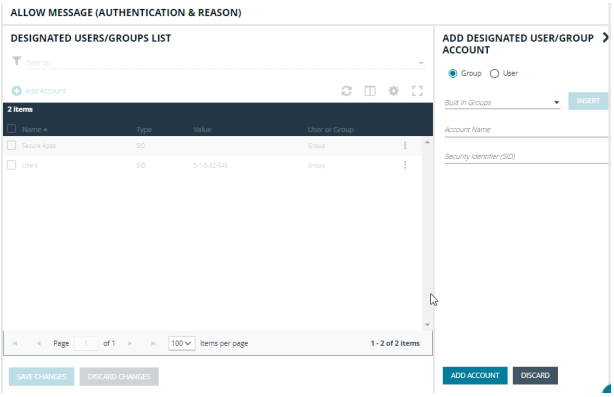
You can add, edit, and remove users and groups from the **Designated Users/Groups List** list in the message configuration. You can manage multiple accounts at once from the **Designated Users/Groups List** page.

> ***Note: Designated User*** *must be selected on step 3.* ***Verify the requestor's identity, on behalf of:*** *for the* ***Edit Designated Users/Groups*** *button to appear in User Authorization.*

1. With **User Authorization** expanded, click **Edit Designated User/Groups**.



2. Click **Add Account**.
3. Select **User** or **Group**, and then add the information.
4. If you select a built-in group, click **Insert** to automatically populate the account name and security identifier (SID).
5. After providing account the information, click **Add Account**.
6. After adding your accounts, click **Save Changes** to return to the message configuration page.



7. Click **Save Changes** again to close the message configuration page.
8. Click **Save** at the top left of the **Policies** page to save your message changes, or they will not be confirmed in the Web Policy Editor.

Configure Multifactor Authentication Using an Identity Provider

Multifactor authentication (MFA) using an identity provider can be configured for messages in Privilege Management. Identity providers supported by Privilege Management include those using OpenID Connect (OIDC) and RADIUS protocols, and BeyondTrust should be setup as a *Native* or *Desktop* app within your Identity Provider configuration.

The RADIUS protocol is supported on Windows OS only.

Add an Identity Provider

1. In the Policy Editor, go to **Messages**.
2. Click **Identity Provider Settings**.
3. On the **Identity Provider Settings** panel, select an identity provider from the list: **OIDC** or **RADIUS**.

4. Enter the following details for the identity provider:
    - OIDC Settings
        - **Authority URI:** The address of your identity provider.
        - **Client ID:** Must match the same value configured for your identity provider's BeyondTrust application.
        - **Redirect URI:** Must match the same value configured for your identity provider's BeyondTrust application. The format is **http://127.0.0.1:*port_number***, where *port_number* is an open port on your network. The *port_number* is only needed if required by your identity provider.
    - RADIUS Settings
        - **Authentication Mechanism:** The authentication type that is required by your RADIUS server. Supported authentication mechanisms are MS-CHAPV2 or PAP.
        - **Host:** The hostname of your RADIUS server.
        - **Port:** The port number for connecting to your RADIUS server.
        - **Shared Secret:** The secret key required by your RADIUS server.
5. Click **Save RADIUS Settings** or **Save OIDC Settings** depending on the type you selected.

After an identity provider is added you can configure any allow message type to use multifactor authentication.

Set up a Multifactor Authentication Message

1. In the Policy Editor, go to **Messages**.
2. Select the message type **Allow Message (with Authentication)**.
3. Expand **Multifactor Authentication**.
4. Select **Idp - OIDC**, **Idp - RADIUS**, or **Idp - None**.
5. Click **Save Changes**.

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 does not 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** on 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**.

Import Template Policies

You can import a template and merge or overwrite the settings in an existing template.

1. In the Policy Editor, expand **Utilities**.
2. Select **Template Policies**.
3. Select one of the following:
    - **Merge Policy**: Merges the configuration to the existing template.
    - **Overwrite Policy**: If you select to overwrite, you can optionally select **Export Existing Policy** to save a copy before overwriting the policy.

4. Select a template from the list: **Discovery**, **QuickStart for Mac**, **QuickStart for Windows**, **Server Roles**, **TAP (High Flexibility)**, **TAP (High Security)**.
5. If you are merging, select **Merge Template Policy** to save the settings. If you are overwriting, select **Overwrite Policy**.

Manage Audit Scripts

When an application is allowed, elevated, or blocked, an event is logged to record details of the action. Actions are recorded in a third party tracking system by using Audit Scripts. You can write Audit Scripts in Powershell, VBScript, or Javascript and configure these scripts through the web policy editor.

1. In the Policy Editor, expand the **Utilities** node.
2. Select **Manage Audit Scripts**.
3. Click **Upload Script** to expand the Upload Script panel.
4. Click the following dropdown menus to further configure the script:
    - **Timeout Options**
    - **Context Options**
5. Click inside the upload box to select the script.

Manage Rule Scripts

You can upload, view, and delete Power Rules from within the Web Policy Editor.

1. In the Policy Editor, expand **Utilities**.
2. Select **Manage Rule Scripts**.
3. Click **Upload Script** to expand the Upload Script panel.
4. Drag and drop the new script into the upload box or click to select a file.

> ***Note:*** *The script uploaded must be a Powershell script.*

5. Click inside the **Timeout options** field to select a value.
6. Click **Upload Script** to save your changes.

> *For more information, please see Apply Power Rules Scripts to Your Application Rules at https://www.beyondtrust.com/docs/privilege-management/windows/epo-admin/utilities/power-rule-scripts.htm.*

Upload and Delete Settings

You can upload settings for an existing Rule Script by clicking the vertical ellipsis icon and selecting **Upload Settings** from the dropdown menu.

> ***Note:*** *The file that is uploaded must be in **.json** format.*

To delete the settings file, click the vertical ellipses again and select **Delete Settings** from the dropdown menu.

Advanced Agent Settings

You can configure the Advanced Agent Settings utility through the web policy editor to deploy additional registry based settings to endpoints that are running Privilege Management for Windows and Mac.

1. In the Policy Editor, expand **Utilities**.
2. Select **Advanced Agent Settings**.
3. Click **Add** to create a new setting.
4. Type the desired value name.
5. Select one of the following to designate the type:
    - **DWORD**
    - **String**
    - **Multi-String**
6. Click **Create** to confirm your changes and create the new setting, or **Discard** to delete your work.

Force Policy Updates

End users working on either Windows or macOS computers can update policy on their computers without administrator assistance.

Force Update Policy for Windows 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.

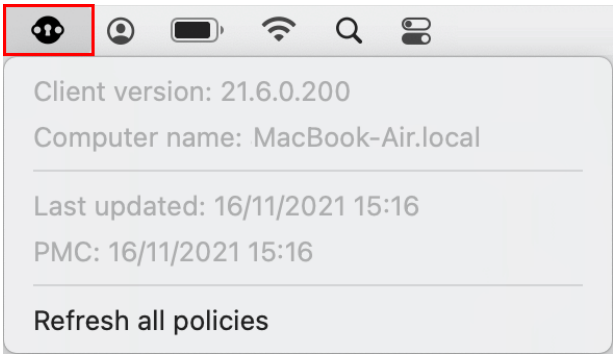
Force Update Policy for macOS End Users

A user can check whether a new policy is available. If it is, then the new policy is downloaded and applied. The immediate availability of a new policy is useful when you have an issue that requires a policy update, without the necessity of waiting for a poll to pull in a new one.

To refresh all policies, select the **Privilege Management for Mac** menu bar icon, and select **Refresh all Policies**.

If a newer policy is found, it is downloaded and applied immediately.

A message confirming the successful update appears. The new policy revision date also appears in the dropdown menu as *Last updated*.



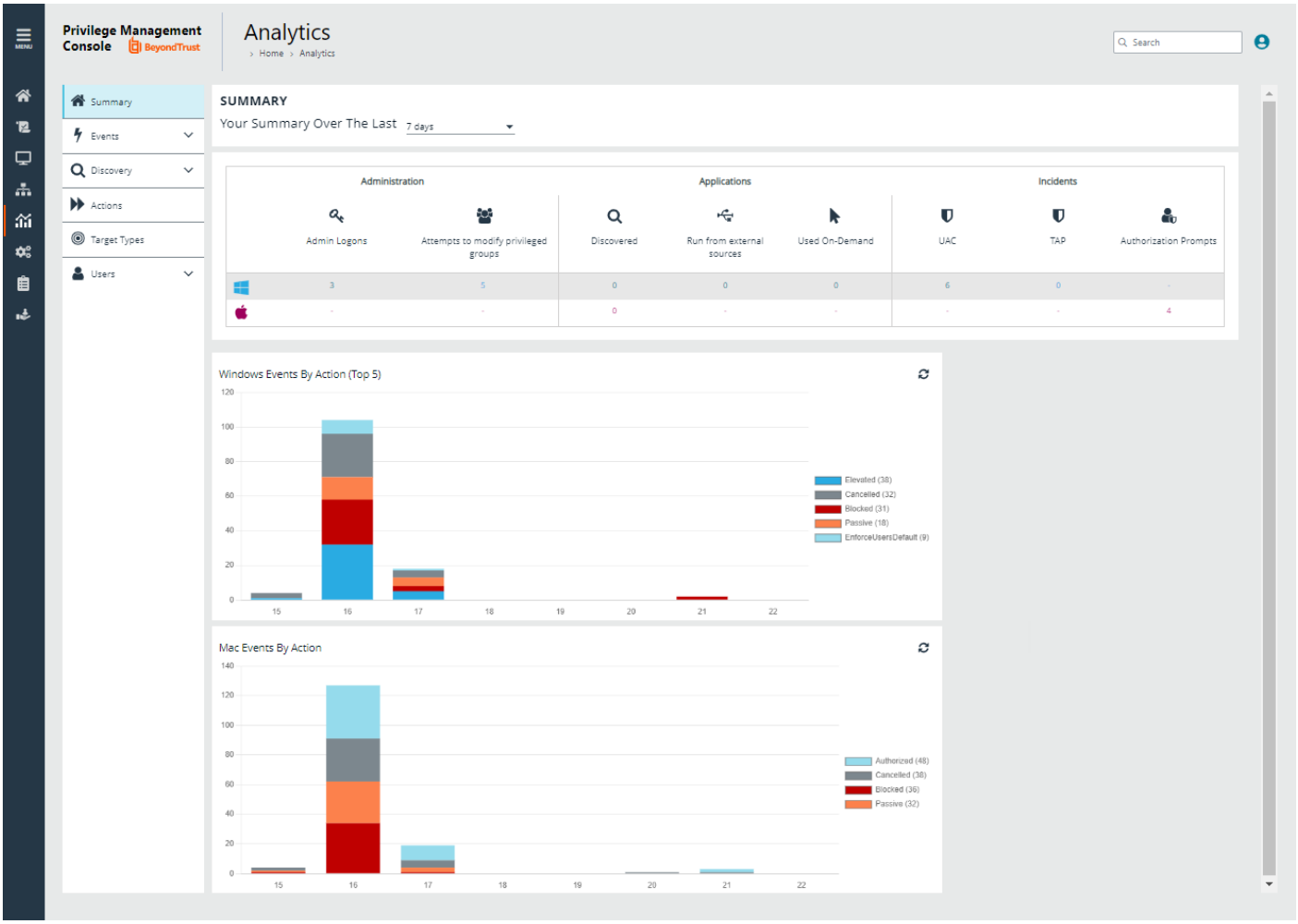
Privilege Management Console Analytics

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.



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.

Table	Description
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 information:

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
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

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**
- **Date First Reported**
- **Date First Executed**

"Discovery by Publisher" Report

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 **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.
- **# 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**
- **Date First Reported**
- **Date First Executed**

"Discovery by Type" Report

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:

- **# 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**
- **Date First Reported**
- **Date First Executed**

"Discovery Requiring Elevation" Report

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:

- **# 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**
- **Date First Reported**
- **Date First Executed**

"Discovery from External Sources" Report

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

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 **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

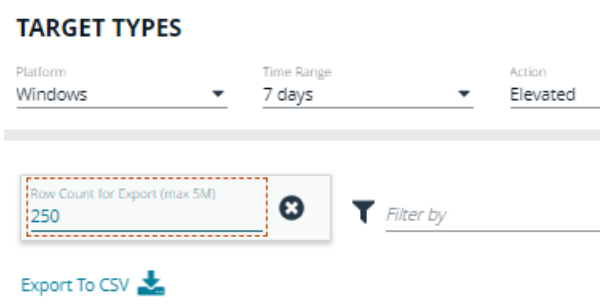
Click the link in the **Description** column to see more detailed information on the application, including the actions over the last 30 days split by the type of token, the top 10 users, the top 10 hosts, the run method, and the portion of those discoveries where admin rights was detected.

Export to a CSV File

The number of items that can be displayed at one time might be limited by the browser display. Use **Export to CSV** to save the items to a CSV file.

On a report page where **Export to CSV** is available, you must select the filter **Row Count for Export (Max 5M)**, and then enter the number of rows to include in the CSV file.

All filters are saved to the file.



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. Click a bar to open the **Target Types** report with the **Platform**, **Time Range**, **Action**, and **Target Type**, 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** report with the **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Top 10 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 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** report with the **Platform**, **Time Range**, **Action** and **Target Type** filters applied.
Top 10 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 **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Distinct 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 **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Top 10 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** report with the **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Distinct 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 **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Top 10 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** report with the **Platform**, **Time Range**, **Action**, **Target Type** filters applied.
Distinct 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** report with the **Action** and **Target Type** filters applied.
Top 10 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** report with the **Platform**, **Time Range**, **Action**, **Target Type** filters applied.
Distinct 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** report with the **Platform**, **Time Range**, **Action**, and **Target Type** filters applied.
Top 10 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 Report

The Target Types report lists all applications active in the time period, grouped by the application description ordered by user count descending.

When a specific platform is selected from the **Platform** list, then the **Action** list populates with actions only available to that platform.

The following columns are available for the **Target Types** report:

- **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

You can drill down on the following items to view more detail:

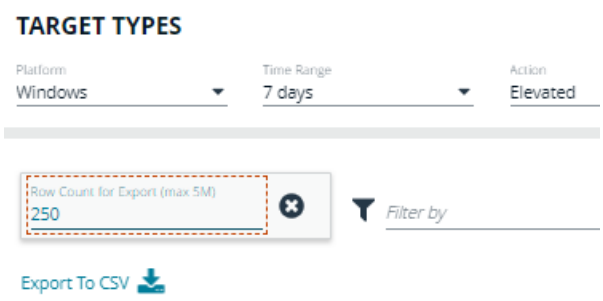
- **Description**: View actions over the time period, the top 10 users, top 10 hosts, the type of run method, and whether admin rights were detected.
- **User Count**: View the user names accessing the application. From the **User List** page, click a user name to open the **User Report** page.
- **Process Count**: Opens the **Events All** report.

Export to a CSV File

The number of items that can be displayed at one time might be limited by the browser display. Use **Export to CSV** to save the items to a CSV file.

On a report page where **Export to CSV** is available, you must select the filter **Row Count for Export (Max 5M)**, and then enter the number of rows to include in the CSV file.

All filters are saved to the file.



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>	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 a bar 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	The average number of *Allow* messages and *Block* messages users receive per day. Click a bar 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 **User Report** page, click the number in the **Applications Used** row to navigate to the **Target Types > All** page.
Messages per action type	The number of 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.

Privileged Logons Report

The **Privileged Logons** 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>	The number of logons by the different account types over time. Click a link for more information about each privileged logon. By default, **Show Admin Logons** and **Show Standard User Logons** filters are applied.
Administrators, Power Users, and Standard Users table	The number of logon events by administrators, power users, and standard users, as well as how many users logged in.
Privileged logons by user type	The total number of privileged logons broken down by standard users and administrator users.
Logons by account privilege	The total number of logons, broken down by logon privilege. Click a bar for more information about the user logons for the time period. By default, **Show Admin Logons**, **Show Standard User Logons**, and **Show Power User Logons** filters are applied.
Logons by account type	The total number of logons, broken down by domain accounts and local accounts. Click a bar for more information about the user logons for the time period. By default, **Account Authority**, **Show Admin Logons**, **Show Standard User Logons**, and **Show Power User Logons** filters applied.
Top 10 logons by chassis type	The total number of logons, broken down by the top 10 chassis types. Click a bar for more information about the user logons for the time period. By default, **Show Admin Logons**, **Show Standard User Logons**, **Show Power User Logons**, and **Chassis Type** filters are applied.

Chart	Information
Top 10 logons by operating system	The total number of logons, broken down the top 10 host operating systems. Click a bar for more information about the user logons for the time period. By default, **Show Admin Logons**, **Show Standard User Logons**, **OS**, and **Show Power User Logons** filters are applied.
Top 10 accounts with admin rights	The top 10 accounts with admin rights that have logged into the most host machines. Click a bar for more information about the user logons for the time period. By default, **Show Admin Logons**, **Show Standard User Logons**, **User Name**, **Show Power User Logons**, and **User Domain** filters are applied.
Top 10 hosts with admin rights	The top 10 host machines that have been logged onto by the most users with admin rights. Click a bar for more information about the user logons for the time period. By default, **Show Admin Logons**, **Show Standard User Logons**, and **Show Power User Logons**, **User Name**, and **User Domain** filters are applied.

User Session report

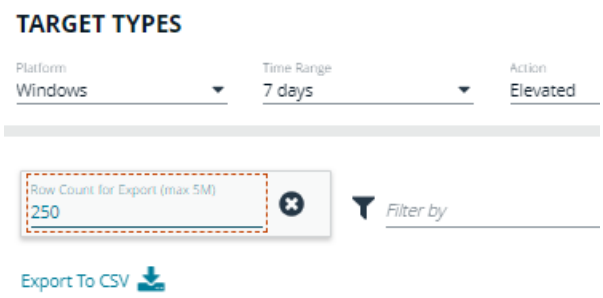
On the **User Session** report, accessed from the **Privileged Logons** report, you can view more details about the privileged logon account sessions. The details include the user name, logon time, account type, and domain, etc.

Export to a CSV File

The number of items that can be displayed at one time might be limited by the browser display. Use **Export to CSV** to save the items to a CSV file.

On a report page where **Export to CSV** is available, you must select the filter **Row Count for Export (Max 5M)**, and then enter the number of rows to include in the CSV file.

All filters are saved to the file.



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	The number of **Users blocked**, **Hosts blocked**, **Applications blocked**, and the **Blocked modifications** within the specified time frame.

Chart	Description
By Privileged Group	The same data grouped by type of account. Click the account type for more information about the account and hosts with the **Group Name** filter applied.
By application	The privileged account modification activity that was blocked, broken down by the description of the application used. Click a bar for 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	The top 10 users who attempted modifications. Click a bar for a more detailed view of the privileged account management account modifications with the **Application User Name** filter applied.
Top 10 hosts attempting account modifications	The top 10 hosts attempting privileged account modifications. Click a bar for 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
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.

Event ID	Description
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.
199	Process execution was blocked, the maximum number of challenge / response failures was exceeded.

Note: *With our SIEM Integration, we only support a subset of all event types.*

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)

SIEM Format Information

PMC supports **Common Event Format (CEF)** and **Elastic Common Schema (ECS)** formats for *Privilege Management* events, *Activity Audit* events, and *Authorization Request* events.

Common Event Format (CEF) for Splunk

CEF Format of Computer (PMfW) Events (since PM Cloud 21.3)

Dataset name	Field Name	Data type	Description
	@timestamp	timestamp	The time at which the event occurred.
Processes	parent_process_exec	string	The executable name of the parent process.
Processes	process_exec	string	The executable name of the process, such as notepad.exe.
Processes	process_hash	string	The digests of the parent process, such as <md5>, <sha1>, etc.
Processes	process_name	string	The friendly name of the process, such as notepad.exe.
Processes	parent_process	string	The full command string of the parent process.
Processes	parent_process_id	number	The numeric identifier of the parent process assigned by the operating system.
Processes	process_id	number	The numeric identifier of the process assigned by the operating system.
Processes	process	string	The full command string of the spawned process.
Processes	user_id	string	The unique identifier of the user account which spawned the process.
Processes	description	string	The description of the process event.
Processes	user	string	The user account that spawned the process.
Processes	action	string	The action taken by the endpoint, such as allowed, blocked, deferred.
Processes	process_path	string	The file path of the process, such as C:\Windows\System32\notepad.exe.

Dataset name	Field Name	Data type	Description
Processes	vendor_product	string	"Beyondtrust Privilege Management"
Processes	dest	string	The endpoint for which the process was spawned.

CEF Format of Activity Audit Events (since PM Cloud 21.6)

Dataset name	Field Name	Data type	Description
	@timestamp	timestamp	The time at which the event occurred.
All_Changes	action	string	The action attempted on the resource, regardless of success or failure.
All_Changes	command	string	Description of the action.
All_Changes	object_category	string	Generic name for the class of the updated resource object. Possible values are: Computer, InstallationKey, User, Group, Policy, PolicyRevision, Settings.
All_Changes	object_id	string	The unique updated resource object ID as presented to the system, if applicable.
All_Changes	src_user	string	For user account changes, the user performing the action.
All_Changes	user	string	The user performing the action.
All_Changes	vendor_product	string	"Beyondtrust Privilege Management"

CEF Format of Authorization Request Events (since PM Cloud 21.6)

Dataset name	Field Name	Data type	Description
	@timestamp	timestamp	The time at which the event occurred.
Processes	process_exec	string	The executable name of the process, such as notepad.exe.
Processes	process_path	string	The file path of the process, such as C:\Windows\System32\notepad.exe.
Processes	process_hash	string	The digests of the parent process, such as <md5>, <sha1>, etc.
Processes	dest	string	The endpoint for which the process was spawned.
Processes	user	string	The user account that spawned the process.
Processes	process_name	string	The friendly name of the process, such as notepad.exe.
Processes	process	string	The full command string of the spawned process.
Processes	vendor_product	string	"Beyondtrust Privilege Management"
All_Ticket_ Management	comments	string	This will show the duration if the request was approved.
All_Ticket_ Management	description	string	Reason for request as given by the user.
All_Ticket_ Management	src_user	string	The requesting user.
All_Ticket_ Management	status	string	Status of ticket: Pending, Approved, Denied.

Dataset name	Field Name	Data type	Description
All_Ticket_Management	ticket_id	string	The ticket id.
All_Ticket_Management	time_submitted	time	The time the request was submitted.
All_Ticket_Management	user	string	User in ticking system who approved or denied.
All_Ticket_Management	tag	string	Indicates type of ticket: incident, change.

Elastic Common Schema (ECS) v1.10 Format

ECS Format of Computer (PMfW) Events (since PM Cloud 21.6)

Field Set Name	Field Name	Data type	Description
	@timestamp	timestamp	The time at which the event occurred.
	message	text	Description of the process.
process.parent	name	keyword	Process name.
process.parent	executable	keyword	Absolute path to the process executable.
process.parent	pid	long	Process id.
process	name	keyword	Process name.
process	command_line	keyword	Full command line that started the process, including the absolute path to the executable, and all arguments.
process	executable	keyword	Absolute path to the process executable.
process	entity_id	keyword	Unique identifier for the process (hash).
process	ppid	long	Parent process' pid.
process	pid	long	Process id.
process	title	keyword	Process title.
host	hostname	keyword	Hostname of the host.
host.user	name	keyword	Short name or login of the user.
host.user	id	keyword	Unique identifier of the user.
event	code	keyword	Type of PMfW event.
event	kind	keyword	"event"
event	category	array of keyword	["process"]
event	provider	keyword	"Beyondtrust Privilege Management"
event	type	array of keyword	Array containing one of: allowed, info, denied
event	action	keyword	The action captured by the event: allowed, deferred, blocked
ecs	version	keyword	1.10

ECS Format of Activity Audit Events (since PM Cloud 21.6)

Field Set Name	Field Name	Data type	Description
	@timestamp	timestamp	The time at which the event occurred.
	labels.related_item_id	object	PM Cloud custom key/value pairs. related_itme_id is the unique updated resource object ID as presented to the system, if applicable.
event	action	keyword	The action captured by the event.
event	reason	keyword	Description of the action.
event	created	date	Event creation date.
event	provider	keyword	Generic name for the class of the updated resource object. Possible values are: Computer, InstallationKey, User, Group, Policy, PolicyRevision, Settings.
event	kind	keyword	"event"
event	category	array of keyword	Array containing one of: authentication, configuration.
event	type	array of keyword	Array containing one of: start, creation, deletion, change.
user	email	keyword	User email address.
ecs	version	keyword	1.10

ECS Format of Authorization Request Events (since PM Cloud 21.6)

Field Set Name	Field Name	Data type	Description
	@timestamp	timestamp	The time at which the event occurred.
	labels.duration	object	PM Cloud custom key/value pairs. Allowed duration if request is approved
	labels.decision	object	PM Cloud custom key/value pairs. Decision of request, one of: Pending, Approved, Denied.
	labels.decision_by_user	object	PM Cloud custom key/value pairs. User who made decision.
process	name	keyword	Process name.
process	entity_id	keyword	Unique identifier for the process (hash).
process	title	keyword	Process title.
process	command_line	keyword	Full command line that started the process, including the absolute path to the executable, and all arguments.
host	hostname	keyword	Hostname of the host.
host.user	name	keyword	Short name or login of the user.
event	reason	keyword	Reason for request as given by the user.
event	ticket_id	keyword	The ticket id.
event	url	keyword	Url for ticket.

Field Set Name	Field Name	Data type	Description
event	created	date	Request creation date.
event	action	keyword	Indicates type of ticket: incident, change.
event	kind	keyword	"event"
event	category	array of keyword	["process"]
event	provider	keyword	"Beyondtrust Privilege Management"
ecs	version	keyword	1.10

"Events All" Report

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

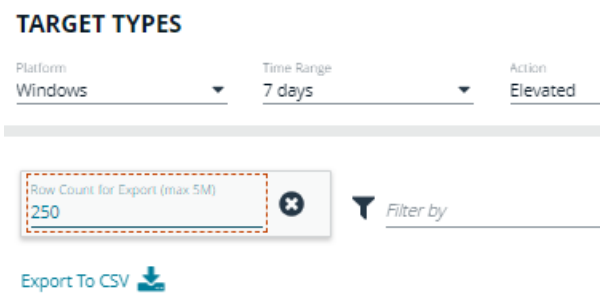
- **Workstyle:** The Workstyle containing the rule that triggered the event
- **Message:** Any message associated with the event
- **Action:** Any action associated with the event
- **Application Group:** The Application Group that the application that triggered the event belongs to
- **PID:** The operating 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
- **Auth Methods**: The type of authentication method selected in the Policy Editor. Multiple values can be present and will be comma separated. Possible values: **Identity Provider**, **Password**, **Challenge Response**, **Smart Card**, and **User Request**.
- **Idp Authentication User Name**: The credential provided when adding an Identity Provider authorization message in the Policy Editor.

Export Events to CSV File

The number of items that can be displayed at one time might be limited by the browser display. Use **Export to CSV** to save the items to a CSV file.

On a report page where **Export to CSV** is available, you must select the filter **Row Count for Export (Max 5M)**, and then enter the number of rows to include in the CSV file.

All filters are saved to the file.



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**
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.

Name	Description
Auth Methods	The type of authentication method selected in the Policy Editor. Multiple values can be present and will be comma separated. Possible values: **Identity Provider**, **Password**, **Challenge Response**, **Smart Card**, and **User Request**
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.
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.

Name	Description
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**
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.

Name	Description
Idp Authentication user name	The credential provided when adding an Identity Provider authorization message in the Policy Editor.
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**
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.

Name	Description
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).
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).

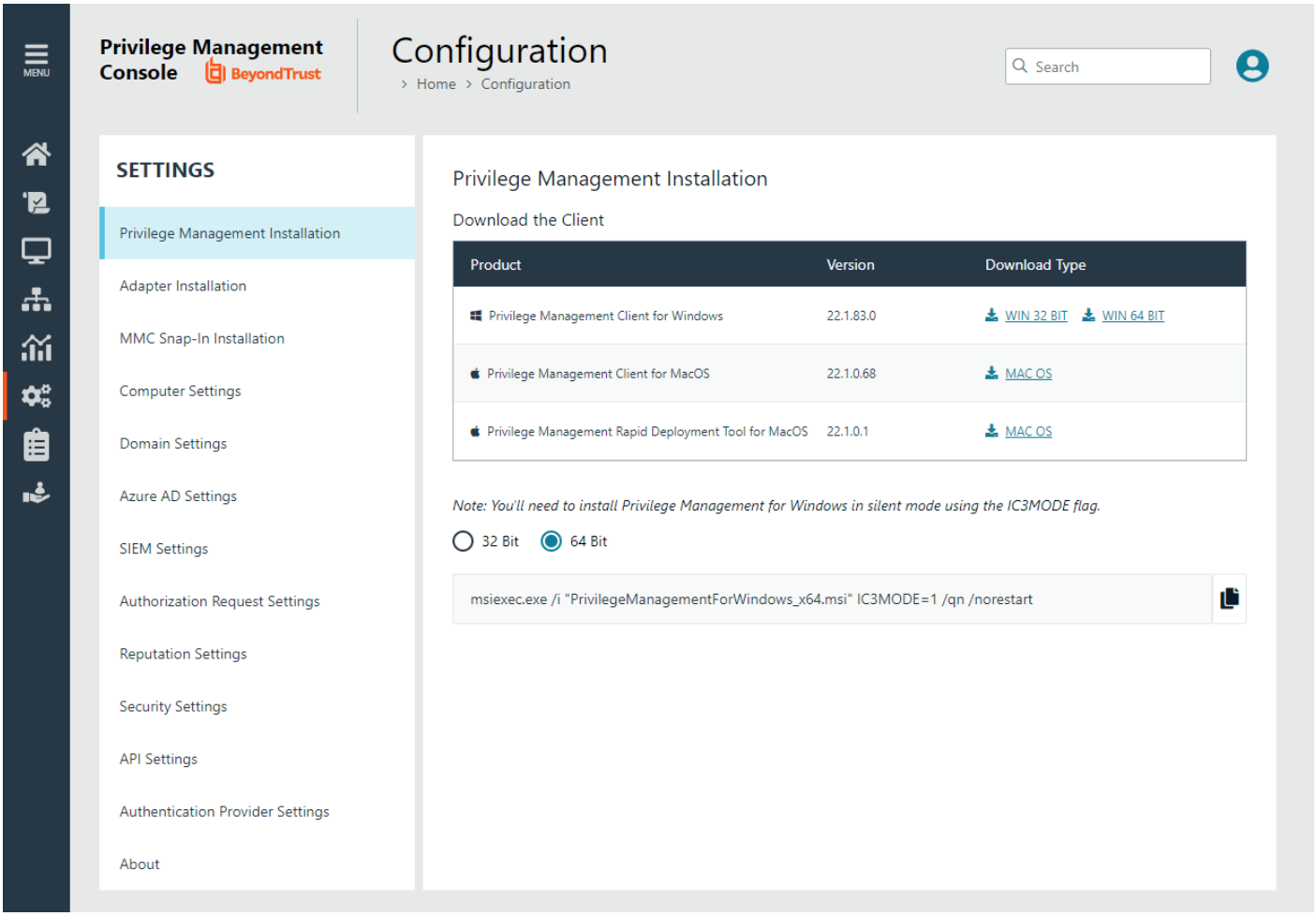
Name	Description
Rule Match Type	Rule Match Type: • **Any** • **Direct match** • **Matched on parent**
Sandbox	The sandboxed setting. Filter options: • **Not Set** • **Any Sandbox** • **Not Sandboxed**
Shell or Auto	Whether the process was launched using the shell **Run with Privilege Management** option or by normal means (opening an application): Filter options: • **Any** • **Shell** • **Auto**
Show Discovery Events	Whether or not you want to show Discovery events. An event is a Discovery event if it has 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.

Name	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**
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**

Name	Description
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.



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

- Privilege Management Installation
- Adapter Installation
- MMC Snap-In Installation
- Computer Settings
- Domain Settings
- Azure AD Settings
- SIEM Settings
- Authorization Request Settings
- Reputation Settings
- Security Settings

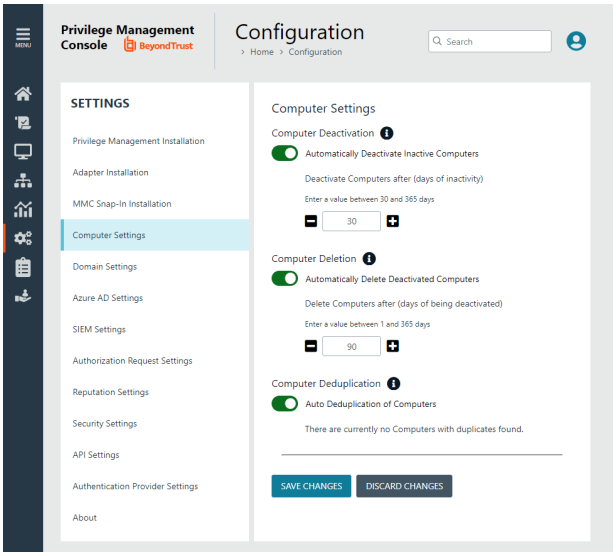
- API Settings
- About

> *For more information, please see the following:*
>
> - *"Privilege Management Console QuickStart" on page 11*
> - *"Install the Windows Adapter" on page 12*
> - *"Install the Mac Adapter" on page 15*
> - *"Configure the Privilege Management MMC PMC snap-in" on page 18*

Computer Settings

On the **Computer Settings** page, you can set properties to help manage computers in your environment:

- Detect duplicate computers
- Deactivate computers
- Delete computers



To access the **Computer Settings** page:

1. On the sidebar menu, select **Configuration**.
2. On the **Settings** panel, click **Computer Settings**.

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 is 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:

1. In the **Computer Deactivation** section, select **Automatically deactivate inactive computers**.
2. Enter the number of days that pass before the computer is deactivated.
3. Click **Save Changes**.

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

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 34*
- *"Deactivate Computers" on page 34*

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

Computer Deletion

You can automatically delete deactivated computers.

To set automatic deactivated computer deletion:

1. In the **Computer Deletion** section, select **Automatically Delete Deactivated Computers**.
2. Enter the number of days that pass after the computer is deactivated.
3. Click **Save Changes**.

Computer Deduplication Settings

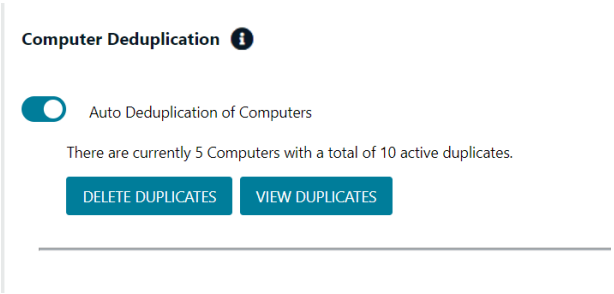
A computer duplicate is one that has the same host name as another computer but has not connected to the Privilege Management Console as recently. Auto deduplication is turned off by default.

To set automatic deduplication of computers:

1. In the **Computer Deduplication** section, select **Auto Deduplication of Computers**. The deduplication job runs nightly and detects duplicate computers.
2. Click **Save Changes**.

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

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



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 (Azure AD or OpenID Connect) 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 SIEM provider. Events include computer, activity, and authorization requests. Events are sent in the selected format (CEF or ECS).

Note: *With our SIEM Integration, we only support a subset of all event types.*

For more information on formats, see "SIEM Format Information" on page 102.

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.

PMC supports the following SIEM providers:

- AWS
- Splunk
- Microsoft Sentinel
- QRadar

> ***Note:*** *There can only be one SIEM tool configured. If you choose to add details for a new SIEM tool, existing settings data will be lost.*

Configure AWS S3 Bucket

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*

Add the AWS S3 Bucket in PMC

1. Select **Configuration**, and then select **SIEM Settings**.
2. Select **Enable SIEM Integration** to turn on the feature.
3. From the **Integration Type** list, select **S3**
4. 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.
5. Select the data format: **CEF - Common Event Format** or **ECS - Elastic Common Schema**.
6. Select **Server-Side Encryption** to encrypt files sent to the S3 bucket using the default AWS encryption key.
7. Click **Validate Settings** to test the connection to your storage site.
8. Click **Save Settings**.

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

Add Splunk to PMC

1. Select **Configuration**, and then select **SIEM Settings**.
2. Select **Enable SIEM Integration** to turn on the feature.

3. From the **Integration Type** list, select **Splunk**.
4. Enter the details for your Splunk configuration:
    - Hostname
    - Index
    - Token
5. Select the data format: **CEF - Common Event Format** or **ECS - Elastic Common Schema**.
6. Click **Validate Settings** to test the connection to Splunk.
7. Click **Save Settings**.

Add Microsoft Sentinel to PMC

1. Select **Configuration**, and then select **SIEM Settings**.
2. Select **Enable SIEM Integration** to turn on the feature.
3. From the **Integration Type** list, select **Sentinel**.
4. Enter the details for your Sentinel configuration:
    - **Workspace ID**: Enter the Sentinel workspace ID. In Sentinel, the workspace ID is located in this path: **Settings > Workspace Settings > Agents Management**.
    - **Workspace Key**: Enter the primary key. In Sentinel, the workspace key is located in this path: **Settings > Workspace Settings > Agents Management**.
    - **Custom Log Table Name**: The table is listed under the **Custom Logs** category in Azure Sentinel. A **_CL** suffix is automatically appended to the end of the custom log table name. A custom log is created if the table name does not exist.
5. Select the data format: **CEF - Common Event Format** or **ECS - Elastic Common Schema**.
6. Click **Validate Settings** to test the connection to Sentinel.
7. Click **Save Settings**.

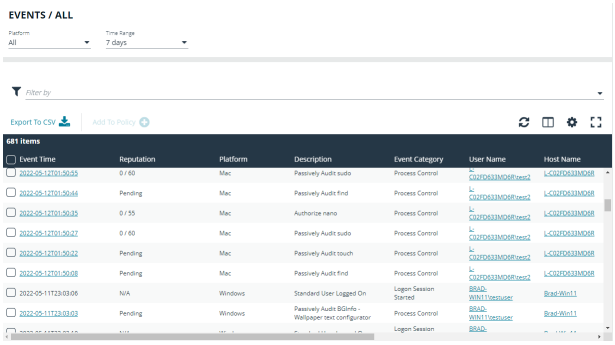
Add QRadar to PM Cloud

1. Select **Configuration**, and then select **SIEM Settings**.
2. Select **Enable SIEM Integration** to turn on the feature.
3. From the **Integration Type** list, select **QRADAR**.
4. Enter the details for your QRadar configuration:
    - Hostname
    - Port
    - Cert
    - Key
5. Click **Validate Settings**.
6. Click **Save Changes** to confirm and save.

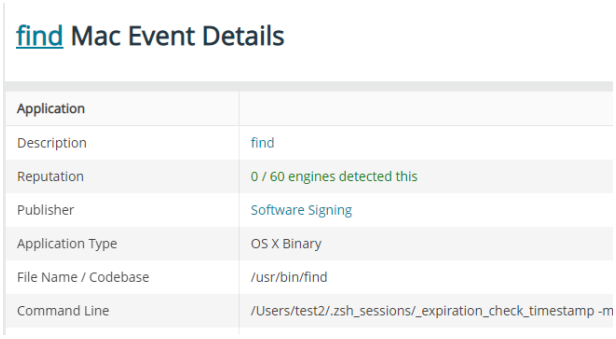
Set Up Reputation Integration

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.



Click the link for an event to view more details. Here, click the link for the reputation score to learn more about the VirusTotal scoring.



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**.

Configure Access to the Management API

The management API requires a secure account. Create an account in the PMC Configuration area.

> *For authentication information to access the API, please see the PM Cloud API Guide at https://www.beyondtrust.com/docs/privilege-management/console/pm-cloud/api/index.htm.*

Create an API Account

When using the PM Cloud Management API, you must set up an account that is used to authenticate access to the API.

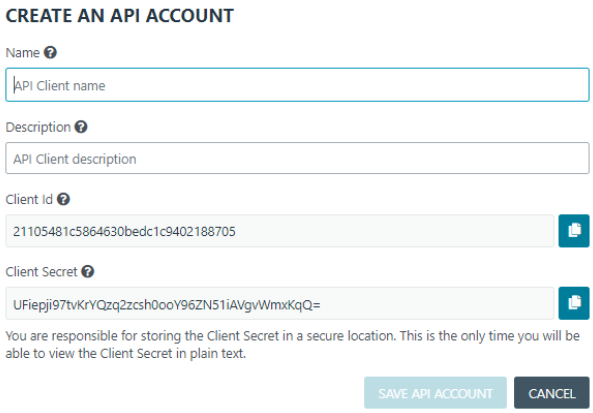
1. Click the **Configuration** menu, and then click **API Settings**.
2. Click **Create an API Account**.

3. Enter a name and description.

   The **Client ID** and **Client Secret** are automatically generated. The secret is only visible when initially generated for security reasons.

   You can use the copy icons to copy the values to the API tool you are using. You can access these after the account is created as well.

4. Click **Save API Account**.



Delete an API Account

1. Click the **Configuration** menu, and then click **API Settings**.
2. Click the trash can icon to delete the account.
3. Click **Delete Anyway** on the confirmation dialog box.

Generate a Client Secret

1. Click the **Configuration** menu, and then click **API Settings**.
2. Click the **Generate new Client secret** icon for the API account you use to access the API.
3. Click **Generate Secret**.
4. The client secret is displayed in the **Client Secret** column. Copy the secret to the authorization page of the API.

Configure Security Settings

Depending on your network security, you might want to set a session timeout for PM Cloud users. If a user is logged on to PM Cloud but inactive, the session ends after the time period runs out.

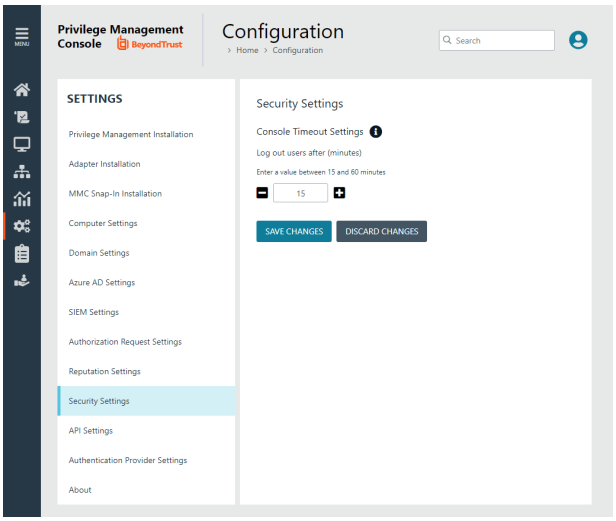
The timeout settings is global and applies to all PM Cloud users.

To access the **Security Settings** page:

1. On the sidebar menu, select **Configuration**.
2. On the **Settings** menu, click **Security Settings**.

To set the console timeout settings:

1. In the **Console Timeout Settings** section, enter a value after which users will be logged out (in minutes) . The default value is 15 minutes.
2. Click **Save Changes**.



Configure OpenID Connect

PMC supports OpenID Connect authentication. You can change your authentication provider from the default AzureB2B to OpenID Connect, or update your OpenID Connect settings, without having to contact Support.

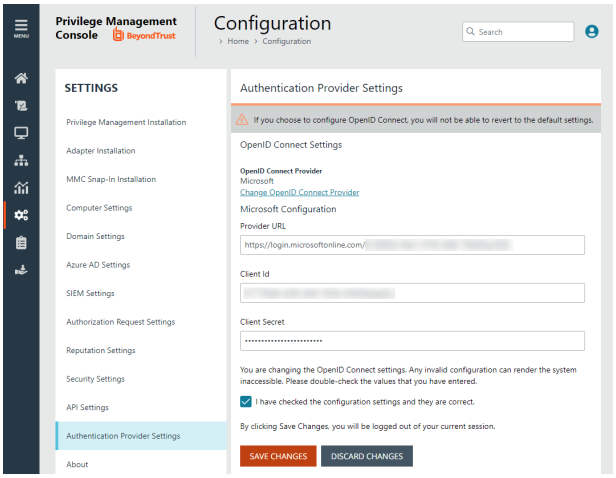
You must first set up a PMC instance in your OpenID Connect provider. Steps are provided in the section below.

Configure an Authentication Provider

When you start from the default configuration, use this procedure to set up the configuration.

To set up an OpenID Connect provider:

1. Select the **Configuration** menu, and then click **Authentication Provider Settings**.
2. Click **Enable OpenID Configuration**. After you have completed and saved the OpenID configuration, this switch no longer appears on this page.
3. Enter information for the following:
    - **Provider URL**: Domain for the authentication. Currently supports Microsoft, Okta, and Ping Identity.
    - **Client ID**: The client ID.
    - **Client Secret**: Secret key.



4. **Check the box**. We recommend reviewing the settings you configured. You can potentially lock yourself out of the system if the settings are incorrect. The **Save Changes** button is only available after you check the box.
5. Click **Save Changes**.

IMPORTANT!

*You will be logged out of the PMC Console. Once logged out, you need to log back in within **15 minutes**, because there is a timer on the page. If you do not log in before the timer expires, the authentication provider settings revert to the previous settings and the new settings are **not saved**.*

If you log on before the timer expires, the newly added authentication provider settings are retained.

PMC OpenID Connect Workflow for Existing Customers

Here is the workflow to get up and running with PMC using OpenID Connect authentication.

- You will receive an email from BeyondTrust after the request is processed.
- In the email, click the link to open the **BeyondTrust OpenID Setup** page.
- Enter the OpenID Connect information: domain, client ID, and client secret. Click **Save Setup**. The OpenID credentials are saved.
- The Privilege Management Console login page opens. Click **Log In**.
- PMC opens to the **Home** page.

Add the PM Cloud Application to Microsoft, Okta, or Ping Identity

PMC supports Microsoft Azure AD, Okta OpenID, and Ping Identity Connect providers. The following sections provide a high-level overview on adding the PMC instance to your respective authentication provider. For complete instructions, refer to the provider's documentation.

***Note:** The migration to OIDC will work when the email address sent from Okta or Azure AD matches for existing users. If email addresses are different or the domain name is not on the list of allowed domains in PM Cloud, then the authentications will fail.*

Add PMC Instance to Microsoft Azure AD

1. Start Microsoft Azure AD.
2. In the menu, click **App Registrations**.
3. Click **New Registration**.
4. Enter a **Name**.
5. Under **Supported account types**, select **Accounts in this org directory only**.
6. Enter the **Redirect URI**. While providing this now is optional and can be changed later, a value is required for most authentication scenarios.
    - From the dropdown list, select the **Public client/native (mobile & desktop)** platform.
    - Select https://<deployment>-services.pm.beyondtrustcloud.com/oauth/signin-oidc.
7. Click **Register**.
8. After PMC registers, select **Authentication** in the menu.
9. Add the following to the **Redirect URIs**: https://<deployment>-services.pm.beyondtrustcloud.com/oauth/signout-callback-oidc.

After you add PMC to Microsoft Azure AD, you can get the information you need to set up the OpenID Connect authentication. The PMC OpenID connect setup wizard requires these values:

- **OpenID Domain**: https://login.microsoftonline.com/<Directory (tenant) ID>. The directory or tenant ID uses the format 31b8dbb9-fb8b-437a-8920-f23c8e0188b1.
- **OpenID Client ID**: Application (client) ID.
- **OpenID Client Secret**: Client secret value.

10. Select **Certificates & secrets** in the menu.
11. Click **New client secret**, and copy the secret ID and value. When generating a new secret, you must select an expiry for the secret. We recommend selecting **Recommended: 6 months**.
12. On the app registration **Overview** page, copy the client ID and the tenant ID.

Add PMC Instance to Okta

1. Start your Okta instance.
2. Click **Create App Integration**.
3. In the **Create a new app integration** section, select **OIDC - OpenID Connect**.
4. Select **Web Application** as the application type.
5. In the **New Web App Integration** section, select **Client Credentials** for the **Grant type**.
6. Add the sign-in and sign-out URIs.
   - **Sign-in redirect URI**: https://{dns}-services.pm.beyondtrustcloud.com/oauth/signin-oidc
   - **Sign-out redirect URI**: https://{dns}-services.pm.beyondtrustcloud.com/oauth/signout-callback-oidc
7. Select the controller access applicable to your organization, and then click **Save**.

   After you add PMC to Okta, you can get the information you need to set up the OpenID Connect authentication.

8. Go to the application instance for PM Cloud.
9. Select **General Settings**, and then click **Edit**.
10. For the PMC OpenID Connect Setup Wizard, you need to copy the following information from the **Edit** page:
    - **Domain**: Prefix the protocol HTTPS://
    - **Client ID**
    - **Client Secret**

> ***Note:*** *Confirm the domain name configured in Okta. This domain name might be different than the domain configured for your email address. For example, the domain managed in Okta might be domain.com but the email address is user@email.com. Both pieces of information are required.*

11. You can now visit the set-up URL and enter the domain, client ID, and client secret information.

Add PMC Instance to Ping Identity

> ***Note:*** *We currently support PingOne, the SaaS service from Ping Identity.*

1. Start up your Ping Identity instance.
2. In the menu, click **Connections**, and then click **Applications**.
3. At the right of the **Applications** title, click the plus sign (**+**) to add an application.
4. Enter a name for the application (required), and then add a short description (optional).
5. Select **OIDC Web App** and click **Save**.
6. Click the **Configuration** tab.
7. To edit the configuration, click the **pencil/edit** icon.
8. Under **Redirect URLs**, click **+ Add**, and then add the sign-in and sign-out URLs. If you are modifying an existing instance, you might need to open the **General** section dropdown first.
    - **Sign-in redirect URL**: https://{dns}-services.pm.beyondtrustcloud.com/oauth/signin-oidc
    - **Sign-out redirect URL**: https://{dns}-services.pm.beyondtrustcloud.com/oauth/signout-callback-oidc
9. Under **Token Endpoint Authentication Method**, select **Client Secret Post**, and then click **Save**.
10. Click the **Resources** tab.
11. To edit the resource, click the **pencil/edit** icon.
12. In the **Scopes** list, click the **+** next to **profile openID** to add it to the **Allowed Scopes**. You can also filter the list of options by **OpenID** to access this option.
13. Click **Save**.
14. To close the panel, at the top right of the **Edit** panel, click the **X**.
15. At the right of the new application entry, toggle the switch to **on** to give access to users.
16. Click the **Configuration** tab again. For the PMC OpenID Connect set-up wizard, you need to copy the following information from the **Configuration** page:
    - **Issuer**: Prefix the protocol HTTPS://
    - **Client ID**
    - **Client Secret**

Change the PM Cloud OpenID Connect Settings

Once you have set up your OpenID Connect Settings to use Microsoft, Okta, or Ping Identity, you might need to switch to another one at some point.

To change your existing OpenID Connect settings:

1. Click the **Configuration** menu, and then select **Authentication Provider Settings**.
2. Click **Change OpenID Connect Provider**.
3. Select a different provider, and then enter the **Provider URL (or Issuer)**, **Client ID**, and **Client Secret** information.
4. Review your settings, and then check the verification box.
5. Click **Save Changes**.

IMPORTANT!

*You will be logged out of the PMC Console. Once logged out, you need to log back in within **15 minutes**, because there is a timer on the page. If you do not log in before the timer expires, the authentication provider settings revert to the previous settings and the new*

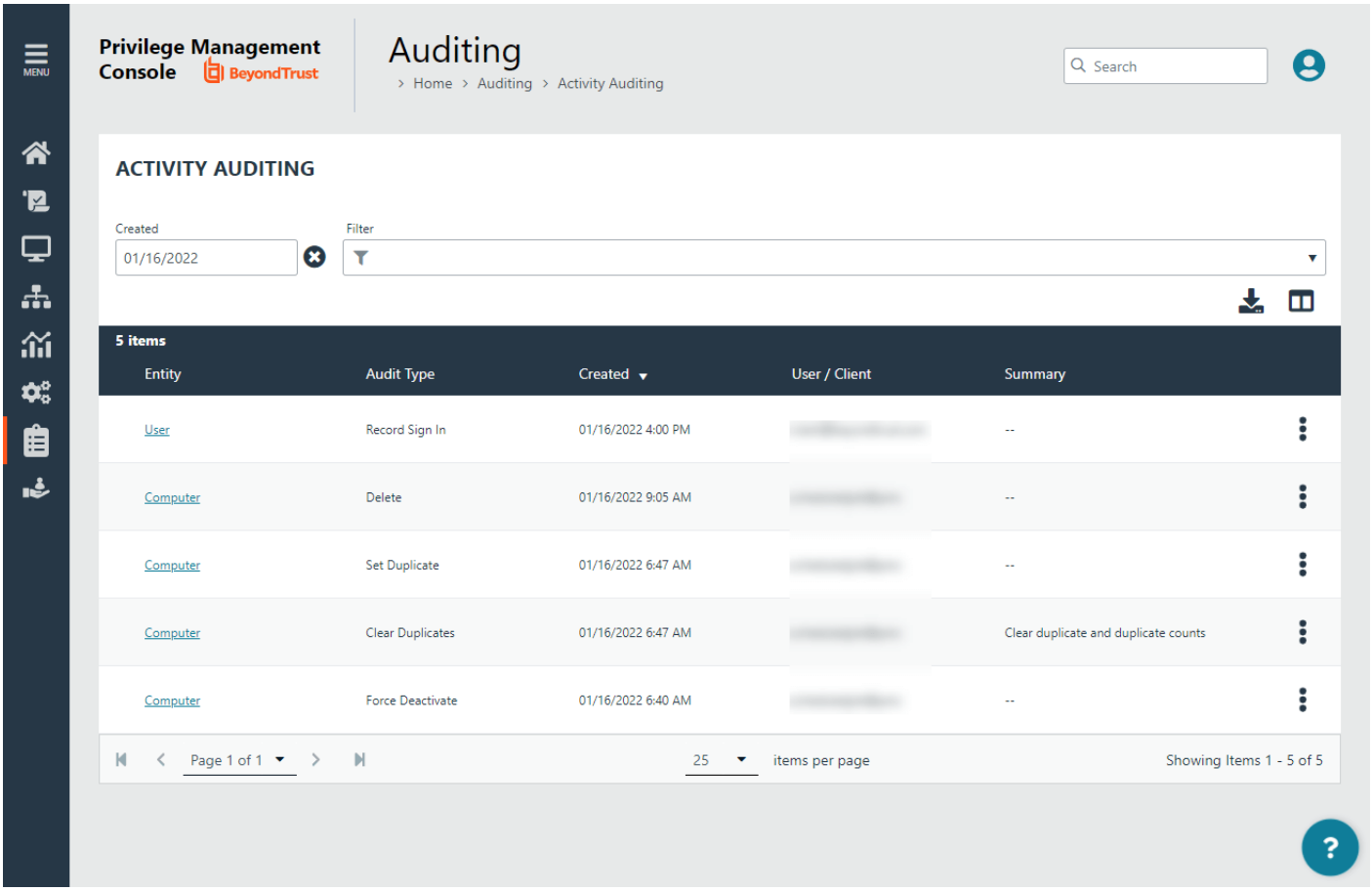
*settings are **not saved**.*

If you log on before the timer expires, the newly added authentication provider settings are retained.

Activity Auditing

The **Activity Auditing** page provides detailed auditing information on user, group, and policy actions.

To access the **Activity Auditing** page, on the sidebar menu, select **Auditing**, and then select **Activity Auditing**.



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

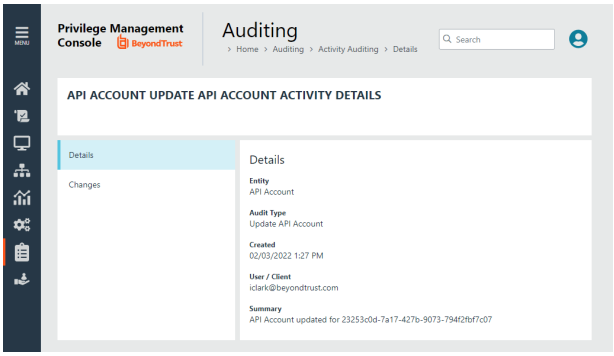
A **Summary** column highlights the changes on an audited activity.

Audited activities include the user who initiated the action and timestamps on when the activity started and ended.

View Activity Details

To view **Activity Details** and **Changes** for an item, at the right of the item row, click the vertical ellipsis icon, and then select **Activity Details**. The **Details** are shown by default.

To view *before* and *after* changes that have occurred for an item, in the left panel, select **Changes**.

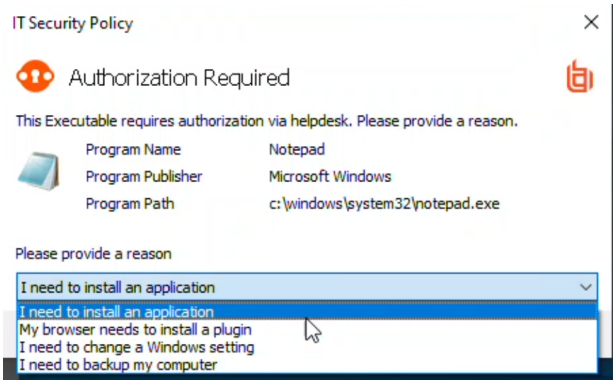


ServiceNow User Request Integration

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 following ServiceNow ticket types are supported in the PM Cloud integration: Incident, Change Request, and Service Catalog.

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.



Configuration includes:

- Download the BeyondTrust Privilege Management app from the ServiceNow store.
- Create a user account in ServiceNow, with required role.
- Activate and configure a connection to ServiceNow in PMC.
- Configure the connection details to PMC in ServiceNow.
- Create an Application Rule in the Policy Editor and apply messages to the rule that are specific to ServiceNow authorization.

Download and Install the Privilege Management App

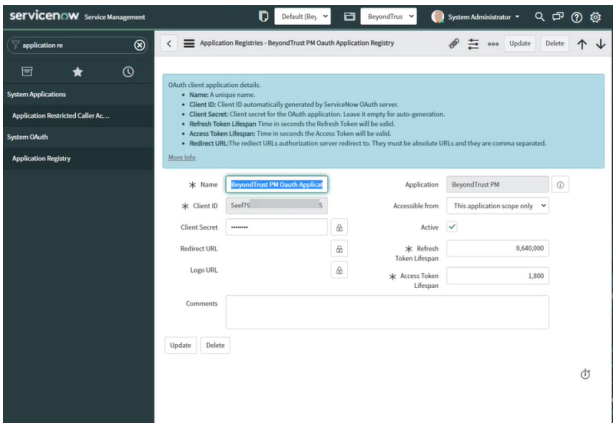
1. Go to the ServiceNow Store.
2. Search for *BeyondTrust*. The search displays all BeyondTrust products that integrate with ServiceNow.
3. Find the **BeyondTrust Privilege Management Integration** app.
4. Download and install the app into your ServiceNow tenant.

Create an OAuth Client for PMC

> ***Note:*** *If the OAuth Client for PMC has not been created automatically, then install it using these steps. Otherwise, proceed to creating a user account in ServiceNow.*

PMC must be added as an OAuth client in ServiceNow.

1. In ServiceNow, go to **Application Registry**.
2. Configure the settings as shown.



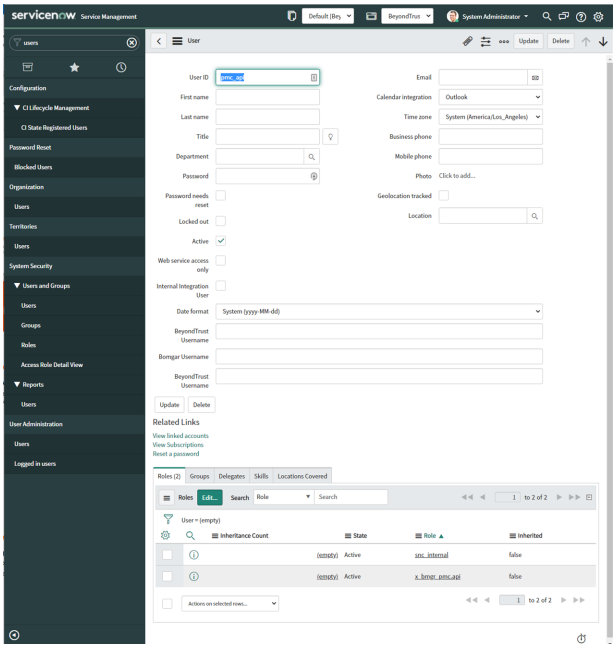
Create a User Account in ServiceNow

The **API Account** is used by BeyondTrust Privilege Management to submit requests via the inbound integration. An OAuth token is also created as an extra layer of security.

IMPORTANT!

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

1. Go to **User Administration > Users**.
2. Enter a **User ID** (**pmc_api**).
3. Enter a password.
4. Select **Web service access only** and click **Submit**.
5. Browse again to **User Administration > Users**.
6. Select the API user.
7. Click the **Roles** tab, and then click the **Edit...** button.
8. From the **Collection** list, add the **x_bmgr_pmc.api** role to the **Roles** list, and then click **Save**.



Assign Users Appropriate Roles

The following roles must be assigned to specific users in the ServiceNow integration:

- **x_bmgr_pmc.itil**: Assign to any users that will be providing technical support for the integration.
- **x_bmgr_pmc.admin**: Assign to any administrator users that you want to manage the ServiceNow integration.

- **x_bmgr_pmc.api**: Assign to API accounts that are used by BeyondTrust Privilege Management to submit requests via the inbound integration.

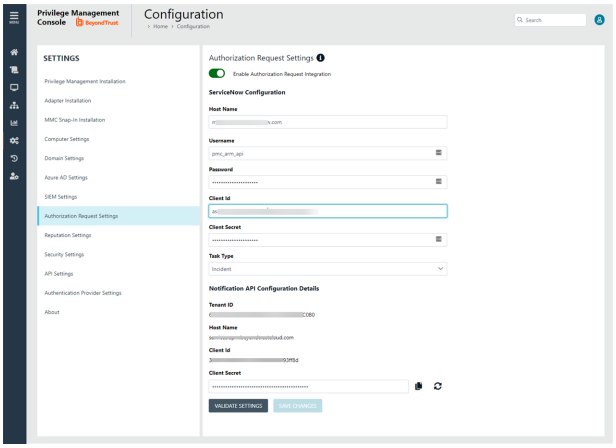
> ***Note:*** *You must elevate the admin role to assign roles.*

To assign a role to a user:

1. Go to **User Administration > Users**.
2. Select a user.
3. Click the **Roles** tab, and then click the **Edit...** button.
4. From the **Collection** list, add the appropriate role for that user to the **Roles** list:
    - **x_bmgr_pmc.itil**
    - **x_bmgr_pmc.admin**
    - **x_bmgr_pmc.api**
5. Click **Save**.

Configure the ServiceNow Integration in PMC

Before you can configure the Connection to PMC in ServiceNow, you must generate the Client ID and Client Secret in the PMC Console. You need this information to complete the configuration in ServiceNow.



To configure the Authorization Request Integration:

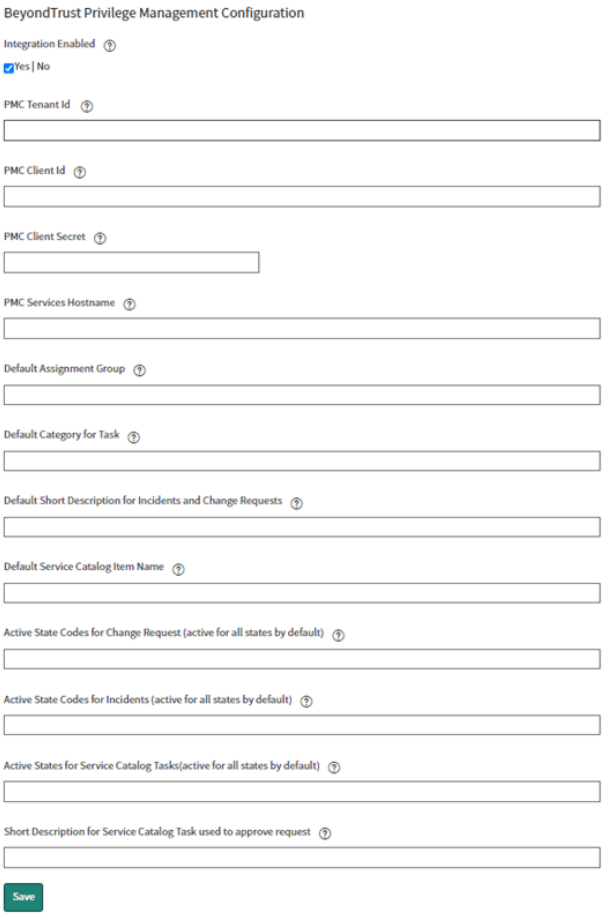
1. Go to **Configuration > Authorization Request Settings**.
2. To activate the integration, select **Enable Authorization Request Integration**.
3. Under **ServiceNow Configuration**, enter the following:
    - **Host name**: The host name provided on the **Configuration** page in ServiceNow.
    - **Username** and **Password**: Enter the user account information you created in ServiceNow.
    - **Task Type**: Select a ServiceNow task type from the list: **Incident**, **Change Request**, or **Service Catalog Request**.
4. Under **Notification API Configuration Details**, the **Tenant ID** and **Host Name** are auto-generated.
5. To create the **Client ID** and **Client Secret** used by the Integration in ServiceNow, click the **Generate** button.
6. To confirm the connection, click **Validate Settings**.
7. Click **Save Changes**.
8. To copy the **Client Secret** information, at the right of the **Client Secret** field, click the **Copy** button.

You can then proceed with configuring the connection to PMC in ServiceNow, and paste the Client Secret information you just copied.

> ***Note:*** *You must also manually copy and paste the Client ID information from PMC to the ServiceNow BeyondTrust Privilege Management Configuration page.*

Configure the Connection to PMC in ServiceNow

A Privilege Management instance is required for full operation. The appliance is setup in ServiceNow to connect ServiceNow with a PMC instance.

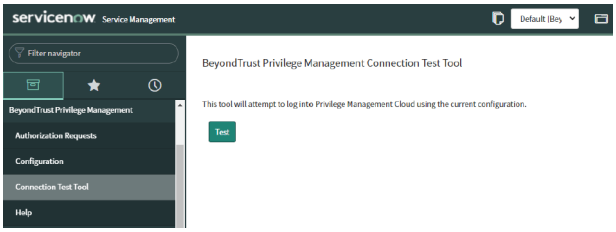


1. Go to **BeyondTrust Privilege Management > Configuration**.
2. To turn on the integration to PMC, select **Yes**.
3. To configure the outbound integration, enter the following:
    - **PMC Tenant ID**: The Tenant ID of the Privilege Management appliance.
    - **PMC Client ID**: The OAuth client ID that is used to authenticate to the Privilege Management appliance. Copy and paste this from the PMC **Authorization Request Settings** page.
    - **PMC Client Secret**: The OAuth client secret that is used to authenticate to the Privilege Management appliance. Copy and paste this from the PMC **Authorization Request Settings** page.
    - **PMC Service Host Name**: The hostname of the Privilege Management appliance.
4. To configure the application defaults (optional), enter the following:
    - **Default Assignment Group**: The default group assigned.
    - **Default Category for Task**: The default category for tasks created by the application. The default is **Software**.
    - **Default Short Description for Incidents and Change Requests**: The default short description created by the application when attempting to create an incident or change request based on the task type.
    - **Default Service Catalog Item Name**: The name of the service catalog item used when creating service catalog requests.
    - **Active State Codes for Change Request**: A comma-separated list of states in which the integration actions are available to users. This list is for change requests only. (For example, **Implement**).
    - **Active State Codes for Incidents**: A comma-separated list of states in which the integration actions are available to users. This list is for incidents only. (For example, **New**, **In Progress**).
    - **Active States for Service Catalog Tasks**: A list of states in which the integration actions are available to users. This list is for Service Catalog tasks only.
    - **Short Description for Service Catalog Task used to approve request**: The default short description, which is matched to place the custom form on the created application request.
5. Click **Save**.

Testing the Configuration

The ServiceNow Connection Test Tool verifies connectivity to the Privilege Management host. It tests the Client ID and Client Secret.

1. Go to **BeyondTrust Privilege Management > Connection Test Tool**.
2. Click **Test**.



Restrict Access to Applications

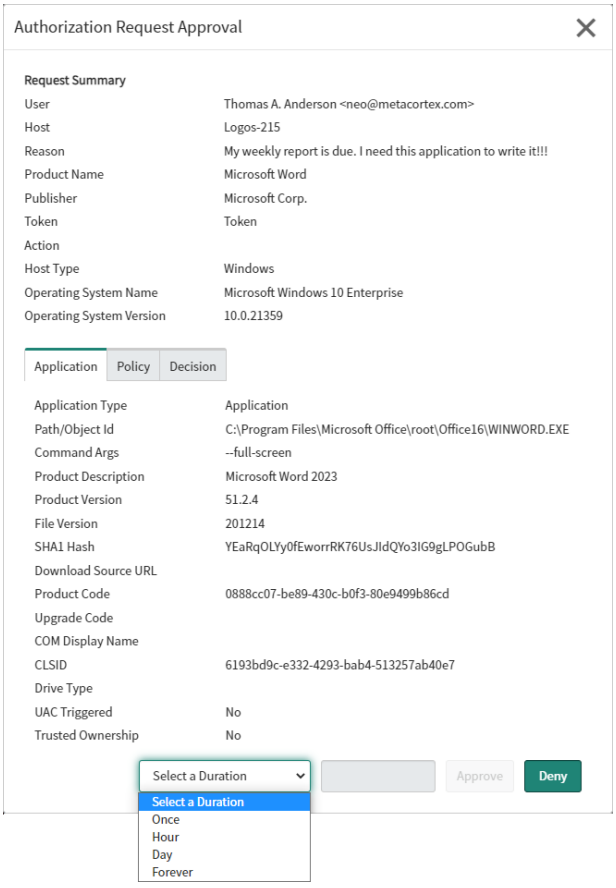
In the ServiceNow authorization request workflow, you can restrict access to application requests. On an approved request, Help Desk can set a time limit in the ServiceNow ticket. The time limit is the length of time the user can use the application before the approval automatically expires.

Under the **Application**, **Policy**, or **Decision** tab, select a Duration.

Access time limit can be one of the following:

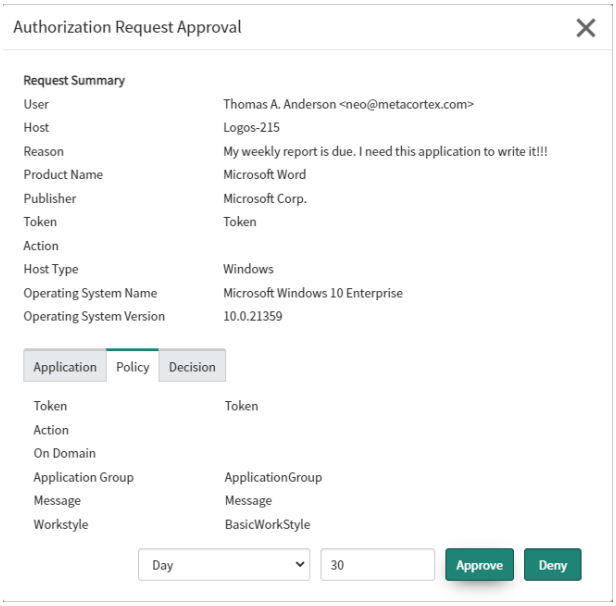
- **Once**: Permits access to the application only one time.
- **Hour**: Enter the number of hours the user will be permitted access, between 1 and 24.
- **Day**: Enter a day between 1 and 31.
- **Forever**: Access to the application never expires.

Click **Approve**.



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.

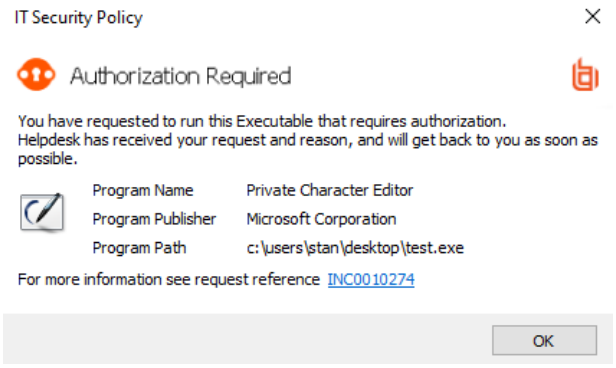
Duration settings are included in the authorization auditing.



The client checks an application's authorization access when the end user attempts to run the program. If the duration settings have been correctly configured, a message appears indicating the outcome of the ServiceNow request. The user receives a new message indicating that the application has been either Denied or Approved once the policy has been updated or when they attempt to run the application again.

A pending message displays to the end user until a decision on their request is made in ServiceNow.

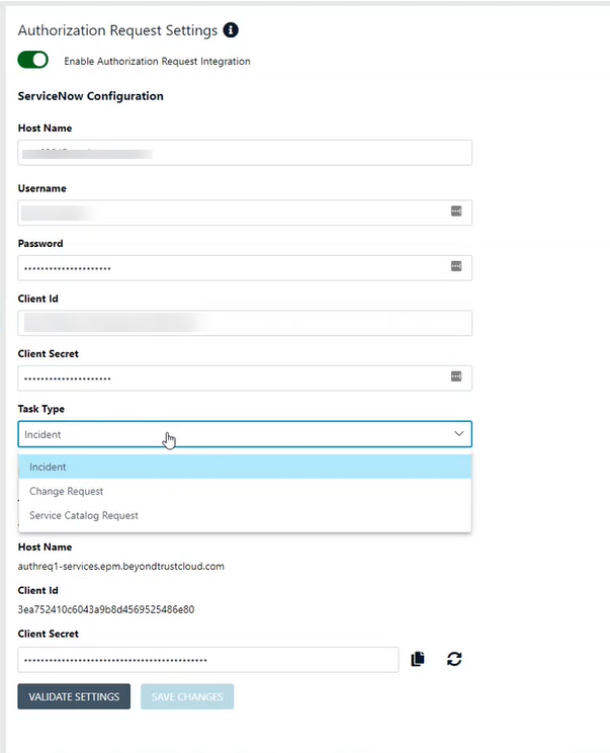
To view the status on their ServiceNow ticket, the end user can click the request reference **link**.



Use Service Catalog as the Task Type

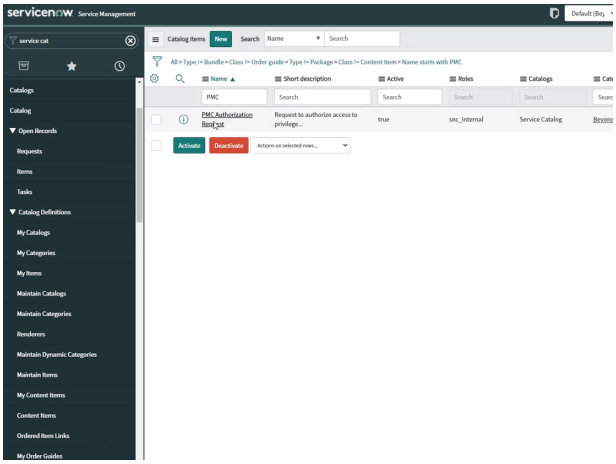
You must configure the following if your ServiceNow infrastructure uses Service Catalog to manage user requests.

- In PMC, select **Service Catalog Request** as the **Task Type** on the **Authorization Request Settings** page.



- In ServiceNow, you must add PMC as a Catalog item.

  Specific details on configuring the catalog item depend on your Service Catalog implementation.



Enable VirusTotal Reputation Score

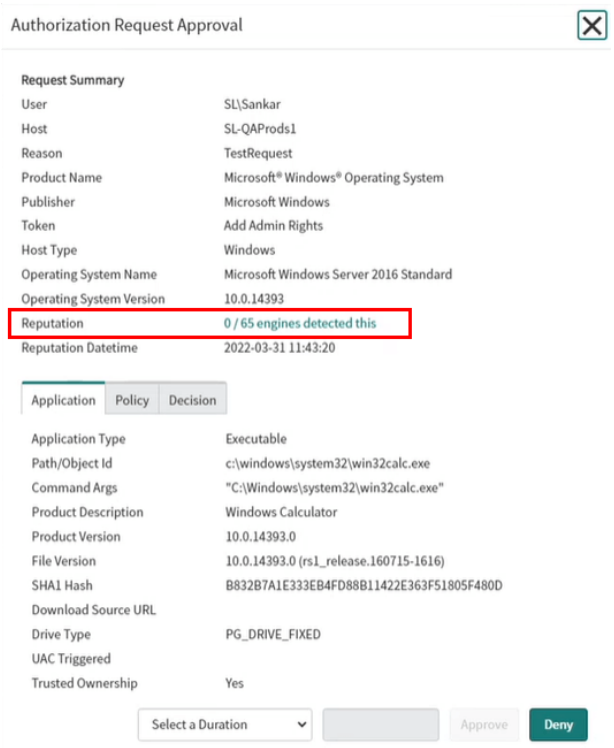
You can enable the VirusTotal Reputation score on ServiceNow tickets to assist with identifying potential malware and malicious content.

1. Go to **BeyondTrust Privilege Management > Configuration**.
2. Select **Reputation Settings** from the menu.
3. Click the toggle switch **Enable VirusTotal Reputation Integration** to turn on the feature.
4. Enter the VirusTotal API key.

> ***Note:*** *You will need a VirusTotal license before you can generate an API key.*

5. Click **Validate Settings** to confirm that the key is valid.

> ***Tip:*** *To view the VirusTotal score on a request, select the ticket in ServiceNow and then click* ***Authorization Request Approval*** *at the top of the incident grid. The VirusTotal reputation score is displayed under the* ***Request Summary****.*
>
> *You can click the score* ***link*** *to go to the engine that determined the score.*



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 131.*

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

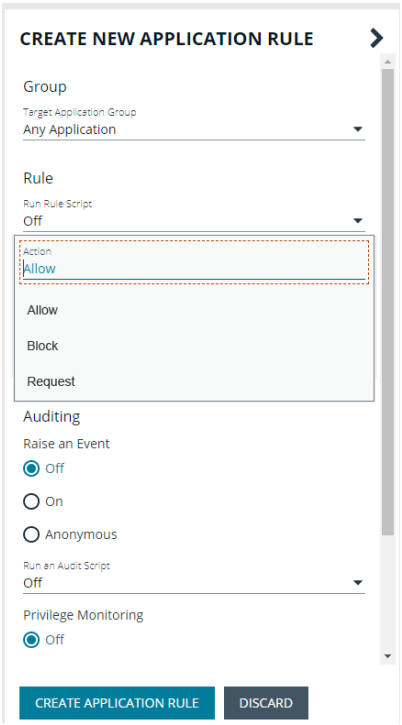
Access Policy Editor

1. Log in to PMC and select **Policies** on 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 43.*

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**.

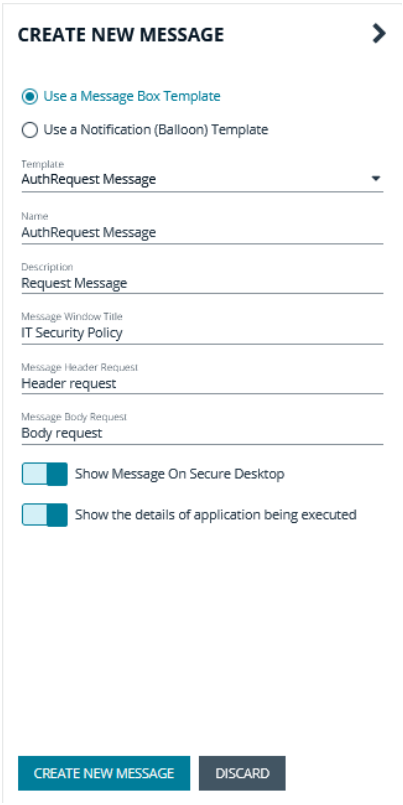


> ***Note:*** *If a message box has not already been created, you will need to create one before the Request option is available.*

> ***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 User Request Message

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

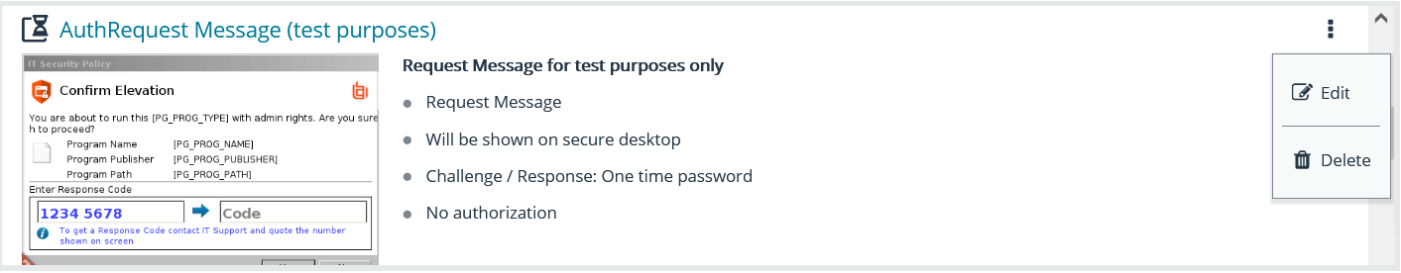


- Template
- Name
- Description
- Message Window Title
- Message Header Request
- Message Body Request

For more information, please see "Messages" on page 76.

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



ServiceNow Authorization Requests Auditing

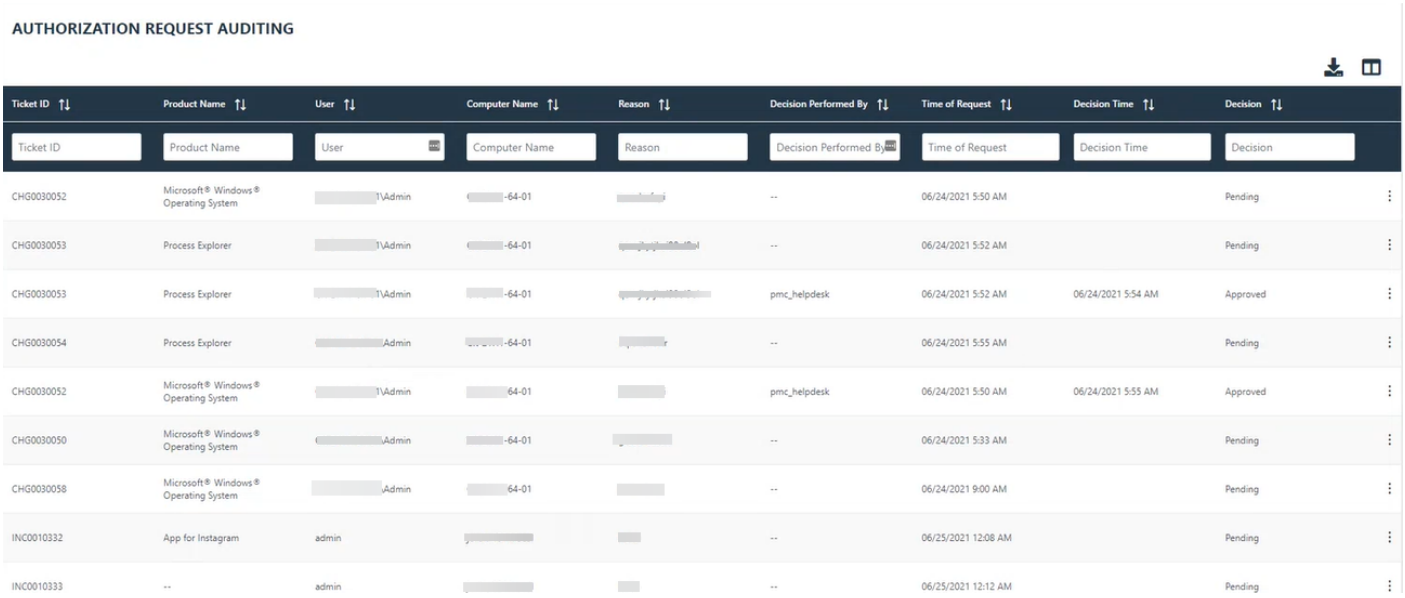
ServiceNow user authorization requests are audited for troubleshooting and logging purposes.

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.



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_HASH_SHA256]	The SHA-256 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

Parameter	Description
[PG_PROG_PUBLISHER]	The publisher of the application
[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.

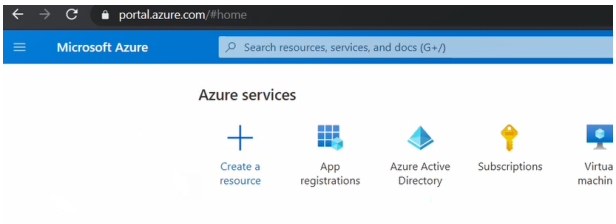
There are two key steps to create a channel:

- 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.

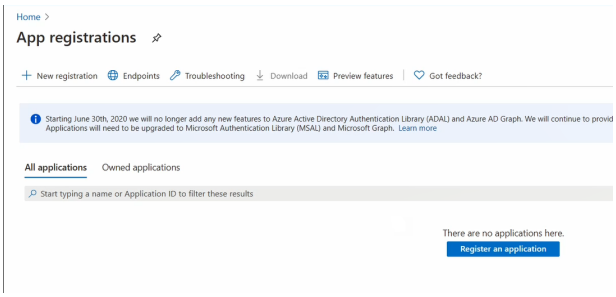
This section details the steps to register an Azure tenant.

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.

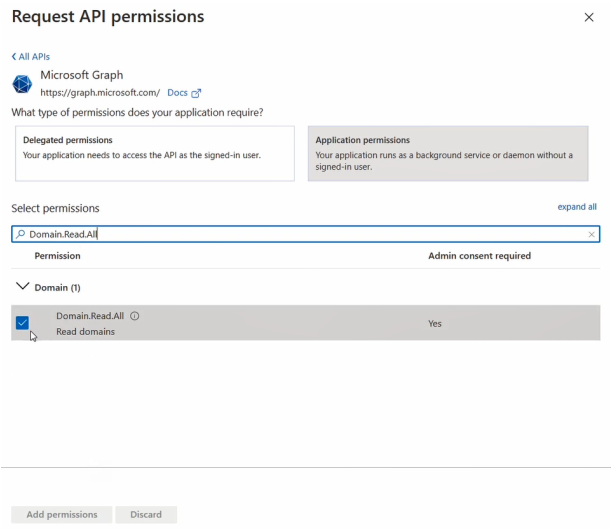


4. Click **New registration**.

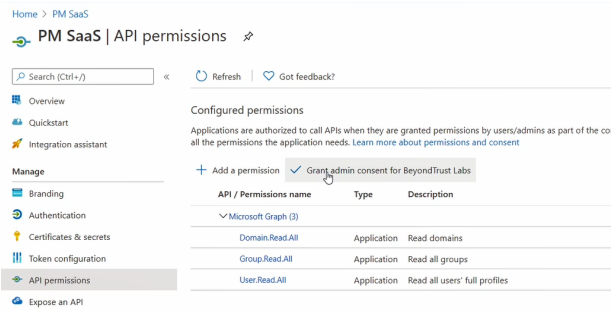


5. Give the registration a name. For example, **PM Cloud Registration**.
6. Select the **Supported account types** you require for your business needs.
7. Ignore the setting **Redirect URI**.
8. Click **Register an application**.
9. Go to **Manage > API Permissions** and click **Add a permission**.
10.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



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



Configure Authentication

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

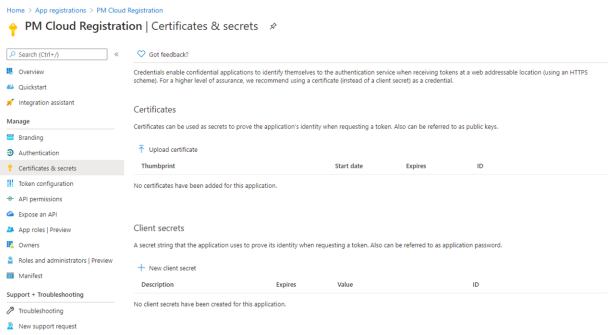
- Certificate authentication
- Client-secret authentication

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**.



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.