Privilege Management
SaaS Administration Guide 20.3

TC:8/11/2020

Table of Contents

Privilege Management SaaS Administration Guide

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

This Administration Guide details the features and functionality of PMC.

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

Sign into Privilege Management Console

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

To log into PMC:

1. Navigate to your PMC instance and click **Sign in**.
2. Click the appropriate email associated with your account.
3. Determine whether or not you would like to remain signed in. Click **Yes** to limit the number of times you'll be asked to sign in, or **No** to be prompted every time.
4. Determined by whoever set up your user account, the date format will be either of the following:

   ```
   dd/mm/yyyy 24hr
   ```

   ```
   mm/dd/yyyy 12hr
   ```

   When you sign in for the first time, you may change the date and time format.

5. Select your time zone from the dropdown menu and click **Confirm**. These settings are specific to you.

Automatic Logout

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

Privilege Management Console Search

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

In PMC, you can search across:

- Groups
- Policies
- Computers
- Users

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

For more information, please see the following:

- "Privilege Management Console Groups" on page 27
- "Privilege Management Console Policies" on page 30
- "Privilege Management Console Computers" on page 33
- "Use Privilege Management Console to Assign Roles to a User Account in Privilege Management Console" 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
- use parameter-based MSI to authorize and assign computers to these groups

Manage Policy

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

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

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

> For more information, please see "Manage Privilege Management Console Policy" on page 18.

Create Groups and Assign Policy

Create Groups

1. Navigate to and click the **Groups** tile.
2. Select **Actions > Create Group**.
3. Enter a **Group Name**. The **Description** and **Annotations** fields are optional.
4. Click **Submit**. Your group is created and appears in the grid list below.

Once the group is created, you can set it as the Default group. If set, the Default group will be selected by default when you add one or more computers to a group. To set the group as the Default group, right-click the group, and then select **Set Default**.

Assign Policy

1. Navigate to and click the **Groups** tile.
2. Select **Actions** > **Assign Policy**. The row briefly flashes green to indicate that PMC has processed your request.
3. Select the policy you want to assign from the dropdown and the associated revision. By default, the revision is the most recent.
4. The text at the bottom tells you how big the policy is and how many computers it will be assigned to. Click **Assign** to assign the policy to your group.

> For details on how you can control the deployment of your policy, please see "Manage Policy Deployment Settings in Privilege Management Console" on page 42.

Install Privilege Management

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

You can view installation package details in the console. Go to **Administration > Access Settings**.

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

Windows endpoints

For 32-bit (x86) systems run:

PrivilegeManagementForWindows_x86.exe

For 64-bit (x64) systems run:

PrivilegeManagementForWindows_x64.exe

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
```

For Mac endpoints run:

PrivilegeManagementConsoleMacOSAdapter.dmg

Install the Windows Adapter

> ***Tip:*** *Setup Information is available for the Windows adapter on the* ***Access Settings*** *page. On the dashboard page, click the* ***Access Settings*** *tile to view the details.*

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

> ***Note:*** *The adapters poll every 60 minutes by default. An additional delay is applied based on the CPU load of the node that the adapter is connected to. The minimum supported value for the adapter poll time is 5 minutes.*

You must install the Privilege Management adapters using this process. You can optionally choose to automatically assign endpoints 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 agents are managed by the operating system, the PMC adapter is responsible for delivering policies and events between the endpoint and PMC servers.

If not using the **GroupID** to automatically assign and authorize computer groups, you can assign and authorize endpoints 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 **Administration** > **Access Settings**. Copy the Tenant ID for this script.
- **InstallationID**: Obtain this value from PMC. Click **Administration** > **Access Settings**. Copy the Installation ID for this script.
- **InstallationKey**: Obtain this value from PMC. Click **Administration** > **Access Settings**. Copy the Installation Key for this script.
- **ServerURI**: This is the URL for PMC. For example, **https://<customerhost>-services.pm.beyondtrust.cloud.com**, where **customerhost** is the DNS name for PMC.

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

- **GroupID**: (Optional). If supplied, this automatically authorizes the endpoint 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 endpoint.*

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

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

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

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

```
SERVICE_STARTUP_TYPE=Disabled
```

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

Example:

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

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

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

For information on how to automatically assign and authorize computer groups, please see "Privilege Management Console Computers" on page 33.

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 endpoint 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

***Tip:** Setup Information is available for the Mac adapter on the **Access Settings** page. On the dashboard page, click the **Access Settings** tile to view the details.*

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

***Note:** The adapters poll every 60 minutes by default. An additional delay is applied based on the CPU load of the node that the adapter is connected to. The minimum supported value for the adapter poll time is 5 minutes.*

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

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

If you are not using the GroupID to automatically assign and authorize computer groups, you can assign and authorize endpoints 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 **Administration** > **Access Settings**. Copy the Installation ID for this script.
- **InstallationKey**: You get this from PMC. Click **Administration** > **Access Settings**. 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 endpoint 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.
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 endpoint.*

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

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

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

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

For more information, please see "Authorize and Assign Computers to a Group in Privilege Management Console" on page 33.

Configure PMC to Connect to the Policy Editor

Tip: *Setup Information is available on the* ***Access Settings*** *page. On the dashboard page, click the* ***Access Settings*** *tile to view the details.*

You need to configure PMC to allow the Privilege Management MMC snap-in to communicate with the PMC services.

1. Click **Administration > Access Settings** from the top menu.
2. Check the **Enable remote MMC client access** box. You need to generate a new GUID and enter it here. Click the Refresh button to generate a new GUID. You need to use the same GUID when you configure the MMC. This is the **MMC Client ID** in the MMC.
3. Click **Save Changes**.

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

For more information, please see "Configure the Privilege Management MMC PMC snap-in" on page 16.

Configure the Privilege Management MMC PMC snap-in

Tip: *Setup Information is available for the MMC snap-in on the* ***Access Settings*** *page. On the dashboard page, click the* ***Access Settings*** *tile 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 more information, please see the following:

- For compatible versions, the Release Notes at https://www.beyondtrust.com/support/changelog.

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 endpoints 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 **Administration > Access Settings** in the PMC Portal.
Authorization Provider	
URL	This is the URL for PMC with **:443/oauth** appended to it. For example, **https://customerhost-services.pm.beyondtrust.cloud.com**, where **customerhost** is the instance hostname for your Privilege Management Console.

Setting	What to Enter
Identification	
MMC Client ID	This needs to be the same GUID you generated and used in the PMC connection settings at **Administration > Access Settings** 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.

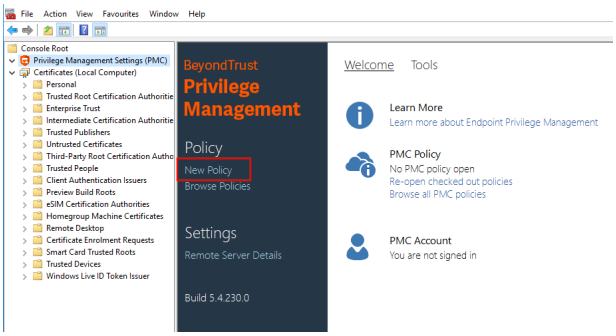
For more information, please see the following:

- "Configure PMC to Connect to the Policy Editor" on page 15

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 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.*

Manage Privilege Management Console Policy

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.

For information on how to set up and configure PMC, please see the following:

- On-Premises Installation Guide at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm
- Azure Installation Guide at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm

Policy Management in Privilege Management Console

Using PMC, you can

- upload and download policy files
- override a policy checkout if you have the appropriate user permissions

Upload File to Create Policy in Privilege Management Console

You can upload an XML policy to PMC. If the policy does not exist, it is enumerated as revision one. If the policy does exist, it is a new revision.

1. Navigate to and click the **Policies** tile.
2. Right-click anywhere on the grid and click **Upload File to Create Policy**.
3. Click the upload icon to browse to the XML file and click **Open**. The XML file is uploaded to the portal.

For more information, please see "Upload Revision of an Existing Policy in Privilege Management Console" on page 19.

Upload Revision of an Existing Policy in Privilege Management Console

You can upload a new revision of an existing policy to PMC. 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. Navigate to and click the **Policies** tile.
2. Right-click on the policy you want to upload a new revision of and click **Upload Revision**.
3. Click the upload icon to 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.

Each time the same policy is checked in from the MMC, 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 in Privilege Management Console" on page 31.

Discard Draft Policy and Undo Check Out

If the 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. Navigate to and click the **Policies** tile.
2. Right-click on the policy that is checked out to the Privilege Management MMC snap-in and click **Discard Draft & Undo Check Out**.
3. You are prompted to check that you do want to perform this action. Click **Continue Anyway** to discard the draft and undo the checkout; otherwise, click **Cancel**.

Download a Policy as an XML File in Privilege Management Console

You can download a policy from PMC as an XML file. This is useful if you need to share the policy with other people in your organization.

To download a policy XML file

1. Navigate to and click the **Policies** tile.
2. Right-click on the policy and click **Download**. The policy is downloaded to your downloaded files location.

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.

Privilege Management Console 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 in Privilege Management Console" on page 40.

Agent and Group Locks

Endpoints 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 endpoint or group will unlock. Once the endpoint 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 Privilege Management Console 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 on Windows endpoints, please see the Windows Administration Guide at https://www.beyondtrust.com/docs/privilege-management/windows/index.htm.

View Policies in the Privilege Management Console 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 Privilege Management Console 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 in Privilege Management Console" on page 31.

Check out a Policy Using the Privilege Management Console MMC Snap-in

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

To check out a policy:

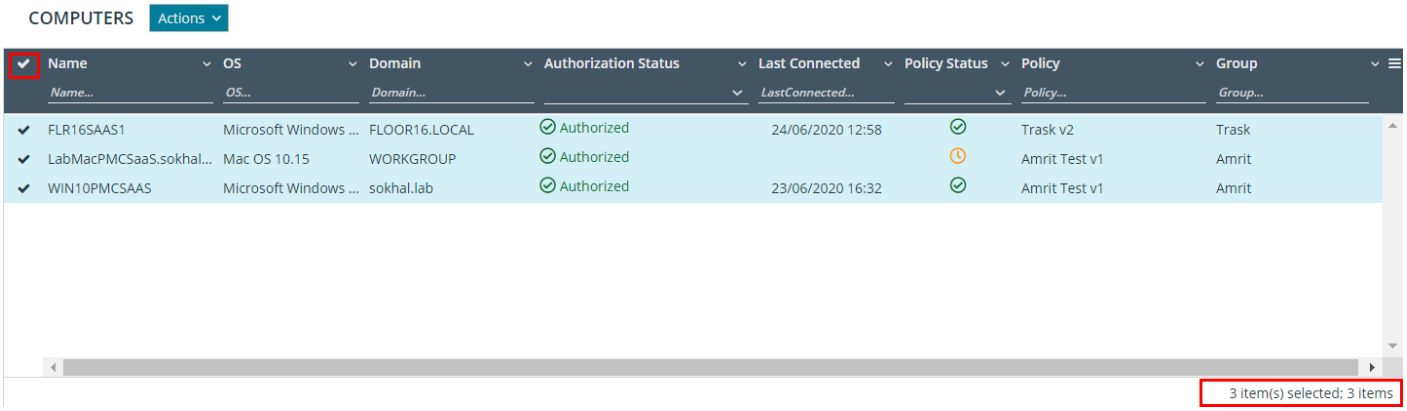
1. In the Privilege Management MMC snap-in, click **Browse all PMC policies** in the PMC **Policy** section.
2. Select your policy from the list and click **Check Out**. You can now edit the policy in the Privilege Management MMC snap-in.

Privilege Management Console Grid Behavior

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

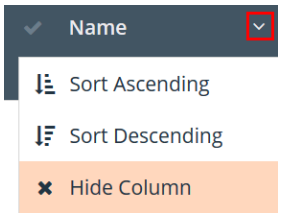
Select All

To select the first 1,000 rows, click the check mark in the top left corner. If you want to select all rows in the grid, first select the first 1,000 rows using the check mark, and then click the link that is displayed, as demonstrated here.

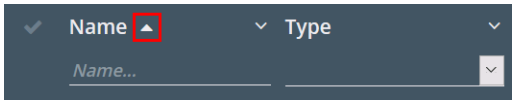


Sort Columns

By default, the grid is ordered by **Name**; however, you can sort by any of the other columns using the arrow adjacent to the column name. Click the down arrow to choose how you want to sort the columns. You can also hide columns using this functionality.

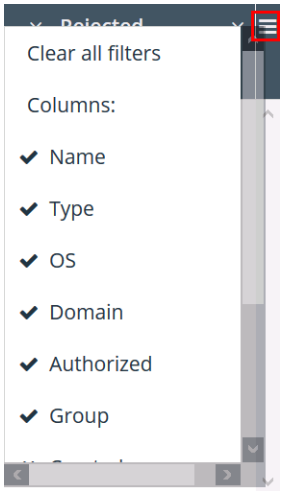


A column that has a sort applied is indicated by a solid triangle adjacent to the **Name** column header. Click the solid triangle to clear the sort from the column.



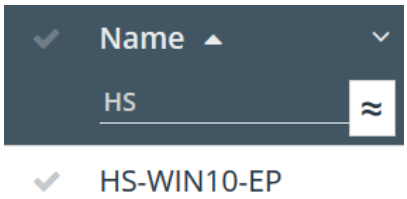
Add or Remove Columns

You can configure the columns on pages with grids by clicking the hamburger icon on the right. To do this, select or clear the tick adjacent to the column you want to see or hide, respectively.



Filter

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



The following grids support filtering:

- **Computers**
- **Policies**
- **Groups**
- **Users**

You can click the filter icon to negate the filter criteria. It will then read **does not contain**.

Data Refresh

When there is new data available for PMC, you will see a blue notification at the bottom right of the screen, stating that new data is available. Click the refresh link in this notification to see the updated data.

Progress and Change Indicators

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

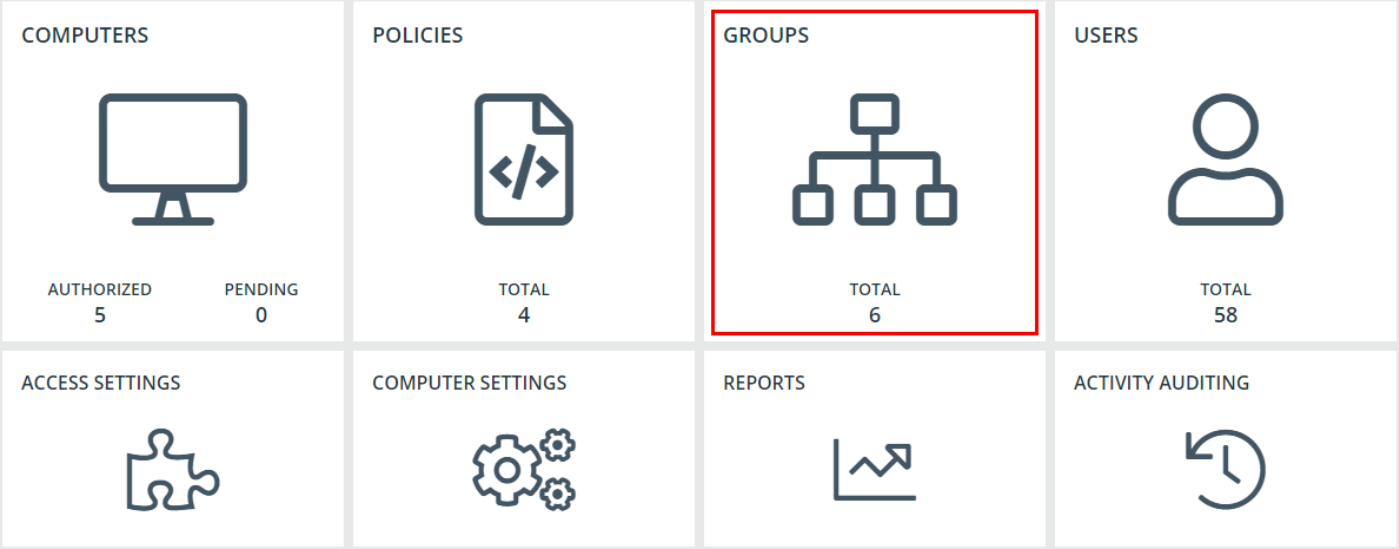
Where actions affect one or more rows, you see the affected rows briefly flash green to indicate that PMC has processed your request.

Error Notifications

If PMC cannot complete an action successfully, it does not make any changes and you get a 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.

Privilege Management Console Groups

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



You can perform the following tasks in the **Groups** tile:

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

For more information, please see the following:

- "Create a Group in Privilege Management Console" on page 27
- "View the Details of a Group in Privilege Management Console" on page 28
- "Edit Properties of a Group in Privilege Management Console" on page 28
- "Set a Default Group in Privilege Management Console" on page 28
- "Assign a Policy to a Group in Privilege Management Console" on page 28
- "Clear a Policy from a Group in Privilege Management Console" on page 29
- "Delete a Group in Privilege Management Console" on page 29

Create a Group in Privilege Management Console

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

1. Navigate to and click the **Groups** tile.
2. Select **Actions > Create Group**.
3. Enter a **Group Name**. The **Description** and **Annotations** fields are optional.
4. Click **Submit**. Your group is created and appears in the grid list below.

Once the group is created, you can set it as the Default group. If set, the Default group will be selected by default when you add one or more computers to a group. To set the group as the Default group, right-click the group, and then select **Set Default**.

View the Details of a Group in Privilege Management Console

1. Navigate to and click the **Groups** tile.
2. Right-click the group you want to view the details for and click **Details** from the menu.
3. These tabs allow you to see additional information for the group and what policy is currently applied to it, if any. You can click **Edit** to change these details.

For more information, please see "Edit Properties of a User Account in Privilege Management Console" on page 40.

Edit Properties of a Group in Privilege Management Console

1. Navigate to and click the **Groups** tile.
2. Right-click the group you want to edit the details for and click **Edit Properties** from the menu.
3. Change the **Group Name**, **Description**, and **Annotations**, as required, and then click **Submit**.

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 in Privilege Management Console

The Default group, when set, appears first in the **Group** dropdown list in PMC.

1. Navigate to and click the **Groups** tile.
2. Right-click the group you want to make the Default group and click **Set Default** from the menu. The row briefly flashes green to indicate that PMC has processed your request and the default column contains a green tick to indicate that it is the Default group.

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

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

Assign a Policy to a Group in Privilege Management Console

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

1. Navigate to and click the **Groups** tile.
2. Right-click the group you want to assign a policy to and click **Assign Policy** from the menu.

3. Choose the policy you want to be assigned to the group from the menu and which revision of that policy.
4. Click **Assign** to assign that policy to the group. The row briefly flashes green to indicate that PMC has processed your request.

Clear a Policy from a Group in Privilege Management Console

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

1. Navigate to and click the **Groups** tile.
2. Right-click the group you want to clear the policy from and click **Clear Policy** from the menu.
3. You are notified how many computers will be affected by the change. Click **Continue Anyway** to clear the policy; otherwise, click **Cancel**.

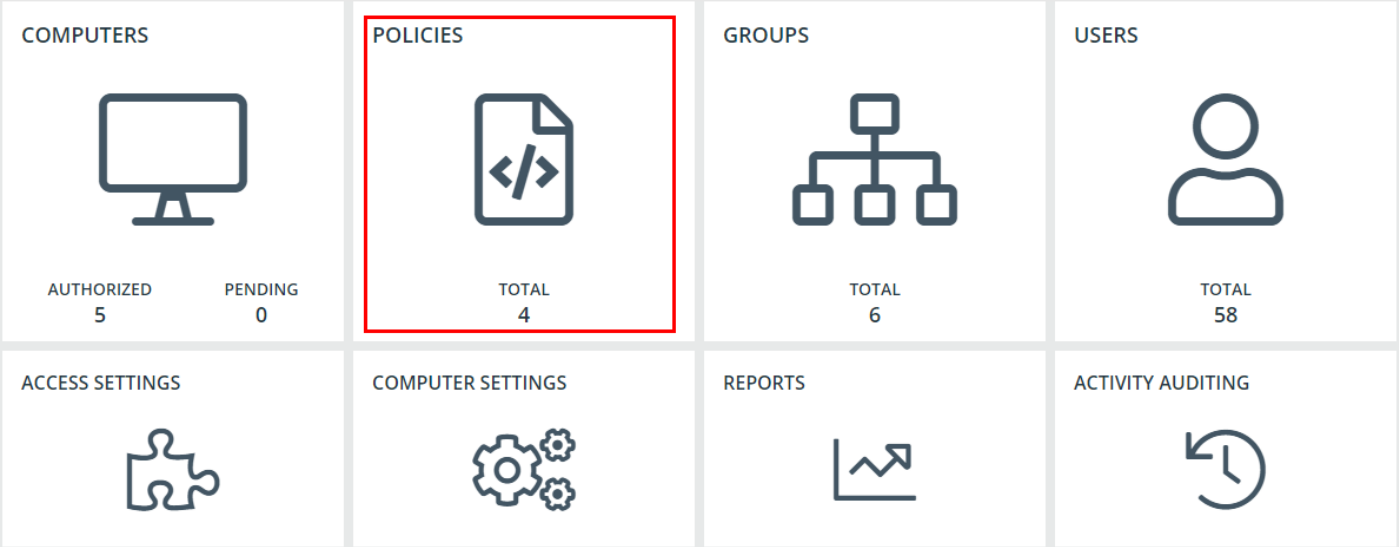
Delete a Group in Privilege Management Console

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. Navigate to and click the **Groups** tile.
2. Right-click the group you want to delete and click **Delete** from the menu.
3. Click **Delete** to continue deleting this group; otherwise, click **Cancel**.

Privilege Management Console Policies

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



Upload a File in Privilege Management Console to Create Policy

You can upload an XML policy to PMC. If the policy does not exist, it is enumerated as revision one. If the policy does exist, it is a new revision.

1. Navigate to and click the **Policies** tile.
2. Right-click anywhere on the grid and click **Upload File to Create Policy**.
3. Click the upload icon to browse to the XML file and click **Open**. The XML file is uploaded to the portal.

For more information, please see "Upload Revision of an Existing Policy in Privilege Management Console" on page 19.

Upload Policy Revision in Privilege Management Console

1. Navigate to and click the **Policies** tile.
2. Right-click on the policy you want to upload a new revision of and click **Upload Revision**.
3. Click the upload icon to 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.

Each time the same policy is checked in from the MMC, 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 in Privilege Management Console" on page 31.

View Policy Details in Privilege Management Console

For a single policy you can view additional details.

1. Navigate to and click the **Policies** tile.
2. Right-click the policy you want to view the details of and click **Details** from the menu. The **Policy Details** screen includes additional information about the policy. You can also download the policy from this area.

Download Policy in Privilege Management Console

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

1. Navigate to and click the **Policies** tile.
2. Right-click on the policy and click **Download**. The policy is downloaded to your downloaded files location.

Edit Properties of Policy in Privilege Management Console

You can edit the details for a single policy.

1. Navigate to and click the **Policies** tile.
2. Right-click the policy you want to view the details of and select **Edit Properties** from the menu.
3. You can edit the **Policy Name**, **Description**, and **Annotations** here. Click **Submit** to save your changes.

Assign a Policy to a Group in Privilege Management Console

A policy can be assigned to one or more groups.

1. Navigate to and click the **Policies** tile.
2. Right-click the policy you want to assign to a group and click **Assign Policy to Group**.
3. Select the group you want to assign the policy to from the dropdown and click **Assign**.
4. The text at the bottom tells you how big the policy is and how many computers it will be assigned to. Click **Assign** to assign your group to the policy. The row briefly flashes green to indicate that PMC has processed your request.

> For details on how you can control the deployment of your policy, please see "Policy Deployment Settings in Privilege Management Console" on page 42.

Discard Policy Draft and Undo Check Out in Privilege Management Console MMC Snap-in

If the 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. Navigate to and click the **Policies** tile.
2. Right-click on the policy that is checked out to the Privilege Management MMC snap-in and click **Discard Draft & Undo Check Out**.

3. You are prompted to check that you do want to perform this action. Click **Continue Anyway** to discard the draft and undo the checkout; otherwise, click **Cancel**.

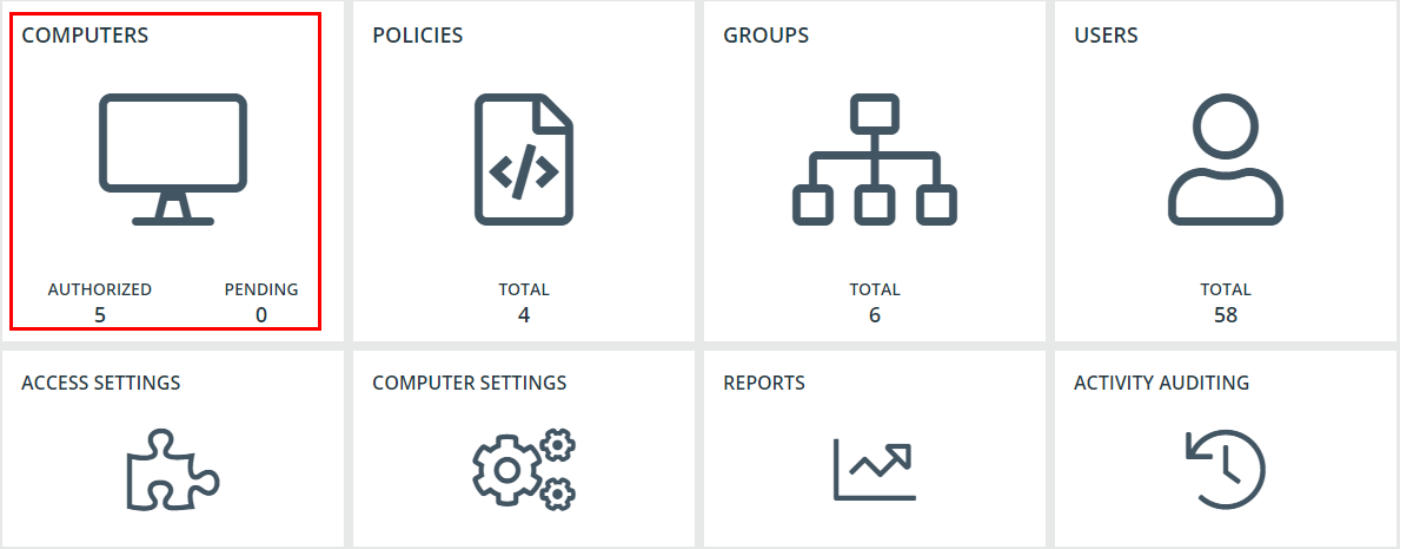
Delete a Policy in Privilege Management Console

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

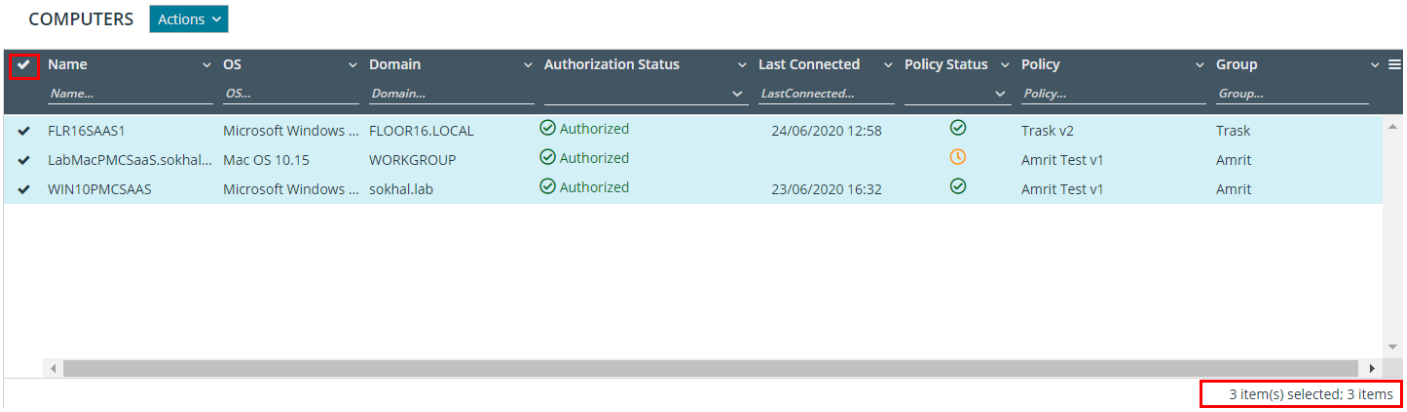
1. Navigate to and click the **Policies** tile.
2. Right-click on the policy that you want to delete and click **Delete**.
3. You are prompted to check that you do want to perform this action. Click **Delete Anyway** to discard the draft and undo the check out; otherwise, click **Cancel**.

Privilege Management Console Computers

The **Computers** tile allows you to see and to interact with the endpoints being managed by PMC.



To select all of the rows listed, check the box in the top hand corner. The number of rows that have been selected can be seen in the lower right corner of the screen.



Authorize and Assign Computers to a Group in Privilege Management Console

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

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

1. Navigate to and click the **Computers** tile.
2. Right-click the computer(s) you want to place in a group and authorize in one step, and then select **Authorize and Assign Group** from the menu.

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

3. Select the group you want to assign it to from the dropdown group and click **Assign**. If you haven't created any groups yet, you will see only **No Group** in the dropdown.
4. If you have a Default group, it will be selected by default, otherwise you can select the group you want to use from the dropdown menu. Click **Assign**. The rows that you have selected will briefly flash green 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 in Privilege Management Console" on page 35
- For information on the grids and filtering, "Privilege Management Console Grid Behavior" on page 24
- For instructions on creating a group, "Privilege Management Console Groups" on page 27

Reject Computers Not Authorized with Privilege Management Console

You can reject endpoints that have not yet been authorized with PMC.

Manual Deactivation

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

For more information, please see "Deactivate Computers in Privilege Management Console" on page 36.

Automatic Deactivation

Alternatively, you can use PMC to manage deactivations automatically.

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

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

For more information, please see "Auto Deactivate Settings" on page 78.

View Details on an Endpoint in Privilege Management Console

For a single computer you can view additional details.

1. Navigate to the **Computers** tile.
2. Right-click the computer you want to view the details of and click **Details** from the menu.

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

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

Update

You can force this page to refresh by clicking **Update** on the right side of the pane. This action gets the latest information from the endpoint.

Apply Policy

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

Click **Actions > Apply Policy**. The policy will update the next time the computer connects to PMC.

Computer Logs

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

Command Log

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

Edit Properties on an Endpoint in Privilege Management Console

1. Navigate to the **Computers** tile.
2. Right-click the computer you want to edit the properties for and click **Edit Properties**.
3. Click the plus sign next to **Annotations** to add an annotation to this computer.
4. Click **OK** to save your annotation and click **Submit** to save it in PMC.

Assign Computers to a Group in Privilege Management Console

1. Navigate to the **Computers** tile.
2. Right-click the computer you want to place in a group and click **Assign Group** from the menu.

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

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

For more information on creating a group in PMC, please see "Create a Group in Privilege Management Console" on page 27.

Clear a Computer from a Group in Privilege Management Console

1. Navigate to and click the **Computers** tile.
2. Right-click the computer you want to clear the group from and click **Clear Group** from the menu. You are prompted to verify if you want to continue with clearing the group from the computer. Click **Continue Anyway** to proceed; otherwise, click **Cancel**.

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 in Privilege Management Console

PMC detects duplicate computers automatically. The task to check for duplicate computers runs every day at 0200 server time on the node where the job service is running. The service checks for computers with the same name. If PMC finds one or more computers with the same name, it adds the **Duplicate** flag to all of them except for the most recently created one.

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**. PMC does not do any additional processing to computers that are flagged as duplicates and they continue to receive policy from PMC. In the **Total Duplicates** column, you can filter that column to a range of numbers.

All computers that do not contact PMC for the number of days specified in the **Auto Deactivate Settings** are deactivated if you have chosen to automatically deactivate inactive computers.

For more information, please see "Auto Deactivate Settings" on page 78.

Deactivate Computers in Privilege Management Console

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

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

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

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

For more information, please see the following:

- "Auto Deactivate Settings" on page 78
- If the computer hasn't been authorized, "Reject Computers Not Authorized with Privilege Management Console" on page 34

Delete Deactivated Computers

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

Right-click on the grid row for the computer, and then select **Deactivate**.

Alternatively, select the computer and then select **Actions > Delete**.

"Update Policy on All" Option in Privilege Management Console

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

1. Navigate to and click the **Computers** tile.
2. Right-click anywhere in the grid, and click **Update Policy on All** from the menu. You are prompted to check you want to continue with updating the policy on all computer(s). Click **Update Policy on All** to proceed; otherwise, click **Cancel**.

For more information, please see "Policy Deployment Settings in Privilege Management Console" on page 42.

"Update Policy on Selected" Option in Privilege Management Console

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

1. Navigate to and click the **Computers** tile.
2. Right-click the computer(s) you want to update the policy on and click **Update Policy on Selected** from the menu. You are prompted to check you want to continue with updating the policy. Click **Update Policy Anyway** to proceed; otherwise, click **Cancel**.

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

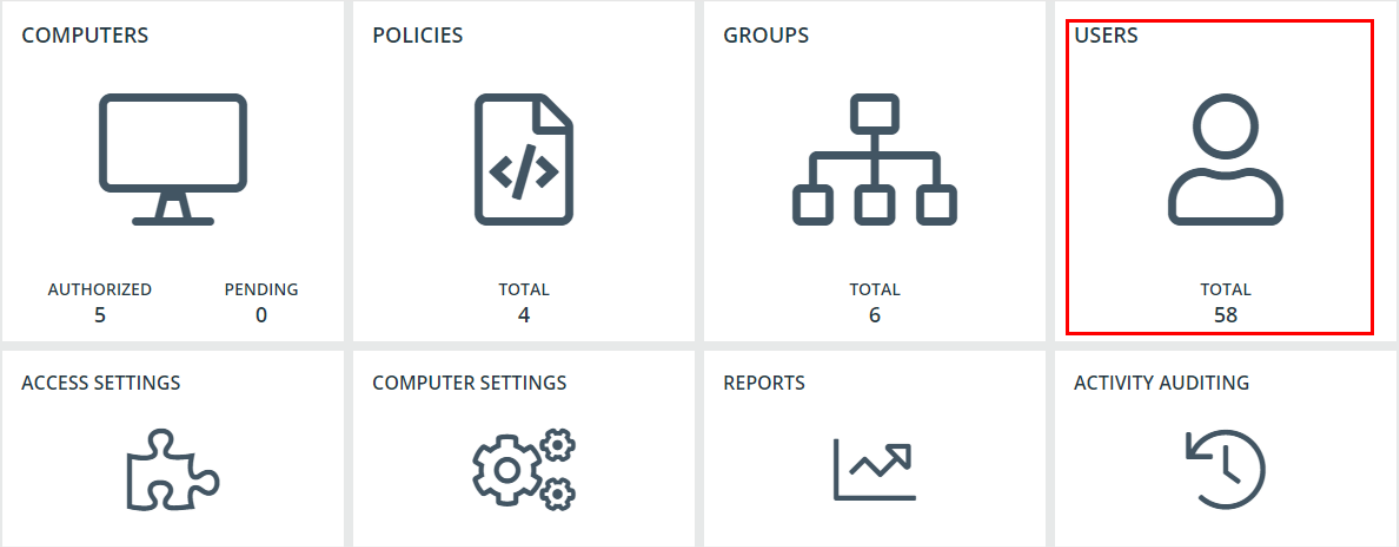
For more information, please see "Policy Deployment Settings in Privilege Management Console" on page 42.

Use Privilege Management Console to Assign Roles to a User Account in Privilege Management Console

1. Navigate to and click the **Users** tile.
2. Right-click on the user you want to assign a new role to and click **Assign Role**. This section allows you to change the role that is assigned to the user.
3. Click **Submit** to save your changes.

Users

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 Privilege Management Console

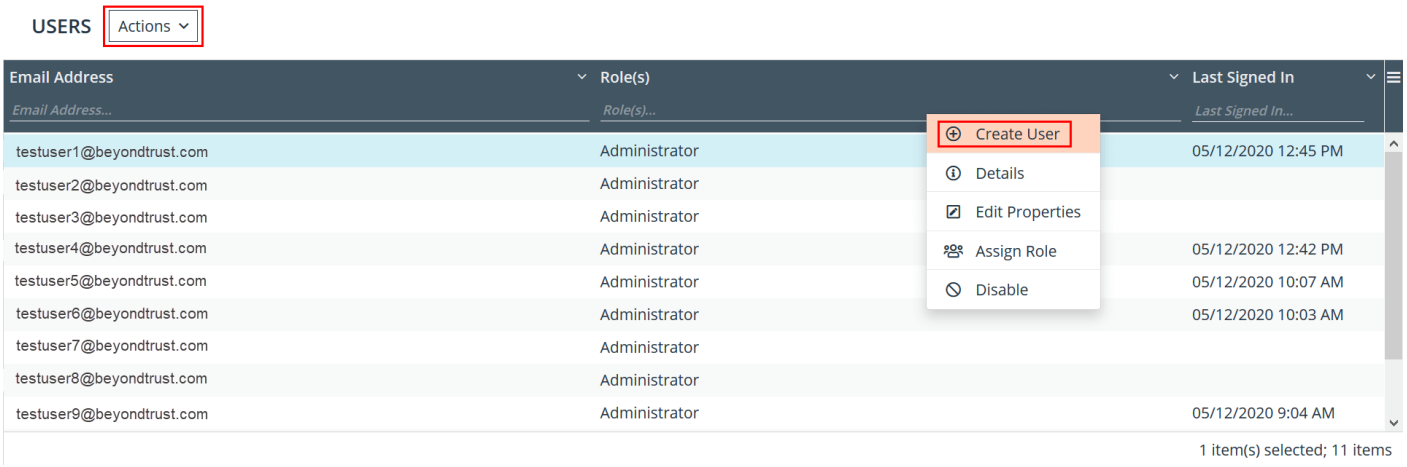
Once the initial administrator account has been created and authorized, you can create additional user accounts in PMC with whichever roles are needed. You can also create future accounts with the **Administrator** role by following the same process outlined below.

IMPORTANT!

The user needs to exist in your authorization provider before you add that user in PMC.

User Creation Process

1. Navigate to and click the **Users** tile.
2. Right-click anywhere on the grid and click **Create User**.



3. Enter your email address.

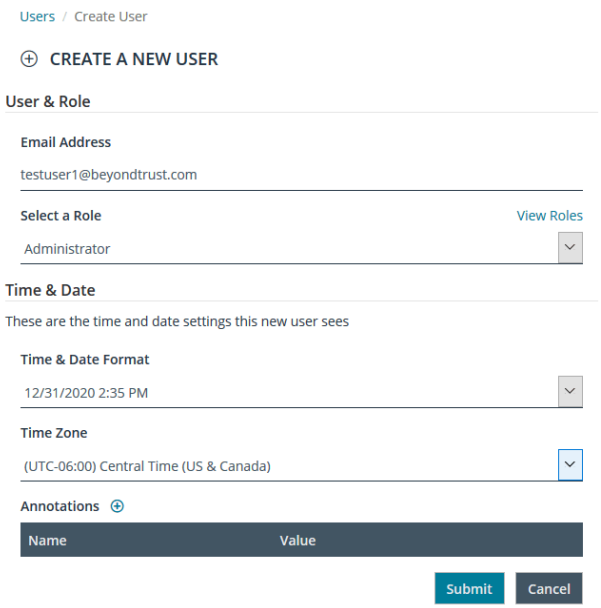
   For Active Directory Federation Services (ADFS) this must take the form:

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

   For Azure AD this must take the form:

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

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

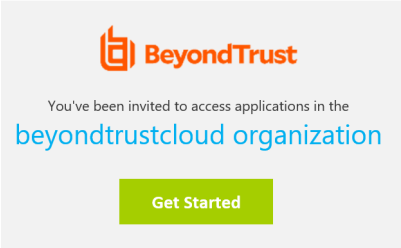


> ***Note:*** *This workflow has been tested and is supported by Azure AD. Other providers may work, but have not yet been tested.*

Registration and User Confirmation

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

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



View Details of a User Account in Privilege Management Console

1. Navigate to and click the **Users** tile.
2. Right-click on the user you want to view the details for and click **Details**. This section shows you the details for the user. You can add annotations if required. You can also edit the details of the user here.

For more information, please see "Edit Properties of a User Account in Privilege Management Console" on page 40.

Edit Properties of a User Account in Privilege Management Console

1. Navigate to and click the **Users** tile.
2. Right-click the user you want to view the details for and click **Edit Properties**. 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 **Submit** 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 in Privilege Management Console

1. Navigate to and click the **Users** tile.
2. Right-click on the user you want to assign a new role to and click **Assign Role**. This section allows you to change the role that is assigned to the user.
3. Click **Submit** to save your changes.

Disable a User Account in Privilege Management Console

1. Navigate to and click the **Users** tile.
2. Right-click the user you want to disable from details and click **Disable**.

3. You are prompted to confirm if you want to disable the user. Click **Disable Anyway** to disable the user; otherwise, click **Cancel**. You can enable the user again later, if required. The row flashes green to indicate that PMC has processed your request and the user is removed from the grid if you are using the default view.

Users that are disabled are not shown by default. To view users that are disabled, click the hamburger icon on the top right of the grid and click **Disabled** to show the **Disabled** column. You can now change the filter for the **Disabled** column to show those users who have been disabled.

For more information, please see "Enable a User Account in Privilege Management Console" on page 41.

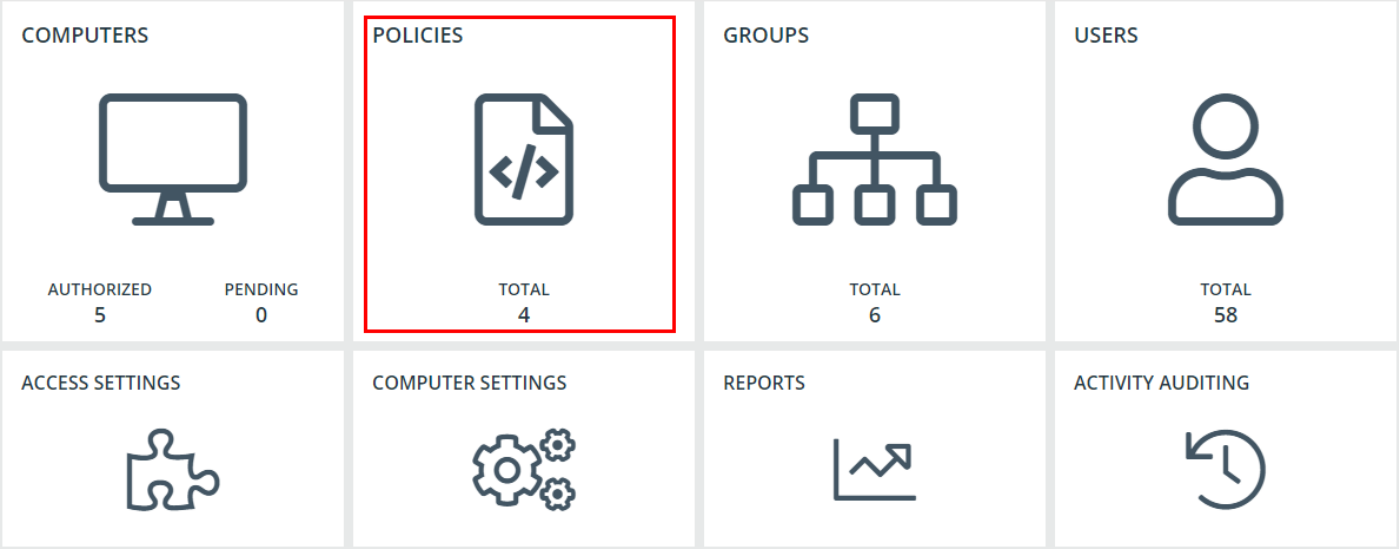
Enable a User Account in Privilege Management Console

Disabled users are not shown by default. To view users that are disabled, click the hamburger icon on the top right of the grid and click **Disabled** to show the **Disabled** column. You can now change the filter for the **Disabled** column to show those users who are disabled.

1. Navigate to and click the **Users** tile.
2. Right-click on the user you want to enable and click **Enable**.
3. The row briefly flashes green to indicate that PMC has processed your request and the user is now enabled.

Policy Deployment Settings in Privilege Management Console

The **Policies** tile allows you change the settings related to policy deployment.

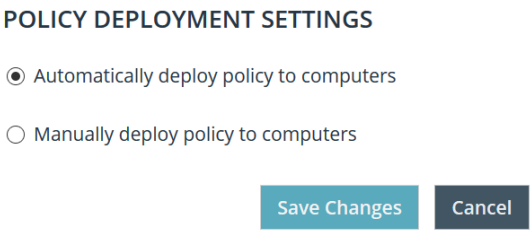


Manage Policy Deployment Settings in Privilege Management Console

Go to **Administration > Access Settings** to choose to deploy the policy automatically or manually to your computers.

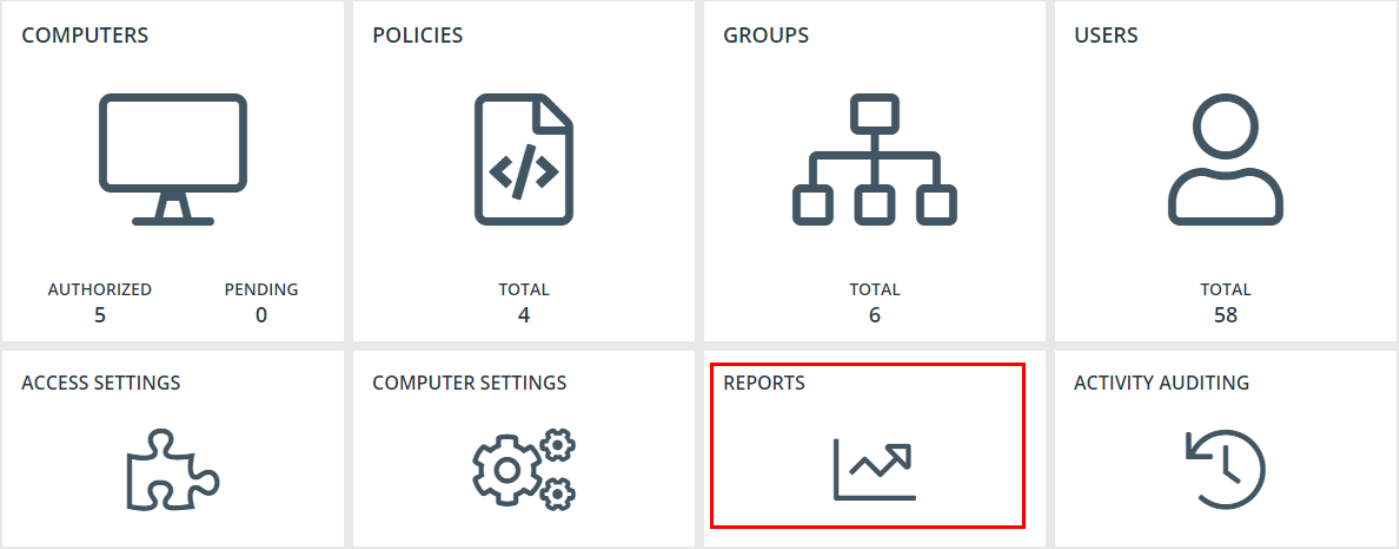
If you select automatic deployment, you do not need to do anything else to deploy a policy that is assigned to a group containing computers.

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



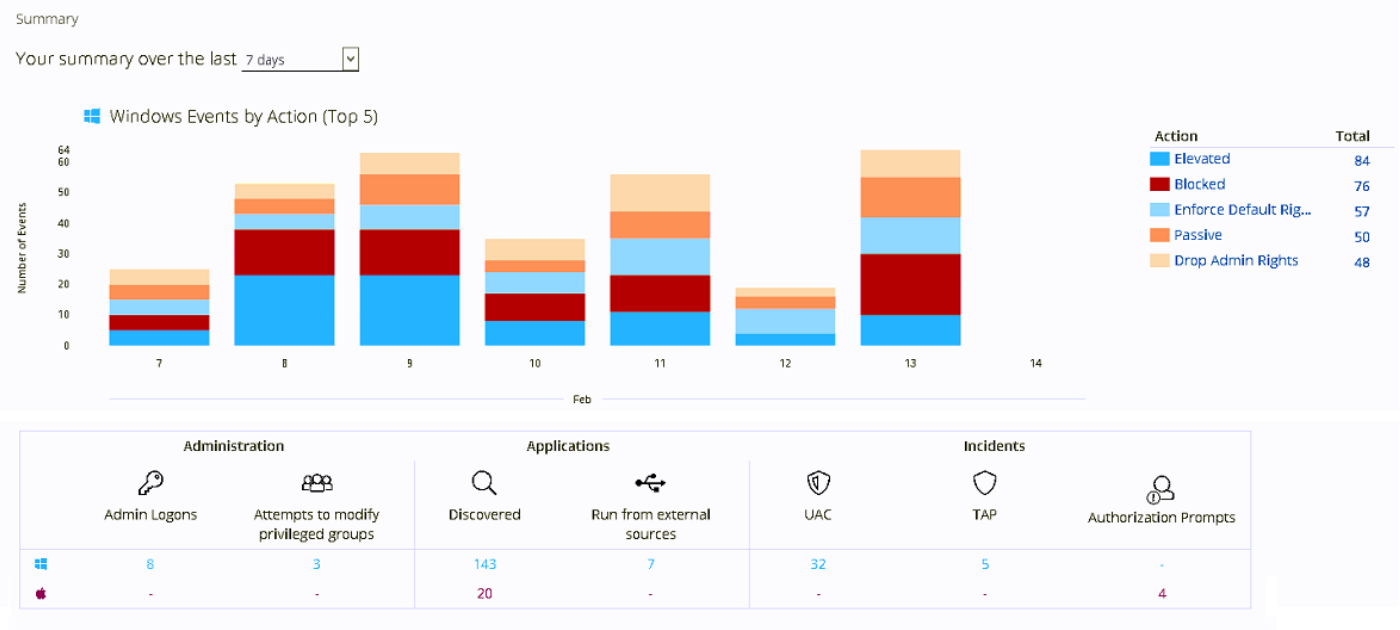
Privilege Management Console Reports

The **Reports** tile allows you to view Reporting within PMC.



Summary Report 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 charts:

Chart	Information
Applications first reported over the last x months (number)	Grouped by: • Admin Rights Detected • Admin Rights Not Detected
Types of newly discovered applications	Grouped by: • Admin Rights Detected • Admin Rights Not Detected
New applications with admin rights detected (top 10 of <number>)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Matched**, **Application Description**, and **Publisher** filters applied.
New applications with admin rights not detected (top 10 of <number>)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Matched**, **Application Description**, and **Publisher** filters applied.
New applications with admin rights detected (by type)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Admin Rights** and **Application Type** filters applied.
New applications with admin rights not detected (by type)	Clicking the **View All** link takes you to the **Discovery > All** report with the **Admin Rights** filter applied. Clicking an application takes you to the **Discovery > All** report with the **Admin Rights** and **Application Type** filters applied.

Privilege Management Console "Discovery by Path" Report

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

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

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

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

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

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

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

The following quick filters are available:

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

Privilege Management Console "Discovery by Publisher" Report

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

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

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

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

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

The following quick filters are available:

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

Privilege Management Console "Discovery by Type" Report

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

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

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

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

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

The following quick filters are available:

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

Privilege Management Console "Discovery Requiring Elevation" Report

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

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

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

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

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

The following quick filters are available:

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

Privilege Management Console "Discovery from External Sources" Report

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

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

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

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

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

This table groups the applications by type. You can click the **+** 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.

Privilege Management Console "Discovery All" Report

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

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

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

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

Privilege Management Console "Actions" Reports

The following reports are available for actions:

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

Privilege Management Console "Actions Elevated" Report

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

This dashboard displays the following charts:

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

Privilege Management Console Actions Blocked Report

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

This dashboard displays the following charts:

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

Privilege Management Console Actions Passive Report

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

This dashboard displays the following charts:

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

Privilege Management Console Actions Canceled Report

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

This dashboard displays the following charts:

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

Privilege Management Console Actions Custom Report

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

This dashboard displays the following charts:

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

Privilege Management Console Actions Drop Admin Rights Report

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

This dashboard displays the following charts:

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

Privilege Management Console Target Types

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

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

- **Description:** The description of a specific application
- **Platform:** The platform that the events came from
- **Publisher:** The publisher of a specific application
- **Product Name:** The product name of a specific application
- **Application Type:** The type of application
- **Product Version:** The version number of a specific application
- **# Process Count:** The number of processes
- **# User Count:** The number of users
- **# Host Count:** The number of hosts

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

Privilege Management Console "Trusted Application Protection" Report

This report shows information about TAP incidents. A TAP incident is a child process of a trusted application that is blocked, due to a Trusted Application policy or a DLL that is blocked from being loaded by a trusted application because it doesn't have a trusted owner or trusted publisher.

Note: *There are no advanced filters for the* ***Trusted Application Protection*** *dashboard.*

Chart	Description
All Trusted Application Protection incidents over the time period	A stacked bar chart showing the number of the different incidents broken down by the trusted application.
Trusted Application Protection incidents, by application	A table listing each trusted application, the number of TAP incidents, the number of targets, the number of users, and the number of hosts affected.
Top 10 targets	The top 10 targets for TAP incidents. Clicking the target name shows you more information about the target including its actions over the time period. Clicking on **Users** shows you more information about the users. Clicking on **Host** shows you more information about the host. Clicking on **Incidents** takes you to the **Process Detail** report with the **Distinct App ID** filter applied.

For more information, please see "Privilege Management Console "Process Detail" Report" on page 61.

Privilege Management Console Users

There are three reports for users:

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

Privilege Management Console User Experience Report

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

This dashboard displays the following charts:

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

Privilege Management Console Users Privileged Logons Report

The **Privileged Logon** report shows you how many accounts with Standard rights, Power User rights, and Administrator rights have generated logon events broken down over the specified time frame.

This dashboard displays the following charts:

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

Privilege Management Console Users Privileged Account Management Report

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

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

Privilege Management Console "Events" Report

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 endpoints in each time group since the last event category. Clicking the chart takes you to more detailed information about the host.

Event Types

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

The following events are logged by Privilege Management:

Event ID	Description
0	Service Control Success
1	Service Error
2	Service Warning
100	Process has started with admin rights added to token.
101	Process has been started from the shell context menu with admin rights added to token.
103	Process has started with admin rights dropped from token.
104	Process has been started from the shell context menu with admin rights dropped from token.
106	Process has started with no change to the access token (passive mode).
107	Process has been started from the shell context menu with no change to the access token (passive mode).
109	Process has started with user's default rights enforced.
110	Process has started from the shell context menu with user's default rights enforced.
112	Process requires elevated rights to run.
113	Process has started with custom token applied.
114	Process has started from the shell context menu with user's custom token applied.
116	Process execution was blocked.

Event ID	Description
118	Process started in the context of the authorizing user.
119	Process started from the shell menu in the context of the authorizing user.
120	Process execution was canceled by the user.
130	A Mac application bundle was installed.
131	A Mac application bundle was deleted.
150	Privilege Management handled service control start action.
151	Privilege Management handled service control stop action.
152	Privilege Management handled service control pause/resume action.
153	Privilege Management handled service control configuration action.
154	Privilege Management blocked a service control start action.
155	Privilege Management blocked a service control stop action.
156	Privilege Management blocked a service control pause/resume action.
157	Privilege Management blocked a service control configuration action.
158	Privilege Management service control action run in the context of the authorizing user.
159	Privilege Management service control start action canceled.
160	Privilege Management service control stop action canceled.
161	Privilege Management service control pause/resume action canceled.
162	Privilege Management service control configuration action canceled.
198	Privileged group modification blocked.
199	Process execution was blocked, the maximum number of challenge / response failures was exceeded.
Configuration Events	
10	License Error
200	Config Config Load Success
201	Config Config Load Warning
202	Config Config Load Error
210	Config Config Download Success
211	Config Config Download Error
User / Computer Events	
300	User User Logon
400	Service Privilege Management Service Start
401	Service Privilege Management Service Stop
Content Events	
600	Process Content Has Been Opened (Updated Add Admin)
601	Process Content Has Been Updated (Updated Custom)
602	Process Content Access Drop Admin (Updated Drop Admin)
603	Process Content Access Was Cancelled By The User (Updated Passive)
604	Process Content Access Was Enforced With Default Rights (Updated Default)

Event ID	Description
605	Process Content Access Was Blocked
606	Process Content Access Was Cancelled
607	Process Content Access Was Sandboxed
650	Process URL Browse
706	Process Passive Audit DLL
716	Process Block DLL
720	Process Cancel DLL Audit

Each process event contains the following information:

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

Privilege Management Console "Events All" Report

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

- **Event Time:** The time of the event
- **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.

Privilege Management Console "Process Detail" Report

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

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

- **Start Time:** The start time of the event
- **Platform:** The platform that the events came from
- **Description:** The description of a specific application
- **Publisher:** The publisher of a specific application
- **Application Type:** The type of application
- **File Name:** The name of the file, where applicable
- **Command Line:** The command line path of the file, if applicable
- **Product Name:** The product name, where applicable
- **Trusted Application Name:** The name of the trusted application
- **Trusted Application Version:** The version of the trusted application
- **Product Version:** The version of the product of applicable
- **Group Policy Object:** The group policy object, if applicable
- **Workstyle:** The workstyle containing the rule that triggered the event
- **Message:** Any message associated with the event
- **Action:** Any action associated with the event
- **Application Group:** The Application Group that the application that triggered the event belongs to
- **PID:** The operating system process identifier
- **Parent PID:** The operating system process identifier of the parent process
- **Parent Process File Name:** The name of the parent process
- **Shell/Auto:** Whether the process was launched using the shell **Run with Privilege Management** option or by normal means (opening an application)
- **UAC Triggered:** Whether or not Windows UAC was triggered
- **Admin Rights Detected:** Whether or not admin rights was detected
- **User Name:** The user name that triggered the event
- **Host Name:** The host name where the event was triggered
- **Rule Script File Name:** The name of the Rule Script (Power Rule) that ran
- **Rule Script Affected Rule:** True when the Rule Script (Power Rule) changed one or more of the default Privilege Management for Windows rules
- **User Reason:** The reason given by the user, if applicable
- **COM Display Name:** The display name of the COM, if applicable
- **Source URL:** The source URL, if applicable

Privilege Management Console Report Filters

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

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

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

Name	Description
Application Hash	This field is used by Reporting. You do not need to edit it.
Application Type	A text field that allows you to filter on the application type. You can obtain the application type from the policy editor.
Authorizing User Name	The name of the user that authorized the message.
Browse Destination URL	The destination URL of the sandbox.
Challenge/Response	Allows you to filter by challenge/response events. For example, you can filter the application that required elevation on those applications that were launched following a completed challenge/response message.
	Filter options: • **All** • **Only C/R**
Client IPV4	This field is used by Reporting. You do not need to edit it.
Client Name	This field is used by Reporting. You do not need to edit it.
COM Application ID	This field is used by Reporting. You do not need to edit it.
COM Display Name	This field is used by Reporting. You do not need to edit it.
COM CLSID	This field is used by Reporting. You do not need to edit it.
Command Line	A text field that allows you to filter on the command line.
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 endpoint the event came from.

Name	Description
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.

Name	Description
Platform	Filters by the type of operating system. • **Windows** Filters by endpoints running a Windows operating system. • **macOS** Filters by endpoints running a Mac operating system.
Process Unique ID	The unique identification of the process.
Product Code	This field is used by Reporting. You do not need to edit it.
Product Name	The product name of the application.
Product Version	The product version of the application.
Program Files Path	Sets the Program Files path used by the **Discovery > Path** report.
Publisher	The publisher of the application.
Range End Time	The end time of the range being displayed.
Range Start Time	The start time of the range being displayed.
Row Limit	The maximum number of rows to be retrieved from the database.
Rule Script Affected Rule	True when the Rule Script (Power Rule) changed one or more of the default Privilege Management rules; otherwise, false.
Rule Script File Name	The Rule Script (Power Rule) file name on disk, if applicable.
Rule Script Name	The name of the assigned Rule Script (Power Rule).
Rule Script Output	The output of the Rule Script (Power Rule).
Rule Script Publisher	The publisher of the Rule Script (Power Rule).
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>*

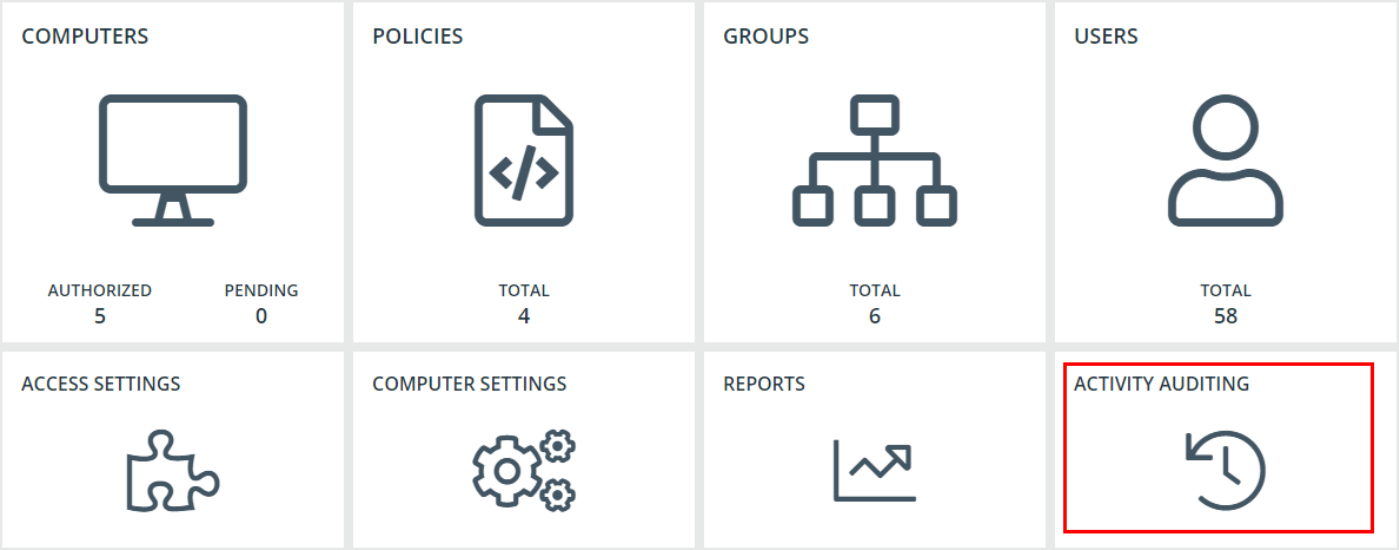
Name	Description
Rule Script Status	The status of the Rule Script (Power Rule). This can be: • **<None>** • **Success** • **Timeout** • **Exception** • **Skipped** • **ValidationFailure**
Rule Script Version	The version of the assigned Rule Script (Power Rule).
Rule Match Type	Rule Match Type: • **Any** • **Direct match** • **Matched on parent**
Sandbox	The sandboxed setting.
	Filter options: • **Not Set** • **Any Sandbox** • **Not Sandboxed**
Shell or Auto	Whether the process was launched using the shell **Run with Privilege Management** option or by normal means (opening an application):
	Filter options: • **Any** • **Shell** • **Auto**
Show Discovery Events	Whether or not you want to show Discovery events. An event is a Discovery event if it's been inserted into the database in the filtered time period.
Source	The media source of the application. For example, whether the application was downloaded from the Internet or removable media.
	Filter options: • **All** • **Downloaded over the internet** • **Removable media** • **Any external source**
System Path	Sets the system path.
Target Description	This field allows you to filter by the target description.

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 Activity Auditing

The **Activity Auditing** tile allows you to view audit activity for PMC administration activity if you have a user role that allows it. Rows that indicate an error are shown in red. You can also filter for those using the **Error** column.



Privilege Management Console Administration

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

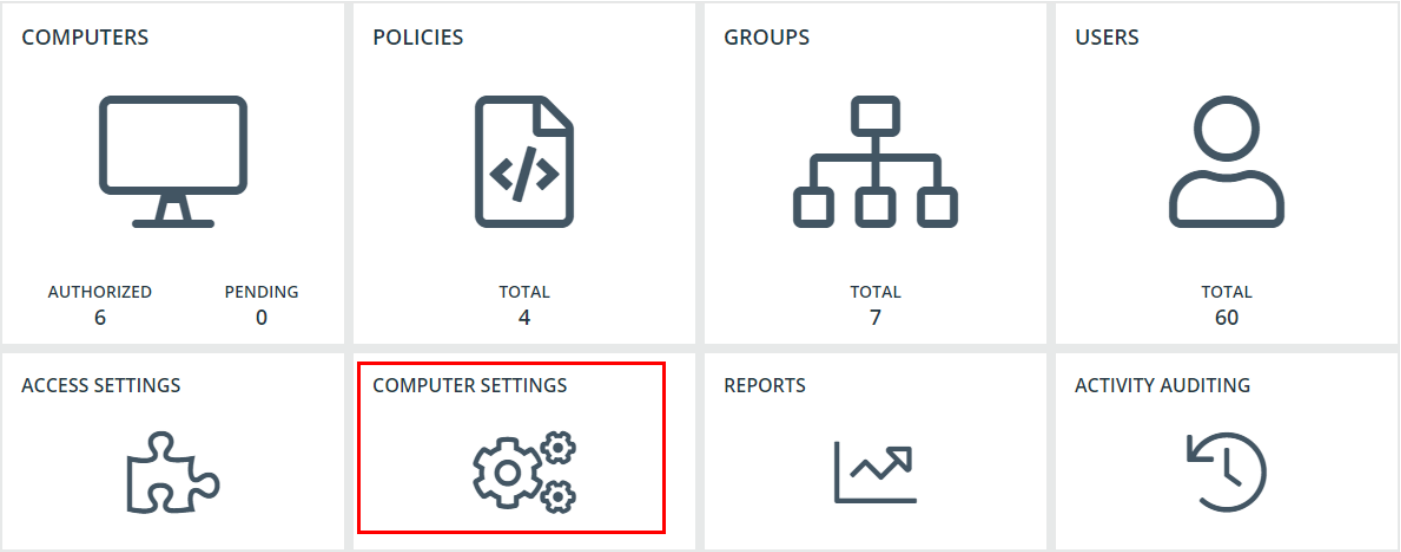
- Computer Settings
- User Management
- User Roles
- Access Settings

For more information, please see the following:

- "Use Privilege Management Console to Assign Roles to a User Account in Privilege Management Console" on page 38
- "Create a User Account in Privilege Management Console" on page 38
- "User Roles in Privilege Management Console" on page 75
- "Privilege Management Console Settings Options" on page 78

Privilege Management Console Computer Settings

The **Computer Settings** tile opens a page where you can manage computer deactivation settings and view a list of inactive computers.



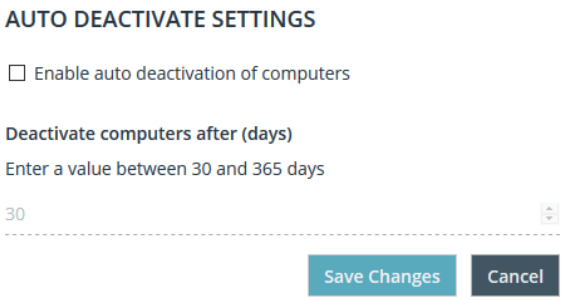
Auto Deactivate Settings

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

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

To enable the automatic deactivation of computers, check the **Enable auto deactivation of computers** box. When you check this box, enter a value between 30 and 365 days. This determines the duration since the computer last contacted PMC before it is automatically deactivated.

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



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 **Enable auto deactivation of computers** setting. The functionality remains unchanged.

You can also manually deactivate computers.

For more information, please see the following:

- "View Duplicate Computers in Privilege Management Console" on page 36
- "Deactivate Computers in Privilege Management Console" on page 36

View Inactive Computers

1. Click the **Computer Settings** tile to view a list of inactive computers.
2. Click **View in List** to open the **Computers** page to view more detailed information on the computers.
3. On the **Computers** page, right-click the computer and select **Deactivate**.

For more information, please see "Deactivate Computers in Privilege Management Console" on page 36.

User Roles in Privilege Management Console

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

There are five user roles:

- Administrator
- Agent administrator
- Policy administrator
- Policy editor
- Standard user

Each user role has various permissions across 11 areas:

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

PMC displays which permissions each user role has.

Privilege Management Console Access Settings

The following settings are available from the **Administration > Access Settings** page:

- Setup Information
- Remote access settings
- Policy deployment settings
- Agent installation keys
- Diagnostics

There is also an **Access Settings** tile on the dashboard.

Setup Information

The Setup Information pane provides installation details for the following components:

- Privilege Management for Windows
- Privilege Management for Mac
- Windows Adapter

- Mac Adapter
- MMC Snap-in

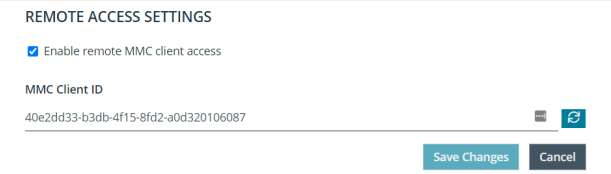
For more information about these topics, please see "Privilege Management Console QuickStart" on page 8.

Remote Access Settings

Set remote access to allow communication from the MMC snap-in to PMC.

You need to configure PMC to allow the Privilege Management MMC snap-in to communicate with the PMC services.

1. Click **Administration > Settings > Remote Access Settings** from the top menu.
2. Check the **Enable remote MMC client access** box. You need to generate a new GUID and enter it here. Click the refresh button to create a new GUID. Use the same GUID when you configure the MMC. This is the **MMC Client ID** in the MMC.



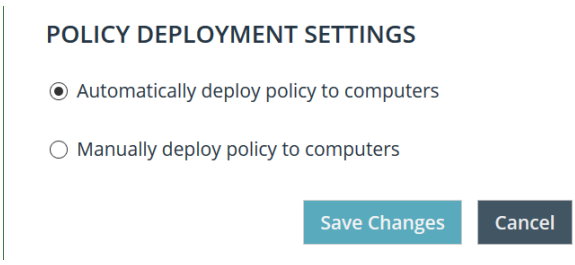
3. Click **Save Changes**.

Policy Deployment Settings

Go to **Administration > Access Settings** to choose to deploy the policy automatically or manually to your computers.

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

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



Agent Installation Keys

This pane contains the Installation ID and Installation Key GUIDs that are required to connect computers to PMC. You can create new installation IDs and installation keys here and delete them if required. Once you revoke an installation key, you don't need to reinstall adapters that have been authorized - only pending ones.

For more information on how these fields are used, please see the following:

- "Install the Windows Adapter" on page 10
- "Install the Mac Adapter" on page 12

View Diagnostics Metrics

The **Diagnostics** pane allows you view various diagnostics for PMC, including:

- **Version**
- **API Connection**
- **User**
- **Tenant Id**
- **ER Database Version**
- **ServerURI**

To access the **Diagnostics** pane, click **Administration > Access Settings**.

Privilege Management Console Settings Options

This menu has three options:

- **Auto Deactivate Settings**
- The **Policy Deployment Settings** tile
- **Remote Access Settings**

For more information, please see the following:

- "Auto Deactivate Settings" on page 78
- "Policy Deployment Settings in Privilege Management Console" on page 42
- "Privilege Management Console Settings Options" on page 78

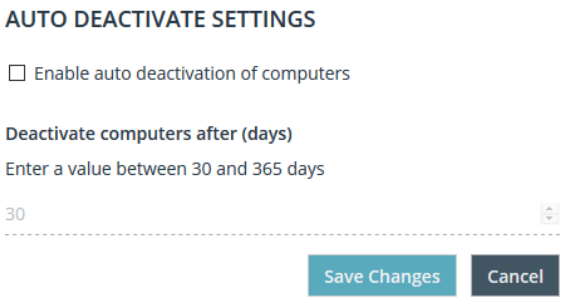
Auto Deactivate Settings

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

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

To enable the automatic deactivation of computers, check the **Enable auto deactivation of computers** box. When you check this box, enter a value between 30 and 365 days. This determines the duration since the computer last contacted PMC before it is automatically deactivated.

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



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 **Enable auto deactivation of computers** setting. The functionality remains unchanged.

You can also manually deactivate computers.

For more information, please see the following:

- "View Duplicate Computers in Privilege Management Console" on page 36
- "Deactivate Computers in Privilege Management Console" on page 36