Privilege Management App
User Guide 24.2

Table of Contents

BeyondTrust Endpoint Privilege Management App

The BeyondTrust Endpoint Privilege Management App for ePO is comprised of two components:

- **Web Policy Editor**: Edit and manage policies through an updated modern user interface.
- **Endpoint Privilege Management Reporting**: Provides overview data and detailed insights on user behavior within your organization.
  - **Add to Policy**: Included in reporting is Add to Policy functionality, which allows you to seamlessly update policy based on user events in reporting event data.

Download the BeyondTrust Endpoint Privilege Management App from the BeyondTrust Customer Portal.

Endpoint Privilege Management App Features Overview

The new features available in the BeyondTrust Endpoint Privilege Management App:

- Better overall policy editing and reporting user experience
- Updated Trusted Application Protection token and template
- Updated QuickStart policy templates
- Add basic admin rights Windows access token
- A more secure elevation token with greater control over granted privileges for rules targeted at actions
- Privileges enhanced Windows access token
- Keeps the same privileges of the process token. Should be used with advanced parent tracking or anti-tamper.
- Ability to require a secret to uninstall EPM agent (Agent Protection)
- Option to use a reason drop down in macOS end user messages
- Disable applications and application rules for easy testing and policy updates
- Windows Hello and macOS Touch ID message authentication
- Windows and Mac AND / OR message logic UX improvements
- Windows and Mac IdP / RADIUS message configuration
- BeyondTrust Password Safe integration
- DLL Control for Windows
- Ability to elevate Store Apps for Windows (depending on app type)
- ACR MFA support for Mac
- Support Azure AD Conditional Access Policies (MFA) for Mac
- And more UX and usability enhancements

Features that will not be available in the BeyondTrust Endpoint Privilege Management App at initial launch:

- Manually update reputation for events

Features that will not be available in the BeyondTrust Endpoint Privilege Management App and are being deprecated:

- Windows workstyle expiry filters
- Windows workstyle time range filters

Configure Endpoint Privilege Management App

The following sections provide details on getting started with the Endpoint Privilege Management App.

Prerequisites

- An ePO account with permissions to edit BeyondTrust policies as per the guide available here: https://www.beyondtrust.com/docs/privilege-management/windows/epo-install/assign-permissions.htm

Install the App

1. Download the latest BeyondTrust Endpoint Privilege Management App from the BeyondTrust Customer Portal (Service Now).
2. Locate an MSI file named **BeyondTrust EPM Console xx.xx.msi**.
3. Once downloaded, double-click the MSI and the installation prompt will be displayed.
4. Follow the on-screen installation steps.

A Windows security alert might be displayed when you try to start the app. Click **Allow access** to proceed.
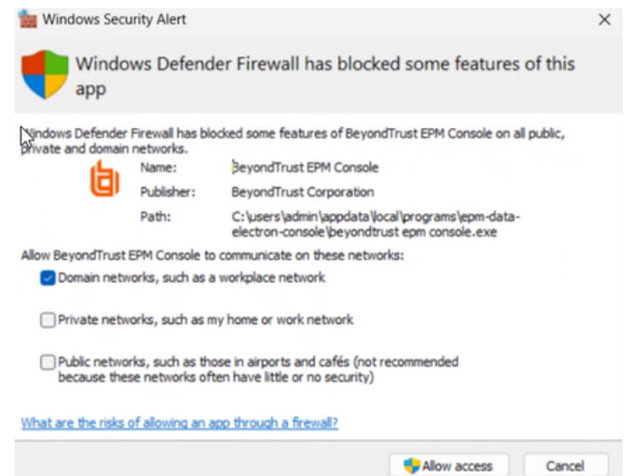
ℹ️ *For more information on installing and configuring the app, see Configure BeyondTrust Reporting at https://www.beyondtrust.com/docs/privilege-management/windows/epo-install/beyondtrust-reporting/index.htm.*

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

5

TC: 4/25/2024

Configure local AD connector

Configure Active Directory (AD) to discover AD groups in your estate. The Policy Editor queries the Active Directory to populate the group information when adding account filters or designated users.

To configure Local AD search for policies:

1. Click **Configuration** and select the **Local AD Configuration** menu item:

2. Provide the following information:

   - **LDAP Server URL**: The LDAP connection string which starts with the prefix *LDAP://* combined with the domain controller in the domain.

   - **Base DN**: The base distinguished name (Base DN) identifies the entry in the directory from which searches initiated by LDAP.

   - **User DN**: The user distinguished name (User DN) and the correct password serve as authentication allowing the application access to populate data in the Policy Editor. For example:

     CN=JeffSmith,OU=Sales,DC=Fabrikam,DC=COM

   - **Password**: Valid password matching the provided user name in **User DN**.

3. Click **Test Connection** to ensure the connection is successful.

4. Click **Save**.

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

6
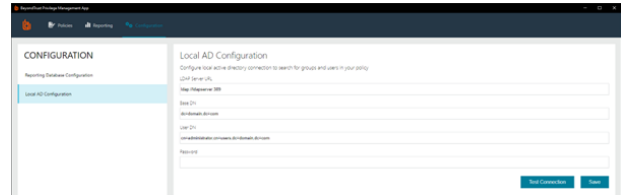
Workstyles

A Workstyle is a container for the rules that will be applied to the computers receiving the policy. If you are using a Windows or macOS Quickstart template, the Workstyles include predefined rule configurations.

If creating policy from a blank template, there is no predefined configuration.

- Add and change the properties for a rule
- Enable Trusted Application Protection (optional)
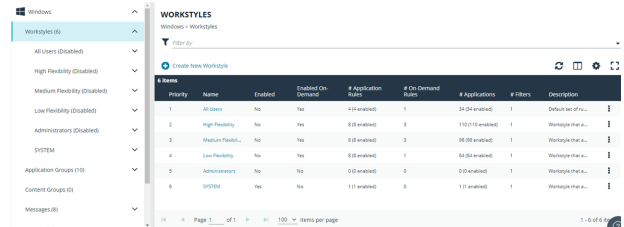- Add monitoring and logging
- Change the ordering of Workstyle processing
- Enable the Workstyle

> ℹ️ For more information about QuickStart templates, see *"Use Quickstart Templates" on page 63*.

Set up Logging for Privileged Applications and Processes

Privilege monitoring logs all privileged actions run by the application or process that would fail under a standard user account. These include file operations, registry operations, and any interactions with other components such as Windows services.

Applications included in privilege monitoring:

- Applications running under a privileged account, such as an administrator or power user.
- An application added to an Application Rule or On-Demand Application Rule that is set up to run with elevated privileges.

Configure privilege monitoring when you create or edit a Workstyle.

Privilege monitoring logs are recorded on each endpoint.

Privilege monitoring is available only on Windows.
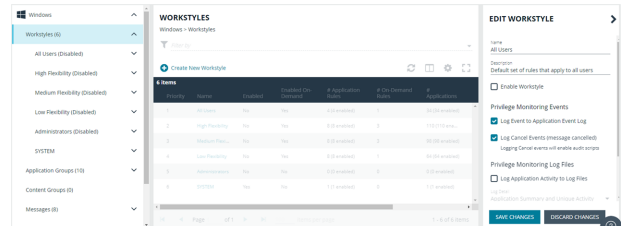
> ℹ️ For more information about privilege monitoring, contact your BeyondTrust consultant.

Privilege Monitoring Events

- **Log Event to Application Event Log:** Logs an event to the Application event log the first time an application performs a privileged operation.
- **Log Cancel Events (message cancelled):** Raises an event when a user cancels an end user message, either by clicking the **Cancel** button, by clicking the **Email** button, or by clicking a **Hyperlink**. You can configure the user action using policy parameter [PG_ACTION], which can be used by the script to perform different audit actions based on the user interaction. To log **Cancel Events**, enable **Raise an Event** for the rule that has been matched.

Privilege Monitoring Log Files

The following privilege monitoring options are available:

- **Log Application Activity to Log Files:** Check the box to turn on logging.
- **Application Summary and Activity:** Select to log information about the application and unique privileged activity (Default option).
- **Application Summary and Detailed Activity:** Select to log information about the application and all privileged activity.
- **Maximum Activity Records Per Process:** Set the maximum number of records logged per process (Default 100).
- **Keep Application Activity Logs for (Days):** Set how long activity logs are kept before they are purged (Default 14 days).

Enable a Workstyle

By default, a Workstyle is disabled when initially created. Enable a Workstyle when configuration is complete and ready for the production environment.

Disable the Workstyle whenever you need to change the configuration.

1. Go to the Policy Editor, and then navigate to Workstyles.
2. Select a Workstyle, and then select **Enable** from the menu.

Set the Order for Workstyle Processing
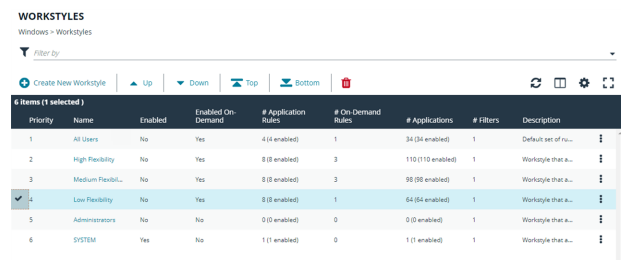
Workstyles are evaluated in the order they are listed. When an application matches on a Workstyle, no further Workstyles are processed for that application.

Ensure the order of the Workstyles is correct because it is possible for an application to match more than one Workstyle.

To change the order:

1. Select a Workstyle in the list to change the order.
2. Use the buttons to move the rule to the preferred location.

   Changes are automatically saved.

Application Rules

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

Create an Application Rule

1. On the **Policy Editor** page, expand **Windows**.
2. Expand the **Workstyles** node, and then expand a Workstyle.
3. Click **Application Rules**, and then click **Create New**.
4. Set the following:

   - **Target Application Group**: Select an Application Group.
   - **Action**: Select **Allow**, **Allow as Password Safe User**, **Block**, or **Request**. The action that occurs if the application in the targeted Application Group is launched by the end user.
   - **Password Safe Account Name**: Enter the Managed Account name configured in Password Safe for the computer.
   - **Run Rule Script**: Assign a rule script that runs before the Application Rule triggers. Select a rule script from the list.
   - **End User Message**: Select a message from the list.
   - **Access Token**: Select the type of token to pass to the Target Application Group. You can select from:
     - **Passive (No Change**: No changes are made to the token. This is essentially an audit feature.
     - **Enforce User's Default Rights**: Removes all rights and uses the user's default token. Windows UAC always tries to add administration rights to the token being used so if the user clicked on an application that triggers UAC, the user cannot progress past the UAC prompt.
     - **Drop Admin Rights**: Removes administration rights from the user's token.
     - **Add Full Admin (Required for installers)**: Standard Windows Admin token containing all Admin privileges. Use the full admin token in scenarios where your users require privileges **SeDebugPrivilege** or **SeLoadDriverPrivilege**. An example use case is MSI files running in a client/server mode where **SeDebugPrivilege** is required to interact with the server component which runs as SYSTEM. This only applies to cases where the standard user needs to run the MSI directly.
     - **Add Basic Admin Rights**: Permits elevation of most applications and tasks. We recommend using this token as the default elevation token. This access token is essentially full admin but excludes the following privileges: **SeDebugPrivilege** and **SeLoadDriverPrivilege**. If users need to debug applications or access drivers, then use the full admin token.
     - **Endpoint Privilege Management Support Token**: Applies Add Full Admin privileges with tamper protection removed.
     - **Keep Privileges - Enhanced**: This token behaves similar to the **Passive (no change)** token in that there is no change to privilege, elevation, or integrity level. Uses the same privileges of the original process token and adds some additional context to it: the token is added to the anti-tamper group and will be tracked by the advanced parent tracking feature. This access token can only be used with application rules.
   - **Raise An Event**: **Off**, **On**, **Anonymous**. Select if an event is raised if this Application Rule is triggered. When on, an event is sent to the local event log file. Anonymous removes user and host name from events so the user / host are not identifiable.
   - **Run an Audit Script**: Select an audit script from the list.
   - **Privilege Monitoring**: **Off**, **On**, **Anonymous**. Select **On** to raise a privileged monitoring event.
   - **Reporting Events**: On by default, click to turn off. When the setting is on, events are raised for viewing in EPM Reporting.
5. Click **Create Application Rule**.

Set the Order for Rules Processing

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

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

Create an On-Demand Application Rule

Create an on-demand rule to start an application with specific privileges (usually admin rights) from a Windows right-click context menu. The on-demand application rule triggers when the context menu item is selected.

Before creating an on-demand rule, you can set the behaviour for the right-click context menu on the **On-Demand Integration Settings** page. In the Policy Editor, go to **Windows > Workstyles > *<workstyle name>* > On-Demand Application Rules**.
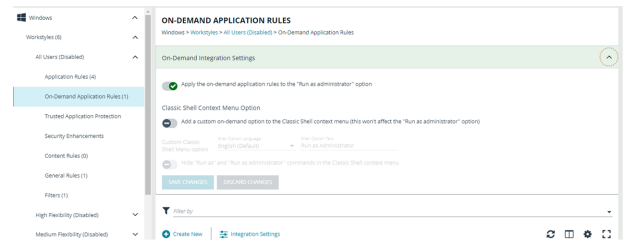
- **Apply the on-demand application rules to the "Run as administrator" option**: Select to override the **Run as administrator** right-click context menu. The labeling of the menu does not change in this instance. This setting applies to all versions of Windows that have the **Run as administrator** context menu.
- **Add a custom on-demand option to the Classic Shell context menu (this won't affect the "Run as administrator" option)**: Select to add a new option to the right-click context menu. Select a language and the option text. You can add text like *Run with Endpoint Privilege Management for Windows*. This setting applies to the Classic Windows Shell only.
- **Hide "Run as" and "Run as administrator" commands in the Classic Shell context menu**: Select to hide these menu items, where present, from the right-click context menu. This setting applies to the Classic Windows Shell only.

To create an On-Demand Application Rule:

1. Expand **Workstyles**, and then expand a Workstyle.
2. Select **On Demand Application Rules**.
3. Click **Create New**.
4. Set the following:
   - **Raise An Event**: **Off**, **On**, **Anonymous**. Select if an event is raised if this Application Rule is triggered. When on, an event is sent to the local event log file. Anonymous removes user and host name from events so the user / host are not identifiable.
   - Click **Create On-Demand Rule**.
   - **Target Application Group**: Select an Application Group.
   - **Action**: Select **Allow**, **Allow as Password Safe User**, **Block**, or **Request**. The action that occurs if the application in the targeted Application Group is launched by the end user.
   - **Password Safe Account Name**: Enter the Managed Account name configured in Password Safe for the computer.
   - **Run Rule Script**: Assign a rule script that is run before the Application Rule triggers. Select a rule script from the list.
   - **End User Message**: Select a message from the list.

- **Access Token**: Select the type of token to pass to the Target Application Group. You can select from:
  - **Passive** (no change): Doesn't make any change to the user's token. This is essentially an audit feature.
  - **Enforce User's default rights**: Removes all rights and uses the user's default token. Windows UAC always tries to add administration rights to the token being used so if the user clicked on an application that triggers UAC, the user cannot progress past the UAC prompt.
  - **Drop Admin Rights**: Removes administration rights from the user's token.
  - **Add Full Admin (Required for installers)**: Standard Windows Admin token containing all Admin privileges. Use the full admin token in scenarios where your users require privileges **SeDebugPrivilege** or **SeLoadDriverPrivilege**. An example use case is MSI files running in a client/server mode where **SeDebugPrivilege** is required to interact with the server component which runs as SYSTEM. This only applies to cases where the standard user needs to run the MSI directly.
  - **Add Basic Admin Rights**: Permits elevation of most applications and tasks. We recommend using this token as the default elevation token. This access token is essentially full admin but excludes the following privileges: **SeDebugPrivilege** and **SeLoadDriverPrivilege**. If users need to debug applications or access drivers, then use the full admin token.
  - **Endpoint Privilege Management Support Token**: Applies Add Full Admin privileges with tamper protection removed.
- **Raise An Event**: **Off**, **On**, **Anonymous**. Select if an event is raised if this Application Rule is triggered. When on, an event is sent to the local event log file. Anonymous removes user and host name from events so the user / host are not identifiable.
- **Run an Audit Script**: Select an audit script from the list.
- **Privilege Monitoring**: **Off**, **On**, **Anonymous**. Select **On** to raise a privileged monitoring event.
- **Reporting Events**: On by default, click to turn off. When the setting is on, events are raised for viewing in EPM Reporting.

Integrate BeyondTrust Password Safe

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

Password Safe must already be installed and configured.

> ℹ️ For more information, see the _Password Safe Integration Guide_ at _https://www.beyondtrust.com/docs/privilege-management/windows/index.htm_.

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

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

Configure Local Account Discovery

Configure a discovery scan to detect unmanaged accounts on an endpoint. The scan results are sent to Password Safe.

1. On the **Policy Editor** page, expand **Windows**.
2. Expand the **Workstyles** node, and then expand a Workstyle.
3. Select **Application Rules** or **On Demand Application Rules**, and then click **Integration Settings**.
4. From the **Activation** list, select **Enabled**.
5. Set an account discovery interval.
6. Click **Update Settings**.

Create a Trusted Application Protection Rule

Use Trusted Application Protection (TAP) rules to dynamically evaluate DLLs for trusted applications for each Workstyle.

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

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

TAP rules affect the following applications:

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

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

To create a TAP rule:

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

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

12

Activate Block Loading of Trusted DLLs

A number of the DLLs from Microsoft's Recommended Blocklist can easily be blocked to prevent potential attacks from threat actors.

1. Go to the **Security Enhancements** tab for the workstyle where you want to enable DLL control.
2. Click the toggle to turn on blocking.

While Microsoft recommends blocking these DLLs, there are legitimate use cases. If required, you can change the setting to allow loading.

1. Select the DLL to unblock, and then click **Allow Loading**.
2. To reverse the action and block the DLL, select the DLL and click **Block Loading**.

    Some of the DLLs are allowed by default. See the next section to see why and if you need to adjust any options.
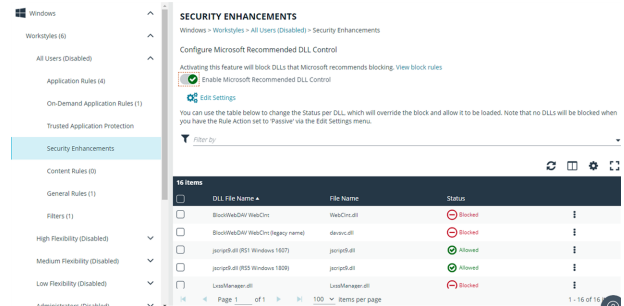
Windows Version Specific DLLs

A number of the recommended DLLs to block are specific to certain versions on certain Windows 10 versions. For example, it is advised to block the DLLs if you are running Windows 10 1607 or Windows 10 1809. These are identified in the list with the either **RS1 Windows 1607** or **RS5 Windows 1809** labels.

Additionally, Windows creates some cached versions of DLLs that have different names and properties. Ensure DLLs with a *Native Image* version are set to blocked, when required. You can identify these in the list with the **Native image** label.

> ℹ️ *For more information, see Microsoft recommended block rules at https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules.*

Configure General Rules on a Workstyle

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

The general rules include the following:

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

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

    - Built-in administrators
    - Power users

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

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

> ℹ️ *For more information, see the following:*
>
> - *Insert Remote PowerShell Commands at https://www.beyondtrust.com/docs/privilege-management/windows/admin/windows-policies/app-groups/remote-powershell-commands.htm*
> - *Access this Computer from the Network on Microsoft-us/previous-versions/windows/it-pro/windows-server-2003/cc740196(v=ws.10)*

Create Filters

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

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

- **Account Filter:** Restrict the Workstyle to specific users or groups of users.
- **Computer Filter:** Restrict the Workstyle to specific computers (names or IP addresses), or Remote Desktop clients.
- **WMI (Windows Management information) Filter:** Restrict the Workstyle based on the success or failure of a WMI query.

The following conditions can be applied to a filter:

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

Account Filters

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

There are two ways to add groups:

- Add local Active Directory domain groups and users
- Set up a connector that populates group information from your local Active Directory domains or your Microsoft Entra ID instance.

> ℹ️ *For more information, see Configure local AD connector.*

To create an account filter:

1. Expand a Workstyle, and then select **Filters**.
2. Click **Create New Filter**, and then select **Account Filter**.
3. Select the new filter in the list, and then select **Go To** from the menu.
4. Select the following to add users or groups:

   - **Add Account** (Windows): Add an account name and SID details. Click **Add Account**.
   - **Add Account from Search** (Windows): Select a connector from the list. Go to step 5.
   - **Add Account:** (macOS). Add the account or group details. User IDs on macOS must be values greater than 500. A value less than that might be used by a system process.

5. If you select **Add Account from Search**, select a connector on the **Add From AD Connectors** page. The default connector is **Built-In**. Enter search criteria in the **Account Name** box to find a specific account.
6. Select the account name, and then select **Add**.

Computer Filters

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

Computer filters can be configured on Windows and macOS computers.

To restrict the Workstyle to specific computers by IP address:

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

To restrict the Workstyle to specific computers by host name:

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

WMI Filters

A WMI filter is applied to a Workstyle based on the outcome of a WMI query.

When a WMI query runs, the client checks whether any rows of data are returned. If any data is returned, then the WMI query is successful. If no data is returned or an error is detected, the WMI query is unsuccessful.

WMI queries are always run as the Windows SYSTEM account, and cannot be executed against remote computers or network resources. WMI filters do not support impersonation levels, and can only be used with **SELECT** queries.

To create a WMI filter:

1. Expand a Workstyle, and then select **Filters**.
2. Click **Create New Filter**, and then select **WMI Filter**.
3. Click the **WMI Filter** link in the list. Alternatively, select **Go To** from the menu for that filter.
4. Click **Create New Query**.
5. Enter the following details:
   - **Description**: Free text to describe the WMI query.
   - **Namespace**: Set the namespace that the query runs against. By default, this is **root\CIMV2**.
   - **Query**: The WMI Query Language (WQL) statement to execute.
   - **Timeout**: The time (in seconds) the client waits for a response before terminating the query. By default, no timeout is set. Long running WMI queries result in delayed application launches. Therefore, we recommend setting a timeout to ensure that queries are terminated in a timely manner.
6. Click **Add Query**.

ℹ️ *For more information, see WMI (Windows Management information) Filters at https://www.beyondtrust.com/docs/privilege-management/windows/admin/windows-policies/workstyles/filters/wmi-filters.htm.*

Application Groups

Application Groups are used to define logical groupings of applications.

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

Overview

When working with Application Groups, you can:

- Create, edit, and delete application groups.
- Change the name or description of the group.
- Delete an application group when it is no longer required.
- Copy an application group, and then edit the properties of the newly created group.
- Copy application definitions from one group to another and from one policy to another.
- View hidden application groups.
- Use the search feature to find an application.
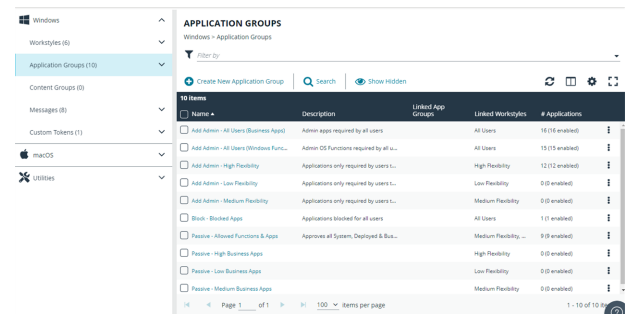
Create an Application Group

There are predefined application groups available that are already populated with applications and linked to workstyles. You can, however, create application groups and customize the application and associated properties.

1. On the **Policy Editor** page, expand **Windows** or **macOS**.
2. Click **Application Groups**.
3. Click **Create New Application Group**.
4. Add a name and description. Click **Create Application Group**.
5. The Application Group is now displayed in the navigation pane and the grid. You are now ready to add applications to the group.

Add an Application to an Application Group

There are three ways to add an application to a group:

- Application definitions: Create an application using the application definitions and properties.
- Reports: Add an application on-the-fly from the **Reports** page using the collected analytics.
- Application templates: Provides a way to pick from a list of known applications.

Copy Application Definitions

For ease-of-use, copy one or more application definitions to save time when setting up an application group. Copy to another application group in the same policy or another policy.
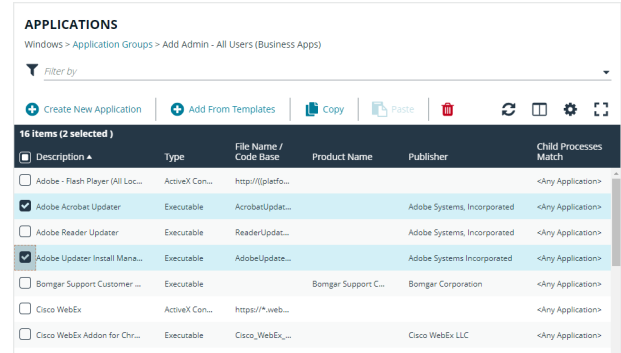
If the **Paste** button is not available, check the XML is a valid application definition. Copy the XML to a text editor to confirm.

Add an Application Using App Definitions

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

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

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

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

To add an application:

1. In the navigation pane, select the Application Group.
2. Click **Create New Application**, and then select the application type.
3. Enter a description in the **Application Description** box. Any value can be added here up to a maximum limit of 1024 characters. The description is not used in rule matching.
4. From the list of application definitions, configure the matching criteria.
5. (Optional) Configure the **Advanced Options**:
   - Allow child processes will match this application definition
   - Force standard user rights on File Open/Save common dialogs
6. Click **OK**.

Add an Application From Reports

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

1. In the console, select **Analytics** from the menu.
2. Expand **Events** and select **All** or **Process Detail**.

3. Select an event in the list and click **Add to Policy**. The Policy Editor opens.
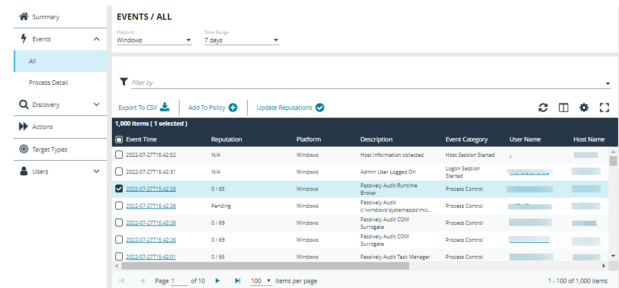
4. On the **Add Applications to Policy** page, select a policy and an application group.

5. Click **Add and Edit**. Alternatively, click **Add and Close** here which adds the application to the Application Group and redirects you back to the report.

6. The policy opens to the **Application Groups > Applications** page where you can edit the application settings. If you are adding one application, then you are directed to the application matching criteria page as shown.
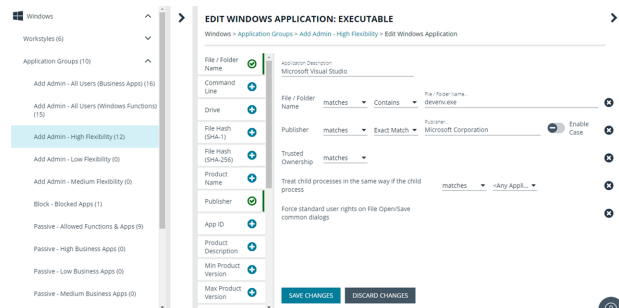
Add an Application From a Template

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

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

Disable an Application

You can temporarily pause the processing of an application rule against an application in an application group. Use this feature if you are rolling out or testing new rules. Disable the application while you investigate and fix any problems.

Environment Variables

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

To use the variables, enter the variable, including the % characters, into a file path or command line. Endpoint Privilege Management expands the environment variable prior to attempting a file path or command line match.

System Variables

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

User Variables

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

Advanced Options

Allow child processes will match this application definition

If selected, then any child processes that are launched from this application (or its children) will also match this rule. The rules are still processed in order, so it is still possible for a child process to match a higher precedence rule (or Workstyle) first. Therefore, this option will prevent a child process from matching a lower precedence rule.

If an application is launched by an on-demand rule and this option is selected, then the children are processed against the on-demand rules, and not the Application Rules. If this option is not selected, then the children will be processed against the Application Rules in the normal way. You can further refine this option by restricting the child processes to a specific Application Group. The default is to match <**Any Application**>, which will match any child process.

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

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

Force standard user rights on File Open/Save common dialogs

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

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

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

Application Definitions

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

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

Name	Description
ActiveX Codebase	When inserting ActiveX controls, this is enabled by default, and we recommend you use this option in most circumstances. You must enter the URL to the codebase for the ActiveX control. You can choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions** Although you can enter a relative codebase name, we strongly recommend you enter the full URL to the codebase, as it is more secure.
ActiveX Version	If the ActiveX control you entered has a version property, then you can choose **Check Min Version** and/or **Check Max Version** and edit the respective version number fields.
App ID	Matches on the App ID of the COM class, which is a GUID used by Windows to set properties for a CLSID. AppIds can be used by 1 or more CLSIDs. The available operators are identical to the File or Folder Name definition.
Application Requires Elevation (UAC)	Checks if an executable requires elevated rights to run and causes UAC (User Account Control) to trigger. This is a useful way to replace inappropriate UAC prompts with EPM end user messages to either block or prompt the user for elevation.
Application Requires Elevation (UAC)	Checks if an MSI requires elevated rights to run and causes User Account Control (UAC) to trigger. 📌 **Note:** *This is supported on install only.*

Name	Description
BeyondTrust Zone Identifier	Matches on the BeyondTrust Zone Identifier tag, where present. If an Alternate Data Stream (ADS) tag is applied by the browser, then also applies a BeyondTrust Zone Identifier tag to the file. The BeyondTrust Zone Identifier tag can be used as matching criteria if required.
CLSID	Matches the class ID of the ActiveX control or COM class, which is a unique GUID stored in the registry.
COM Display Name	If the class you entered has a Display Name, then it will automatically be extracted, and you can choose to match on this property. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a regular expression. The available operators are identical to File or Folder Name definition.
Command Line	If the filename is not specific enough, you can match the command line, by checking this option and entering the command line to match. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a regular expression. The available operators are identical to File or Folder Name definition. PowerShell removes double quotes from command strings prior to transmitting to the target. Therefore, we do not recommend that Command Line definitions include double quotes, as they will fail to match the command.
Controlling Process	Target content based on the process (application) that will be used to open the content file. The application must be added to an Application Group. You can also define whether any parent of the application will match the definition.
Drive	This option can be used to check the type of disk drive where the file is located. Choose from one of the following options: • **Fixed disk:** Any drive that is identified as being an internal hard disk. • **Network:** Any drive that is identified as a network share. • **RAM disk:** Any drive that is identified as a RAM drive. • **Any Removable Drive or Media:** If you want to target any removable drive or media, but are unsure of the specific drive type, choose this option which will match any of the removable media types below. Alternatively, if you want to target a specific type, choose from one of the following removable media types: ◦ **Removable Media:** Any drive that is identified as removable media. ◦ **USB:** Any drive that is identified as a disk connected by USB. ◦ **CD/DVD:** Any drive that is identified as a CD or DVD drive. ◦ **eSATA Drive:** Any drive that is identified as a disk connected by eSATA.
File or Folder Name	Applications are validated by matching the file or folder name. You can choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions**

Name	Description
	Although you can enter relative file names, we strongly recommend you enter the full path to a file or the COM server. Environment variables are also supported. We do not recommend you use the definition File or Folder Name **does NOT Match** in isolation for executable types, as it will result in matching every application, including hosted types, such as installer packages, scripts, batch files, registry files, management consoles, and Control Panel applets. When creating blocking rules for applications or content, and the **File or Folder Name** is used as matching criteria against paths which exist on network shares, this should be done using the UNC network path and not by the mapped drive letter.
File Hash (SHA-1 Fingerprint)	If a reference file was entered, then a SHA-1 hash of the PowerShell script is generated. This definition ensures the contents or the script file (which can normally be edited by any user) remain unchanged, as changing a single character in the script will cause the SHA-1 hash to change. While SHA-1 is supported, SHA-256 is recommended.
File Hash (SHA-256)	Set the SHA-256 file hash on an application. The SHA-256 hash is supported on all appropriate applications, both Windows and macOS operating systems. On the Windows operating system, you can select either **match** or **does NOT match**. The **does NOT match** setting is not available on macOS. We recommend using SHA-256 rather than SHA-1.
File Version	If the file, service executable, or COM server you entered has a File Version property, then it will automatically be extracted and you can choose Check Min Version and/or Check Max Version, and then edit the respective version number fields.
Parent Process	This option can be used to check if an application's parent process matches a specific Application Group. You must create an Application Group for this purpose or specify an existing Application Group in the Parent Process group. Setting match all parents in tree to True will traverse the complete parent/child hierarchy for the application, looking for any matching parent process, whereas setting this option to False will only check the application's direct parent process.
Product Code	If the file you entered has a Product Code, then it will automatically be extracted, and you can choose to check this code.
Product Description	If the file you entered has a Product Description property, then it will automatically be extracted, and you can choose to match on this property. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (? and *) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Product Name	If the file, COM server, or service executable you entered has a Product Name property, then it will automatically be extracted and you can choose to match on this property. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (? and *) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Product Version	If the file, COM server, or service executable you entered has a Product Version property, then it will automatically be extracted and you can choose Check Min Version and/or Check Max Version and edit the respective version number fields.
Publisher	Checks for the existence of a valid publisher. If you browsed for an application, then the certificate

Name	Description
	subject name will automatically be retrieved, if the application is signed. For Windows system files, the Windows security catalog is searched, and if a match is found, the certificate for the security catalog is retrieved. Publisher checks are supported on Executables, Control Panel Applets, Installer Packages, Windows Scripts, and PowerShell Scripts. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Service Actions	Define the actions which are allowed. Choose from: • **Service Stop:** Grants permission to stop the service. • **Service Start:** Grants permission to start the service. • **Service Pause / Resume:** Grants permission to pause and resume the service. • **Service Configure:** Grants permission to edit the properties of the service.
Service Display Name	Matches on the name of the Windows service, for example, **W32Time**. You may choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions**
Service Name matches	Matches on the name of the Windows service, for example, **W32Time**. You may choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions**
Source URL	Use to check where the application or installer was originally downloaded from if the application was downloaded using a web browser. The application is tracked by Endpoint Privilege Management at the point it is downloaded, so that if a user decided to run the application or installer at a later date, the source URL can still be verified. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a Regular Expression. The available operators are identical to the File or Folder Name definition.
Trusted Ownership	Use to check if an application's file is owned by a trusted owner (the trusted owner accounts are SYSTEM, Administrators, or Trusted Installer).
Upgrade Code	If the file you entered has an **Upgrade Code**, then it will automatically be extracted and you can choose to check this code.
Windows Store Application	Matches on the version of the Windows Store application, for example, **16.4.4204.712**. You can

Name	Description
Version	choose **Check Min Version** and/or **Check Max Version** and edit the respective version number fields.
Windows Store Package Name	Matches on the name of the Windows Store Application, for example, **microsoft.microsoftskydrive**. You can choose to match based on the following options (wildcard characters **?** and ***** may be used): • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions**
Windows Store Publisher	Matches on the publisher name of the Windows Store Application, for example, **Microsoft Corporation**. By default, a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a wildcard match (**?** and *****) or a Regular Expression. The other available operators are: • **Exact Match** • **Starts With** • **Ends With** • **Contains** • **Regular Expressions** The **Browse File** and **Browse Apps** options can only be used if configuring EPM settings from a Windows 8 client.

Application Details

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

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

Batch Files

Matching criteria

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches

- Source URL matches
- BeyondTrust Zone Identifier exists

COM Classes

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

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

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

Matching criteria:

- File or Folder Name matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Product Name matches
- Publisher matches
- CLSID matches
- App ID matches
- COM Display Name matches
- Product Description matches
- Product Version matches
- File Version matches
- Trusted Ownership matches
- Application Requires Elevation (UAC): Match if **Application Requires Elevation (User Account Control)** is always enabled, as COM classes require UAC to elevate
- Source URL matches

Control Panel Applet

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Product Name matches
- Publisher matches

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

Executables

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Product Name matches
- Publisher matches
- Product Description matches
- Product Version matches
- File Version matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Installer Package

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

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

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

TC: 4/25/2024

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

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

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

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Product Name matches
- Publisher matches
- Product Version matches
- Product Code matches
- Upgrade Code matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Insert Endpoint Privilege Management Policy Editor Snap-ins

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Publisher matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

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

28

TC: 4/25/2024

Management Console

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Publisher matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

PowerShell Scripts

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

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

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Publisher matches
- Trusted Ownership matches
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

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

29

Example PowerShell Configurations

Create New Configuration, Save to Local File

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


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

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

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

## Add Message ##
# Create a new message object
$PGMessage = New-Object Avecto.Defendpoint.Settings.message $PGConfig
#Define the message Name, Description and OK action and the type of message
$PGMessage.Name = "Elevation Prompt"
$PGMessage.Description = "An elevation message"
$PGMessage.OKAction = [Avecto.Defendpoint.Settings.Message+ActionType]::Proceed
$PGMessage.Notification = 0
# Define whether the message is displayed on a secure desktop
$PGMessage.ShowOnIsolatedDesktop = 1
# Define How the message contains
$PGMessage.HeaderType = [Avecto.Defendpoint.Settings.message+MsgHeaderType]::Default
$PGMessage.HideHeaderMessage = 0
$PGMessage.ShowLineOne = 1
$PGMessage.ShowLineTwo = 1
$PGMessage.ShowLineThree = 1
$PGMessage.ShowReferLink = 0
$PGMessage.ShowCancel = 1
$PGMessage.ShowCRInfoTip = 0
```

```
# Define whether a reason settings
$PGMessage.Reason = [Avecto.Defendpoint.Settings.message+ReasonType]::None
$PGMessage.CacheUserReasons = 0
# Define authorization settings
$PGMessage.PasswordCheck =
Avecto.Defendpoint.Settings.message+AuthenticationPolicy]::None
$PGMessage.AuthenticationType = [Avecto.Defendpoint.Settings.message+MsgAuthenticationType]::Any
$PGMessage.RunAsAuthUser = 0
# Define Message strings
$PGMessage.MessageStrings.Caption = "This is an elevation message"
$PGMessage.MessageStrings.Header = "This is an elevation message header"
$PGMessage.MessageStrings.Body = "This is an elevation message body"
$PGMessage.MessageStrings.ReferURL = "http:\\www.bbc.co.uk"
$PGMessage.MessageStrings.ReferText = "This is an elevation message refer"
$PGMessage.MessageStrings.ProgramName = "This is a test Program Name"
$PGMessage.MessageStrings.ProgramPublisher = "This is a test Program Publisher"
$PGMessage.MessageStrings.PublisherUnknown = "This is a test Publisher Unknown"
$PGMessage.MessageStrings.ProgramPath = "This is a test Path"
$PGMessage.MessageStrings.ProgramPublisherNotVerifiedAppend = "This is a test verification
failure"
$PGMessage.MessageStrings.RequestReason = "This is a test Request Reason"
$PGMessage.MessageStrings.ReasonError = "This is a test Reason Error"
$PGMessage.MessageStrings.Username = "This is a test Username"
$PGMessage.MessageStrings.Password = "This is a test Password"
$PGMessage.MessageStrings.Domain = "This is a test Domain"
$PGMessage.MessageStrings.InvalidCredentials = "This is a test Invalid Creds"
$PGMessage.MessageStrings.OKButton = "OK"
$PGMessage.MessageStrings.CancelButton = "Cancel"
# Add the PG Message to the PG Configuration
$PGConfig.Messages.Add($PGMessage)

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

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

## Add Policy Rule ##
```

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

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

Open Local User Policy, Modify then Save

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

Open Local Configuration and Save to Domain GPO

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

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

32

Registry Settings

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Remote PowerShell Commands

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

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

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

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

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

ℹ️ *For more information, see:*

- *"Application Definitions" on page 21 for more about command line matching.*
- *To manage remote PowerShell scripts instead of a single cmdlet, see "Insert Remote PowerShell Scripts" on page 34.*

Messaging

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

Insert Remote PowerShell Scripts

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

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

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

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

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

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

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

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

Matching criteria:

- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Publisher matches

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

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

Messaging

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

Uninstaller (MSI or EXE)

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

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

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

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

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

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

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

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

Upgrade Considerations

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

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

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

1. Select the Application Group you want to add the uninstaller to.
2. Right-click and select **Insert Application** > **Uninstaller**.
3. Enter a description, if required. By default, this is the name of the application you are inserting.
4. Click **Browse File** to select an uninstaller file and populate the available matching criteria for the selected uninstaller file.

5. Configure the matching criteria for the executable. You can configure:

- **File or Folder Name matches**
- **Upgrade Code matches**
- **Product Name matches**
- **Publisher matches**

Windows Services

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

Matching criteria:

- File or Folder Name matches
- Command Line matches
- Drive matches
- File Hash (SHA-1) matches
- File Hash (SHA-256) matches
- Product Name matches
- Publisher matches
- Product Description matches
- Product Version matches
- File Version matches
- Service Name matches
- Service Display Name matches
- Service Actions match

Windows Store Applications

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

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

Windows Scripts

Matching criteria:

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

- File Hash (SHA-256) matches
- Publisher matches
- Trusted Ownership matches
- Application Requires Elevation (UAC)
- Parent Process matches
- Source URL matches
- BeyondTrust Zone Identifier exists

Content Groups

Build a Content Group using the definitions provided to control access to privileged content. Content Groups are added to a Content Rule in a Workstyle. When matches are detected on computers receiving the policy, the rule triggers and the rule behavior applies (allow or block rule).

There are two main use cases for applying content control:

- Allow modification: Allows standard users to modify privileged content, without having to assign admin rights to either the user, or the application used to modify the content.

  Add a Content Group to a content rule where the content can be assigned admin rights. When this is done, any user who receives the Workstyle can modify matching content without requiring an administrator account.

- Block access to content or directories.

  Add a Content Group to a content rule where the ability to open the content can be controlled with a Block action. When this is done, any user who can open and read the content is blocked from opening the content.

Content Definitions

A Content Group is composed of one or more definitions. All definitions that make up a Content Group must match before the Content Rule triggers.

The following content definitions are available:

- File or Folder Name
- Drive
- Controlling Process

Review the next sections to learn more before building a Content Group.

File or Folder Name

Validate applications by matching the file or folder name. You can choose to match based on the following options (wildcard characters **?** and ***** may be used):

- **Exact Match**
- **Starts With**
- **Ends With**
- **Contains**
- **Regular Expressions**

Although you can enter relative filenames, we strongly recommend that you enter the full path to a file or the COM server. Environment variables are also supported.

We do not recommend using the **File or Folder Name does NOT Match** definition in isolation for executable types, as it results in matching every application, including hosted types such as Installer packages, scripts, batch files, registry files, management consoles, and Control Panel applets.

When creating blocking rules for applications or content, and using the **File or Folder Name** definition as matching criteria against paths which exist on network shares, use the Universal Naming Convention (UNC) network path rather than a mapped drive letter.

Drive

Verify the type of disk drive where the file is located. Choose from one of the following options:

- **Fixed disk:** Any drive that is identified as being an internal hard disk.
- **Network:** Any drive that is identified as a network share.
- **RAM disk:** Any drive that is identified as a RAM drive.
- **Any Removable Drive or Media:** If you want to target any removable drive or media, but are unsure of the specific drive type, this option will match any of the removable media types below. Alternatively, if you want to target a specific type, choose one of the following removable media types:
  - **Removable Media:** Any drive that is identified as removable media.
  - **USB:** Any drive that is identified as a disk connected via USB.
  - **CD/DVD:** Any drive that is identified as a CD or DVD drive.
  - **eSATA Drive:** Any drive that is identified as a disk connected via eSATA.
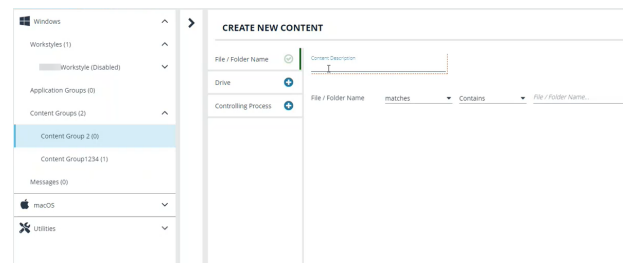
Controlling Process

Use this definition to target content based on the process (application) used to open the content file. The application must have been added to an Application Group. You can also define whether any parent of the application matches the definition.

Create a Content Group

> **⊙ IMPORTANT!**
>
> *We recommend adding a controlling process for each content definition. If a controlling process is not added to a content definition, then performance issues can occur on computers the policy is applied to.*

1. Expand the Windows panel of the Policy Editor.
2. Click **Content Groups**, and then click **Create New Content Group**.
3. Enter a name, and then click **Create Content Group**.
4. Select the saved content group, and then click **Create New Content**.
5. Configure the definitions.
6. Click **Create Content**.

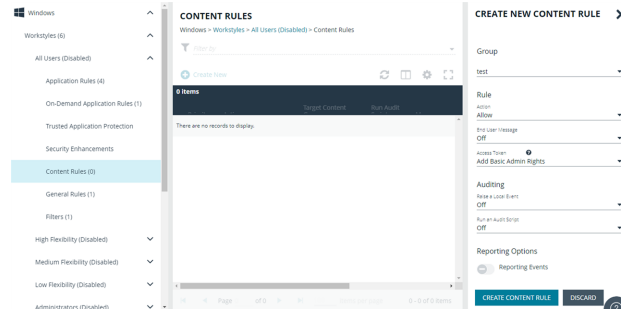
After the content is added, add the Content Group to an existing Content Rule or create a new one.

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

39

TC: 4/25/2024

Create a Content Rule

1. Expand a Workstyle, and then go to **Content Rules**.

2. Click **Create New**.

3. Select the rule properties:

- **Group**: Select a Content Group.

- **Action**: Select **Allow** or **Block**. The action that occurs if the content in the Content Group is accessed by the end user.

- **End User Message**: Select a message from the list.

- **Access Token**: Select the type of token to pass to the Content Group. You can select from:

  - **Passive** (no change): Doesn't make any change to the user's token. This is essentially an audit feature.

  - **Enforce User's Default Rights**: Removes all rights and uses the user's default token. Windows UAC always tries to add administration rights to the token being used so if the user clicked on an application that triggers UAC, the user cannot progress past the UAC prompt.

  - **Drop Admin Rights**: Removes administration rights from the user's token.

  - **Add Full Admin (Required for installers)**: Standard Windows Admin token containing all Admin privileges.

  - **Add Basic Admin Rights**: Gives greater control over the privileges granted when targeting rules at actions. This excludes the following privileges: **SeDebugPrivilege**, **SeLoadDriverPrivilege**.

  - **Endpoint Privilege Management Support Token**: Applies Add Full Admin privileges with tamper protection removed.

  - **Keep Privileges - Enhanced**: Keeps the same privileges of the process token and adds some additional context to it. Use the token with features such as Advanced Parent Tracking or Anti-tamper.

- **Raise a Local Event**: **Off**, **On**, **Anonymous**. Select if an event is raised if this Content Rule is triggered. When on, an event is sent to the local event log file. Anonymous removes user and host name from events so the user / host are not identifiable.

- **Run an Audit Script**: Select an audit script from the list.

- **Reporting Events**: When the setting is on, events are raised for viewing in Endpoint Privilege Management app reporting.

4. Click **Create Content Rule**.

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

40

TC: 4/25/2024

Messages

You can define two types of end user messages:

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

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

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

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

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

Create a Message

> 📌 ***Note:*** *Message templates vary between Windows and macOS.*

1. In the Policy Editor, go to **Messages**.
2. Click **Create New Message** (Windows options shown in image at right).
3. (Windows only). Select a message type: *message box* or *notification*.
4. Select a message template from the list.
5. Enter a name. The default name is the name of the template.
6. Enter a description.
7. (Windows only). Enter the title that displays in the title bar of the window.
8. Enter text for the message header.
9. Enter text for the body.
10. (Windows only). Select **Show Message On Secure Desktop** to show the message on the secure desktop.
11. (Windows only). Turn off **Show the details of application being executed** to hide the details from being displayed. This option is enabled by default.
12. Click **Create New Message**.

You can edit or delete messages at any time.

> 💡 **Tip:** Click **Preview** when editing a message to view a draft. Message preview is available for Windows and macOS messages.

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

42

TC: 4/25/2024

Manage Languages

You can configure message text to display a language of your choice. Click **Add Languages** and select the language from the dropdown list.

If you are using more than one language, select a language and click **Set As Default**. The default language is English.

If you delete the default language, then the language at the top of the list is set to the default. You must always have at least one language selected.
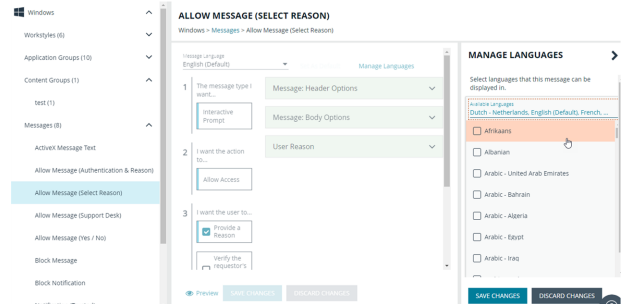
The Endpoint Privilege Management app checks the locale of the user's language and tries to match it to a language set up in the app.

- If there is a match, the strings for that language are displayed for the message text.
- If there isn't a match, the language assigned as the default language is used.

The Endpoint Privilege Management app does not localize the text in the language you select. You must edit the message text in your chosen language.

If you import a policy with messages in a supported language, then the strings display in that language. The screen capture shows an example where a policy file was imported in Dutch.
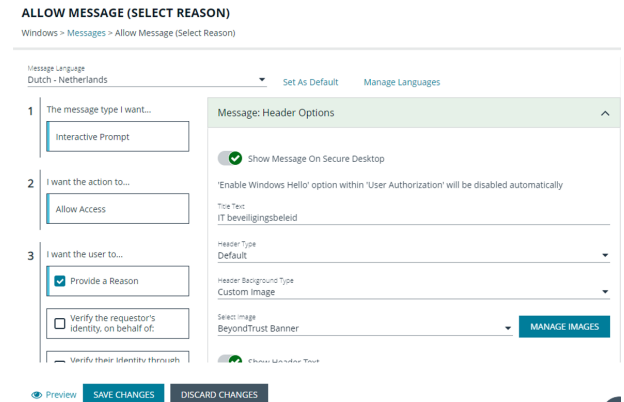
Add ActiveX Message

When you are elevating the installation of an ActiveX control in an application group, a built-in progress dialog box displays during the installation. You can customize the messaging on the installation progress dialog box.

ActiveX messages can be displayed in multiple languages. The regional language of the end user can be detected, and if ActiveX strings in that language are configured, the correct translation is displayed.

> 📌 **Note:** *If language settings for the region of the end user are not configured, then the default language text is displayed. To change the default language, select a language and click **Set Default**.*

To create an ActiveX message:

1. Go to the **Messages** tab, and then click **Create New Message**.
2. Select **Use ActiveX Control** from the list.
3. Fill in the text fields that will display on the dialog box.
4. Click **Create New Message**.
5. If you want to select a language other than English, click the newly created message in the navigation panel, and then click **Manage Languages**.
6. Select and save the language.

Customize a Message

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

- General message features such as **Header** and **Body** options.
- **User Reason** settings when you want your end users to provide a reason before proceeding.
- **User Authorization** where a user must provide password, smart card, or both types of authentication information.
- **Multifactor Authentication** where an Identity Provider is configured.
- **Challenge/Response Authorization** where a user must enter a response code before proceeding.

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

Set up the Message Header Options

You can configure the following message header options:

- **Show Message On Secure Desktop:** (Windows only). Select to show the message on the secure desktop. We recommend this if the message is being used to confirm the elevation of a process, for enhanced security.
- **Title Text:** (Windows only). Add text that appears in the title bar of the dialog box.
- **Header Type:** Select the type of header: **Default**, **Error**, **None**, **Question**, **Warning**.
- **Header Background Type:** Select **Solid** or **Custom Image**.
    - If you select **Solid**, use the color picker to select a header background color.
    - If you select **Custom Image**, you must select an image from the **Select Image** dropdown list. To use additional images, see "Manage Images" on page 45.
- **Show Header Text:** Select if you want to display header text.
- **Header Text:** Add text that displays next to the header type icon.
- **Header Text Color:** Select the color for the header text.

> 📌 **Note:** *(Windows only). For a **Notification** type of message, you can only configure the **Title Text**.*

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

Manage Images

To use different images in the header than the default BeyondTrust ones (such as your own company's logo, for branding purposes), you can import images into the **Manage Images** list.

Image requirements:

- File type must be **.png**
- Maximum file size is 240KB
- Recommended size is 450x50 pixels
- Images smaller than 450x50 pixels and greater than 600x100 pixels will be rejected.

To upload an image:

1. To the right of the **Select Image** field, click **Manage Images**.
2. Click **Import Image**.
3. On the **Upload Image** panel, drag or click to select an image to upload.
4. Enter the image name and a description.
5. Click **Upload Image**. The image is added to the list and is available for selection as a custom image.

You can delete images you imported. You cannot delete the BeyondTrust images.

To delete an image:

1. To the right of the **Select Image** field, click **Manage Images**.
2. Select an image. You cannot delete an image already in use. Select another image to use before proceeding.
3. Click the **Delete** button.

Edit an Image

To edit an image that you uploaded:

1. To the right of the **Select Image** field, click **Manage Images**.
2. Select the image, and then select **Edit** from the menu.
3. Update the name and/or description for the image, and then click **Save Changes**.

Set up the Message Body Options

You can configure the following message body options:

- **Body Text:** Add additional information for the end user.
- **Message Mode:** (Windows only). From the list, select **Automatic** or **Custom**. You can decide what information you want to display on the message. By default, all rows are *on* and will be displayed as part of the message. The **Automatic** default values are:
  - **Show Line One:** The *Program Name* or the *Content Name*.
  - **Show Line Two:** The *Program Publisher* or the *Content Owner*.
  - **Show Line Three:** The *Program Path* or the *Content Program*.

- **Show Reference Hyperlink:** Turn the option *on* (it is *off* by default). Update text for existing link on the message. In some cases, you might want to provide a website with more information for your end users. The URL appears *below* the body text.

> *Example:* Here are some link ideas.
> - *Web pages that provide support resources, terms of use statements, and web-based submission forms*
> - *Web-based ITSM solutions, including those that support parameterization of URLs for prepopulation of fields*
> - *Teams and other community support products*
> - *Email via mailto links, for integration with email based ITSM solutions*

- **Publisher:** Enter a publisher name and information to display if the verification for the publisher fails.
- **Buttons:** Customize the labels for the **OK** and **Cancel** buttons (Mac sample message shown in image at right).

> *Note:* (Windows only). For a **Notification** type of message, you can only configure the **Body Text**.

Additional body message design properties are available when using the **User Request Message** template. You can customize the text for the interactive prompts displayed during the request workflow, such as *request text*, *pending text*, *approval text*, *denial text*, and *referral text*.
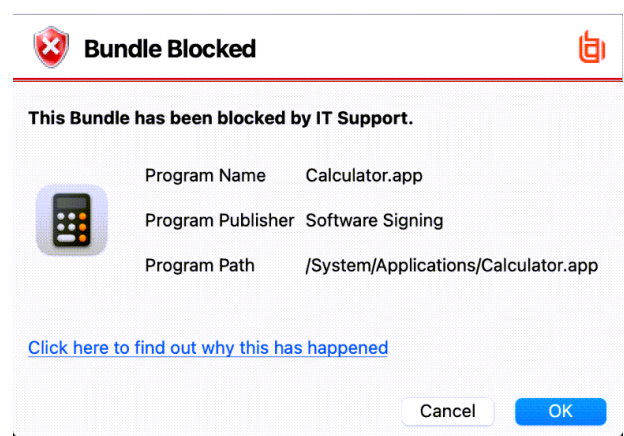
> *Tip:* Click **Preview** when editing a message to view a draft. Message preview is available for Windows and macOS messages.

Add User Reason

You can configure the message to prompt the user to provide a reason for the request.

To set up the User Reason option:

1. Under section 3 on the left, check the **Provide a Reason** box.
2. Select the **User Reason Type**, a *textbox* or a *dropdown*.
3. (Optional). Select if you want to **Remember the User Reason (per application)**.
4. (Optional). You can change the default **Reason Text** and **Reason Error Message Text**.
5. (Optional). If you select the *drop-down* type, you can change the default **Drop-down List Prompt Text**.
6. (Optional). With the drop-down option, you can use the default **User Reason List** to be displayed for the user to choose from. You can also:

   - Change the text of the default list options.
   - Delete one or more of the default options.
   - Click the **Add User Reason** option to add your own user reason to the list.
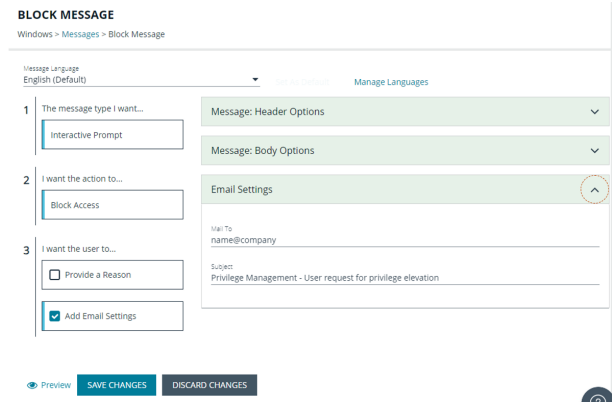
7. Click **Save Changes**.

Email Settings (Windows Only)

Email settings can be configured when using the Block Message template.

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

Configure the following:

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

Add Challenge/Response Authorization

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

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

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

To add a shared key:

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

To configure Challenge/Response Authorization:

1. In the Policy Editor, click **Messages**.
2. Create a message following the steps provided earlier. If this is an existing message, select **Edit** from the menu.
3. Under section 3 on the left, check the **Request Access via Challenge/Response** box.

TC: 4/25/2024

4. Open the **Challenge / Response Authorization** dropdown, and set the following:

- **Header text:** The text that introduces the challenge/response authorization.
- **Hint text:** The text that is in the response code field for challenge/response messages.
- **Authorization Period (per application):** Set this option to determine the length of time a successfully returned challenge code is active for.
  - **One Use Only:** A new challenge code is presented to the user on every attempt to run the application.
  - **Entire Session** (Windows only): A new challenge code is presented to the user on the first attempt to run the application. After a valid response code is entered, the user is not presented with a new challenge code for subsequent uses of that application until they next log on.
  - **As defined by helpdesk** (Windows only): A new challenge code is presented to the user on the first attempt to run the application. If this option is selected, the responsibility of selecting the authorization period is delegated to the helpdesk user at the time of generating the response code. The helpdesk user can select one of the three above authorization periods. After a valid response code is entered, the user does not receive a new challenge code for the duration of time specified by the helpdesks.
- **Suppress messages once authorized** (Windows only): Select to suppress messages. This setting is not shown when set to **One Use Only**.
- **Show Information Tip** (Windows only): Select to add helpful information for the end user.
- **Information Tip Text:** Add text that appears above the challenge and response code fields. In Windows, this only appears if the **Show Information Tip** option above is selected.
- **Error Message Text:** Add text to display to the end user if they enter an incorrect response code.
- **Maximum Attempts:** Select from **Unlimited** and **Three Attempts**.
- **Maximum Attempts Exceeded Message Text:** The message is only displayed when **Three Attempts** is selected. Add text to display to the end user if they exceed the allowed number of challenge/response attempts.

> **Tip:** Click **Preview** when editing a message to view a draft. Message preview is available for Windows and macOS messages.

Add User Authorization

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

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

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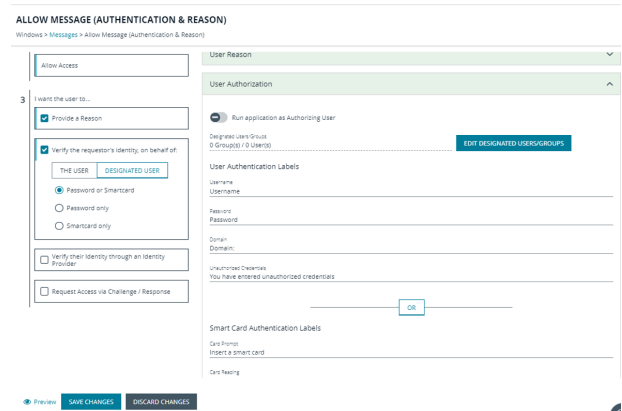4. Select the authorization method: **Password or Smartcard**, **Password only**, or **Smartcard only**.
5. Click **User Authorization** to expand and customize labels and descriptions. The available fields will change depending on which method of authorization is selected, as noted here:

   - **The User:** When selected, enter the password. Optionally, customize the message that displays to users when the credentials are not approved.
   - **Designated User:** When selected, click the **Edit Designated Users/Groups** button to add the authorized users/groups. A designated user can be selected from a local account, Active Directory domain, or Azure Active Directory. Only Azure Active Directory groups are supported.

     - After the groups are added, enter the *user name*, *password*, and *domain*.
     - (Optional). Select **Run application as Authorizing User**. When selected, the application runs in the context of the authenticating user. When not selected, the application runs in the context of the logged on user.
     - (Optional). Customize the message that displays to users when the credentials are not approved.

   - **Windows Hello:** Select to use the Windows Hello service to authenticate the user. Windows Hello must be installed on the endpoint to use this feature.

     - Windows Hello is not supported with the **Designated User** option.
     - Set Authentication to the **Password or Smartcard** or the **Password only** option.
     - Windows Hello is unavailable when using Secure Desktop.

   - **TouchID:** Select to use TouchID to authenticate the user. TouchID must be configured on the endpoint to work with the policy editor messages.

     - TouchID is not supported with the **Designated User** option.
     - Set Authentication to the **Password or Smartcard** or the **Password only** option.

   - **Smart Card:** When smart card authorization is included, you can:

     - (Optional). Customize the **Smart Card Authentication Labels** that display to the user. The hint field is only displayed if your smart card authentication environment is configured to use them.
     - (Mac only). Select the **Sudo User Authorization** option.

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

Edit Designated Users

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

There are two ways to add groups:

- Add local Active Directory domain groups and users
- Set up a connector that populates group information from your local Active Directory domains or your Microsoft Entra ID instance.
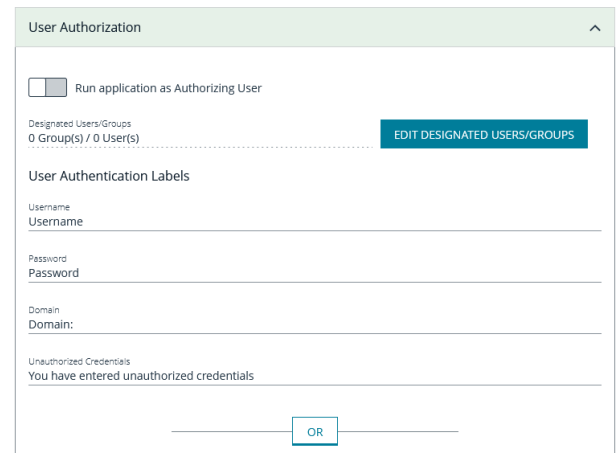
> For more information, see *Configure local AD connector*.

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

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

2. Select one of the following:
   - **Add Account**: Add an account name and SID details. Click **Add Account**.
   - **Add Account from Search**: Select a connector on the **Add From AD Connectors** page. The default connector is **Built-In**. Enter search criteria in the **Account Name** box to find a specific account. Select the account name, and then select **Add**.

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

50

TC: 4/25/2024

3. Select **User** or **Group**, and then add the information.

4. If you select a built-in group, click **Insert** to automatically populate the account name and security identifier (SID).

5. After providing account the information, click **Add Account**.

6. After adding your accounts, click **Save Changes** to return to the message configuration page.
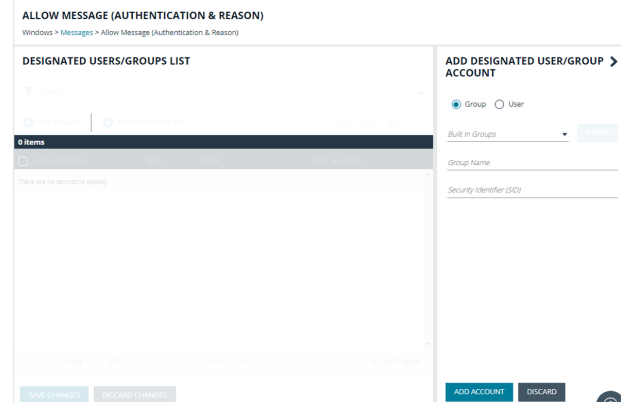
7. Click **Save Changes** again to close the message configuration page.

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

Configure Multifactor Authentication Using an Identity Provider

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

The RADIUS protocol is supported on Windows OS only.

Add an Identity Provider

1. In the Policy Editor, click **Messages**.
2. Click **Identity Provider Settings**.
3. On the **Identity Provider Settings** panel, select an identity provider from the list: **OIDC** or **RADIUS**.
4. Enter the following details for the identity provider:

   - **OIDC** Settings
     - **Authority URI:** The address of your identity provider.
     - **Client ID:** Must match the same value configured for your identity provider's BeyondTrust application.
     - **Redirect URI:** Must match the same value configured for your identity provider's BeyondTrust application. The format is **http://127.0.0.1:***port_number***, where *port_number* is an open port on your network. The *port_number* is only needed if required by your identity provider.

   - **RADIUS** Settings
     - **Authentication Mechanism:** The authentication type that is required by your RADIUS server. Supported authentication mechanisms are MS-CHAPV2 or PAP.
     - **Host:** The hostname of your RADIUS server.
     - **Port:** The port number for connecting to your RADIUS server.
     - **Shared Secret:** The secret key required by your RADIUS server.

5. Click **Save RADIUS Settings** or **Save OIDC Settings** depending on the type you selected.

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

Set up a Multifactor Authentication Message

1. In the Policy Editor, click **Messages**.
2. Click **Create New Message**.
3. Select the template **Allow Message (with Authentication)**, and then click **Create New Message**.
4. Select the message in the **Messages** navigation pane.
5. Under section 3 on the left, check the **Verify their Identity through an Identity Provider** box.
6. Expand **Multifactor Authentication**.
7. Select **Idp - OIDC** or **Idp - RADIUS**.
8. In the **Suppress Message when Authenticated for (Mins)** box, enter a value (maximum 720) to set the number of minutes that the authentication message is suppressed. The message will not be shown again for the given number of minutes after a successful authentication.
9. Enter information that displays on the message dialog box such as authentication failure text and authentication success text. Optionally, you can use the default text provided.
10. Enter the ACR value. The value is optional and required only if your identity provider uses it.
11. Click **Save Changes**.

Custom Tokens

A token is assigned to an application to change the privileges associated with the activity permitted for that application. Create a custom token to manually configure group membership, privileges, and process access rights.

Custom tokens can be used with on-demand rules, application rules, and content rules. By design, custom tokens only work for *allow* rules.

Changing the properties of an access token is designed for more advanced configurations.

Here are some scenarios on customizing the properties of a token:

- Run remote PowerShell commands and scripts with a custom token that removes the SeRemoteShutDown privilege. This prevents the commands and scripts from shutting down servers during core business hours, even if the command or script indicates to do so.
- Create a custom token to run an application with custom privileges configured in the token. The user can run the application but with modified privileges as configured in the token.

Create a Custom Token

You can select from a list of Windows access tokens as the foundation to creating the custom token. After selecting the token, customize the following properties: group, privileges, and process access rights.

- Groups: Add local or Active Directory domain groups to the token.
- Privileges: Add or remove privileges that will be applied to the application.
- Process access rights: The process access rights allow you to choose the rights other processes have over a process launched with that custom token.
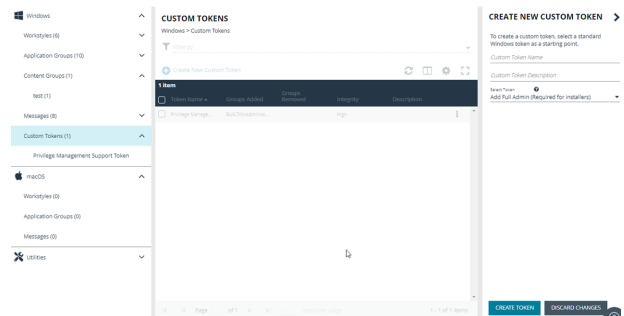
Create a Token

Follow these steps to create custom tokens according to your needs:
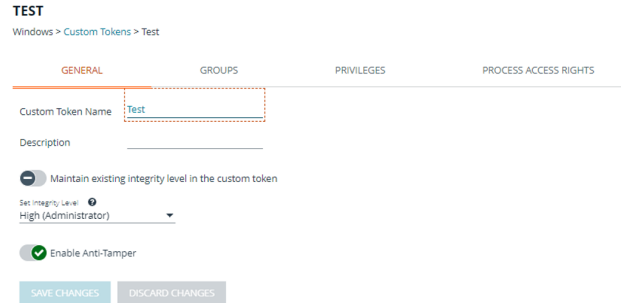
1. Navigate to the policy and click **Custom Tokens**.
2. Click **Create New Custom Token**.
3. Enter a name and description.
4. Select the level of permissions for the token:
   - **Add Full Admin (Required for installers)**: Preselected Windows administrator privileges.
   - **Drop Admin Rights**: Preselected Windows privileges that do not include administrator privileges.
   - **Blank**: Select this option to personalize the privileges for the token.
5. Click **Create Token**.
6. On the main **Custom Tokens** page, select the token and click **Edit** from the menu.
7. See the following sections for more details on the properties to configure.

TC: 4/25/2024

Set Integrity Level and Anti-Tamper

Follow these instructions to fine-tune your token settings for optimal application performance and security:

1. Click the **General** tab.
2. Select an integrity level or select **Maintain existing integrity level in the custom token** to use the existing Windows integrity level for the selected token type.

   - **System**: Included for completion and is not required.
   - **High**: Set the integrity level associated with an administrator.
   - **Medium**: Set the integrity level associated with a standard user.
   - **Low**: Set the integrity level associated with protected mode (an application might fail to run or function in protected mode)
   - **Untrusted**: Included for completion and is not required.

3. By default, anti-tamper protection is on. Anti-tamper protection prevents elevated processes from tampering with the files, registry, and service that make up the client installation. It also prevents any elevated process from reading or writing to the local policy cache.

   Keep anti-tamper enabled, except in scenarios where elevated tasks require access to protected areas, such as when using an elevated logon script to update the local policy.

4. Click **Save Changes**.

Add Groups

There are two ways to add groups:

- Add local Active Directory domain groups and users
- Set up a connector that populates group information from your local Active Directory domains or your Microsoft Entra ID instance.

> ℹ️ *For more information, see Configure local AD connector.*

1. If you want the user to be the owner, regardless of the presence of the administrators group, select **Ensure the User is always the Token Owner**.

   By default, the owner of a custom token that includes the administrators group has the owner set to the administrators group. If the administrators group is not present in the custom token, then the user is set as the owner.

2. Select one of the following:

   - **Add Account**: Add an account name and SID details. Click **Add Account**.

   - **Add Account from Search**: Select a connector on the **Add From AD Connectors** page. The default connector is **Built-In**. Enter search criteria in the **Account Name** box to find a specific account. Select the account name, and then select **Add**.

3. Select from a list of known Active Directory Built-in groups.

4. Click **Add Account**.

5. Click **Save Changes**.
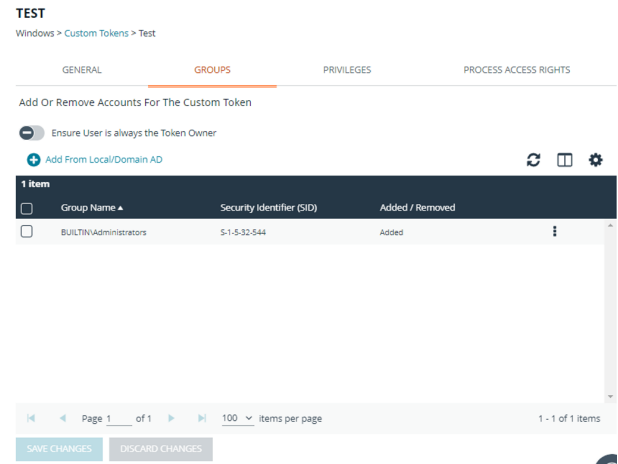
Change Privileges

On the **Privileges** tab, select the privileges to add to or remove from the custom token.

1. Select a privilege, and then select

   - **Add Privilege** to add the privilege to the custom token.

   - **Remove Privilege** to remove the privilege to the custom token.

2. To reset the default state of a privilege, select the privilege and select **No Change**.

3. Click **Remove all existing privileges in Custom Token before applying privileges** to clear all privileges in the custom token before applying privileges. If not selected, the privileges are added or removed from the user's default custom token.
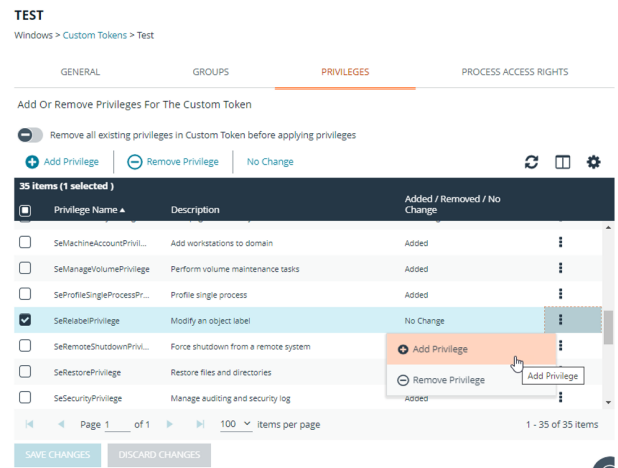
Change Process Access Rights

The process access rights allow you to select the rights other processes have over a process launched with a custom token.

Tokens that include the administrators group have a secure set of access rights applied by default, which prevents code injection attacks on elevated processes initiated by processes running with standard user rights in the same session.

A custom token requires at least one enabled access right. If all access rights are disabled, then the default access rights are enabled: GENERIC_ READ, READ_CONTROL, and SYNCHRONIZED. Edit the access rights if you do not want to use the default values.

TEST
Windows > Custom Tokens > Test

| GENERAL | GROUPS | PRIVILEGES | PROCESS ACCESS RIGHTS |

Select Which Process Access Rights Are To Be Enabled Or Disabled For The Custom Token

15 items

	Access Right Name ▲	Description	Enabled / Disabled	
☐	GENERIC_READ	Read access	Enabled	⋮
☐	PROCESS_CREATE_PROCESS	Required to create a process	Disabled	⋮
☐	PROCESS_CREATE_THREAD	Required to create a thread	Disabled	⋮
☐	PROCESS_DUP_HANDLE	Required to duplicate a handle using...	Disabled	⋮
☐	PROCESS_QUERY_INFORMATION	Required to retrieve certain informat...	Disabled	⋮
☐	PROCESS_QUERY_LIMITED_INFORM...	Required to retrieve certain informat...	Disabled	⋮
☐	PROCESS_SET_INFORMATION	Required to set certain information ...	Disabled	⋮
☐	PROCESS_SET_QUOTA	Required to set memory limits using ...	Disabled	⋮

|◄ ◄ Page 1 of 1 ► ►| 100 ⌄ items per page   1 - 15 of 15 items

| SAVE CHANGES | DISCARD CHANGES |

Access Rights

Access Rights	Description
GENERIC_READ	Read access.
PROCESS_CREATE_PROCESS	Required to create a process.
PROCESS_CREATE_THREAD	Required to create a thread.
PROCESS_DUP_HANDLE	Required to duplicate a handle using **DuplicateHandle**.
PROCESS_QUERY_INFORMATION	Required to retrieve certain information about a process, such as its token, exit code, and priority class.
PROCESS_QUERY_LIMITED_ INFORMATION	Required to retrieve certain information about a process.
PROCESS_SET_INFORMATION	Required to set certain information about a process, such as its priority class.
PROCESS_SET_QUOTA	Required to set memory limits using **SetProcessWorkingSetSize**.
PROCESS_SUSPEND_RESUME	Required to suspend or resume a process.
PROCESS_TERMINATE	Required to terminate a process using **TerminateProcess**.
PROCESS_VM_OPERATION	Required to perform an operation on the address space of a process.
PROCESS_VM_READ	Required to read memory in a process using **ReadProcessMemory**.
PROCESS_VM_WRITE	Required to write to memory in a process using **WriteProcessMemory**.
READ_CONTROL	Required to read information in the security descriptor for the object, not including the information in the SACL.
SYNCHRONIZE	Required to wait for the process to terminate using the wait functions.

Policy Editor Utilities

Licensing

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

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

To add a license:

1. Go to the **Policies** page and then select **Edit & Lock Policy** for the policy you want to edit.
2. Expand the **Utilities** node.
3. Click the **Licenses** node.
4. Click **Add**.
5. Enter the license key, and then click **Add License**.

Import Policy

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

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

Import Template Policies

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

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

4. Select a template from the list: **Discovery**, **QuickStart for Mac**, **QuickStart for Windows**, **Server Roles**, **TAP (High Flexibility)**, **TAP (High Security)**.

5. If you are merging, select **Merge Template Policy** to save the settings. If you are overwriting, select **Overwrite Policy**.

Manage Audit Scripts

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

1. In the Policy Editor, expand the **Utilities** node.

2. Select **Manage Audit Scripts**.

3. Click **Upload Script** to expand the Upload Script panel.

4. Click the following menus to further configure the script:

   - **Timeout Options**
   - **Context Options**

5. Click inside the upload box to select the script.

Manage Rule Scripts

You can upload, view, and delete Power Rules in the Policy Editor.

The script must be a Windows PowerShell script in JSON format.

1. In the Policy Editor, expand **Utilities**.

2. Select **Manage Rule Scripts**.

3. Click **Upload Script** to expand the **Upload Script** panel.

4. Select a value from the **Timout options** list.

5. Drag and drop the new script into the upload box or click to select a file.

6. Click **Upload Script** to save your changes.

After a script is uploaded, you can delete or upload an updated script at any time.

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

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

59

TC: 4/25/2024

Advanced Agent Settings

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

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

Set Up Agent Protection

Add agent protection to your endpoints to prevent admin users from tampering with the product, including stopping the services running or deleting its files from an endpoint.

EPM components protected and the level of protection are provided in the table.

Action	EPM Component
Blocks uninstalls	- Defendpoint client - PMC adapter - AD connector - Package Manager
Prevents stopping services	- Defendpoint client - BeyondInsight adapter - ePO service
Blocks DLL injections	- Defendpoint client - PMC adapter - ePO service - BeyondInsight adapter

Action	EPM Component
Blocks access to registry settings	• Defendpoint client • ePO service • BeyondInsight adapter • Password Safe service
File protection (deleting, moving, renaming, writing security attributes, or taking ownership)	• C:\ProgramData\Avecto • C:\Program Files\Avecto\Privilege Guard Client\ • C:\Windows\System32\drivers\PGDriver.sys • C:\Program Files (x86)\Avecto\Privilege Guard Client • C:\Program Files (Arm)\Avecto\Privilege Guard Client

Set up Protection

The setup is a two-part process:

- Generate public-private key pair.
  - The public key is stored in a policy and distributed to all . The public key is automatically inserted into the policy.
  - The password-protected private key must be stored securely by the administrator. The private key and private key password are required when you want to disable agent protection.
- Enable protection.

Generate Key Pairs

To generate the key pair:

1. In the Policy Editor, expand **Utilities**.
2. Select **Agent Protection Settings**.
3. Click **Generate Key**.
4. Enter a password to encrypt the private key.
5. Click **Generate Key**.
6. The private key is automatically downloaded to the local computer. The file name is **private.pem**. The public key is automatically inserted into the policy.

Enable Agent Protection

To enable protection:

1. In the Policy Editor, expand **Utilities**.
2. Select **Advanced Agent Settings**.
3. Click **Add**.
4. Enter **AgentProtectionState** in the **Name** box.
5. Select **64 bit**.

6. Ensure type is **DWORD**.

7. In the **Decimal** box, set the value to **1**. The **Hex** value automatically populates with the same value. There are three possible states: **0** = off, **1** = enabled, **2** = disabled.

Agent protection is enabled after the policy is deployed and loaded by the Windows computers.

> ℹ️ *For more information about using agent protection, see Set up Agent Protection at*
> *https://www.beyondtrust.com/docs/privilege-management/windows/admin/install-upgrade/install-pm-windows.htm.*

Regenerate UUIDs

When importing and exporting policies from external sources, it can sometimes be necessary to regenerate the internal policy **Universally Unique Identifier (UUID)**, so that Reporting manages the events correctly. For most normal scenarios in which this is required (policy duplication, for example), this is handled seamlessly.

However, duplication by importing a text XML file will not be covered because sometimes you will not want to regenerate the UUIDs, such as when restoring a policy from a backup.

To regenerate UUIDs:

1. In the Policy Editor, expand **Utilities**.
2. Select **Regenerate UUIDs**.
3. Click the **Regenerate UUIDs** button.

A success message displays at the bottom center of the page.

Use Quickstart Templates

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

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

Customize the QuickStart Policy

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

At a minimum you need to:

- Configure the users or groups that can authorize requests that trigger messages.
- Assign users and groups to the high, medium, and low flexibility Workstyles.
- Populate the **Block - Blocklisted Apps** Application Group with any applications that you want to block for all users.
- Set your shared key so you can generate an Endpoint Privilege Management for Windows for Mac Response code.

QuickStart Template Summary

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

Workstyles

Name	Description
All Users	Contains rules that apply to all standard users regardless of the level of flexibility they need: • Block any applications in the **Block - Blocklisted Apps** group. • Allow Endpoint Privilege Management Support tools. • Allow standard Windows functions, business applications, and applications installed through trusted deployment tools to run with admin rights (Windows QuickStart template). • Allow standard macOS functions, business applications, and applications installed through trusted deployment tools to run with admin rights (Mac QuickStart template). • Allow approved standard user applications to run passively.
High Flexibility	Contains rules for users that require a lot of flexibility, such as software developers: • Allow known business applications and operating system functions to run. • Allow users to run signed applications with admin rights. • Allow users to run unknown applications with admin rights once they confirm that the application should be elevated. • Allow applications that are in the **Add Admin – High Flexibility** group to run with admin rights.

Name	Description
	• Allow unknown business application and operating system functions to run on-demand.
Medium Flexibility	Contains rules for users that require some flexibility, such as sales engineers: • Allow known business applications and operating system functions to run. • Allow users to run signed applications with admin rights once they confirm that the application must be elevated. • Prompt users to provide a reason before they can run unknown applications with admin rights. • Allow applications that are in the **Add Admin – Medium Flexibility** group to run with admin rights. • Allow unknown business application and operating system functions to run on-demand. • Restricted OS functions that require admin rights are prevented and require support interaction.
Low Flexibility	Contains rules for users that don't require much flexibility, such as helpdesk operators: • Prompt users to contact support if a trusted or untrusted application requests admin rights. • Prompt users to contact support if an unknown application tries to run. • Allow known approved business applications and operating system functions to run (Windows only).
Administrators	Provides visibility on the Administrator accounts in use. Contains general rules to: • Capture user and host information. • Block users from modifying local privileged group memberships.
SYSTEM	Protects the **Restricted System Functions** application group against potentially malicious behaviour by a user who can perform elevated PowerShell commands.

Application Groups

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

Name	Description
Add Admin - General (Business Apps) (Windows) Authorize - All Users (Business Apps) (macOS)	Contains applications that are approved for elevation for all users, regardless of their flexibility level.
Add Admin - General (Windows Functions) Authorize - All Users (macOS Functions)	Contains operating system functions that are approved for elevation for all users.
Add Admin - High Flexibility (Windows) Authorize - High Flexibility (macOS)	Contains the applications that require admin rights that should only be provided to the high flexibility users.
Add Admin - Low Flexibility	Contains the applications that require admin rights that should only be provided to the low flexibility users.
Add Admin - Medium Flexibility	Contains the applications that require admin rights that should

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

64

TC: 4/25/2024

Name	Description
Authorize - Medium Flexibility (macOS)	only be provided to the medium flexibility users.
Add Admin - Protected Operations	
Passive - High Flexibility (Business Apps)	Contains applications that are allowed for High Flexibility users without providing admin authorization.
Passive - Medium Business Apps	Contains applications that are allowed for Medium Flexibility users without providing admin authorization.
Passive - Low Flexibility (Business Apps)	Contains applications that are allowed for Low Flexibility users without providing admin authorization.
Block - Blocklisted Apps	Contains applications that are blocked for all users.
Passive - All Users Functions & Apps	Contains trusted applications, tasks and scripts that should execute as a standard user.
(Default) Any Application	Contains all application types and is used as a catch-all for unknown applications.
(Default) Any Trusted & Signed UAC Prompt (Windows) (Default) Any Trusted & Signed Authorization Prompt (macOS)	Contains signed (trusted ownership) application types that request admin rights or authorization.
(Default) Any UAC Prompt (Windows) (Default) Any Authorization Prompt (macOS)	Contains application types that request admin rights or authorization.
(Default) Any Sudo Command (macOS)	Contains all sudo commands and is used as a catch-all for unknown sudo commands.
(Default) Endpoint Privilege Management Tools	Provides access to a BeyondTrust executable that collects Endpoint Privilege Management troubleshooting information.
(Default) Child Processes of TraceConfig.exe	
(Default) Signed UAC Prompt (Windows) (Default) Any Signed Authorization Prompt (macOS)	Contains signed (trusted ownership) application types that request admin rights or authorization.
(Default) Software Deployment Tool Installs	Contains applications that can be installed by deployment tools such as System Center Configuration Manager (SCCM).
(Default) Authorize - System Trusted	Contains operating system functions that are authorized for all users.
(Default) Passive - System Trusted	Contains system applications that are allowed for all users.
(Recommended) Restricted Functions	Contains OS applications and consoles that are used for system administration and trigger UAC/authorization when they are executed.
(Recommended) Restricted Functions (On Demand)	Contains OS applications and consoles that are used for system administration.

Name	Description
(Default) Trusted Parent Processes	Trusted processes for reference in parent-rules.

Messages

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

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

Use the Server Role Template

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

Server Roles Template Summary

This template policy contains the following elements.

Workstyles

Name	Description
Server Role - Active Directory - Template	Supports server management of the Active Directory role.
Server Role - DHCP - Template	Supports server management of the DHCP role.
Server Role - DNS - Template	Supports server management of the DNS role.

Name	Description
Server Role - File Services - Template	Supports server management of the File Services role.
Server Role - Hyper V - Template	Supports server management of the Hyper-V role.
Server Role - IIS - Template	Supports server management of the IIS role.
Server Role - Print Services - Template	Supports server management of the Print Services role.
Server Role - Windows General - Template	Supports general server management operations.

Application Groups

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

Content Groups

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

Search a Policy

The search feature facilitates ease-of-use searching when trying to find specific details about policy configuration.

- Finds all search results for workstyles in the policy.
- Displays the exact location in the policy.
- Provides linked text to go to that area of the policy and edit the policy, if necessary.

  If you are viewing the policy in *read-only* mode, you can click the link to drill down, but you cannot edit the policy setting.

- Searches on Windows and macOS policies, and includes:
  - Application Groups
  - Applications (including application matchers)
  - Application Rules
  - On-Demand Rules
  - Account Filters
  - Computer Filters
- Saves the 5 most recent searches.
- Displays up to a maximum of 500 matches to ensure optimal performance.

Reporting

Analytics provides detailed activity information for computers in your environment. Areas covered include:

- Summary dashboard
- Events
- Discovery
- Actions
- Target types
- Users

The Analytics UI offers an interactive experience. View high-level data points or drill down to see more detail.

- Bar charts and graphs provide a big picture view of the data. You can drill down on a particular data point to see more detail.
- Filters help to refine the scope of data displayed when you want to focus in on certain data points.
- Links on certain data points that lead to additional event detail
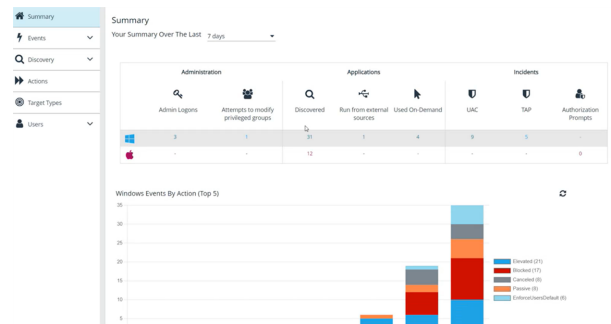
Event Data Caching

Event data is cached to reduce load times. The data is cached only for the following reports: Events > All, Events > Process Detail, Target Types and Discovery reports.

The expiry of the cache depends on the **Time Range** filter set for the report:

- 24 hours is live
- 7 days expires after 1 hour
- 30 days or higher expires after 24 hours

Export to a CSV File

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

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

All filters are saved to the file.

Summary Dashboard

The bar charts on the dashboard represent the most important activity that has occurred in the time period defined by the quick filter.

The **Administration**, **Applications**, and **Incidents** tables provide information to help inform Workstyle development or to show anomalous user behavior in your organization.

When available, drill down to see more details.

Events Reporting

The Events Summary dashboard 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.

Event reporting includes:

- **Events All Reports**:
- **Process Detail Report**: Provides information about a specific process control event. Only processes that match rules in Workstyles are displayed.

Event Types

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

The following events are logged by Endpoint Privilege Management:

Event ID	Description
100	Process has started with admin rights added to token.
101	Process has been started from the shell context menu with admin rights added to token.
103	Process has started with admin rights dropped from token.
104	Process has been started from the shell context menu with admin rights dropped from token.
106	Process has started with no change to the access token (passive mode).
107	Process has been started from the shell context menu with no change to the access token (passive mode).
109	Process has started with user's default rights enforced.
110	Process has started from the shell context menu with user's default rights enforced.
112	Process requires elevated rights to run.
113	Process has started with Custom Token applied.
114	Process has started from the shell context menu with user's Custom Token applied.
116	Process execution was blocked.
118	Process started in the context of the authorizing user.
119	Process started from the shell menu in the context of the authorizing user.
120	Process execution was canceled by the user.
199	Process execution was blocked, the maximum number of challenge / response failures was exceeded.

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

Discovery Reporting

The following discovery reports are available:

- **Dashboard**: Displays information about applications discovered for the first time. An application is first discovered when an event is received by the Reporting database.
- **Discovery by Path**: Displays all distinct applications installed in certain locations that are discovered during the selected time frame.
- **Discovery by Publisher**: 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.
- **Discovery by Type**: Displays applications filtered by type. When there is more than one application per type, click the link in the **Type** column to see more information about each application.
- **Discovery Requiring Elevation**: Displays the applications that were elevated or required admin rights.
- **Discovery from External Sources**: Displays all applications that have originated from an external source, such as the internet or an external drive.
- **Discovery All**: 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. Click the plus (**+**) icon to view the different versions.

Actions Reporting

Data is collected for the following actions:

- **Elevated**: Shows the elevated application activity by target type.
- **Blocked**: Shows the blocked application activity by target type.
- **Passive**: Shows the passive application activity by target type.
- **Canceled**: Shows the canceled application activity by target type.
- **Custom**: Shows the custom application activity by the type of action.
- **Drop Admin Rights**: Shows the drop admin application activity by target type.

When viewing the data, use the interactive graphs to see high-level metrics and drill down to see more information on the collected data.

Target Types Reporting

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

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

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

71

TC: 4/25/2024

Users Reporting

There are three reports for users:

- **User Experience**: Shows the number of users that interacted with EPM events, and is broken down over the selected time frame.
- **Users Privileged Logons**: Shows the number of accounts with standard user rights, power user rights, and administrator rights have generated logon events broken down over the selected time frame. On the **User Session** report, accessed from the **Privileged Logons** report, view more details about the privileged logon account sessions. The details include the user name, logon time, account type, and domain, etc.
- **Users Privileged Account Management**: Shows any blocked attempts to modify privileged accounts over the selected time interval.