



BeyondTrust

Privilege Management Reporting 24.1 Dashboard Guide

Table of Contents

Endpoint Privilege Management Reporting Dashboard Guide	4
Reporting Concepts	4
Operating Systems	4
Naming Conventions and Navigation	5
Interface	5
Navigation Panel	5
Dashboard and Reports Panel	5
Quick Filter Panel	6
Advanced Filter Panel	10
Top Toolbar	11
Export Reports	12
Permalink to Reports	12
Filter Data in Endpoint Privilege Management Reporting	13
Endpoint Privilege Management Reporting Quick Filter Panel Details	14
Endpoint Privilege Management Reporting Top Advanced Filter Details	19
Dashboard and Reports	24
"Summary" Dashboard in Endpoint Privilege Management Reporting	25
Discovery Dashboard in Endpoint Privilege Management Reporting	27
"Discovery By Path" Report in Endpoint Privilege Management	29
"Discovery By Publisher" Report in Endpoint Privilege Management	30
"Discovery By Type" Report in Endpoint Privilege Management	31
"Discovery Requiring Elevation" Report in Endpoint Privilege Management	32
"Discovery From External Sources" Report in Endpoint Privilege Management	33
"Discovery All" Report in Endpoint Privilege Management	34
Actions Dashboard in Endpoint Privilege Management Reporting	35
"Actions Elevated" Report in Endpoint Privilege Management	36
"Actions Blocked" Report in Endpoint Privilege Management	37
"Actions Passive" Report in Endpoint Privilege Management	38
"Actions Canceled" Report in Endpoint Privilege Management	39
"Actions Other" Report in Endpoint Privilege Management	40
"Actions Custom" Report in Endpoint Privilege Management	41

"Target Types" Dashboard in Endpoint Privilege Management Reporting	42
"Target Types Applications" Report in Endpoint Privilege Management	43
"Target Types Services" Report in Endpoint Privilege Management	44
"Target Types COM" Report in Endpoint Privilege Management	45
"Target Types Remote PowerShell" Report in Endpoint Privilege Management	46
"Target Types All" Report in Endpoint Privilege Management	47
"Trusted Application Protection" Dashboard in Endpoint Privilege Management	48
"Workstyles" Dashboard in Endpoint Privilege Management Reporting	49
"Users" Dashboard in Endpoint Privilege Management Reporting	52
"Deployments" Dashboard in Endpoint Privilege Management	55
Requests Dashboard in Endpoint Privilege Management	56
"Events" Dashboard in Endpoint Privilege Management	57
"Database Administration" Report in Endpoint Privilege Management	60
The Endpoint Privilege Management Purge Tool Utility	61
Use Export Views in Endpoint Privilege Management Reporting	62

Endpoint Privilege Management Reporting Dashboard Guide

Endpoint Privilege Management Reporting includes a rich set of dashboards and reports designed to simplify the centralized management and auditing of Endpoint Privilege Management activity throughout the desktop and server estate.

A dashboard is a report, that at the top level, presents you with a series of charts and summarized data. Some dashboards have sub-reports that are presented as charts or tabular data.

This guide explains each of the dashboards in Endpoint Privilege Management Reporting, and the reports and event data accessible from each view.

Reporting Concepts

There are several concepts in Reporting that are described here.

Dashboards, Tables, and Reports

- A **dashboard** is anything in Reporting where visual charts are displayed.
- A **table** is anything in Reporting that has a tabular format.
- A **report** is a dashboard or a table. It is a generic term used to describe any form of data displayed in Reporting.

Drilldown

Drilldown is a user action in a report in which you click on a link to see the data at a greater level of granularity.

Permalink

Permalink refers to a link at the bottom of most reports that generates a unique URL that allows someone else to view that exact page once they login.

Operating Systems

All dashboards have a Microsoft Windows view to display events from Windows endpoints. Some dashboards and reports also have a macOS view.

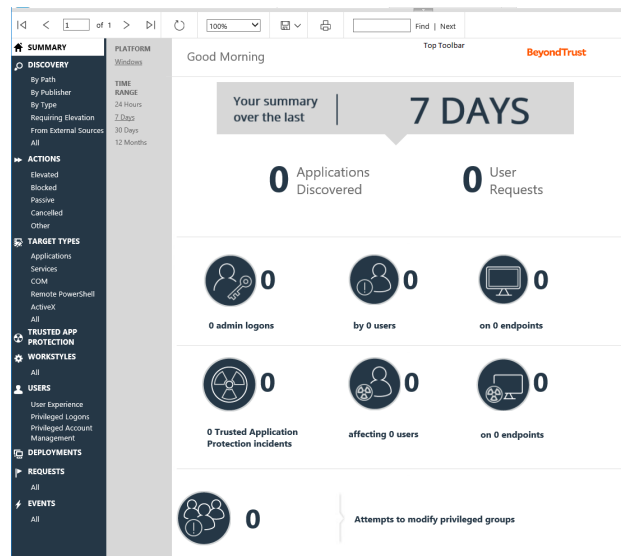
Naming Conventions and Navigation

This section covers the Endpoint Privilege Management Reporting interface elements and how to export and link to a specific report.

Interface

The Endpoint Privilege Management Reporting interface allows you to switch between dashboards and reports and to filter data as required. Shown in the image from left to right are the navigation panel, the quick filter panel, and the dashboard and reports panel.

There is a link at the bottom of each report called **permalink** that creates a static link to that report with your choice of filters applied.



Navigation Panel

The side navigation panel takes you to each top-level dashboard and the reports in that dashboard. Reports that are post-fixed with **All** indicate the data is in tabular form.

Dashboard and Reports Panel

This is the area where dashboards and reports are displayed. A dashboard is a report with multiple charts covering a wide range of data. A report is a summary table or a page focused on a particular entity.

The graphical elements of a dashboard or report are interactive. You can click on a chart to view the data at an additional level of granularity.

Quick Filter Panel

Name	Description
Platform	<ul style="list-style-type: none"> • Windows Filters by endpoints running a Windows operating system. • macOS Filters by endpoints running a Mac operating system.
Time Range	<p>This is the time range that the actions are audited. For example, you can filter by the number of elevated actions in the last 24 hours in the Actions > Elevated report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • 24 Hours • 7 Days • 30 Days • 12 Months
First Reported	<p>This is the time range filtered by the date the application was first entered in the database. For example, you can filter on the new Windows applications by publisher that were first reported in the last 7 days in the Discovery > By Publisher report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months
First Executed	<p>This is the time range the application was first executed. For example, you can filter on the new Windows applications, by type, that were first executed in the last 30 days in the Discovery > By Type report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months

Name	Description
Filter by Target Type	<p>This filter allows you to filter by a type of target. For example, you can filter on the applications canceled in the time range in the Actions > Canceled report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Applications • Services • COM • Remote PowerShell • ActiveX • URL • Content
Filter by Action	<p>This filter allows you to filter by a type of action. For example, you can filter on the services elevated in the time range in the Target Types > Services report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Elevated • Blocked • Passive • Sandboxed • Canceled

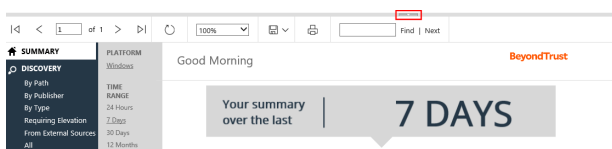
Name	Description
Filter by App Type	<p>This filter allows you to filter by application type. For example, you can filter by applications that are executables used in the time range in Target Types > Applications.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Executable • Control Panel Applet • Management Console • Installer Package • Uninstaller • Windows Script • PowerShell Script • Batch File • Registry Settings • Windows Store • Binary • Bundle • Package • System Preference • Sudo Control • Script
Filter by Event Category	<p>This filter allows you to filter by the category of the event. For example, you can filter by process events only that occur in the time range in the Events > All report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Process • DLL Control • Content • URL • Privileged Account Protection • Agent Start • User Logon • Services

Name	Description
Elevate Method	<p>Allows you to filter by the elevation method used. For example, in the Discovery > Requiring Elevation report, you can filter by new applications which were accessed using on-demand elevation within the time range.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Admin account used • Auto-elevated • On-demand
Path	<p>Allows you to filter by the path. For example, to filter on applications that were launched from the System path.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • System • Program Files • User Profiles
Source	<p>The media source of the application. For example, was the application downloaded from the internet or is it from removable media?</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Any external source • Downloaded from internet • Removable media
Challenge / Response	<p>Allows you to filter by challenge/response events. For example, you can filter the application that required elevation on those applications launched following a completed challenge/response message.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Only C/R
Admin Rights	<p>Allows you to filter by the admin rights token.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Detected • Not Detected

Name	Description
Authorization	Allows you to filter by authorization. You can choose from: <ul style="list-style-type: none"> • All • Required • Not Required
Group By	You can choose from: <ul style="list-style-type: none"> • All • Publisher • Application Group • Message • Workstyle
Ownership	Allows you to group by the type of owner. You can choose from: <ul style="list-style-type: none"> • All • Trusted owner • Untrusted owner
Matched	Allows you to filter on the type of matching. You can choose from: <ul style="list-style-type: none"> • All • Matched directly • Matched as child
Other Actions	Allows you to filter by other actions. You can choose from: <ul style="list-style-type: none"> • Custom • Drop Admin Rights • Enforce Default Rights
Details	Process Details

Advanced Filter Panel

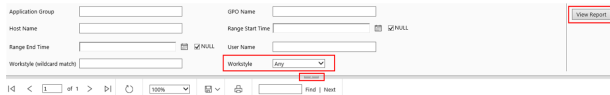
The **Filter Panel** dropdown bar is located above the **Toolbar**. Click the bar to toggle the filter panel.



The **Filter Panel** is available from most dashboards and reports, and allows you to filter data based on a number of event properties. To access the **Filter Panel** at any time, click the filter dropdown button shown above.

For example, if you want to filter the Summary report to only include a specific Workstyle:

1. Open the report to filter.
2. Open the **Filter Panel** by clicking the filter dropdown list.
3. Select the Workstyle you are interested in from the **Workstyle** dropdown list.




4. Click **View Report**.
5. Close the **Filter Panel**.

The report then shows information from the **Developers** Workstyle only.


The filter options match text on substrings; partial or complete words can match on a filter.


Certain filter options support comma-separated values so you can specify a list of filter values. For example, to restrict the results to three users, enter **user1,user2,user3** in the **User Name** field.

 **Note:** Multiple ! strings are accepted. For example, **!L-CZC13127L30I,!L-CNU410DJJ7**

Any text field supports wildcards, comma-separated values (CSV) and the Does Not Match(!) options:

Filtering Effect	Filter Panel Operator	Effect
List separator	Comma (,)	Value1,value2,value3
Wildcard	%	part% part%part2,part3%part4
Negation or "Not"	!	!value !value1,!value2

 **Note:** When filtering tabular reports such as the **Users > All** table, an applied filter is displayed at the top of the relevant column. To remove a filter, click on the **x** next to the filter text.

 **Tip:** The **Filter Panel** includes several properties that can be used to filter the events in the dashboard or report currently in view. Please see "[Endpoint Privilege Management Reporting Top Advanced Filter Details](#)" on page 19.

Top Toolbar

You can use the toolbar to navigate between report pages, change the magnification, search, export, refresh, print, and export to a data feed.



Note: The Toolbar and the Filter Panel are standard Microsoft SSRS components. Please see [What is SQL Server Reporting Services \(SSRS\)](https://docs.microsoft.com/en-us/sql/reporting-services/create-deploy-and-manage-mobile-and-paginated-reports) at <https://docs.microsoft.com/en-us/sql/reporting-services/create-deploy-and-manage-mobile-and-paginated-reports>.

Export Reports

Dashboards and reports can be exported to any of the following formats using the **Export** dropdown menu on the toolbar:

- XML file with report data
- CSV (comma delimited)
- PDF
- MHTML (web archive)
- Excel
- TIFF file
- Word

Exported data is based on the data currently displayed in the dashboard or report.



For more information, please see the following:

- ["Permalink to Reports" on page 12](#)
- On supported SQL wildcard character filter options, <https://docs.microsoft.com/en-us/sql/t-sql/language-elements/like-transact-sql>
- ["Export Reports" on page 12](#)

Permalink to Reports

Each dashboard and report includes a permalink located at the bottom of each report. Permalinks can be used to link directly to views which are configured with advanced filters, eliminating the need to repeatedly set filters for common views.

The permalink is unique to the current report and filters. Changing a filter results in a new permalink being created for that modified view.

To obtain a permalink from a dashboard or report, click the **Permalink** link at the bottom of the page. The page reloads with a URL that can be copied in the address bar of your web browser.

To copy the permalink URL, right-click the **Permalink** option and select **Copy Shortcut**. Alternatively, you can **Add** the URL as a browser favorite to return easily to a view that may be difficult to recreate.

Filter Data in Endpoint Privilege Management Reporting

There are two ways to filter data:

- **Quick Filter Panel Details:** The Quick Filter panel on the left pane shows the most commonly used filters in the dashboards and reports. This filter panel is always displayed and cannot be collapsed.
- **Top Advanced Filter Details:** The Top Advanced filter contains more advanced filters that you can use to view data at a higher level of granularity.



For more information, please see the following:

- ["Endpoint Privilege Management Reporting Quick Filter Panel Details" on page 14](#)
- ["Endpoint Privilege Management Reporting Top Advanced Filter Details" on page 19](#)

Endpoint Privilege Management Reporting Quick Filter Panel Details

The quick filter panel has different options, depending on which report you are currently viewing.

Name	Description
Platform	<ul style="list-style-type: none"> • Windows: Filters by endpoints running a Windows operating system. • macOS: Filters by endpoints running a Mac operating system.
Time Range	<p>The span of time that actions are audited. For example, you can filter on the number of elevated actions in the last 24 hours in the Actions > Elevated report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • 24 Hours • 7 Days • 30 Days • 12 Months
First Reported	<p>This is the time range filtered by the date the application was first entered in the database. For example, you can filter on the new Windows applications by publisher that are first reported in the last 7 days in the Discovery > By Publisher report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months
First Executed	<p>This is the time range the application was first executed. For example, you can filter on the new Windows applications, by type that are first executed in the last 30 days in the Discovery > By Type report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months

Name	Description
Filter by Target Type	<p>Filter by type of target. For example, you can filter on the applications that are canceled in the time range in the Actions > Canceled report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Applications • Services • COM • Remote PowerShell • ActiveX • URL • Content
Filter by Action	<p>Filter by type of action. For example, you can filter on the services that are elevated in the time range in the Target Types > Services report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Elevated • Blocked • Passive • Sandboxed • Canceled

Name	Description
Filter by App Type	<p>Filter by application type. For example, you can filter by applications that are executables used in the time range in Target Types > Applications.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Executable • Control Panel Applet • Management Console • Installer Package • Uninstaller • Windows Script • PowerShell Script • Batch File • Registry Settings • Windows Store • Binary • Bundle • Package • System Preference • Sudo Control • Script
Filter by Event Category	<p>Filter by the category of the event. For example, you can filter by process events only that are raised in the time range in the Events > All report.</p> <p>You can choose from:</p> <ul style="list-style-type: none"> • All • Process • DLL Control • Content • URL • Privileged Account Protection • Agent Start • User Logon • Services

Name	Description
Elevate Method	Filter by the elevation method used. For example, in the Discovery > Requiring Elevation report, you can filter by new applications accessed using on-demand elevation within the time range. You can choose from: <ul style="list-style-type: none"> • All • Admin account used • Auto-elevated • On-demand
Path	Filter by the path. For example, filter on applications that were launched from the System path. You can choose from: <ul style="list-style-type: none"> • All • System • Program Files • User Profiles
Source	The media source of the application. For example, was the application downloaded from the internet or is it from removable media? You can choose from: <ul style="list-style-type: none"> • All • Any external source • Downloaded from internet • Removable media
Challenge / Response	Filter by challenge/response events. For example, you can filter the application that required elevation on those applications that were launched following a completed challenge/response message. You can choose from: <ul style="list-style-type: none"> • All • Only C/R
Admin Rights	Filter by the admin rights token. You can choose from: <ul style="list-style-type: none"> • All • Detected • Not Detected
Authorization	Filter by authorization. You can choose from: <ul style="list-style-type: none"> • All • Required • Not Required

Name	Description
Group By	You can choose from: <ul style="list-style-type: none"> • All • Publisher • Application Group • Message • Workstyle
Ownership	Group by the type of owner. You can choose from: <ul style="list-style-type: none"> • All • Trusted owner • Untrusted owner
Matched	Filter on the type of matching. You can choose from: <ul style="list-style-type: none"> • All • Matched directly • Matched as child
Other Actions	Filter by other actions. You can choose from: <ul style="list-style-type: none"> • Custom • Drop Admin Rights • Enforce Default Rights
Details	Process Details

Endpoint Privilege Management Reporting Top Advanced Filter Details

Name	Description
Action	<p>There are nine actions to choose from:</p> <ul style="list-style-type: none"> • Elevated • Blocked • Passive • Custom • Drop Admin Rights • Enforce Admin Rights • Canceled • Sandboxed • Allowed
Activity ID	<p>Each Activity Type in Endpoint Privilege Management has a unique ID. This is generated in the database as required.</p> <p>For example, if you are in the Target Types Dashboard and drill down in the Top 10 Activities chart, the Events > All report opens. If you look in the top advanced filter you will see that the Activity ID is populated.</p>
Admin Rights Required	<p>There are three options to choose from:</p> <ul style="list-style-type: none"> • All • Detected • Not Detected <p>Allows you to filter if Admin Rights are required, not required or both. For example, if you are in the Discovery > All report and set the side quick filter to Admin Rights, only applications that required admin rights are listed.</p>
Agent Version	The version of the Endpoint Privilege Management agent.
Application Desc	<p>A text field that allows you to filter on the application name.</p> <p>For example, in the Discovery report you can filter by paint in the Application Desc field. This filters applications that contain the string paint in the description.</p>
Application Group	A text field that allows you to filter on the Application Group. You can obtain the Application Group from the policy editor. It is also available in some reports such as Process Detail that is accessed from Events All .
Application Type	A text field that allows you to filter on the application type. You can obtain the application type from the policy editor. It's also available in some reports such as Process Detail that is accessed from Events All .
Auth Methods	The type of authentication method selected in the Policy Editor. Multiple values can be present and will be comma separated. Possible values: Identity Provider , Password , Challenge Response , Smart Card , and User Request
Auth User Name	The name of the user that authorized the message.
Browse Source URL	The source URL of the sandbox.

Name	Description
Browse Destination URL	The destination URL of the sandbox.
Chassis	The physical form of the endpoint. Other is a virtual machine.
Command Line	A text field that allows you to filter on the command line. It is also available in some reports such as Process Detail that is accessed from Events > All .
Context	This field is used by Reporting. You do not need to edit it.
Date Field to filter on	<p>There are three options to choose from:</p> <ul style="list-style-type: none"> • Time Generated: This is the time that the event was generated. One application can have multiple events. Each event has a Time Generated attribute. • Time App First Discovered: This is the time that the first event for a single application was entered into the database. This can be delayed if the user is working offline. • Time App First Executed: This is the first known execution time of events for that application.
Default UI Language	The default language of the endpoint.
Device Type	<p>The type of device that the application file was stored on. You can select from:</p> <ul style="list-style-type: none"> • Any • Removeable Media • USB Drive • Fixed Drive • Network Drive • CDROM Drive • RAM Drive • eSATA Drive • Any Removeable Drive or Media
Distinct Application ID	This field is used by Reporting. You do not need to edit it.
Elevation Method	<p>There are five options to choose from:</p> <ul style="list-style-type: none"> • Not Set • All • Admin account • Auto-elevated • On-demand <p>These allow you to filter events by the type of elevation used.</p>
Event Number	<p>This field is used by Reporting. You do not need to edit it.</p> <p>This number assigned to the event type.</p>

Name	Description
External Source	<p>There are four options to choose from:</p> <ul style="list-style-type: none"> • Not Set • Downloaded over the internet • Removeable media • Any external source <p>These allow you to filter by the type of external source that the application file came from.</p>
File Name	You can filter by a partial file name string if required. For example, in the Process Detail report.
File Version	You can filter on the file version in the Advanced View of the Process Detail report.
GPO Name	You can filter on the Group Policy Object (GPO) name in some of the advanced reports such as Process Detail .
Host Name	This field allows you to filter by the name of the endpoint the event came from.
Idp Authentication user name	The credential provided when adding an Identity Provider authorization message in the Policy Editor.
BeyondTrust Zone Identifier	The BeyondTrust Zone Identifier. This tag will persist to allow you to filter on it even if the ADS tag applied by the browser is removed.
Ignore "Admin Required" Events	This field is used by Reporting. You do not need to edit it.
Just Discovery Events	This field is used by Reporting. You do not need to edit it.
Message Name	The name of the message that was used.
Message Type	<p>The type of Message:</p> <ul style="list-style-type: none"> • Any • Prompt • Notification • None
Number to Get	The number of rows to get from the database.
Operating System Type	<p>The type of operating system:</p> <ul style="list-style-type: none"> • Server • Workstation
Operating System	The operating system of the client machine.
Parent PID	The operating system process identifier of the parent process.
PID	The operating system process identifier.
Product Name	The product name of the application.
Product Version	The product version of the application.
Program Files Path	Sets the Program Files path used by the Discovery > By Path report.
Publisher	The publisher of the application.
Range End Time	The end time of the range being displayed.
Range Start Time	The start time of the range being displayed.

Name	Description
Request Type	The type of request: <ul style="list-style-type: none"> • Blocked with reason • Canceled challenge
Row Limit	The maximum number of rows to be retrieved from the database.
Rule Match Type	Rule Match Type: <ul style="list-style-type: none"> • Any • Direct match • Matched on parent
Sandbox	The sandboxed setting: <ul style="list-style-type: none"> • Not Set • Any Sandbox • Not Sandboxed
Rule Script Affected Rule	True when the Rule Script (Power Rule) changes one or more of the Default Endpoint Privilege Management rules, otherwise false.
Rule Script File Name	The Rule Script (Power Rule) file name on disk if applicable.
Rule Script Name	The name of the assigned Rule Script (Power Rule).
Rule Script Output	The output of the Rule Script (Power Rule).
Rule Script Publisher	The publisher of the Rule Script (Power Rule).
Rule Script Result	The result of the Rule Script (Power Rule). This can be: <None> Script ran successfully [Exception Message] Script timeout exceeded: <X> seconds Script execution canceled Set Rule Properties failed validation: <reason> Script execution skipped: Challenge Response Authenticated Script executed previously for the parent process: Matched as a child process so cached result applied Script execution skipped: <app type> not supported Script execution skipped: PRInterface module failed signature check Set RunAs Properties failed validation: <reason>
Rule Script Status	The status of the Rule Script (Power Rule). This can be: <None> Success Timeout Exception Skipped ValidationFailure
Rule Script Version	The version of the assigned Rule Script (Power Rule).

Name	Description
Shell or Auto	Whether the process was launched using the shell Run with Endpoint Privilege Management option or by normal means (opening an application): <ul style="list-style-type: none"> • Any • Shell • Auto
Source URL	The source URL (where the file was downloaded from).
System Path	Sets the system path used by the Discovery > By Path report.
Target Description	This field allows you to filter by the target description.
Target Type	The type of target that triggered the event: <ul style="list-style-type: none"> • Any • Application • URL • Services • COM • Remote PowerShell • ActiveX • Content
Trusted Application Name	The trusted application that triggered the event.
Trusted Application Version	The trusted application version number.
Trusted File Owner	Whether the file owner of the target file is trusted. To be a trusted owner the user must be in one of the following Windows groups: <ul style="list-style-type: none"> • TrustedInstaller • System • Administrator
UAC Triggered	Whether or not Windows UAC was triggered: <ul style="list-style-type: none"> • Not Set • Triggered UAC • Did not trigger UAC
User Name	The user name of the user who triggered the event.
User Profiles Path	Sets the User Profiles path used by the Discovery > By Path report.
Workstyle	The name of the Workstyle that contained the rule that matched the application.

Dashboard and Reports

Reporting includes several high level dashboards that summarize the Endpoint Privilege Management events.

Summary Dashboard	Displays bar charts for the most important activity that has occurred in the selected time period. Typically this information can result in Workstyle changes or investigation of anomalies. The charts allow you to view details when you click on an Action, either on a chart or in the legend. The bar charts are separated by Windows and Mac Events by Action .
Discovery Dashboard	Summarizes all the unique applications discovered. It differentiates between those that used elevated privileges and those that ran with standard privileges. The Discovery reports display the data from different angles such as by the location of the executable or the type of the executable. These dashboards only show new application items in the chosen time interval. For example, the Discovery dashboard can answer the question <i>what's new this week and how is it affecting my users?</i>
Actions Dashboard	Summarizes audited items categorized by the type of action taken. This allows you to focus on the topic of interest. For example, elevation or blocking. The Actions reports show audits only of the selected type (Elevated, Blocked, Passive, Canceled, Other).
Target Types Dashboard	Shows all the Endpoint Privilege Management activity over the specified time interval by target type. The Target Types > All report lists the targets in tabular form sorted by user count. The subheadings below the Target Types dashboard link filter the dashboard to show audits only of the selected type (Applications, Services, COM, Remote PowerShell, ActiveX, All).
Trusted Application Protection Dashboard	Summarizes all the Trusted Application Protection incidents. Incidents are defined as a child process blocked from running because it matched the rules in the Trusted Application Protection policy or a DLL blocked from loading by a Trusted Application because it did not have a trusted owner or trusted publisher.
Workstyles Dashboard	Summarizes all the Endpoint Privilege Management Workstyle usage, including coverage statistics. The dashboard includes a report called All that lists the total number of different action types each Workstyle controlled. The dashboard allows analysis from the perspective of a specific Workstyle. <ul style="list-style-type: none"> • User Experience: Summarizes how users interacted with messages, challenge / response dialog boxes and the shell integration in a specified time range. • Privileged Logons: Provides a number of reports relating to logon events and the type of user, for example administrator and standard user. • Privileged Account Protection: Summarizes any audited attempts to modify privileged accounts.
Deployments Dashboard	Summarizes Endpoint Privilege Management Client deployments. The report shows the versions of Endpoint Privilege Management that are currently installed across the organization. It includes asset information about endpoints such as operating system and default language to assist with Workstyle targeting.
Requests Dashboard	Summarizes information about user requests raised over the specific time frame. A blocked message with a reason entered or a canceled challenge / response message is a request.
Events Dashboard	Summarizes information about the types of events raised in the specified time frame. It also shows the time elapsed since a host raised an event.

"Summary" Dashboard in Endpoint Privilege Management Reporting

The **Summary** dashboard displays bar charts for the most important activity that has occurred in the time period defined by the quick filter. The legends to the right of the charts display totals for the shown activities. You can use this information to inform Workstyle development or to show anomalous user behavior in your organization.

A warning message might display on the **Summary** page if there is a backlog of event processing. Verify your database configuration is set up to manage processing a large number of events.

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

Table	Description
Applications Discovered	<p>The total number of newly discovered Applications filtered by the type of user rights required:</p> <ul style="list-style-type: none"> • Admin rights required • Standard rights required <p>Discovered applications are shown in the Applications table. Click the number next to the OS icon to show details.</p>
User Requests	<p>The total number of User Requests filtered by the type of request:</p> <ul style="list-style-type: none"> • Blocked (user provided reason) • User canceled challenge <p>Click the chart or legend to open the Requests All report with the Request Type filter applied.</p>
Admin logons, by users, on endpoints	<p>Summarizes the number of admin logons, the number of users, and the number of endpoints used.</p> <p>Admin Logons are shown in the Administration table. Click the number next to the OS icon to show details.</p>
Trusted Application Protection	<p>The number of Trusted Application (TAP) incidents, how many users, and how many endpoints were affected.</p> <p>TAP events are shown in the Incidents table. Click the number next to the OS icon to show details.</p>
Attempts to modify privileged groups	<p>The number of blocked attempts to modify privileged groups.</p> <p>Attempts to modify privileged groups are shown in the Administration table. Click the number next to the OS icon to show details.</p>
Application run from external sources	<p>The number of applications run from external sources.</p> <p>Applications Run from external sources are shown in the Applications table. Click the number next to the OS icon to show details.</p>
Activities blocked	<p>The number of applications blocked.</p> <p>Click the chart or legend to open the Target Types All report with the Filter by Action filter applied.</p>
Applications used On-Demand privileges	<p>The number of applications launched using on-demand privileges.</p> <p>Click the chart or legend to open the Target Types All report with the Shell or Auto filter applied. <i>Shell</i> indicates that on-demand privileges were used.</p>

Table	Description
UAC matches	<p>The number of applications that triggered User Account Control (UAC).</p> <p>UAC events are shown in the Incidents table. Click the number next to the OS icon to show details.</p>
Hosts audited	<p>The number of endpoints that were audited.</p> <p>The graph shows you the times since the most recent events.</p> <p>Click the icon, number, or text to open the Deployments Dashboard. Click the i icon to open the Events All report</p>
Events audited	<p>The number of events that were audited.</p> <p>The graph shows you the number of each type of event.</p> <p>Click the icon, number, or text to open the Events All report.</p>



For more information, please see the following:

- ["Discovery All" Report in Endpoint Privilege Management" on page 34](#)
- ["Requests Dashboard in Endpoint Privilege Management" on page 56](#)
- ["Privileged Logons Report in Endpoint Privilege Management" on page 52](#)
- ["Trusted Application Protection" Dashboard in Endpoint Privilege Management" on page 48](#)
- ["Target Types All" Report in Endpoint Privilege Management" on page 47](#)
- ["Deployments" Dashboard in Endpoint Privilege Management" on page 55](#)
- ["Events All" on page 57](#)

Discovery Dashboard in Endpoint Privilege Management Reporting

The report displays information about applications discovered by the reporting database for the first time. An application is first discovered when an event is received by the Endpoint Privilege Management Reporting database.

Operating Systems Terminology

The **Discovery Dashboard** displays events from Windows and macOS operating systems. The terminology differences are:

Operating System	Terminology
Windows	<i>Admin Rights Required</i> (shown here)
macOS	<i>Authorization</i>

The terminology is shown when you switch operating systems using the **Platform** filter.

The **Discovery Dashboard** has the following charts:

Chart	Description
Applications first reported in the specified time frame	A chart showing the number of applications discovered filtered by the types of rights detected: <ul style="list-style-type: none"> • Admin Rights Detected • Admin Rights Not Detected Click the Admin rights detected or Admin rights not detected lines in the graph to open the Discovery Dashboard report with the Admin Rights Required filter applied.
Types of newly discovered applications	A chart showing the number of applications discovered by the type of application. The types are different for Windows and macOS operating system. Click the chart to open the Discovery Dashboard report with the Admin Rights Required filter applied.

The Discovery Dashboard has the following tables:

New applications with admin rights (top 10)	A list of discovered applications that are running with admin rights. This list is ordered by the number of users. Click View all to see the full list. Click any of the applications in the list to open the Discovery Dashboard report with the Admin Rights Required and Matched filter applied.
New applications with standard rights (top 10)	A list of discovered applications that are running with standard, not admin rights. This list is ordered by the number of users. Click View all to see the full list. Click any of the applications in the list to open the Discovery Dashboard report with the Admin Rights Required and Matched filter applied.

New applications with admin rights (by type)	A list of the types of applications that required admin rights that were newly discovered within the time interval. They are ordered by the total number of applications for each type. Click View all to see the full list. Click any of the applications in the list to open the Discovery Dashboard report with the Admin Rights Required and Matched filter applied.
New applications with standard rights (by type)	The types of applications that did not require admin rights that were newly discovered within the time interval. They are ordered by the total number of applications for each type. Click any of the applications in the list to open the Discovery Dashboard report with the Admin Rights Required and Matched filter applied.



For more information, please see the following:

- ["Platform" on page 14](#)
- ["First Reported" on page 14](#)
- ["Admin Rights" on page 17](#)

"Discovery By Path" Report in Endpoint Privilege Management

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

- **System:** C:\Windows\
- **Program Files:** C:\Program Files\, C:\Program Files (x86)\
- **User Profiles:** C:\Users



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

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

- **Path:** The Path category that the application was installed in. You can click the + icon to expand the row and see each application.
- **# Users:** The number of users.
- **Median # processes / user:** The median number of processes per user.
- **# Hosts:** The number of hosts. Drill down to view a list of hosts the application events came from.
- **# Processes:** The number of processes. Drill down to see the **Events All** table and lists the events received in the time period for the selected application.
- **# Applications:** The number of applications.
- **Date first reported:** The date the application was first entered in the database.
- **Date first executed:** The first known date the application was executed.



For more information on the quick filters that are available, please see the following:

- ["Platform" on page 14](#)
- ["First Reported" on page 14](#)
- ["First Executed" on page 14](#)
- ["Path" on page 17](#)
- ["Authorization" on page 17 \(macOS only\)](#)
- ["Source" on page 17 \(Windows only\)](#)
- ["Admin Rights" on page 17 \(Windows only\)](#)
- ["Ownership" on page 18 \(Windows only\)](#)
- ["Matched" on page 18 \(Windows only\)](#)

"Discovery By Publisher" Report in Endpoint Privilege Management

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

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

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

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

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



For more information on the quick filters that are available, please see the following:

- ["Platform" on page 14](#)
- ["First Reported" on page 14](#)
- ["First Executed" on page 14](#)
- ["Path" on page 17](#)
- ["Authorization" on page 17 \(macOS only\)](#)
- ["Source" on page 17 \(Windows only\)](#)
- ["Admin Rights" on page 17 \(Windows only\)](#)
- ["Ownership" on page 18 \(Windows only\)](#)
- ["Matched" on page 18 \(Windows only\)](#)

"Discovery By Type" Report in Endpoint Privilege Management

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

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

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

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

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



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["First Reported" on page 14](#)
- ["First Executed" on page 14](#)
- ["Path" on page 17](#)
- ["Authorization" on page 17 \(macOS only\)](#)
- ["Source" on page 17 \(Windows only\)](#)
- ["Admin Rights" on page 17 \(Windows only\)](#)
- ["Ownership" on page 18 \(Windows only\)](#)
- ["Matched" on page 18 \(Windows only\)](#)

"Discovery Requiring Elevation" Report in Endpoint Privilege Management

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

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

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

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

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



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["First Reported" on page 14](#)
- ["First Executed" on page 14](#)
- ["Elevate Method" on page 17](#)
- ["Path" on page 17](#)
- ["Source" on page 17](#)
- ["Challenge / Response" on page 17](#)
- ["Ownership" on page 18 \(macOS only\)](#)
- ["Matched" on page 18](#)

"Discovery From External Sources" Report in Endpoint Privilege Management

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

The following columns are available for the **Windows Discovery from External Sources** table:

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

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

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



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["First Reported" on page 14](#)
- ["First Executed" on page 14](#)
- ["Path" on page 17](#)
- ["Source" on page 17](#)
- ["Admin Rights" on page 17](#)
- ["Ownership" on page 18](#)
- ["Matched" on page 18](#)

"Discovery All" Report in Endpoint Privilege Management

The table lists all applications discovered in the time period, grouped by the application description so that if multiple versions of the same application exist, they are grouped on the same line. Click **+** in the **Version** column to expand the list.

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

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

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

- *i* icon: Opens the **Applications report** for that specific application.
- **# Users:** Displays a list of users the application events came from.
- **# Hosts:** Displays a list of hosts the application events came from.
- **# Processes:** Displays the **Events All** table.



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["First Reported" on page 14](#)
- ["First Executed" on page 14](#)
- ["Path" on page 17](#)
- ["Authorization" on page 17 \(macOS only\)](#)
- ["Source" on page 17 \(Windows only\)](#)
- ["Admin Rights" on page 17 \(Windows only\)](#)
- ["Ownership" on page 18 \(Windows only\)](#)
- ["Matched" on page 18 \(Windows only\)](#)

Actions Dashboard in Endpoint Privilege Management Reporting

The **Actions** dashboard breaks down the application activity by the type of action. It also lists the most active targets.

The **Actions** dashboard has the following charts:

Chart	Description
All actions over the specified time frame	<p>A chart showing the number of targets filtered by the type of action for each time frame.</p> <p>The types of action are:</p> <ul style="list-style-type: none"> • Enforce default rights • Drop admin rights • Canceled • Passive • Sandboxed • Blocked • Elevated • Custom <p>Click the chart to open the Target Types All report with the Filter by Action filter applied.</p>
Distinct target count by action	<p>A chart showing the target count filtered by the type of action.</p> <p>The types of action are:</p> <ul style="list-style-type: none"> • Enforce default rights • Drop admin rights • Canceled • Passive • Sandboxed • Blocked • Elevated • Custom <p>Click the chart to open the Target Types All report with the Filter by Action filter applied.</p>
Top 10 targets	<p>A chart showing the ten most used targets by process count.</p> <p>Click the chart to open the Events All report with the Target Description filter applied.</p>



For more information, please see the following:

- ["Target Types All" Report in Endpoint Privilege Management" on page 47](#)
- ["Events" Dashboard in Endpoint Privilege Management" on page 57](#)
- ["Time Range" on page 14](#)
- ["Filter by Target Type" on page 15](#)

"Actions Elevated" Report in Endpoint Privilege Management

The **Actions Elevated** report shows three charts for the Elevated action.

- Elevated actions filtered by the target type per time period.

Click an area in the chart to open the **Target Types > All** report with the **Filter By Target Type** and **Filter by Action** filters applied.

- Distinct target count by the target type for the duration of the time period.

Click an area in the chart or the URLs in the legend to open the **Target Types > All** report with the **Filter By Target Type** and **Filter by Action** filters applied.

- The top 10 Targets.

Click an area in the chart opens the **Events > All** table with the **Action** and **Target Description** filters applied.

The target types are:

- All
- Application
- Services
- COM
- Remote PowerShell
- ActiveX
- URL
- Content



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Target Type" on page 15](#)
- ["Other Actions" on page 18](#)

"Actions Blocked" Report in Endpoint Privilege Management

The **Actions Blocked** report shows three charts for the blocked action:

- Blocked actions filtered by the target type per time period.
Clicking an area in the chart opens the **Target Types > All** report with the **Filter by Action** and **Filter By Target Type** applied.
- Distinct target count by the target type for the duration of the time period.
Clicking an area in the chart or the URLs in the legend opens the **Target Types > All** report with the **Filter by Action** and **Filter By Target Type** applied.
- The top 10 targets.
Clicking an area in the chart opens the **Events > All** table with the **Target Description** filter applied.

The target types are:

- All, Application
- Services
- COM
- Remote PowerShell
- ActiveX
- URL
- Content



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Target Type" on page 15](#)
- ["Other Actions" on page 18](#)

"Actions Passive" Report in Endpoint Privilege Management

The **Actions Passive** report shows three charts for the passive action:

- Passive actions filtered by the target type per time period.
Click an area in the chart to open the **Target Types > All** report with the **Filter by Action** and **Filter By Target Type** applied.
- Distinct target count by the target type for the duration of the time period.
Click an area in the chart or the URLs in the legend to open the **Target Types > All** report with the **Filter by Action** and **Filter By Target Type** applied.
- The Top 10 Targets.
Click an area in the chart to open the **Events > All** table with the **Target Description** filter applied.

The target types are:

- All
- Application
- Services
- COM
- Remote PowerShell
- ActiveX
- URL
- Content



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Target Type" on page 15](#)
- ["Other Actions" on page 18](#)

"Actions Canceled" Report in Endpoint Privilege Management

The **Actions Canceled** report shows three charts for the canceled action:

- Canceled actions filtered by the target type per time period.
Click an area in the chart to open the **Target Types > All** report with the **Filter by Action** and **Filter By Target Type** applied.
- Distinct target count by the target type for the duration of the time period.
Click an area in the chart or the URLs in the legend to open the **Target Types > All** report with the **Filter by Action** and **Filter By Target Type** applied.
- The top 10 Targets.
Click an area in the chart to open the **Events > All** table with the **Target Description** filter applied.

The target types are:

- All
- Application
- Services
- COM
- Remote PowerShell
- ActiveX
- URL
- Content



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Target Type" on page 15](#)
- ["Other Actions" on page 18](#)

"Actions Other" Report in Endpoint Privilege Management

The **Other** report is similar to the **Action** report but shows the less common action types. The default token type in this view is **Custom**.

The **Actions Other** report shows three charts for the other action:

- Actions with a Custom Token applied filtered by the target type per time period.
Click an area in the chart to open the **Target Types > All** report with the **Filter by Action** and **Filter By Target Type** applied.
- Actions with a Custom Token applied filtered by the target type for the duration of the time period.
Click an area in the chart or the URLs in the legend to open the **Target Types > All** report with the **Filter by Action** and **Filter By Target Type** applied.
- The top 10 actions with a Custom Token applied.
Click an area in the chart to open the **Events > All** table with the **Target Description** filter applied.

The target types are:

- All
- Application
- Services
- COM
- Remote PowerShell
- ActiveX
- URL
- Content



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Target Type" on page 15](#)
- ["Other Actions" on page 18](#)

"Actions Custom" Report in Endpoint Privilege Management

The **Actions Custom** report shows three charts for the custom action:

- Custom actions filtered by the target type per time period.
Click an area in the chart to open the **Target Types > All** report with the **Filter by Action** and **Filter By Target Type** applied.
- Distinct target count by the target type for the duration of the time period.
Click an area in the chart or the URLs in the legend to open the **Target Types > All** report with the **Filter by Action** and **Filter By Target Type** applied.
- The top 10 Targets.
Click an area in the chart to open the **Events > All** table with the **Target Description** filter applied.

The target types are:

- All
- Application
- Services
- COM
- Remote PowerShell
- ActiveX
- URL
- Content



For more information on the available quick filters, please see the following:

- ["Time Range" on page 14](#)
- ["Filter by Target Type" on page 15](#)

"Target Types" Dashboard in Endpoint Privilege Management Reporting

The **Targets Types** dashboard breaks down the target activity by the type of target.

Chart	Description
All activity over the last (time interval)	<p>A chart showing the target count filtered by target type across the specified time period.</p> <p>The types of target are:</p> <ul style="list-style-type: none"> • ActiveX • Application • Content Control • URL • Remote PowerShell • COM • Service Control <p>Click the chart to open the Target Types All report with the Filter by Target Type filter applied.</p>
By type	<p>A chart and table showing the total target count by target type.</p> <p>The types of target are:</p> <ul style="list-style-type: none"> • ActiveX • Application • Content Control • URL • Remote PowerShell • COM • Service Control <p>Click the chart to open the Target Types All report with the Filter by Target Type filter applied.</p>
Top 10 activities	<p>A chart showing the 10 most common activities by process count. A unique activity is defined by the type of action and the target name.</p> <p>Click the chart to open the Target Types All report with the Filter by Target Type filter applied.</p>



For more information, please see the following:

- ["Target Types All" Report in Endpoint Privilege Management" on page 47](#)
- ["Time Range" on page 14](#)
- ["Filter by Action" on page 15](#)
- ["Group By" on page 18](#)

"Target Types Applications" Report in Endpoint Privilege Management

The **Target Types Applications** report shows three charts for the application target type:

- Applications activity over the time period.

Click an area in the chart to open the **Target Types > All** report with the **Filter By Target Type** and **Application Type** filters applied.

- Applications filtered by the application type active during the time period.

Click an area in the chart or the URLs in the legend to open the **Target Types > All Report** with the **Filter By Target Type** and **Application Type** filters applied.

- The top 10 application activities.

Click an area in the chart to open the **Events > All** table.

The application types are:

- Windows Store Application
- PowerShell Script
- Installer Package
- Uninstaller
- Control Panel Applets
- Registry Settings
- Windows Script
- Management Console Snapin
- Executable
- Uninstaller
- Batch File
- Binary
- Bundle
- Package
- System Preference
- Sudo Control
- Script



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Action" on page 15](#)
- ["Filter by App Type" on page 16](#)

"Target Types Services" Report in Endpoint Privilege Management

The **Target Types Services** report shows three charts for the **Service** target type:

- Services target types filtered by type of action over the time period. Click an area in the chart to open the **Target Types > All** report with the **Filter By Action** and **Filter by Target Type** filters applied.
- Services filtered by the type of action for the duration of the time period. Click an area in the chart or the URLs in the legend to open the **Target Types > All Report** with the **Filter By Action** and **Filter by Target Type** filters applied.
- The top 10 services activities. Click an area in the chart to open the **Events > All** table with the **Target Type** and **Activity ID** filters applied.

The types of action are:

- Elevated
- Blocked
- Passive
- Sandboxed
- Custom
- Drop Admin Rights
- Enforce default rights
- Canceled



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Action" on page 15](#)

"Target Types COM" Report in Endpoint Privilege Management

The **Target Types COM** (Component Object Model) report shows three charts for the COM target type:

- COM target types filtered by type of action over the time period. Click an area in the chart to open the **Target Types > All** report with the **Filter By Action** and **Filter by Target Type** filters applied.
- COM target types filtered by the type of action for the duration of the time period. Click an area in the chart or the URLs in the legend to open the **Target Types > All** report with the **Filter By Action** and **Filter by Target Type** filters applied.
- The top 10 COM target types. Click an area in the chart to open the **Events > All** table with the **Filter by Action** and **Filter by Target Type** filters applied.



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Action" on page 15](#)

"Target Types Remote PowerShell" Report in Endpoint Privilege Management

The **Target Types Remote PowerShell** report shows three charts for the Remote PowerShell target type:

- Remote PowerShell target types filtered by type of action over the time period. Click an area in the chart to open the **Target Types > All** report with the **Filter By Action** and **Filter by Target Type** filters applied.
- Remote PowerShell target types filtered by the type of action for the duration of the time period. Click an area in the chart or the URLs in the legend to open the **Target Types > All** with the **Filter By Action** and **Filter by Target Type** filters applied.
- The top 10 Remote PowerShell activities. Click an area in the chart to open the **Events > All** table with the **Target Type** and **Activity ID** filters applied.



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Action" on page 15](#)

"Target Types All" Report in Endpoint Privilege Management

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

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

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

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

- **i icon:** Opens the **Application** report with the **Application Desc** and **Publisher** filters applied.
- **Process Count:** Opens the **Events > All** Table with the **Distinct Application ID** filter applied.
- **User Count:** Displays a list of users who generated events with that application within the time period.
- **Host Count:** Displays a list of hosts that generated events with that application within the time period.

If you want to see only applications controlled automatically or only applications launched using the shell menu, you can use the **Shell** or **Auto** filter. The values can be useful in discovering how many times applications are automatically elevated in comparison to deliberately elevated by the user through shell elevation.



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Action" on page 15](#)
- ["Filter by Target Type" on page 15](#)

"Trusted Application Protection" Dashboard in Endpoint Privilege Management

The report shows information about Trusted Application Protection (TAP) incidents. A TAP incident is a child process of a Trusted Application blocked due to a Trusted Application policy, or, a DLL blocked from loading by a Trusted Application because it does not have a trusted owner or trusted publisher.



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

Chart	Description
Trusted Application Protection incidents over the time period.	<p>A column chart showing the number of incidents filtered by the trusted application.</p> <p>Click the chart to open the Process Details table with the Trusted Application Protection Dashboard with time range filters applied.</p>
Trusted Application Protection incidents, by application	<p>A table listing each trusted application, the number of TAP incidents, the number of Targets, the number of Users, and the number of Hosts affected.</p> <p>Click the Incidents number to open the Process Details report with the Trusted Application Name filter applied.</p> <p>Click the Targets number to open the Targets > All table with the Trusted Application Name filter applied.</p>
Top 10 targets (top # of total #)	<p>The top 10 targets for TAP incidents.</p> <p>Click the Target to open the Application report with the Application Type and Distinct Application ID filters applied.</p> <p>Click the Incident number to open the Process Details report with the Distinct Application ID filter applied. Clicking the Users or Hosts number opens the Users or Hosts list respectively.</p>

"Workstyles" Dashboard in Endpoint Privilege Management Reporting

The **Workstyles** report displays how the Workstyles you deployed are used within the specified time period.

The **Workstyles** Dashboard has the following charts:

Chart	Description
All Workstyles over the time period	<p>A table showing the number of Workstyles that matched, the number of hosts, the number of users, and the applications affected by those Workstyles. Workstyles are shown as a percentage of the total in the database, irrespective of any filters apart from Time Range.</p> <p>Click the count for Workstyles, users, or hosts to display a list of the entities. Click the count of applications affected to open the Target Types > All table.</p>
Summary by process activity (top 10)	<p>Shows the top 10 most active Workstyles filtered by the type of action.</p> <p>The types of actions are:</p> <ul style="list-style-type: none"> • Elevated • Blocked • Enforce default token • Custom • Canceled • Sandboxed • Passive • Drop admin Rights <p>Click the chart to open the Events All report with the Action and Workstyle (may include wildcard match) filters applied.</p>
% Coverage by Workstyle (Top 10)	<p>A chart showing the percentage of users and hosts that the most active Workstyles cover. The Workstyles are ordered by the total number of users and hosts affected.</p> <p>Click this chart to display a list of users or hosts affected by the Workstyle.</p>
Process Coverage by Workstyle	<p>A chart showing the process activity by Workstyle.</p> <p>Click this chart to open the Events All report with the Filter by Event Category and Workstyle filters applied.</p>
Process Coverage by Group Policy Object	<p>A chart showing the process activity filtered by policy.</p> <p>Click this chart to open the Events All report with the Filter by Event Category and GPO Name filters applied.</p>
Top 10 Elevating Workstyles	<p>A chart showing the Workstyles responsible for the most individual applications being elevated.</p> <p>Click the chart to open the Target Types All report with the Filter by Action filter applied.</p>
Top 10 Blocking Workstyles	<p>A chart showing the Workstyles responsible for the most individual applications being blocked.</p> <p>Click the chart to open the Target Types all report with the Filter by Action filter applied.</p>

Chart	Description
Top 10 Passive Workstyles	A chart showing the Workstyles responsible for the most individual applications being passively audited. Click the chart to open the Target Types All report with the Filter by Action filter applied.
Top 10 Custom Token Workstyles	A chart showing the Workstyles responsible for the most individual applications having a Custom Token applied. Click the chart to open the Target Types All report with the Filter by Action filter applied.



For more information on the available quick filters, please see the following:

- ["Events All" on page 57](#)
- [""Target Types All" Report in Endpoint Privilege Management" on page 47](#)
- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Action" on page 15](#)
- ["Filter by Target Type" on page 15](#)

Workstyles All

This table lists all Workstyles by actions in the time period, grouped by the Workstyle name.

The following columns are available for the **Workstyles All** table:

- **Workstyle Name:** The name of the Workstyle.
- **GPO Name:** The Group Policy Object name.
- **Elevated:** The count of the Elevated events.
- **Passive:** The count of the Passive events.
- **Blocked:** The count of the Blocked events.
- **Sandboxed:** The count of the Sandboxed events.
- **Canceled:** The count of the Canceled events.
- **Custom:** The count of the Custom events.
- **Drop Admin:** The count of the Drop Admin events.
- **Enforce Default:** The count of the events enforced by default.
- **Total:** The total number of events.
- **Policy Name:** The name of the policy that includes the Workstyle.

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

- The **i** icon opens a Workstyle report.
- Click any of the numbers to see the list of events in **Events > All**.



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Target Type" on page 15](#)

"Users" Dashboard in Endpoint Privilege Management Reporting

The **Users** report links to the **User Experience** report.

User Experience Report in Endpoint Privilege Management

The report shows how users interacted with Messages, Challenge/Response dialog boxes, and the Shell (On-Demand) menu.

Chart	Description
User Experience over the time period	<p>A chart showing the percentage of users that experienced each interaction type filtered by the specified time period.</p> <p>Click the chart to display a list of users presented with that interaction.</p>
Message Distribution	<p>A chart showing how many users are in the defined categories of messages per time period.</p> <p>Click the chart to display a list of users in that category.</p>
Messages per action type	<p>A table showing message types displayed for Allowed and Blocked actions.</p> <p>Click the Prompts, Notifications or counts, or table to open the Events All report with the Action and Message Type filters applied.</p>



For more information on the available quick filters, please see the following:

- ["Events All" on page 57](#)
- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Action" on page 15](#)

Privileged Logons Report in Endpoint Privilege Management

The **Privileged Logon** report shows you how many accounts with **Standard** rights, **Power User** rights and **Administrator** rights generated logon events filtered by the time frame.

Chart	Description
Privileged Logons over the last (time interval)	<p>A chart and table showing the number of logons by the account types over time.</p> <p>Click the chart to open the User Logons table with the Show Administrator Logons, Show Power User Logons and Show Standard User Logons filters applied.</p>
Logons by Account Privilege	<p>A chart showing the total number of logons filtered by the different account types.</p> <p>Click the chart to open the User Logons table with the Show Administrator Logons, Show Power User Logons and Show Standard User Logons filters applied.</p>
Logons by Account Type	<p>A chart showing the total number of logons filtered by Domain Accounts and Local Accounts.</p> <p>Click the chart to open the User Logons table with the Account Authority filter applied.</p>
Top 10 Logons by Chassis Type	<p>A chart showing the total number of logons filtered by the top 10 Chassis types.</p> <p>Click the chart to open the User Logons table with the Chassis Type filter applied.</p>

Chart	Description
Top 10 Logons by host Operating System	A chart showing the total number of logons filtered the top 10 host operating systems. Click the chart to open the User Logons table with the OS filter applied.
Top 10 Accounts with Admin Rights	A chart showing the top 10 accounts with Admin rights that have logged into the most host machines. Click the chart to open the User Logons table with the User Domain and User Name filter applied.
Top 10 hosts with Admin Rights	A chart showing the top 10 host machines logged on to by the most users with Admin Rights Click the chart to open the User Logons table with the Host Name , Show Administrator Logons filter applied.



For more information on the available quick filters, please see the following:

- For enabling user logon audits, the [Collect User Information](#) section of the [Endpoint Privilege Management Administration Guide](#)
- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)

Privileged Account Management

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

Chart	Description
Privileged Account Management over the last (time interval)	A chart breaking down the PAM events by time period. Click the chart to display the Privileged Account Management table with the Range Start Time and Range End Time filters applied.
Table showing users blocked, hosts blocked, applications blocked and total blocked modifications	A table showing the number of Users blocked, the number of Hosts blocked, the number of Applications blocked, and the Total number of blocked events within the specified time frame. Click the count numbers to open the Privileged Account Management table.
By Privileged Group	A chart showing the Privileged Account Modification activity blocked by Windows group name. Click the chart to open the Privileged Account Protection table with the Group Name filter applied.
Top 10 applications attempting account modifications	A chart showing the Privileged Account Modification activity that was blocked broken down by the Application Description. Click the chart to open the Privileged Account Management table with the Application Description filter applied.
Top 10 users attempting account modifications	A chart showing the top 10 users who attempted modifications. Click the chart to open the Privileged Account Management table with the User Name filter applied.
Top 10 hosts attempting account modifications	A chart showing the top 10 Hosts attempting privileged account modifications. Click the chart to open the Privileged Account Management table with the Host Name filter applied.



For more information on the available quick filters, please see the following:

- *For a list of Group Accounts that are considered privileged and for guidance on enabling generation of Privileged Account Management audits, the Prohibit Privileged Account Management section of the [Endpoint Privilege Management Administration Guide](#)*
- *["Platform" on page 14](#)*
- *["Time Range" on page 14](#)*

"Deployments" Dashboard in Endpoint Privilege Management

The **Deployments** dashboard shows you the versions of Endpoint Privilege Management that are currently installed in your organization. The dashboard filters the deployments by operating system, default language, chassis type, and operating system type.

Chart	Description
By Endpoint Privilege Management Client Version	<p>A chart showing the versions of the Endpoint Privilege Management agents that are deployed filtered by the number of deployments.</p> <p>Click the chart to display the Deployments table with the Agent Version filter applied.</p>
By Operating System	<p>A chart showing the number of deployments filtered by the operating system.</p> <p>Click the chart to display the Deployments table with the Operating System filter applied.</p>
By Default Language	<p>A chart showing the number of deployments filtered by the default language.</p> <p>Click the chart to display the Deployments table with the Default UI Language filter applied.</p>
By Chassis Type	<p>A chart showing the number of deployments filtered by chassis type.</p> <p>Clicking the chart displays the Deployments table with the Chassis filter applied.</p>
By Operating System Type	<p>A chart showing the number of deployments filtered by the type of operating system.</p> <p>Click the chart to display the Deployments table with the Operating System Type filter applied.</p>



For more information on the available quick filters, please see the following:

- For guidance on enabling collection of host information audits, the [Endpoint Privilege Management Administration Guide](#)
- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)

Requests Dashboard in Endpoint Privilege Management

This report shows information about user requests raised over the specified time frame. A Blocked message with a reason entered or a canceled Challenge/Response message are requests.

Chart	Description
All Requests over the last (time interval)	A column chart showing the number of the different request types filtered by the time period. Click the chart to open the Requests All report with the Request Type filter applied for the date range.
Requests by Workstyle	A chart showing the number of different request types filtered by the Workstyle. Click the chart to open the Requests All report with the Request Type and Workstyle (may include wildcard match) filters applied.
Requests by Target Type	A chart showing the number of the different request types filtered by the Target Type. Click the chart to open the Requests All report with the Request Type filter applied for the date range.
Top 10 Activities Requested	A chart showing the number of the different request types filtered by the Target Name. Click the chart to open the Requests All report with the Request Type and Application Desc filters applied.

Requests All

This report lists all the requests over the specified time period. Filters can be added using the dropdown **Filter Panel** and the table can be sorted by a specific column by clicking on the vertical arrows next to each column name.

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

- **Start Time:** The start time of the event.
- **Description:** The description of the application.
- **Workstyle:** The name of the Workstyle that triggered the event.
- **User Name:** The user name of the user who triggered the event.
- **Host Name:** The host name where the event was triggered.
- **User Reason:** The reason the user provided for the request.
- **Request Type:** The type of request.
- **Reputation:** The reputation of the application.

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

- The **i** icon opens the **Event** report for that request.



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Target Type" on page 15](#)

"Events" Dashboard in Endpoint Privilege Management

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

Chart	Description
Events over the last (time interval)	A column chart showing the number of the different Event Types filtered by the time period. Clicking the chart opens the Events All report with the Filter by Event Category filter applied.
Event Types	A chart showing the number of events received filtered by the Event Type. Clicking the chart opens the Events All report with the Event Number filter applied.
By Category	A chart displaying the events received filtered by Category. Clicking the chart opens the Events All report with the Filter by Event Category filter applied.
Time since last endpoint event	A chart showing the number of endpoints in each time since last event category.



For more information, please see the following:

- ["Events All" on page 57](#)
- [""Deployments" Dashboard in Endpoint Privilege Management" on page 55](#)
- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)

Events All

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

- **Event Time:** The time of the event.
- **Reputation:** The reputation of the event, where applicable.
- **Platform:** The platform the event came from.
- **Description:** The description of the event.
- **User:** The user name of the user who triggered the event.
- **Host:** The host name where the event was triggered.
- **Workstyle:** The Workstyle containing the rule that triggered the event.
- **Event Category:** The category of the event.
- **Event Type:** The type of event.

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

- **i** icon: opens the event report listing all the fields for that event.
- **Description:** opens the **Applications** Report.
- **User:** opens the **User** Report.
- **Host:** opens the **Host** Report.
- **Workstyle:** opens the **Workstyle** Report.



For more information on the available quick filters, please see the following:

- ["Platform" on page 14](#)
- ["Time Range" on page 14](#)
- ["Filter by Event Category" on page 16](#)

Process Detail

The **Process Detail** report provides a higher level of detail for Process events than the **Events > All** table. Other event categories are not shown in this table. You can access the **Process Detail** report by clicking on **Process Detail** from the Quick Filter panel in the **Events > All** report.

The following columns are available for the Windows and macOS **Process Details** table:

- **Start Time:** The start time of the event.
- **Platform:** The platform that the event occurred on.
- **Description:** The description of the application.
- **Publisher:** The publisher of the application.
- **Application Type:** The type of application.
- **File Name:** The name of the file.
- **Command Line:** The command line of the process that triggered the event.
- **Product Name:** The product name of the application.
- **Product Version:** The product version of the application.
- **Trusted Application:** The name of the trusted application.
- **Trusted Application Version:** The version of the trusted application.
- **Group Policy Object:** The name of the Endpoint Privilege Management policy (Windows only).
- **Workstyle:** The name of the Workstyle that the event was triggered from.
- **Message:** The message name if the event triggered a message.
- **Action:** The action associated with the event.
- **Application Group:** The Application Group the application assignment rule belongs to.
- **PID:** The process identifier of the process.
- **Parent PID:** The parent process identifier.
- **Parent Process File Name:** The parent process file name.
- **Shell / Auto:** Whether the process was triggered on-demand or automatically (Windows only).
- **UAC Triggered:** Whether user account control was triggered (Windows only).
- **Admin Rights Required:** Whether or not admin rights were required (Windows only).
- **Authorization Required:** Whether or not authorization rights were required (macOS only).
- **User Name:** The name of the user who triggered the event.
- **Host Name:** The name of the host where the event was triggered.
- **Rule Script File Name:** The name of the Rule Script (Power Rule).
- **Rule Script Affected Rule:** True when the Rule Script (Power Rule) changed one or more of the Default Endpoint Privilege Management rule, otherwise false.
- **User Reason:** The reason given by the user if applicable.

- **COM Display Name:** The COM name if applicable (Windows only).
- **Source URL:** The URL of the event if applicable (Windows only).
- **BeyondTrust Zone Identifier:** The BeyondTrust Zone identifier if present.
- **Uninstall Action:** This can be **None**, **Uninstall**, **Change/Modify**, or **Repair**.
- **Auth Methods:** The type of authentication method selected in the Policy Editor. Multiple values can be present and will be comma separated. Possible values: **Identity Provider**, **Password**, **Challenge Response**, **Smart Card**, and **User Request**.
- **Idp Authentication User Name:** The credential provided when adding an Identity Provider authorization message in the Policy Editor.

Export Events to CSV File

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

All event filters will be saved to the file.

"Database Administration" Report in Endpoint Privilege Management

The **Database Administration** report is an optional feature and will only be available if you check the **Install audit database administration report** box during the Reporting Pack installation.

To view the report, navigate to it from the Reporting root directory.

In your web browser, go to the URL <https://hostname/ReportServer>. If you are using a named SSRS instance, the URL is https://hostname/ReportServer_InstanceName:

1. Click the **BeyondTrust Endpoint Privilege Management** link where **Reporting** or **Avecto Privilege Guard** is the name of your Reporting database.
2. From the top of the list, click the **Admin** link.
3. Click the **ErpEventsAdmin** link.

The **Database Administration** report provides application event purge and exclusion functions. In some situations applications create an audit data volume that exhausts capacity. These functions allow you to respond to excess event data quickly.

Chart	Description
Events generated over the last 12 months	Displays the number of events across all your applications for the last 12 months.
Events totals (over all time)	Displays the number of events in the database filtered by processes, events, user sessions, and host sessions.
Purging options	Purging data removes the data from the database using the Purging Options available from the report: <ul style="list-style-type: none"> • Purge data older than 6 months • Purge data older than 3 months • Purge data older than 1 month • Purge all data
Top 20 applications in database	The table displays the top 20 applications in the database by the number of events they generate. Click Purge to purge the events from that application. Future events will still be captured. Click Purge & Exclude to purge the events from that application and stop future events from being collected. Excluded applications appear in the table at the bottom and can be removed from the exclusion list.

The Endpoint Privilege Management Purge Tool Utility

Reporting includes an optional **ER Purge Tool**, which allows old data to be purged from the Endpoint Privilege Management database. The ER Purge Tool can be downloaded from the BeyondTrust website. After you install the ER Purge Tool, you can run it from the Windows Start Menu.



Note: Before purging large sets of data, please ensure your SQL Transaction logs can grow to accommodate this. It may be necessary to delete data in stages when setting this up for the first time.



For more information about the **ER Purge Tool**, please see the [Endpoint Privilege Management Reporting Installation Guide](https://www.beyondtrust.com/docs/privilege-management/windows/index.htm) at <https://www.beyondtrust.com/docs/privilege-management/windows/index.htm>.

Use Export Views in Endpoint Privilege Management Reporting

BeyondTrust provides four denormalized export views for Endpoint Privilege Management events:

- ExportDefendpointStarts
- ExportLogons
- ExportPrivilegedAccountProtection
- ExportProcesses

For each view, the following data is sent to the Endpoint Privilege Management Reporting database. These export views are correct as of Endpoint Privilege Management Reporting 4.5.

ExportDefendpointStarts

Column_name	Type	Length	Index	Description	Example
SessionID	bigint		3	Ascending Identity	1
SessionGUID	uniqueidentifier			UUID of the session	5CD221E9-CEB5-441D-B380-CB266400B320
SessionStartTime	datetime			Time session started	2017-01-03 10:24:00.000
SessionEndTime	datetime			Always NULL (not used)	NULL
HostSID	nvarchar	200	1	Host SID	S-1-21-123456789-123456789-1635717638-390614945
AgentVersion	nvarchar	20		Endpoint Privilege Management Client Version	4.0.384.0
ePOMode	int			1 if DP client is in ePO mode. 0 otherwise.	1
CertificateMode	int			Certificate Mode	0
PolicyAuditMode	int			Policy Audit Mode	7
DefaultUILanguage	int			Locale Identifier of UI Language	2057
DefaultLocale	int			Locale Identifier of Locale	2057
SystemDefaultTimezone	int			Not set so always 0	0
ChassisType	nvarchar	40		Chassis Type	Other
HostName	nvarchar	1024	2*	Host name	EGHostWin1
HostNameNETBIOS	nvarchar	15	2*	Host NETBIOS	EGHOSTWIN1
OS	nvarchar	20		OS Version	6.3
OSProductType	int	4		OS Product Type.	1
PlatformType	nvarchar	10		Platform Type	Windows
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638

Column_name	Type	Length	Index	Description	Example
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomainNameNETBIOS	nvarchar	15		Host Domain NETBIOS	EGDOMAIN

ExportLogons

Column_name	Type	Length	Index	Description	Example
LogonID	bigint		3	Ascending Identity	1
LogonGUID	uniqueidentifier			UUID of the logon	819EF606-F9B6-40BE-9C0C-A033A34EC4F8
HostSID	nvarchar	200	1	Host SID	S-1-21-123456789-123456789-1635717638-390614945
UserSID	nvarchar	200		User SID	S-1-21-123456789-123456789-1635717638-1072059836
LogonTime	datetime			Logon Date/Time	2017-01-03 10:24:00.000
IsAdmin	bit			1 if an admin, 0 otherwise	0
IsPowerUser	bit			1 if a power user, 0 otherwise	0
UILanguage	int			Locale Identifier of the UI Language	1033
Locale	int			Locale Identifier of the Locale	2057
UserName	nvarchar	1024		User name	EGUser1
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserNameNETBIOS	nvarchar	15		User NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Docking Station
HostName	nvarchar	1024	2*	Host name	EGHostWin1
HostNameNETBIOS	nvarchar	15	2*	Host NETBIOS	EGHOSTWIN1
OS	nvarchar	20		OS Version	6.3
OSProductType	int			OS Product Type	1
PlatformType	nvarchar	10		Platform Type	Windows
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomainNameNETBIOS	nvarchar	15		Host Domain NETBIOS	EGDOMAIN
PolicyName	nvarchar	1024		Policy Name	EventGen Test Policy
WorkstyleName	nvarchar	1024		Workstyle name	EventGen Test Workstyle

ExportPrivilegedAccountProtection

Column_name	Type	Length	Index	Description	Example
ID	bigint		1	Ascending Identity	1
TimeGenerated	datetime			Event Generation Date/Time	
CommandLine	nvarchar	1024		Command Line	<None>
PrivilegedGroupName	nvarchar	200		Privileged Group Name	Administrators
PrivilegedGroupRID	nvarchar	10		Privileged Group Relative Identifier	544
Access	nvarchar	200		Group Access Details	Add Member, Remove Member, List Members, Read Information
PolicyGUID	uniqueidentifier			Policy UUID	E7654321-AAAA-5AD2-B954-12342918D604
PolicyName	nvarchar	1024		Policy Name	EventGen Test Policy
WorkstyleName	nvarchar	1024		Workstyle name	EventGen Test Workstyle
FileName	nvarchar	255		File name	<None>
ApplicationHash	nvarchar	40		Application SHA1	921CA2B3293F3FCB905B24A9536D8525461DE2A3
ProductCode	nvarchar	1024		Product Code	<None>
UpgradeCode	nvarchar	1024		Upgrade Code	<None>
FileVersion	nvarchar	1024		File Version	<None>
MD5	nvarchar	32		MD5 Hash	3279476E39DE235B426D69CFE8DEBF55
UserSID	nvarchar	200		User SID	S-1-21-123456789-123456789-1635717638-1072059836
UserName	nvarchar	1024		User Name	EGUser1
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserNameNETBIOS	nvarchar	15		User Domain NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Other

Column_name	Type	Length	Index	Description	Example
HostSID	nvarchar	200		Host SID	S-1-21-123456789-123456789-1635717638-390614945
HostName	nvarchar	1024		Host Name	EGHostWin1
HostNameNETBIOS	nvarchar	15		Host NETBIOS	EGHOSTWIN1
OS	nvarchar	20		OS Version	6.3
OSProductType	int			OS Product Type	1
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomainNameNETBIOS	nvarchar	15		Host domain NETBIOS	EGDOMAIN
FileOwnerUserSID	nvarchar	200		File Owner SID	S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464
FileOwnerUserName	nvarchar	1024		File Owner	NT SERVICE\TrustedInstaller
FileOwnerDomainName	nvarchar	1024		File Owner Domain	NT SERVICE
ApplicationURI	nvarchar	1024		URI of a macOS application	com.apple.preference.datetime
ApplicationDescription	nvarchar	2048		Application description	lusrmgr.msc
FirstDiscovered	datetime			First time app was seen	2017-01-03 10:25:50.110
FirstExecuted	datetime			First time app was executed	2017-01-03 10:24:00.000
PlatformType	nvarchar	10		Platform Type	Windows
ProductName	nvarchar	1024		Product name	<None>
ProductVersion	nvarchar	1024		Product version	<None>
Publisher	nvarchar	1024		Publisher	Microsoft Windows
TrustedOwner	bit			1 if a trusted owner, 0 otherwise	1

ExportProcesses

Column_name	Type	Length	Index	Description	Example
ProcessID	bigint		4	Ascending Identity	1
ProcessGUID	uniqueidentifier		2	UUID of the process	98C99D96-6DFA-4C95-9A87-C8665C166286
EventNumber	int			Event Number. See List of Events section.	153
TimeGenerated	datetime			Event generation date/time	2017-02-20 13:11:11.217
TimeReceived	datetime			Event received at ER date/time	2017-02-20 13:16:28.047
EventGUID	uniqueidentifier			Event UUID	9F8EB86C-AA0D-42B9-8720-166FAB91F1ED
PID	int			Process ID	8723
ParentPID	int			Parent Process ID	142916
CommandLine	nvarchar		1024	Command Line	"C:\cygwin64\bin\sh.exe"
FileName	nvarchar		255	File Name	c:\cygwin64\bin\sh.exe
ProcessStartTime	datetime		1	Date/Time Process Started	2017-02-20 13:11:11.217
Reason	nvarchar		1024	Reason entered by user	<None>
ClientIPV4	nvarchar		15	Client IP Address	10.0.9.58
ClientName	nvarchar		1024	Client Name	L-CNU410DJJ7
UACTriggered	bit			1 if UAC shown	0
ParentProcessUniqueID	uniqueidentifier			Parent process UUID	C404C7F5-3A93-4C0E-81BC-9902D220C21E
COMCLSID	uniqueidentifier			COM CLSID	NULL
COMAppID	uniqueidentifier			COM Application ID	NULL
COMDisplayName	nvarchar	1024		COM Display Name	<None>
ApplicationType	nvarchar	4		Application Type	svc
TokenGUID	uniqueidentifier			UUID of token in policy	F30A3824-27AF-4D69-9125-C78E44764AC1
Executed	bit			1 if executed, 0 otherwise	1
Elevated	bit			1 if elevated, 0 otherwise	1

Column_name	Type	Length	Index	Description	Example
Blocked	bit			1 if blocked, 0 otherwise	0
Passive	bit			1 if passive, 0 otherwise	0
Cancelled	bit			1 if cancelled, 0 otherwise	0
DropAdmin	bit			1 if admin rights dropped, 0 otherwise	0
EnforceUsersDefault	bit			1 if user default permissions were enforced, 0 otherwise	0
Custom	bit			1 if Custom Token, 0 otherwise	0
SourceURL	nvarchar	2048		Source URL	<None>
AuthorizationChallenge	nvarchar	9		Challenge Response authorization code	<None>
WindowsStoreAppName	nvarchar	200		Windows Store application name (appx app type only)	<None>
WindowsStoreAppPublisher	nvarchar	200		Windows Store application publisher (appx app type only)	<None>
WindowsStoreAppVersion	nvarchar	200		Window Store application version (appx app type only)	<None>
DeviceType	nvarchar	40		Device Type	Fixed Disk
ServiceName	nvarchar	1024		Service name (svc events only)	<None>
ServiceDisplayName	nvarchar	1024		Service Display Name (svc app type only)	<None>
PowerShellCommand	nvarchar	1024		PowerShell Command (ps1/rpsc/rpss app types only)	<None>
ApplicationPolicyDescription	nvarchar	1024		Policy Description	<None>

Column_name	Type	Length	Index	Description	Example
SandboxGUID	uniqueidentifier			Sandbox UUID (sandbox events only)	NULL
SandboxName	nvarchar	1024		Sandbox Name (sandbox events only)	NULL
BrowseSourceURL	nvarchar	2048		Sandbox browse source (sandbox events only)	<None>
BrowseDestinationURL	nvarchar	2048		Sandbox destination source (sandbox events only)	<None>
Classification	nvarchar	200		Sandbox classification (sandbox events only)	Private (Local)
IEZoneTag	nvarchar	200		IE Zone Tag	<None>
OriginSandbox	nvarchar	40		Origin Sandbox	<None>
OriginIEZone	nvarchar	40		Origin IE Zone	<None>
TargetSandbox	nvarchar	40		Target Sandbox	<None>
TargetIEZone	nvarchar	40		Target IE Zone	<None>
AuthRequestURI	nvarchar	1024		Authorization request URL (osx challenge/response only)	<None>
PlatformVersion	nvarchar	10		Platform Version	<None>
ControlAuthorization	bit			1 is Endpoint Privilege Management authorized this macOS application	0
TrustedApplicationName	nvarchar	1024		Name of the trusted application	Microsoft Word
TrustedApplicationVersion	nvarchar	1024		Version of the trusted application	11.1715.14393.0
ParentProcessFileName	nvarchar	1024		Parent process file name	Google Chrome
ApplicationHash	nvarchar	40		SHA1 of the application	C22FF10511ECCEA1824A8DE64B678619C21B4BEE
ProductCode	nvarchar	1024		Product Code	<None>
UpgradeCode	nvarchar	1024		Upgrade Code	<None>
FileVersion	nvarchar	1024		File Version	<None>

Column_name	Type	Length	Index	Description	Example
MD5	nvarchar	32		MD5 hash of the app	6E641CAE42A2A7C89442AF99613FE6D6
TokenAssignmentGUID	uniqueidentifier			UUID of the token assignment in the policy	E7654321-BBBB-5AD2-B954-1234DDC7A89D
TokenAssignmentIsShell	bit			Token assignment is for shell	1
UserSID	nvarchar	200		User SID	S-1-21-123456789-123456789-16357176381125883508
UserName	nvarchar	1024		User Name	EGUser18
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserDomainNameNETBIOS	nvarchar	15		User Domain NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Laptop
HostSID	nvarchar	200		Host SID	S-1-21-123456789-123456789-1635717638775838649
HostName	nvarchar	1024	3*	Host Name	EGHostWin18
HostNameNETBIOS	nvarchar	15	3*	Host NETBIOS	EGHOSTWIN18
OS	nvarchar			OS Version	10.0
OSProductType	int			OS Product Type	
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomainNameNETBIOS	nvarchar	15		Host Domain NETBIOS	EGDOMAIN
AuthUserSID	nvarchar	200		Authorizing User SID	<None>
AuthUserName	nvarchar	1024		Authorizing User	<None>
AuthUserDomainSID	nvarchar	200		Authorizing User Domain SID	<None>
AuthUserDomainName	nvarchar	1024		Authorizing User Domain	<None>
AuthUserDomainNameNETBIOS	nvarchar	15		Authorizing User Domain NETBIOS	<None>
FileOwnerUserSID	nvarchar	200		File Owner SID	S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464
FileOwnerUserName	nvarchar	1024		File Owner	NT SERVICE\TrustedInstaller
FileOwnerDomainSID	nvarchar	200		File Owner Domain SID	S-1-5-80
FileOwnerDomainName	nvarchar	1024		File Owner Domain	NT SERVICE

Column_name	Type	Length	Index	Description	Example
FileOwnerDomainNameNETBIOS	nvarchar	15		File Owner Domain NETBIOS	<None>
ApplicationURI	nvarchar	1024		URI of the macOS Application	com.apple.preference.datetime
ApplicationDescription	nvarchar	2048		Application Description	c:\cygwin64\bin\sh.exe
FirstDiscovered	datetime			Time application first seen	2017-02-07 09:14:39.413
FirstExecuted	datetime			Time application first executed	2017-02-07 09:07:00.000
PlatformType	nvarchar	10		Platform Type	Windows
ProductName	nvarchar	1024		Product Name	ADeIRCP Dynamic Link Library
ProductVersion	nvarchar	1024		Product Version	15.10.20056.167417
Publisher	nvarchar	1024		Publisher	Adobe Systems, Incorporated
TrustedOwner	bit			1 if a trusted owner, 0 otherwise	0
MessageGUID	uniqueidentifier			UUID of the message in the policy	00000000-0000-0000-0000-000000000000
MessageName	nvarchar	1024		Name of the message in the policy	Block Message
MessageType	nvarchar	40		Message Type	Prompt
AppGroupGUID	uniqueidentifier			UUID of the Application Group in the Policy	47E4A204-FC06-428B-8E73-1E36E3A65430
AppGroupName	nvarchar	1024		Application Group Name in the Policy	Test Policy.test
PolicyID	bigint			Internal ID of the Policy	2
PolicyGUID	uniqueidentifier			UUID of the Policy	E7654321-AAAA-5AD2-B954-12342918D604
PolicyName	nvarchar	1024		Policy Name	EventGen Test Policy
WorkstyleName	nvarchar	1024		Workstyle Name	EventGen Test Workstyle
ContentFileName	nvarchar	255		Content File Name	c:\users\user.wp-epo-win7-64\downloads\con29 selectable feestable (1).pdf
ContentFileDescription	nvarchar	1024		Content File Description	<None>
ContentFileVersion	nvarchar	1024		Content File Version	<None>
ContentOwnerSID	nvarchar	200		Content Owner SID	S-1-21-123456789-123456789-1635717638-1072059836

Column_name	Type	Length	Index	Description	Example
ContentOwnerName	nvarchar	1024		Content Owner	EGUser1
ContentOwnerDomainSID	nvarchar	200		Content Owner Domain SID	S-1-5-21-2217285736-120021366-3854014904
ContentOwnerDomainName	nvarchar	1024		Content Owner Domain	BEYONDTRUST TEST58\BEYONDTRUSTTEST58.QA
ContentOwnerDomainNameNetBIOS	nvarchar	15		Content Owner Domain NETBIOS	BEYONDTRUSTTEST58
UninstallAction	nvarchar	20		The uninstall action carried out	Change/Modify
TokenName	nvarchar	20		The name of the event action	Blocked
TieStatus	int			Threat Intelligence Exchange status for the reputation of this application	0
TieScore	int			Threat Intelligence Exchange score for the application	
VtStatus	int			VirusTotal status for the reputation of this application	
RuleScriptFileName	nvarchar	200		The name in config of the script associated with the rule	Get-McAfeeGTIReputation
RuleScriptName	nvarchar	200		The name of the script set by interface	Get-McAfeeGTIReputation
RuleScriptVersion	nvarchar	20		Version number of the script.	1.1.0
RuleScriptPublisher	nvarchar	200		Publisher that signed the script	BeyondTrust
RuleScriptRuleAffected	bit			True when the script has set all settable rule properties; otherwise false	True
RuleScriptStatus	nvarchar	100		Success OR Why the configured script didn't run or set rule properties	Success
RuleScriptResult	nvarchar	1024		Result of the script run	Script ran successfully
RuleScriptOutput	nvarchar	1024		The output of the script	

Column_name	Type	Length	Index	Description	Example
AuthorizationSource	nvarchar	200		The Authorizing User Credential Source	
AuthMethods	nvarchar	1024		The type of authentication method selected in the Policy Editor.	Possible values: Identity Provider, Password, Challenge Response, Smart Card and User Request. Multiple values can be present and will be comma separated.
IdPAuthentication	nvarchar	400		The credential provided when adding an Identity Provider authorization message in the Policy Editor.	