BeyondTrust

Privilege Management
Enterprise Reporting Dashboard Guide
5.3.24.0 GA

TC:2/6/2019

Table of Contents

Introduction

Defendpoint Enterprise Reporting includes a rich set of dashboards and reports designed to simplify the centralized management and auditing of Defendpoint 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 within Enterprise Reporting, as well as the reports and event data accessible from each view.

Enterprise Reporting Concepts

There are several concepts in Enterprise Reporting that are described here.

Dashboards, Tables and Reports

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

Drill-Down

Drill-down is a user action in a report where you click on a link to see the data pertaining to that link at a greater level of granularity.

Permalink

Permalink refers to a link at the bottom of most reports that allows you to generate a unique URL that means someone else can view that exact page after they login.

Operating Systems

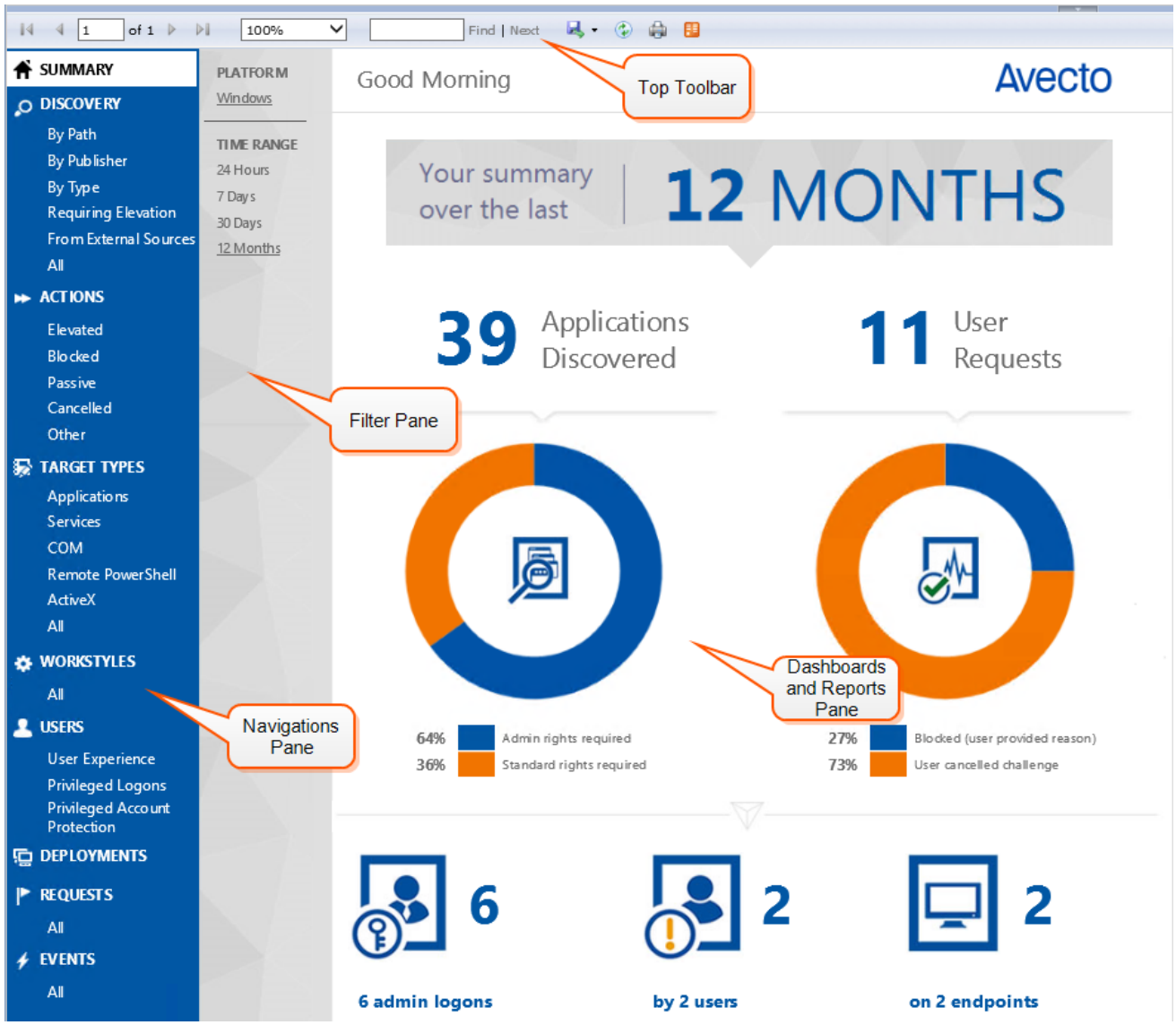
All dashboards have a Microsoft Windows view to display events from Windows endpoints. Some dashboards and reports also have a macOS view.

Name Conventions and Navigation

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

Interface

The Enterprise Reporting interface allows you switch between dashboards and reports and filter to data as required.



There is a link at the bottom of each report called **permalink**. This can be used to create a static link to that report with your choice of filters applied, see "Permalink to Reports" on page 12.

Navigation Panel

The side navigation panel takes you to each top-level dashboard and the reports within that dashboard. Reports that are post-fixed with 'All' means 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

The quick panel on the left-hand side displays a set of pre-defined filters relevant to the current dashboard or report to refine the data.

Name	Description

Platform	• Windows
	  ◦ Filters by endpoints running a Windows operating system.
	• OS X
	  ◦ Filters by endpoints running a Mac operating system.

Time Range	This is the time range that the actions are displayed over. For example, you can filter to the number of elevated actions in the last 24 hours in the **Actions** > **Elevated** report. You can choose from: • 24 Hours • 7 Days • 30 Days • 12 Months
First Reported	This is the time range filtered by the date the application was first entered into the database. For example, you can filter to the new Windows applications by publisher that were first reported in the last 7 days in the **Discovery** > **By Publisher** report. You can choose from: • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months

Name	Description
First Executed	This is the time range over which the application was first executed. For example, you can filter to the new Windows applications, by type that were first executed in the last 30 days in the **Discovery** > **By Type** report. You can choose from: • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months
Filter by Target Type	This filter allows you to filter by a type of target. For example, you can filter to the applications that have been canceled across your time range in the Actions > Canceled report. You can choose from: • All • Applications • Services • COM • Remote PowerShell • ActiveX • URL • Content
Filter by Action	This filter allows you to filter by a type of action. For example, you can filter to the services that have been elevated across your time range in the **Target Types** > **Services** report. You can choose from: • All • Elevated • Blocked • Passive • Sandboxed • Canceled

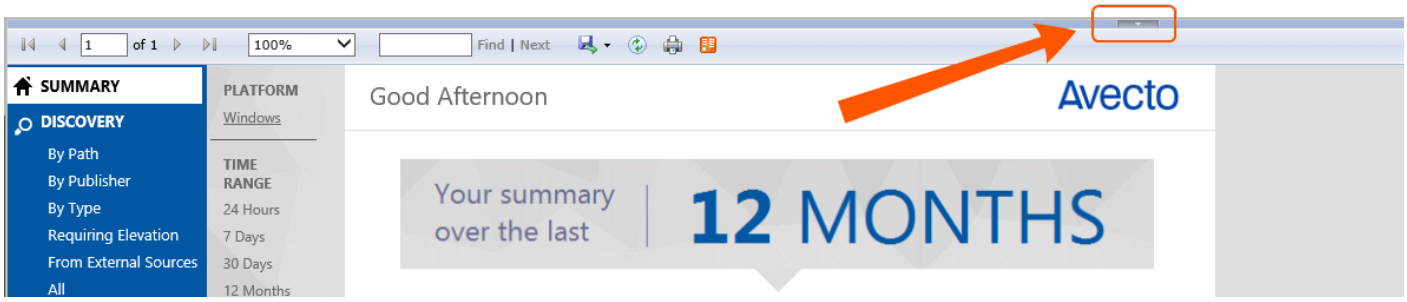
Name	Description
Filter by App Type	This filter allows you to filter by application type. For example, you can filter by applications that are executables that have been used across your time range in **Target Types** > **Applications**. You can choose from: • All • Executable • Control Panel Applet • Management Console • Installer Package • Uninstaller • Windows Script • PowerShell Script • Batch File • Registry Settings • Windows Store • Binary • Bundle • Package • System Preference • Sudo Control
Filter by Event Category	This filter allows you to filter by the category of the event. For example, you can filter by process events only, that have been raised across your time range in the **Events** > **All** report. You can choose from: • All • Process • DLL Control • Content • URL • Privileged Account Protection • Agent Start • User Logon • Services

Name	Description
Elevate Method	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 You can choose from: • All • Admin account used • Auto-elevated • On-demand
Path	Allows you to filter by the path. For example, to filter on applications that were launched from the System path. You can choose from: • All • System • Program Files • User Profiles
Source	The media source of the application. For example, was the application downloaded from the internet or, was it taken from removable media? You can choose from: • All • Any external source • Downloaded from internet • Removable media
Challenge / Response	Allows you to filter by challenge/response events. For example, you can filter the application that required elevation on those applications that were launched following a completed challenge/response message. You can choose from: • All • Only C/R
Admin Rights	Allows you to filter by the admin rights token. You can choose from: • All • Detected • Not Detected

Name	Description
Authorization	Allows you to filter by authorization. You can choose from: • All • Required • Not Required
Group By	You can choose from: • All • Publisher • Application Group • Message • Workstyle
Ownership	Allows you to group by the type of owner. You can choose from: • All • Trusted owner • Untrusted owner
Matched	Allows you to filter on the type of matching. You can choose from: • All • Matched directly • Matched as child
Other Actions	Allows you to filter by other actions. You can choose from: • Custom • Drop Admin Rights • Enforce Default Rights
Details	Process Details

Advanced Filter Panel

Directly above the **Toolbar** you will see the **Filter Panel** drop-down bar. Click this bar to toggle the filter panel.

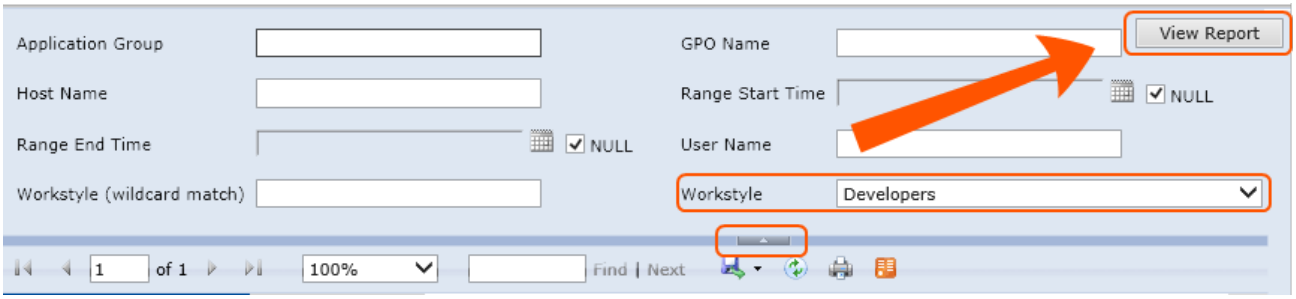


The Filter Panel is available from most dashboards and reports, and allows you to filter data based on a number of event properties. To access the Filter Panel at any time, click the filter drop-down button shown above.

The Filter Panel includes several properties that can be used to filter the events represented in the dashboard or report currently in view. These are listed in section "Top Advanced Filter Details" on page 18.

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

1. Open the report you wish to filter.
2. Open the **Filter Panel** by clicking the filter drop-down list.
3. Select the workstyle you're interested in from the **Workstyle** drop-down list.



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

The report then shows information from the 'Developers' workstyle only.

The filter options automatically perform substring matches on text meaning that any partial or complete words can be matched against.

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 you would enter '`user1,user2,user3`' in the **User Name** field.

The filter options support SQL wildcard characters.
See http://msdn.microsoft.com/en-us/library/ms179859.aspx for the Guide to SQL wildcards.

> ***Note:*** *Multiple "!" strings are accepted e.g. "!L-CZC13127L30l,!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 will be displayed at the top of the relevant column. To remove a filter, click on the 'x' next to the filter text.*

Top Toolbar

You can use the toolbar to navigate between report pages, change the magnification, search, export (see "Export Reports" on page 12), refresh, print, and export to a data feed.

The Toolbar and the Filter Panel are standard Microsoft SSRS components. For more information on Microsoft SSRS see http://msdn.microsoft.com/en-us/library/ms159106.aspx

Export Reports

Dashboards and reports can be exported to any of the following formats using the **Export** drop-down 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 within the dashboard or report.

Permalink to Reports

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

The permalink is unique to the current report and filters, so changing a filter will result 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. This will reload the page, but with a URL in the address bar of your web browser that can be copied.

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

Filter Data

There are two ways to filter data:

- "Quick Filter Panel Details" on page 13
    - The Quick Filter panel on the left-hand side 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" on page 18
    - The Top Advanced filter contains more advanced filters that you can use to view data at a higher level of granularity.

Quick Filter Panel Details

The quick filter panel has different options depending on which report you're currently viewing.

Name	Description

Platform	• Windows
	  ◦ Filters by endpoints running a Windows operating system.
	• OS X
	  ◦ Filters by endpoints running a Mac operating system.

Time Range	This is the time range that the actions are displayed over. For example, you can filter to the number of elevated actions in the last 24 hours in the **Actions** > **Elevated** report. You can choose from: • 24 Hours • 7 Days • 30 Days • 12 Months
First Reported	This is the time range filtered by the date the application was first entered into the database. For example, you can filter to the new Windows applications by publisher that were first reported in the last 7 days in the **Discovery** > **By Publisher** report. You can choose from: • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months

Name	Description
First Executed	This is the time range over which the application was first executed. For example, you can filter to the new Windows applications, by type that were first executed in the last 30 days in the **Discovery** > **By Type** report. You can choose from: • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months
Filter by Target Type	This filter allows you to filter by a type of target. For example, you can filter to the applications that have been canceled across your time range in the Actions > Canceled report. You can choose from: • All • Applications • Services • COM • Remote PowerShell • ActiveX • URL • Content
Filter by Action	This filter allows you to filter by a type of action. For example, you can filter to the services that have been elevated across your time range in the **Target Types** > **Services** report. You can choose from: • All • Elevated • Blocked • Passive • Sandboxed • Canceled

Name	Description
Filter by App Type	This filter allows you to filter by application type. For example, you can filter by applications that are executables that have been used across your time range in **Target Types** > **Applications**. You can choose from: • 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
Filter by Event Category	This filter allows you to filter by the category of the event. For example, you can filter by process events only, that have been raised across your time range in the **Events** > **All** report. You can choose from: • All • Process • DLL Control • Content • URL • Privileged Account Protection • Agent Start • User Logon • Services

Name	Description
Elevate Method	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 You can choose from: • All • Admin account used • Auto-elevated • On-demand
Path	Allows you to filter by the path. For example, to filter on applications that were launched from the System path. You can choose from: • All • System • Program Files • User Profiles
Source	The media source of the application. For example, was the application downloaded from the internet or, was it taken from removable media? You can choose from: • All • Any external source • Downloaded from internet • Removable media
Challenge / Response	Allows you to filter by challenge/response events. For example, you can filter the application that required elevation on those applications that were launched following a completed challenge/response message. You can choose from: • All • Only C/R
Admin Rights	Allows you to filter by the admin rights token. You can choose from: • All • Detected • Not Detected

Name	Description
Authorization	Allows you to filter by authorization. You can choose from: • All • Required • Not Required
Group By	You can choose from: • All • Publisher • Application Group • Message • Workstyle
Ownership	Allows you to group by the type of owner. You can choose from: • All • Trusted owner • Untrusted owner
Matched	Allows you to filter on the type of matching. You can choose from: • All • Matched directly • Matched as child
Other Actions	Allows you to filter by other actions. You can choose from: • Custom • Drop Admin Rights • Enforce Default Rights
Details	Process Details

Top Advanced Filter Details

Name	Description
Action	There are nine actions to choose from: • Elevated, Blocked, Passive, Custom, Drop Admin Rights, Enforce Admin Rights, Canceled, Sandboxed, Allowed.
Activity ID	Each Activity Type in Defendpoint has a unique ID. This is generated in the database as required. For example, if you are in the **Target Types** Dashboard and drill down in the **Top 10 Activities** chart, you are taken to the **Events** > **All** report. If you look in the top advanced filter you will see that the Activity ID is populated.
Admin Rights Required	There are three options to choose from: • All • Detected • Not Detected These allow you to filter on if Admin Rights were 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.
Agent Version	The version of the Defendpoint agent.
Application Desc	A text field that allows you to filter on the application name. For example in the **Discovery** report you could filter by "paint" in the **Application Desc** field. This would filter to application that contain the string "paint" in their descriptions.
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's also available in some reports such as **Process Detail** which 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** which is accessed from **Events All**.
Auth User Name	The name of the user that authorized the message.
Browse Source URL	The source URL of the sandbox.
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's also available in some reports such as **Process Detail** which is accessed from **Events** > **All**.
Context	This field is used by Enterprise Reporting. You do not need to edit it.

Name	Description
Date Field to filter on	There are three options to choose from: • 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. These allow you to filter by the time the event was generated, the application was first discovered or the time the application was first executed.
Default UI Language	The default language of the endpoint.
Device Type	The type of device that the application file was stored on. You can select from: • 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 Enterprise Reporting. You do not need to edit it.
Elevation Method	There are five options to choose from: • Not Set, All, Admin account, Auto-elevated, On-demand These allow you to filter events by the type of elevation used.
Event Number	This field is used by Enterprise Reporting. You do not need to edit it. This number assigned to the event type.
External Source	There are four options to choose from: • Not Set, Downloaded over the internet, Removeable media, Any external source These allow you to filter by the type of external source that the application file came from.
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.

Name	Description
Host Name	This field allows you to filter by the name of the endpoint the event came from.
Avecto Zone Identifier	The Avecto 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 Enterprise Reporting. You do not need to edit it.
Just Discovery Events	This field is used by Enterprise Reporting. You do not need to edit it.
Message Name	The name of the message that was used.
Message Type	The type of Message: • Any • Prompt • Notification • None
Number to Get	The number of rows to get from the database.
Operating System Type	The type of operating system: • 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.
Request Type	The type of request: • Blocked with reason • Canceled challenge
Row Limit	The maximum number of rows to be retrieved from the database.
Rule Match Type: • Any • Direct match • Matched on parent	Rule Match Type: • Any • Direct match • Matched on parent

Name	Description
Sandbox	The sandboxed setting: • Not Set • Any Sandbox • Not Sandboxed
Rule Script Affected Rule	True when the Rule Script (Power Rule) changed one or more of the Default Defendpoint rule, 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).
Shell or Auto	Whether the process was launched using the shell 'Run with Defendpoint' option or by normal means (opening an application): • 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.

Name	Description
Target Type	The type of target that triggered the event: • 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 considered trusted. To be a trusted owner the user must be in one of the following Windows groups; TrustedInstaller, System, Administrator.
UAC Triggered	Whether or not Windows UAC was triggered: • 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

Enterprise Reporting includes several high level dashboards that summarize the Defendpoint events.

Summary Dashboard – Displays the most important activity that has occurred in the time period. Typically this information could result in workstyle changes or investigation of anomalies.

Discovery Dashboard - Summarizes all the unique applications that have been 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 “what’s new this week and how’s it affecting my users?”.

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 Defendpoint 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 beneath 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. These are defined as a child process being blocked from running because it matched the rules in the Trusted Application Protection policy or a DLL being blocked from being loaded by a Trusted Application because it didn't have a trusted owner or trusted publisher.

Workstyles Dashboard - Summarizes all the Defendpoint workstyle usage, including coverage statistics. This dashboard includes a report called **All**. This report lists the total number of different action types each workstyle has controlled. This dashboard allows analysis from the perspective of a specific workstyle.

- User Experience - Summarizes how users have interacted with messages, challenge / response dialogs and the shell integration within the specified time range.
- Privileged Logons - 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 Defendpoint Client deployments. The report shows which versions of Defendpoint are currently installed across the organisation. 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 that have been raised over the specific time frame. A blocked message with a reason entered or a canceled challenge / response message is considered to be a request.

Events Dashboard - Summarizes information about the different types of events that have been raised over the specified time frame. It also shows the time elapsed since a host raised an event.

Summary Dashboard

The **Summary** dashboard summarizes the most important activity that has occurred in the time period defined by the quick filter. You can use this information to inform workstyle development or to show anomalous user behavior in your organization.

The Summary Dashboard includes the following charts:

Chart	Description
Application Discovered	The total number of newly discovered **Applications** split by the type of user rights required: • Admin rights required • Standard rights required Clicking the legend takes you to the > "Discovery All" on page 31 report with the **Admin Rights Required** filter applied.
User Requests	The total number of **User Requests** split by the type of request: • Blocked (user provided reason) • User canceled challenge Clicking the chart or legend takes you to the "Requests All" on page 48 report with the **Request Type** filter applied.
Admin logons, by users, on endpoints	Summarizes the number of admin logons, how many users carried them out and how many endpoints were used. Clicking the chart or legend takes you to the "Privileged Logons" on page 44 report with the **Show Administrator Logons** and **Show Standard User Logons** filters applied.
Trusted Application Protection	The number of Trusted Application incidents, how many users, and how many endpoints were affected. Clicking the number of incidents takes you to the **Process Details** report with the "Trusted Application Protection Dashboard" on page 41 filter applied.
Attempts to modify privileged groups	The number of blocked attempts to modify privileged groups Clicking the icon, numbers or text takes you to the **Privileged Account Management** table.
Application run from external sources	The number of applications that were run from external sources. Clicking the icon, numbers or text takes you to the "Target Types All" on page 39 report with the **External Source** filter applied.
Activities blocked	The number of applications that were blocked. Clicking the icon, number or text takes you to the "Target Types All" on page 39 report with the **Filter by Action** filter applied.
Applications used On-Demand privileges	The number of applications that were launched using on-demand privileges. Clicking on the icons, numbers or text takes you to the "Target Types All" on page 39 report with the **Shell or Auto** filter applied. 'Shell' means that on-demand privileges were used.
UAC matches	The number of applications that triggered User Account Control (UAC). Clicking the number takes you to the **Applications** table with the **UAC** filter applied.

Chart	Description
Hosts audited	The number of endpoints that were audited. The graph shows you the times since the most recent events. Clicking the icon, number or text takes you to the "Deployments Dashboard" on page 47. You can click the 'i' icon to go to the > "Events All" on page 49 report.
Events audited	The number of events that were audited. The graph shows you the number of each type of event. Clicking the icon, number or text takes you to the "Events All" on page 49 report.

Discovery Dashboard

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

Operating Systems Terminology

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

Operating System	Terminology
Windows	"Admin Rights Required" (shown here)
Mac	"Authorization"

The different 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 that have been discovered split by the types of rights detected: • Admin Rights Detected • Admin Rights Not Detected Clicking on the **Admin rights detected** or **Admin rights not detected** lines in the graph takes you to the "Discovery Dashboard" on page 26 report with the **Admin Rights Required** filter applied.
Types of newly discovered applications	A chart showing the number of applications that have been discovered by the type of application. The types are different for Windows and Mac operating system. Clicking the chart takes you to the "Discovery Dashboard" on page 26 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. Clicking any of the applications in the list takes you to the "Discovery Dashboard" on page 26 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. Clicking any of the applications in the list takes you to the "Discovery Dashboard" on page 26 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. Clicking any of the applications in the list takes you to the "Discovery Dashboard" on page 26 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. Clicking any of the applications in the list takes you to the "Discovery Dashboard" on page 26 report with the **Admin Rights Required** and **Matched** filter applied.

The following quick filters are available:

- "Platform" on page 13
- "First Reported" on page 13
- "Admin Rights" on page 16

Discovery By Path

This table displays all distinct applications installed within certain locations that have been discovered during the specified time frame.

For Windows the locations are:

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

For OS X the locations are:

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

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

The following columns are available for the Windows and OS X Discovery By Path table:

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

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

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

The following quick filters are available:

- "Platform" on page 13
- "First Reported" on page 13
- "First Executed" on page 14
- "Path" on page 16
- "Authorization" on page 17 - Mac only
- "Source" on page 16 - Windows only
- "Admin Rights" on page 16 - Windows only
- "Ownership" on page 17 Windows only
- "Matched" on page 17 - Windows only

Discovery By Publisher

This table displays the discovered applications grouped by publisher. Where there is more than one application per publisher the **+** symbol allows you to expand the entry to examine each application.

The following columns are available for the Windows and OS X Discovery By Publisher table:

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

- The *i* icon takes you to the **Applications report** for that specific application.
- **# Users** – takes you to a list of users that the application events came from.
- **# Hosts** – takes you to a list of hosts that the application events came from.
- **# Processes** – takes you to the **Events All** table and lists the events received in the time period for the selected application.

The following quick filters are available:

- "Platform" on page 13
- "First Reported" on page 13
- "First Executed" on page 14
- "Path" on page 16
- "Authorization" on page 17 - Mac only
- "Source" on page 16 - Windows only
- "Admin Rights" on page 16 - Windows only
- "Ownership" on page 17 - Windows only
- "Matched" on page 17 - Windows only

Discovery By Type

This table displays applications that have broken down by type. Where there is more than one application per type the **+** symbol allows you to expand the entry to examine each application.

The following columns are available for the Windows and OS X 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 when the application was first entered into the database.
- **Date first executed** – The first known date that the application was executed.

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

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

The following quick filters are available:

- "Platform" on page 13
- "First Reported" on page 13
- "First Executed" on page 14
- "Path" on page 16
- "Authorization" on page 17 - Mac only
- "Source" on page 16 - Windows only
- "Admin Rights" on page 16 - Windows only
- "Ownership" on page 17 - Windows only
- "Matched" on page 17 - Windows only

Discovery Requiring Elevation

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

The following columns are available for the Windows and OS X Discovery Requiring Elevation table:

- **Description** – The description of a specific application.
- **Publisher** – The publisher of a specific application.
- **Name** – The product name of a specific 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. This can be 'All', 'Admin account used', 'Auto-elevated' or 'on-demand'.
- **Date first reported** – The date when the application was first entered into the database.
- **Date first executed** – The first known date that the application was executed.

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

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

The following quick filters are available:

- "Platform" on page 13
- "First Reported" on page 13
- "First Executed" on page 14
- "Elevate Method" on page 16
- "Path" on page 16
- "Source" on page 16
- "Challenge / Response" on page 16
- "Ownership" on page 17 – Mac Only
- "Matched" on page 17

Discovery From External Sources

This table displays all applications that have 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 a specific application.
- **Publisher** – The publisher of a specific application.
- **Name** – The product name of a specific 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 a specific application.
- **Date first reported** – The date when the application was first entered into the database.
- **Date first executed** – The first known date that the application was executed.

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

- The *i* – icon takes you to the **Applications report** for that specific application.
- **# Users** – takes you to a list of users that the application events came from.
- **# Hosts** – takes you to a list of hosts that the application events came from.
- **# Processes** – takes you to the **Events All** table and lists the events received in the time period for the selected application.

The following quick filters are available:

- "Platform" on page 13
- "First Reported" on page 13
- "First Executed" on page 14
- "Path" on page 16
- "Source" on page 16
- "Admin Rights" on page 16
- "Ownership" on page 17
- "Matched" on page 17

Discovery All

This 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. These can be expanded by clicking on the '+' symbol in the **Version** column.

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

- **Description** – The description of a specific application.
- **Publisher** – The publisher of a specific application.
- **Name** – The product name of a specific application.
- **Type** – The Type of application.
- **Version** – The version number of a specific application.
- **# Users** – The number of users.

- **Median # processes / user** – The median number of processes per user.
- **# Hosts** – The number of hosts.
- **# Processes** – The number of processes.
- **Date first reported** – The date when the application was first entered into the database.
- **Date first executed** – The first known date that the application was executed.
- **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:

- The *i* icon – takes you to the **Applications report** for that specific application.
- **# Users** – takes you to a list of users that the application events came from.
- **# Hosts** – takes you to a list of hosts that the application events came from.
- **# Processes** – takes you to the **Events All** table.

The following quick filters are available:

- "Platform" on page 13
- "First Reported" on page 13
- "First Executed" on page 14
- "Path" on page 16
- "Authorization" on page 17 - Mac only
- "Source" on page 16 - Windows only
- "Admin Rights" on page 16 - Windows only
- "Ownership" on page 17 - Windows only
- "Matched" on page 17 - Windows only

Actions Dashboard

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	A chart showing the number of targets broken down by the type of action for each time frame. The types of action are: • Enforce default rights, Drop admin rights, Canceled, Passive, Sandboxed, Blocked, Elevated, Custom. Clicking on the chart takes you to the "Target Types All" on page 39 report with the **Filter by Action** filter applied.
Distinct target count by action	A chart showing the target count broken down by the type of action. The types of action are: • Enforce default rights, Drop admin rights, Canceled, Passive, Sandboxed, Blocked, Elevated, Custom. Clicking on the chart takes you to the "Target Types All" on page 39 report with the **Filter by Action** filter applied.
Top 10 targets	A chart showing the ten most used targets by process count. Clicking on the chart takes you to the "Events All" on page 49 report with the **Target Description** filter applied.

The following quick filters are available:

- "Time Range" on page 13
- "Filter by Target Type" on page 14

Actions Elevated

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

- Elevated actions broken down by the target type per time period.
  - Clicking on an area in the chart takes you to 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 entire duration of the time period.
  - Clicking on an area in the chart or the URLs in the legend takes you to the **Target Types** > **All** report with the **Filter By Target Type** and **Filter by Action** filters applied.
- The top 10 Targets.
  - Clicking on an area in the chart takes you to 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

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Target Type" on page 14
- "Other Actions" on page 17

Actions Blocked

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

- Blocked actions broken down by the target type per time period.
    - Clicking on an area in the chart takes you to 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 entire duration of the time period.
    - Clicking on an area in the chart or the URLs in the legend takes you to the **Target Types** > **All** report with the **Filter by Action** and **Filter By Target Type** applied.
- The top 10 targets.
    - Clicking on an area in the chart takes you to the **Events** > **All** table with the **Target Description** filter applied.

The target types are:

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

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Target Type" on page 14
- "Other Actions" on page 17

Actions Passive

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

- Actions that were passive broken down by the target type per time period.
    - Clicking on an area in the chart takes you to 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 entire duration of the time period.
    - Clicking on an area in the chart or the URLs in the legend takes you to the **Target Types** > **All** report with the **Filter by Action** and **Filter By Target Type** applied.
- The Top 10 Targets.
    - Clicking on an area in the chart takes you to the **Events** > **All** table with the **Target Description** filter applied.

The target types are:

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

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Target Type" on page 14
- "Other Actions" on page 17

Actions Canceled

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

- Canceled actions broken down by the target type per time period.
    - Clicking on an area in the chart takes you to 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 entire duration of the time period.
    - Clicking on an area in the chart or the URLs in the legend takes you to the **Target Types** > **All** report with the **Filter by Action** and **Filter By Target Type** applied.
- The top 10 Targets.
    - Clicking on an area in the chart takes you to the **Events** > **All** table with the **Target Description** filter applied.

The target types are:

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

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Target Type" on page 14
- "Other Actions" on page 17

Actions Other

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 that had a custom token applied broken down by the target type per time period.
    - Clicking on an area in the chart takes you to the **Target Types** > **All** report with the **Filter by Action** and **Filter By Target Type** applied.
- Actions that had a custom token applied broken down by the target type for the entire duration of the time period.
    - Clicking on an area in the chart or the URLs in the legend takes you to the **Target Types** > **All** report with the **Filter by Action** and **Filter By Target Type** applied.

- The top 10 actions that had a custom token applied.
    - Clicking on an area in the chart takes you to the **Events** > **All** table with the **Target Description** filter applied.

The target types are:

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

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Target Type" on page 14
- "Other Actions" on page 17

Actions Custom

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

- Custom actions broken down by the target type per time period.
    - Clicking on an area in the chart takes you to 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 entire duration of the time period.
    - Clicking on an area in the chart or the URLs in the legend takes you to the **Target Types** > **All** report with the **Filter by Action** and **Filter By Target Type** applied.
- The top 10 Targets.
    - Clicking on an area in the chart takes you to the **Events** > **All** table with the **Target Description** filter applied.

The target types are:

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

The following quick filters are available:

- "Time Range" on page 13
- "Filter by Target Type" on page 14

Target Types Dashboard

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

Chart	Description
All activity over the last (time interval)	A chart showing the target count split by target type across the specified time period. The types of target are: • ActiveX, Application, Content Control, URL, Remote PowerShell, COM, Service Control Clicking on the chart takes you to the "Target Types All" on page 39 report with the **Filter by Target Type** applied.
By type	A chart and table showing the total target count by target type. The types of target are: • ActiveX, Application, Content Control, URL, Remote PowerShell, COM, Service Control Clicking on the chart takes you to the "Target Types All" on page 39 report with the **Filter by Target Type** applied.
Top 10 activities	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. Clicking on the chart takes you to the "Target Types All" on page 39 report with the **Filter by Target Type** applied.

The following quick filters are available:

- "Time Range" on page 13
- "Filter by Action" on page 14
- "Group By" on page 17

Target Types Applications

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

- Applications activity over the time period.
  - Clicking on an area in the chart takes you to the **Target Types** > **All** report with the **Filter By Target Type** and **Application Type** filters applied.
- Applications broken down by the application type active during of the time period.
  - Clicking on an area in the chart or the URLs in the legend takes you to the **Target Types** > **All Report** with the **Filter By Target Type** and **Application Type** filters applied.
- The top 10 application activities.
  - Clicking on an area in the chart takes you to 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

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Action" on page 14
- "Filter by App Type" on page 15

Target Types Services

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

- Services target types split by type of action broken down over the time period.
    - Clicking on an area in the chart takes you to the **Target Types** > **All** report with the **Filter By Action** and **Filter by Target Type** filters applied.
- Services broken down by the type of action for the entire duration of the time period.
    - Clicking on an area in the chart or the URLs in the legend takes you to the **Target Types** > **All Report** with the **Filter By Action** and **Filter by Target Type** filters applied.
- The top 10 services activities.
    - Clicking on an area in the chart takes you to 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

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Action" on page 14

Target Types COM

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

- COM target types split by type of action broken down over the time period.
    - Clicking on an area in the chart takes you to the **Target Types** > **All** report with the **Filter By Action** and **Filter by Target Type** filters applied.
- COM target types split by the type of action for the entire duration of the time period.
    - Clicking on an area in the chart or the URLs in the legend takes you to the **Target Types** > **All Report** with the **Filter By Action** and **Filter by Target Type** filters applied.
- The top 10 COM target types.
    - Clicking on an area in the chart takes you to the **Events** > **All** table with the **Filter by Action** and **Filter by Target Type** filters applied.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Action" on page 14

Target Types Remote PowerShell

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

- Remote PowerShell target types split by type of action broken down over the time period.
    - Clicking on an area in the chart takes you to the **Target Types** > **All** report with the **Filter By Action** and **Filter by Target Type** filters applied.
- Remote PowerShell target types split by the type of action for the entire duration of the time period.
    - Clicking on an area in the chart or the URLs in the legend takes you to the **Target Types** > **All Report** with the **Filter By Action** and **Filter by Target Type** filters applied.
- The top 10 Remote PowerShell activities.
    - Clicking on an area in the chart takes you to the **Events** > **All** table with the **Target Type** and **Activity ID** filters applied.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Action" on page 14

Target Types All

This 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 OS X Discovery All table:

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

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

- The *i* icon – takes you to the **Application** report with the **Application Desc** and **Publisher** filters applied.
- **Process Count** – takes you to the **Events** > **All** Table with the **Distinct Application ID** filter applied.

- **User Count** – takes you to a list of users who generated events with that application within the time period.
- **Host Count** – takes you to 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. These values can be useful in discovering how many times applications are being automatically elevated in comparison to being deliberately elevated by the user by means of shell elevation.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Action" on page 14
- "Filter by Target Type" on page 14

Trusted Application Protection Dashboard

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

For more information about Trusted Application Protection for child processes and DLL control please see the Administration Guide.

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

Chart	Description
Trusted Application Protection incidents over the time period.	A column chart showing the number of the different incidents broken down by the trusted application. Clicking the chart takes you to the **Process Details** table with the "Trusted Application Protection Dashboard" on page 41 with the time range filters applied.
Trusted Application Protection incidents, by application	A table listing each trusted application, the number of TAP incidents, the number of Targets, the number of Users, and the number of Hosts affected. Clicking the Incidents number takes you to the **Process Details** report with the **Trusted Application Name** filter applied. Clicking the Targets number takes you to the **Targets** > **All** table with the **Trusted Application Name** filter applied.
Top 10 targets (top # of total #)	The top 10 targets for TAP incidents. Clicking the Target takes you to the **Application** report with the **Application Type** and **Distinct Application ID** filters applied. Clicking the Incident number takes you to the **Process Details** report with the **Distinct Application ID** filter applied. Clicking the Users or Hosts number takes you to the Users or Hosts list respectively.

Workstyles Dashboard

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

The Workstyles Dashboard has the following charts:

Chart	Description
All workstyles over the time period	A table showing the number of workstyles that were matched, the number of hosts, the number of users, and the applications affected by those workstyles. These are also shown as a percentage of the total in the database, irrespective of any filters apart from Time Range. Clicking the count for workstyles, users or hosts takes you to a list of the entities. Clicking on the count of applications affected takes you to the **Target Types** -> **All table**.
Summary by process activity (top 10)	Shows the top 10 most active workstyles split by the type of action. The types of action are: • Elevated • Blocked • Enforce default token • Custom • Canceled • Sandboxed • Passive • Drop admin Rights Clicking the chart takes you to the "Events All" on page 49 report with the **Action** and **Workstyle (may include wildcard match)** filters applied.
% Coverage by Workstyle (Top 10)	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. Clicking on this chart takes you to a list of users or hosts affected by the workstyle.
Process Coverage by Workstyle	A chart showing the process activity by workstyle. Clicking on this chart takes you to the "Events All" on page 49 report with the **Filter by Event Category** and **Workstyle** filters applied.
Process Coverage by Group Policy Object	A chart showing the process activity broken down by policy. Clicking on this chart takes you to the "Events All" on page 49 report with the **Filter by Event Category** and **GPO Name** filters applied.
Top 10 Elevating Workstyles	A chart showing the workstyles responsible for the most individual applications being elevated. Clicking on the chart takes you to the > "Target Types All" on page 39 report with the **Filter by Action** filter applied.
Top 10 Blocking Workstyles	A chart showing the workstyles responsible for the most individual applications being blocked. Clicking on the chart takes you to the > "Target Types All" on page 39 report with the **Filter by Action** filter applied.

Chart	Description
Top 10 Passive Workstyles	A chart showing the workstyles responsible for the most individual applications being passively audited. Clicking on the chart takes you to the > "Target Types All" on page 39 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. Clicking on the chart takes you to the > "Target Types All" on page 39 report with the **Filter by Action** filter applied.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Action" on page 14
- "Filter by Target Type" on page 14

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 - takes you to a Workstyle report.
- Any of the numbers can be clicked to see the list of events in **Events** > **All**.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Target Type" on page 14

Users Dashboard

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

User Experience

This report shows how users have interacted with Messages, Challenge/Response dialogs, and the Shell (On-Demand) menu.

Chart	Description
User Experience over the time period	A chart showing the percentage of users that have experienced each interaction type broken down by the specified time period. Clicking on the chart takes you to a list of users presented with that interaction.
Message Distribution	A chart showing how many users fall into the defined categories of messages per time period. Clicking on the chart takes you to a list of users in that category.
Messages per action type	A table showing what message types were displayed for **Allowed** and **Blocked** actions. Clicking on the Prompts, Notifications or counts or table takes you to the "Events All" on page 49 report with the **Action** and **Message Type** filters applied.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Action" on page 14
- "Filter by Target Type" on page 14

Privileged Logons

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

Please refer to the Defendpoint Administration Guide section 'Collect User Information' for guidance on enabling generation of user logon audits.

Chart	Description
Privileged Logons over the last (time interval)	A chart and table showing the number of logons by the different account types over time. Clicking the chart takes you to the **User Logons** table with the **Show Administrator Logons**, **Show Power User Logons** and **Show Standard User Logons** filters applied.
Logons by Account Privilege	A chart showing the total number of logons broken down by the different account types. Clicking the chart takes you to the **User Logons** table with the **Show Administrator Logons**, **Show Power User Logons** and **Show Standard User Logons** filters applied.
Logons by Account Type	A chart showing the total number of logons broken down by Domain Accounts and Local Accounts. Clicking the chart takes you to the **User Logons** table with the **Account Authority** filter applied.

Chart	Description
Top 10 Logons by Chassis Type	A chart showing the total number of logons broken down by the top 10 Chassis types. Clicking the chart takes you to the **User Logons** table with the **Chassis Type** filter applied.
Top 10 Logons by host Operating System	A chart showing the total number of logons broken down the top 10 host operating systems. Clicking the chart takes you to 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. Clicking the chart takes you to 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 that have been logged on to by the most users with Admin Rights Clicking the chart takes you to the **User Logons** table with the **Host Name**, **Show Administrator Logons** filter applied.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13

Privileged Account Management

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

Please refer to the Defendpoint Administration Guide section **Prohibit Privileged Account Management** for a list of Group Accounts that are considered privileged and for guidance on enabling generation of Privileged Account Management audits.

Chart	Description
Privileged Account Management over the last (time interval)	A chart breaking down the PAM events by time period. Clicking the chart drills through to 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 block events within the specified time frame. Clicking the count numbers takes you to the **Privileged Account Management** table.
By Privileged Group	A chart showing the Privileged Account Modification activity that was blocked by Windows group name. Clicking the chart takes you to 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. It drills through to the Privileged Account Management table with the **Application Description** filter applied.

Chart	Description
Top 10 users attempting account modifications	A chart showing the top 10 users who attempted modifications. It drills through to 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. It drills through to the Privileged Account Management table with the **Host Name** filter applied.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13

Deployments Dashboard

The **Deployments** dashboard shows you which versions of Defendpoint are currently installed in your organization. It also breaks down the deployments by operating system, default language, chassis type and operating system type.

Please refer to the Defendpoint Administration Guide section **Collect Host Information** for guidance on enabling collection of host information audits.

Chart	Description
By Defendpoint Client Version	A chart showing the versions of the Defendpoint agents that are deployed broken down by the number of deployments. Clicking the chart takes you to the **Deployments** table with the **Agent Version** filter applied.
By Operating System	A chart showing the number of deployments broken down by the operating system. Clicking the chart takes you to the **Deployments** table with the **Operating System** filter applied.
By Default Language	A chart showing the number of deployments broken down by the default language. Clicking the chart takes you to the **Deployments** table with the **Default UI Language** filter applied.
By Chassis Type	A chart showing the number of deployments broken down by chassis type. Clicking the chart takes you to the **Deployments** table with the **Chassis** filter applied.
By Operating System Type	A chart showing the number of deployments broken down by the type of operating system. Clicking the chart takes you to the **Deployments** table with the **Operating System Type** filter applied.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13

Requests Dashboard

This report shows information about user requests that have been raised over the specified time frame. A Blocked message with a reason entered or a canceled Challenge/Response message is considered a request.

Chart	Description
All Requests over the last (time interval)	A column chart showing the number of the different request types broken down by the time period. Clicking the chart takes you to the "Requests All" on page 48 report with the **Request Type** filter applied for the date range.
Requests by Workstyle	A chart showing the number of different request types broken down by the workstyle. Clicking the chart takes you to the "Requests All" on page 48 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 broken down by the Target Type. Clicking the chart takes you to the "Requests All" on page 48 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 broken down by the Target Name. Clicking the chart takes you to the "Requests All" on page 48 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 drop-down **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 gave 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 - takes you to the **Event** report for that request.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Target Type" on page 14

Events Dashboard

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

Chart	Description
Events over the last (time interval)	A column chart showing the number of the different Event Types broken down by the time period. Clicking on the chart takes you to the "Events All" on page 49 report with the **Filter by Event Category** filter applied.
Event Types	A chart showing how many events have been received broken down by the Event Type. Clicking on the chart takes you to the "Events All" on page 49 report with the **Event Number** filter applied.
By Category	A chart breaking down the events received broken down by Category. Clicking on the chart takes you to the "Events All" on page 49 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. Clicking on the chart takes you to a list of hosts in the "Deployments Dashboard" on page 47 report.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13

Events All

The following columns are available for the Windows and OS X Events All table:

- **Event Time** – The time of the event.
- **Platform** – The platform that the event came from.
- **Description** – The description of the event.
- **User** – 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.
- **Publisher** – The publisher of the application.

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

- The *i* icon takes you to the event report listing all the fields for that event.
- **Description** - takes you to the Applications Report.
- **User** - takes you to the User Report.

- **Host** - takes you to the Host Report.
- **Workstyle** - takes you to the Workstyle Report.

The following quick filters are available:

- "Platform" on page 13
- "Time Range" on page 13
- "Filter by Event Category" on page 15

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 OS X 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 Defendpoint policy.
    - This will only appear for the Windows platform.
- **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.
    - This will only appear for the Windows platform.
- **UAC Triggered** – Whether user account control was triggered.
    - This will only appear for the Windows platform.
- **Admin Rights Required** – Whether or not admin rights were required.
    - This will only appear for the Windows platform.

- **Authorization Required** – Whether or not authorization rights were required.
    - This will only appear for the OS X platform.
- **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 Defendpoint rule, otherwise false.
- **User Reason** – The reason given by the user if applicable.
- **COM Display Name** – The COM name if applicable.
    - This will only appear for the Windows platform.
- **Source URL** – The URL of the event if applicable.
    - This will only appear for the Windows platform.
- **Avecto Zone Identifier** – The Avecto Zone identifier if present.
- **Uninstall Action** - This can be None, Uninstall, Change/Modify or Repair.

Database Administration Report

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

In order to view the report, you need to navigate to it from the Enterprise Reporting root directory.

In your web browser go to the URL http://hostname/ReportServer. If you are using a named SSRS instance the URL will be http://hostname/ReportServer_InstanceName:

1. Click the 'Avecto Enterprise Reporting' link where 'Enterprise Reporting' or 'Avecto Privilege Guard' is the name of your Enterprise 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	Shows you the number of events across all your applications for the last 12 months.
Events totals (over all time)	Shows you the number of events in the database broken down between processes, events, user session and host sessions .

Chart	Description
Purging options	Purging data removes the data from the database using the **Purging Options** available from the report: • 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	This table shows you top 20 applications in the database by the number of events they are generating. 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 Purge Tool Utility

Enterprise Reporting includes an optional **ER Purge Tool**, which allows old data to be purged from the Defendpoint database. The ER Purge Tool can be downloaded from the Avecto website. Once you have installed the ER Purge Tool, it can be run from the Windows Start Menu.

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

For a full description of the **ER Purge Tool** please refer to the Enterprise Reporting Installation Guide.