Privilege Management ePO Extension 5.3.0 Release Notes

January 7th, 2019

New Features:

- A new Avecto-supported integration for ServiceNow using Power Rules will allow you to directly raise tickets in ServiceNow from Defendpoint. A new document called Service Now Integration Power Rules Guide is available to support this feature.
- Power Rules allows you to integrate with third party tools and/or dynamically alter the outcome of a Defendpoint Application Rule using PowerShell scripts. A new document called Power Rule Core Scripting Guide is available to support this feature.
- Added the ability to add application to policy from events for Events > All and Events > Process Details.
- Added the ability to view the current reputation for the following reports: Target Types > All, Events > All.
-] There is a new macOS QuickStart Template available for use in the policy editor. Full details of this can be found in the Defendpoint ePO Extension Administration Guide for this release.

Enhancements

- There have been some updates to the Windows QuickStart Template.
  - The General Rules workstyle has been renamed to All Users.
  - The Add Admin General (Business Apps) has been renamed to Add Admin - All Users (Business Apps).
  - The Add Admin - General (Windows Functions) has been renamed to Add Admin - All Users (Windows Functions).
  - The Allow - Approved Standard User Apps Application Group has been deleted.
  - Both Control - Restricted Functions Application Groups have been renamed to Restricted Functions and hidden.
  - The Allow Message (Authentication) has been renamed to Allow Message (Authentication & Reason).
- The Advanced Policy Editor Settings and Advanced Sandbox Environment pages in the Utilities menu are no longer shown for policies unless they contain existing Sandboxing functionality to reduce confusion.
- 'User' context is now available in addition to 'System' context when you add a PowerShell Audit Script.

Policy Editor Bugs Fixed

- The maximum size of audit scripts has been increased from 32KB to 64KB.
- The Save button is now enabled when you have added an Application Group for macOS policies.
- Page formatting now persists when you attempt to add a second Custom Token with the same name to your Windows policy.
- The shared key for response codes is no longer shown in the event when an exception is reported in the Orion log.
- Spaces before and after the File/Folder name matching criteria are now trimmed to ensure rules are correctly matched.

Report Display Bugs Fixed

- Inconsistencies in the data displayed on the drill-down from the Summary report have been fixed.
- The ® symbol is now correctly displayed in the reports where it appears.
- Fixed a sporadic issue that caused an the Event time to be incorrectly rendered in Events > All.

Database Bugs Fixed

> ***Note:*** *These bugs apply to the reporting database that the Defendpoint ePO Extension connects to. You need to upgrade your database to version 5.3 or higher to obtain these fixes.*

- Previously only the Host Name or the User Name was unique. We have now added the SID and Domain Name as part of the key.
- Fixed multiple issues in some SSRS reports when using a German server locale.
- Event 198 is no longer incorrectly duplicated in some scenarios when adding a user to a group using lusrmgr.msc.
- If an application has more than one entry in the DistinctApplications table, PurgeApplication now correctly deletes all variants.
- Improved the robustness of CopyFromStaging to ensure it can recover from an unplanned shutdown.
- Fixed an issue to ensure that CopyFromStaging waits to obtain a lock when the database is hosted in Azure SQL.
- CopyFromStaging now runs successfully when the Event description is longer than 1024 characters.

Compatibility:

This section details the versions of software that this version of the Defendpoint ePO Extension maintains compatibility with. We support all versions supported by McAfee and have an ongoing testing program. Please contact Avecto support if you'd like to use a newer version not listed here.

Defendpoint Windows Client

The following Avecto Defendpoint Windows Client versions are compatible with this version of the Defendpoint ePO Extension

> ***Note:*** *Version 5.2.21.0 GA of the Windows Client is compatible with ePO Server 5.3/5.9.*

> ***Note:*** *Version 5.2.28.0 SR1 of the Windows Client is compatible with ePO Server 5.9/5.10.*

- Recommended: 5.3 (all versions)
- 5.2 (all versions)
- 5.1 (all versions)
- 5.0 (all versions)
- 4.4 (all versions)
- 4.3 (all versions)
- 4.1 (all versions)
- 4.0 (all versions)
- 4.0 (all versions)
- 3.8 (All versions)

Defendpoint Mac Client

The following AvectoDefendpoint Mac Client versions are compatible with this version of the Defendpoint ePO Extension.

> ***Note:*** *Version 5.2.27899.0 GA of the Mac Client is compatible with ePO Server 5.3/5.9.*

> ***Note:*** *Version 5.2.29409.0 SR1 of the Mac Client is compatible with ePO Server 5.9/5.10.*

- Recommended: 5.2.29409.0 SR1
- 5.2.27899.0 GA

Enterprise Reporting Database

The following Enterprise Reporting versions are compatible with this version of the Defendpoint ePO Extension.

> ***Note:*** *If you are using an older version of the database, some reports may not return data and there may be reduced levels of performance.*

- Recommended: 5.3 GA
- 5.1.99.0 SR1
- 5.1.21.0 GA
- 5.0.25.0 GA
- 4.5.13.0 GA
- 4.3.116 - This is the minimum version required to see Mac Events
- 4.1 (all versions)

> ***Note:*** *Using ePO to query fields, or import events that contain fields, that are not present in Enterprise Reporting database causes an error to be displayed. Fields won't be present in the Enterprise Reporting database if the functionality was implemented in a subsequent release, for example Trusted Application Protection was implemented in Enterprise Reporting 5.0 and the 'Uninstaller' Application Type was implemented in Enterprise Reporting 5.1.*

Browser Compatibility

The following browsers are compatible with the Defendpoint ePO Extension and Avecto Reports:

- Safari v10 and higher
- Internet Explorer version 11.6 and higher
- Chrome (latest version)
- Firefox (latest version)

Please also refer to the McAfee ePO browser compatibility list as required https://kc.mcafee.com/corporate/index?page=content&id=KB51569.

McAfee Agent

The following McAfee Endpoint Security products are compatible with this version of the Defendpoint Client:

- l Recommended: 5.5.x
- l 5.0.x (all versions)

> ***Note:*** *Version 4.8 and older of the McAfee agent are not supported with this release.*

McAfee ePO Server

> ***Note:*** *Version 5.1 of ePO Server is not supported.*

The following McAfee Endpoint Security versions are compatible with this version of the Defendpoint Client:

- Recommended: 5.10.x
- 5.9.x
- 5.3.x (all versions)

McAfee Endpoint Security (ENS)

The following McAfee Endpoint Security versions are compatible with this version of the Defendpoint Client:

- Endpoint Security (ENS) Adaptive Threat Protection (ATP) 10.x
  - With Generic Privilege Escalation Prevention (GPEP) enabled and disabled
- ENS Firewall 10.x
- ENS Threat Prevention 10.x
- ENS Web Control 10.x

McAfee MOVE Multi-Platform Client

The following McAfee MOVE Multi-Platform Client versions are compatible with this version of the Defendpoint Client:

> ***Note:*** *We do not support the agentless version of McAfee MOVE.*

If the version of McAfee MOVE is compatible with the McAfee Agent you're using then Defendpoint is also compatible.