

Defendpoint ePO Extension Release Notes

Software Version: 5.2.0.137 GA

Document Version: 1.1

Copyright Notice

The information contained in this document (“the Material”) is believed to be accurate at the time of printing, but no representation or warranty is given (express or implied) as to its accuracy, completeness or correctness. Avecto Ltd, its associated companies and the publisher accept no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance placed on this Material for any purpose.

Copyright in the whole and every part of this document belongs to Avecto Ltd (“the Owner”) and may not be used, sold, transferred, copied or reproduced in whole or in part in any manner or form or in or on any media to any person other than in accordance with the terms of the Owner’s Agreement or otherwise without the prior written consent of the Owner.

Accessibility Notice

In the event that you are unable to read any of the pages or documents on this website, please contact us and we will arrange to get an accessible version to you.

Chapter 1 - Release Notes

1.1 - New Features

16864 - Added the ability to manage Mac policy and administer Mac endpoints using ePO.

This includes the following functionality:

- Installing the Defendpoint client for Mac and ePO Defendpoint adapter for Mac using the Defendpoint ePO Extension.
- Sending Defendpoint policies to a Mac endpoint from the Defendpoint ePO Extension.
- Importing applications from events into an Application Group.
- Sending McAfee Threat and Avecto Reporting events from Mac endpoints to the ePO Server.
- Added support for multiple policies.

78383 - Updated Avecto Reporting with a new graphical reporting suite. The reports available to you are:

- Summary
- Discovery
- Actions
- Target Types
- Trusted App Protection
- Users
- Events

*The **Add to Policy** functionality and **Reputation** in the new reporting suite is going to be added in the next release of the Defendpoint ePO Extension.*

*The **Pre-Caching** Server Task has been removed from the Defendpoint ePO Extension as it is no longer required for the new reporting suite.*

79258 - Added the ability to view McAfee Threat Events and Avecto Reporting events in Queries and Reports and Dashboards within ePO.

82105 - Added the ability to filter on the Account Name/Group Name **or** the User ID/Group ID in the Mac Account Filter.

Prior to this release, the Account Name was not used by Defendpoint to match against in Mac Account Filters. This means that if you have an Account Filter for Mac that has an Account Name and User ID, the behavior of that filter will change with this release as Defendpoint will now try to match against both the Account Name and the User ID. You can delete any information in the Account Name to ensure you continue to match on just the User ID. If you populate just the Account Name, Defendpoint will only match against that.

1.2 - Bugs

76217 - Fixed an issue that caused an error to be displayed and the associated policy to be cleared.

77935 - Fixed an issue on certain builds of the Defendpoint ePO Extension that caused an error to be displayed when you added an application to an application rule using the **Add Applications from Events** functionality.

78338 - The dialog box to create a new On-Demand rule now states **On-Demand** rather than **Shell**.

78380 - Several column headers have been updated:

- **Shell > On-Demand**
- **# App Assignments > # Application Rules**
- **# Shell Assignments > # On-Demand Rules**

78596 - Criteria that is not specifically selected using the associated check box is now disabled to indicate it's not set irrespective of if you've entered a value for it.

80216 - The **User Reason Type** in the **Request Message Enter Reason** text box is now correctly set to **Text Box** rather than **Off**.

80356 - Applied a fix from McAfee to the Defendpoint ePO Extension to manage an issue with the Data Exchange Layer (DXL) where the Defendpoint ePO Extension doesn't load.

82595 - The correct version of the Defendpoint ePO Extension is now displayed in all areas of the interface.

Chapter 2 - 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.

2.1 - Defendpoint Windows Client

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

Version 5.2.28.0 SR1 of the Windows Client is certified with ePO Server 5.10.

- **Recommended:** 5.2.28.0 SR1
- 5.2.21.0 GA (certified with ePO Server 5.9)
- 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)

2.2 - Defendpoint Mac Client

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

Version 5.2.29409.0 SR1 of the Mac Client is certified with ePO Server 5.10.

- **Recommended:** 5.2.29409.0 SR1
- 5.2.27899.0 GA (certified with ePO Server 5.9)

2.3 - Enterprise Reporting Database

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

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

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.

2.4 - McAfee Agent

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

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

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

2.5 - McAfee ePO Server

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

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

2.6 - 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

2.7 - McAfee MOVE Multi-Platform Client

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

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.

Chapter 3 - Version History

3.1 - 5.1.0.10 GA

- ["New Features" below](#)
- ["Bug Fixes" below](#)

3.1.1 - New Features

74189 - Added a new 'Uninstaller' Application Type. This feature allows end users to uninstall applications from machines managed by Defendpoint.

3.1.2 - Bug Fixes

- ["Policy Editor Specific Bug Fixes" below](#)
- ["ePO Report Specific Bug Fixes" below](#)

Policy Editor Specific Bug Fixes

74535 - The Action drop-down now defaults to 'Block Execution' which matches the MMC Policy Editor.

75472 - The Template button is now correctly disabled on the Edit Application page when adding an Uninstaller Application.

ePO Report Specific Bug Fixes

73911 - You can now add child or parent applications to policy or update the reputation after you have drilled down from the Discovery > All report.

74151 - You can now select the Shell and Auto advanced filters without receiving an error.

3.2 - 5.0.0.67 GA

- ["New Features" above](#)
- ["Enhancements" on the next page](#)
- ["Bug Fixes" above](#)

3.2.1 - New Features

67673 – Added a new QuickStart template for Defendpoint configuration. This is a best practice configuration consisting of three layers of workstyles with different levels of flexibility.

69185 – Added the ability to show and hide Sandboxing specific controls in the Policy Editor.

70508 – Added two new templates for Trusted Application Protection (TAP); High Flexibility and High Security. These provide additional protection for applications (such as document readers and web browsers) that are commonly used to deliver malware. These templates automatically prevent untrusted executable, script and DLL payloads from being executed from web pages and documents.

73773 - The 'Internet Zone' column has been renamed 'Avecto Zone Identifier' as it reports on this tag.

3.2.2 - Enhancements

54871 – There have been several branding updates throughout the product.

68873 – Defendpoint Client is compatible with McAfee MOVE.

73636 – You can now match on the presence of the Avecto Zone Identifier tag in the Policy Catalog.

ePO Reporting Specific Enhancements

50239 - The User Details report now has an advanced filter .

61300 - The Hostname and Username are now available in Queries and Reports for Enterprise Reporting.

72998 - You can now drill-down directly to the Application report from the Top 10 Targets legend on the Actions reports.

Policy Editor Specific Enhancements

68395 - Added a new registered server called 'Avecto Admin' to support Enterprise Reporting purge tasks.

70254 - Update Audit Event Check boxes for Application Rules.

73620 - The Block notification message now displays correctly with the right image.

74108 – Renamed the 'Kind' column to 'Type' in the Messages page and updated the wording in the 'Type' column to align to the type of message you have created. In addition, the relevant columns are now correctly populated based on the type of message.

74177 - Updated the colors in the Messages grid to maintain consistency with the MMC Policy Editor.

74208 – You can now match on the Avecto Zone Identifier in the policy editor.

3.2.3 - Bug Fixes

Policy Editor Specific Bug Fixes

67223 - Removed the option 'Application Requires Elevation (UAC)' for PowerShell applications as it's not possible.

68899 - The Challenge / Response shared key is now correctly copied across when duplicating a policy in ePO.

74177 - Updated the colors in the Message grid to maintain consistency with the MMC Policy Editor.

ePO Report Specific Bug Fixes

67300 - PID, ParentPID, ActivityID filters have been added to the Advanced filter in the Events > All report.

71975 - Null publishers are handled when drilling down into child or parent application link and no error is generated.