Avecto

ePO Extension Release Notes

Software Version: 4.5.0.14567 GA

Document Version: 1.0

Document Date: 30 May 2017

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 - Defendpoint ePO Extension

- **Release Notes** detailed below

1.1 - Release Notes

- **New Features** detailed below
- **Enhancements** detailed below
- **Bug Fixes** detailed below

1.1.1 - New Features

14262 - Added the ability to generate response codes within the Defendpoint ePO Extension.

10086 - Added remote API support for creating/importing/exporting of Defendpoint policies in the native format.

58145 - Added support for McAfee ePO 5.9 to the Defendpoint ePO Extension and updated the product ID and version to meet McAfee recommended practice.

The Defendpoint 4.5 client for Mac is not supported with McAfee ePO 5.9.

1.1.2 - Enhancements

- **Reporting** detailed below
- **Policy Editor** detailed below

59836 - Tested and confirmed compatibility with McAfee Agent 5.0.4.449 Hotfix.

Reporting

51341 - Added database views for exporting Avecto Event data into SIEM products such as Splunk. Please see the Exported Views appendix in the Enterprise Reporting Dashboard Guide for more information.

66522 - Added the ability to use the standard Enterprise Reporting user accounts in the Defendpoint ePO Extension. This is available in the Registered Server configuration page.

Policy Editor

3622 - Added support for duplicating rules.

55906 - You can now use the **Add to Policy** option on the Requests > All table.

1.1.3 - Bug Fixes

- **Reporting** detailed below
- **Policy Editor** detailed on the next page

Reporting

53386 - Fixed the size for the process coverage by workstyle pie chart to ensure it's not too small.

53588 -The breadcrumb trail navigation no longer retains filter properties in the Events > All report.

56137 - Privilege Account Management events are now shown in the Events > All report when a 4.1 database is used.

56979 - The Application Details now has an advanced filter which is consistent with Enterprise Reporting.

59205 - The time range in the Advanced Filter is no longer incorrectly incremented every time a filter is changed.

59211 - No applications were being displayed when you drilled down from New Applications table and the '==Application Description' filter was set in the Advanced Filter options.

59212 - Advanced filters are now retained when you navigate to other dashboards from the New Applications table.

59289 - The Advanced Filter is now applied correctly across all the dashboards.

60062 - You can no longer drill down if no audited child processes or parent processes were found. Previously, attempting to do this gave an error.

63218 - Removed the string 'Target' from strings where it appeared in the form 'Target Application Group'.

64808 - Changed instances of 'Privileged Account Protection' to 'Privileged Account Management'.

64822 - The GetUserSessions procedure can now limit the number of returned results.

64879 - The GetDistinctApplicationX procedure can now limit the number of returned results.

64880 - The GetHostsFromMostRecentEventTime procedure can now limit the number of returned results.

64881 -The GetItemListForPrivAccountProtection procedure can now limit the number of returned results.

64882 - The GetPrivilegedGroupModificationsBlockedForInterval procedure can now limit the number of returned results

64553 - Privileged Logons now have Unique User Logons in the table.

66254 - UAC Triggered filter now works in the Discovery > All report in ePO Avecto Reporting.

66258 - A 'Rule Match' has been added to the Target Types > All report in the advanced filter.

66321 - Changed instances of 'Authorization Key' and 'Authorization Code' to 'Shared Key' for consistency.

Policy Editor

59520 - Changed the alignment of the check boxes for the On-Demand configuration as it was potentially confusing.

61958 - The field 'unauthorizedCredentials' is now correctly recognized when the 'Allowed Message' is loaded.

62551 - Policies imported from the Microsoft Management Console (MMC) no longer display an error when clicking on the 'On Demand Application Rules' option.

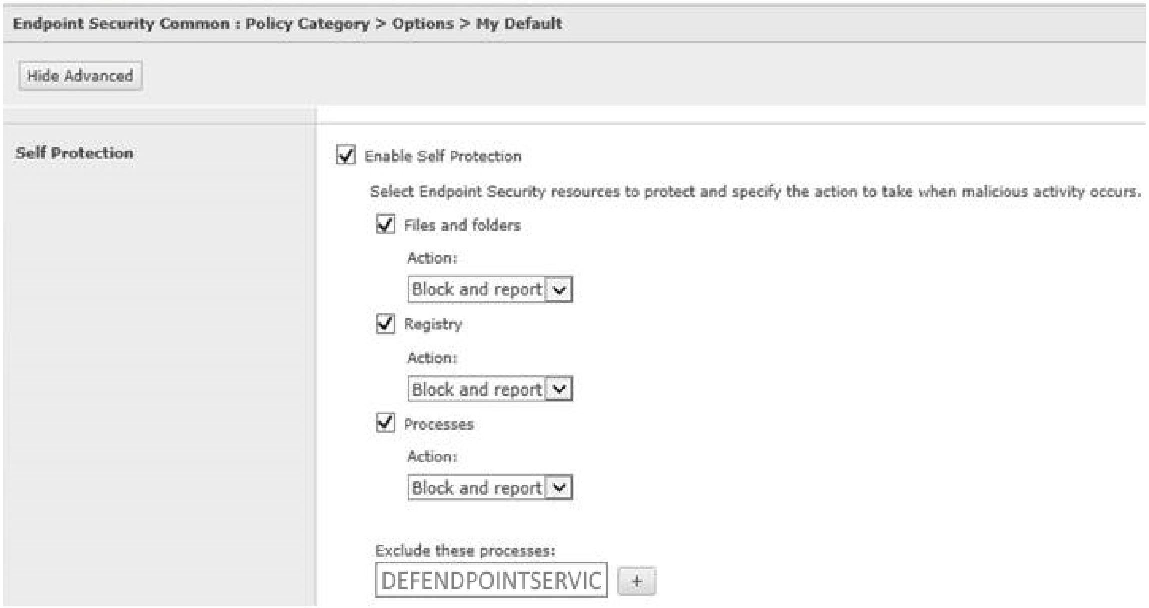
62935 - An error is no longer shown if a user is an owner of a Defendpoint policy but only has View policy settings role and attempts to edit and save policy.

67034 - The 'Add to Policy functionality' now correctly ignores URL, Content and Privilege Application Management events.

1.1.4 - Known Issues

If you are using McAfee Endpoint Security v10 there are some additional steps you may need to go through to configure Defendpoint. These are detailed below.

1. Navigate to **Policy Catalog** and select 'McAfee Endpoint Security' from the **Product** drop-down menu.
2. In the **Self Protection** section, see if the **Enable Self Protection** check box is selected. If it is, follow the steps below:
   a. If they are not already selected, select the three check boxes below for **Files and folders**, **Registry** and **Processes**.
   b. Type 'DEFENDPOINTSERVICE.EXE' into the **Exclude these processes** text box and click **Save**.



Endpoint Security Common : Policy Category > Options > My Default

Self Protection

☑ Enable Self Protection

Select Endpoint Security resources to protect and specify the action to take when malicious activity occurs.

☑ Files and folders

Action: Block and report

☑ Registry

Action: Block and report

☑ Processes

Action: Block and report

Exclude these processes: DEFENDPOINTSERVIC

Chapter 2 - Backward Compatibility

This section details the versions of software that this version of the Defendpoint ePO Extension maintains backwards compatibility with.

2.1 - Defendpoint Windows Client

The following Avecto Defendpoint Windows Client versions are compatible with the Defendpoint ePO Extension 4.5.0.14567.

- 3.8 (GA through to and including SR11)
- 4.0 (GA through to and including SR7)
- 4.0.384 (ePO-WIN10)
- 4.1 (GA through to and including SR10)
- 4.3.50 (GA through to and including SR6)
- 4.4.92.0 (GA)
- 4.4.145.0 (SR1)

2.2 - Enterprise Reporting Database

The following Enterprise Reporting versions are compatible with the Defendpoint ePO Extension 4.5.0.14567.

- 4.1.160 GA
- 4.1.291 SR1
- 4.3.116 GA
- 4.5.13.0 GA

2.3 - McAfee Agent

The following McAfee agent versions are compatible with the Avecto ePO extension 4.5.0.14567.

- 4.8.1938 (P3)
- 5.0.3.272 (XP supported)
- 5.0.4.283
- 5.0.5.658

2.4 - McAfee ePO Server Version

The following ePO Server versions are compatible with the Defendpoint ePO Extension 4.5.0.14567.

- 5.1.3
- 5.3.2
- 5.9

2.5 - McAfee Endpoint Security

The following McAfee Endpoint Security versions are compatible with the Defendpoint ePO Extension 4.5.0.14567.

- Endpoint Security (ENS) Adaptive Threat Protection (ATP) v10
- ENS Firewall v10
- ENS Threat Prevention v10
- ENS Web Control v10

Chapter 3 - Version History

3.1 - 4.4.12591 GA Release

New Features

Added support to enable On-Demand support for the Modern UI in Windows 8 and 10. Please refer to the Admin Guide for more information.

Added support for Enterprise Reporting 4.1 SR1.

Bug Fixes

36560 - Fixed Users > Privileged Account Protection drill downs from the pie chart legend and associated table.

41122 - Fixed Discovery Summary report to match ER Host and User Details graphs.

54918 - Fixed an issue ensuring that the Save button is enabled when you make changes in the Policy Editor to the On-demand policy rules.

55108 - Fixed an error message when navigating to Deployment Report.

58341 - Fixed an issue that caused an error when the event for a child process was selected.

58346 - Fixed a missing "group” attribute when creating/editing custom token groups.

58745 - Events Logon (300), Defendpoint Service start (400) and PAP (198) are now correctly shown in the Events --> All screen.

58811 - Applications are correctly displayed in the drill-down from the Top 10 Targets bar chart in the Actions dashboard.

3.2 - 4.3.11275 GA Release

Enhancements

- Application/Content/URL Groups can be duplicated in the policy editor.
- Database server registration has additional options including support for NTLMv2, SSL and default instances.
- Reporting query performance is logged and is available in a table under Options. This can be exported in multiple formats.

- Times on reports are now shown using the time zone of the ePO server. Note all events are stored in the database in UTC.
- Added a new chart called “Time since last endpoint event” to the Events report.
- ePO extension supports 4.1/4.2/4.3 format ER databases.
- Server Task error reporting is improved to report the error to the ePO Server Task Log screen.
- You can now purge Enterprise Reporting events from the database.

Bug Fixes

- Multiple fixes for inconsistencies and errors when drilling down through charts and tables in ER Reporting
- Fixed a delay connecting to ER hosted on default database instances. This is now a radio button option in the server registration.
- VirusTotal integration now shows only Known or Unknown state as required by terms and conditions.
- Privileged Account Management events (198) now have a detailed report.
- Fixed inconsistency between event IDs in reporting and event import in the editor.
- Fixes to TIE update reputation task to ensure all reputations are updated.
- Breadcrumb trail for Activities are now shown properly.
- Monitor consistency enhancements for the display of percentages.
- Distinct Application Pie chart fixed to work for 24-hour time period.
- Fixed reputation rendering of detailed reports when some values were in Pending state.
- Added Time Range filter to application details.
- Update of reputation in Event Import now only updates the selection application, not all related ones.
- Reputation update on Discovery->External Sources now shows a progress bar.
- Target Types top 10 dashboard now combines applications properly
- When adding a Message from a template in the policy editor, the description is now improved.
- Policy editor now correctly handles blank lines in the Advanced Agent settings.
- Policy editor now detects changes in the Messages->Reasons dropdown and enables the Save button properly.
- Adding a group into the account filter via LDAP Built-in groups now sets the “Group” flag correctly.
- Policy editor now saves hashes in the correct case so application hash matching now works for applications imported from reporting.

3.3 - 4.1.8554 SR1 Release

New Features

- Policy Editor support for configuration of choosing whether to use designated user authorization or Challenge/Response on same custom message

Bug Fixes

- Policy Editor: Fix incorrect labels for IE Zones in URL definitions
- Policy Editor: Fix application Sandbox Context for applications

3.4 - 4.1.205 GA Release

New Features

- Policy editor support for all new 4.1 Defendpoint Client features notably email attachment sandboxing (Defendpoint Client release 4.1.149)
- Support for 4.1 client events (ePO Threat Event and Avecto Reporting)
- New Reporting screens for the discovery of applications
- Application Reputation lookup via Intel Threat Intelligence Exchange (TIE) using Data Exchange Layer (DXL) and VirusTotal.

Enhancements

- New summary screen for reporting
- Improved event staging performance especially when queues are large
- Improved Event Import within the policy to support new fields and reputation information
- Added support for the custom sandbox setup script in the policy editor
- If connected to an older reporting database, the user is warned when reporting is clicked
- Improved installation means the Avecto parser is no longer required to be installed as this is not required for ePO installations
- Bug Fixes
- Reports now work for non-admin users with Defendpoint permissions
- Multiple fixes for reporting chart drill downs consistency
- Branding updates
- Error when adding Register Server for reporting Queries and Reports fixed
- Fixed the display of Logon (300) and Defendpoint Start(400) events in reporting
- WMI filter “all items checkbox” now retains correct state in the policy editor
- Event import from an application now includes additional fields including the SHA1 hash
- Purge server task for the Avecto part of Threat events now no longer deletes everything when greater than 20 days
- Help file is no longer part of the extension. It is now part of the associated documentation and has be rewritten in significant areas for clarity.
- If the reporting database is unavailable a custom error page with the cause is displayed

3.5 - 4.0.384 SR2 Release

Enhancements

- Added support for Windows 10 managed endpoints.

Bug Fixes

- The SID field in an account filter is no longer a mandatory field, which allows you to target local accounts by account name.
- Fixed a bug which caused Content Control matching criteria to fail when configuring rules in the ePO Policy Editor.

3.6 - 4.0.378 SR1 Release

- Added support for Windows 10.
- Added direct link to Applications list report via Target Types > All.
- Added Distinct Message information to User Details report.
- Reporting tabular views now support exporting of data.

- New rewritten and updated help file.
- Fixed Policy Editor so that Content Control works properly.
- Reporting now works for non-admin users when the permissions are enabled.
- Added workaround for ePO issue which causes an error when adding the Registered Database Server. The side effect is that MySQL appears as an option for database type but only SQL Server should be selected.
- Fixed Policy Editor Account Filter so that SID field is not mandatory.
- Fixed incorrect values on the Target Types > Service Control > Top 10 Service Control Targets chart.
- Fixed inconsistent on drill down from Targets > COM - Top 10 COM chart.
- Fixed internationalisation for Unknown Action Category.
- Fixed inconsistent drill down from Targets (Grouped) > Publisher - Sandboxed Targets by Publisher pie chart.
- Editing a policy from the Workstyles > All now locks it.
- Added an additional decimal point to Actions pie chart percentages.
- Fixed inconsistent drill down from Requests Dashboard > Requests by Workstyle.
- Drill down from User Experience bar chart now filters the list properly.
- Stop the prefix of username being displayed as None when no domain is present.
- Fixed User Details - Top 10 Targets graph which was always empty.
- Fixed inconsistent values from drill down from Home > Targets Blocked.
- Fixed inconsistent drill down from Home - Number of Applications discovered.
- Fixed inconsistent drill down from Application > Top 10 Users + Top 10 Hosts.
- Fixed error when clicking chart legend on Requests interval.
- Changed drill down from Home > Targets Blocked from Home page to go to correct report.
- Fixed inconsistency when drilling down from bar charts on Workstyles dashboard.

3.7 - 4.0.200 GA Release

Features/Enhancements

New Module – sandboxing

- Defendpoint sandboxing module provides an extra level of reassurance to cover the most common entry point for malware and hackers - the internet. All while removing traditional barriers so users can be free.
- Leverages the Windows Security Model
- Lightweight design and seamless user experience
- Documents automatically classified, with internet documents remaining isolated

New Feature – Content Control

- Elevate, block or sandbox specific content for more control than ever before
- Grant privileged access to protected files and directories
- Whitelist/blacklist ability to read configurations and documents
- Provide gated access to content through customizable messaging, including challenge/response

New Feature - Workstyle Wizard

- Simplify and accelerate creation of Workstyles and rules
- Choose between monitoring and enforcement workstyle

- Select modules and features to be applied to the Workstyle
- Automatically creates target groups, rules, messages and notifications based on selection

New Feature – PowerShell Scriptable Auditing

- Added ability to audit Defendpoint activity using PowerShell scriptable events.

New Feature - Avecto Reporting in ePO

- Optional Avecto Enterprise Reporting in McAfee ePO web interface. Data stored outside McAfee ePO database.
- Add to application groups directly from report views
- User experience dashboard to expose blocks and requests for access
- Faster access to key application data

Changes Specific to ePO Edition

- Search policy contents to find existing applications
- Added Autosave when editing configurations in ePO, to avoid loss of settings should the connection be lost.
- Application definitions in ePO now accept class ID's without requiring braces { }.
- Graphical message preview in ePO web interface.
- Uses ePO LDAP server connection for account lookup.
- Improved control of which audit events are transmitted to ePO.
- ePO Server event filtering supported for Threat Events which would be stored in the ePO. server database.
- Added ability to delete engineering Key values in ePO Management Console.

Other changes

- Policies are now named Workstyles
- Shell Rules are now named on-demand Application Rules
- Added support for %APPDATA%, %LOCALAPPDATA%, %PROGRAMDATA%, %ALLUSERSPROFILE% environment variables
- Added 'Home page' to management console that provides overview of loaded configuration, and provides quick links to Defendpoint tools/utilities.
- Added new Workstyle 'Overview' tab that provides summary of the rules and settings within the highlighted Workstyle.
- Optimized License event auditing so that 'No License' events are only issued once.
- Added several built-in application groups for common application types.
- Added separator in Token/Message/Application Group dropdown to differentiate between built-in and custom.
- Added new 'Activity Type' variable to improve End User Messages.
- Added new Application definitions for Sandbox Classification and Sandbox Context, to allow targeting of applications running in, or originating from a sandbox.
- Expanded definition matching criteria to allow 'Contains', 'Starts with', 'End with' and 'Exact match'
- Added new End User Message templates that cover a much broader set of use cases, and included four new Avecto message banners.
- Added new arguments to the Defendpoint Client installer to allow override of the default Hook method.
- Added new 'Avecto Task Manager' utility to Defendpoint Client that provides contextual information on running processes managed by Defendpoint.

- Implemented several improvements to the PGCaptureConfig utility.
    - Now uses SFTP for secure transfer of system information.

Bug Fixes

- Resolved occasional unhandled exception observed when installing a specific ActiveX control
- Resolved COM Class elevation errors for power users and administrators.
- Resolved system hang during reboot after installation/upgrade caused by PGDriver.sys.
- Resolved issue elevating Flash Player 12 installer.
- Resolved various DPI issues in message prompt.
- Anti-tamper is now disabled on domain controllers.
- Resolved incompatibility with Cygwin