Avecto defendpoint

Defendpoint Management Console Release Notes

Software Version: 5.1.149.0 SR1

Document Version: 1.1

Document Date: April 2018

Chapter 1 - Release Notes

- **New Features** detailed below
- **Bugs Fixed** detailed below

1.1 - New Features

72507 - Added support for Trusted Application Protection (TAP) DLL audit events for endpoints being managed by iC3 version 2.0 and above. The following TAP DLL audit events are now sent to iC3 2.0 and above from the endpoint:
706 - Passive Event
716 - Blocked
720 - Canceled

1.2 - Bugs Fixed

60202 - The Defendpoint Event import from a database for an Application Group now states the correct syntax for 'Server \ Instance'.

76560 - All language changes in a policy are now preserved when the policy is saved using the PowerShell API.

79954 - Fixed an issue that caused the Policy Editor to crash if the nodes were expanded in a specific configuration and the 'Show Hidden Groups' option was selected.

Chapter 2 - Supported Operating Systems

These platforms are supported with the latest service pack or update is applied.

- Windows 7
- Windows 8 and 8.1
- Windows 10 builds 1507, 1607, 1703, and 1709
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Chapter 3 - Prerequisites

- **Defendpoint Management Console** detailed below
- **Defendpoint Activity Viewer** detailed below

3.1 - Defendpoint Management Console

- Microsoft .NET Framework 2.0 (Required to run PowerShell audit scripts)
- Microsoft .NET Framework 4.5.1 (Required for iC3 connectivity)
- Microsoft Visual C++ 2015 Redistributable
  - Microsoft Visual C++ 2017 Redistributable is also supported
- Microsoft Group Policy Management Console (for Active Directory integration)
- Microsoft SQL Server 2012

The executable version of the installation package includes all necessary prerequisites (excluding the Group Policy Management Console), and will automatically install them as necessary.

Microsoft SQL Server 2012 Native Client is required for connectivity with Enterprise Reporting.

3.2 - Defendpoint Activity Viewer

- Microsoft SQL Server Compact 4.0
- Microsoft .Net Framework 4.0 Client

Chapter 4 - Version History

4.1 - 5.1.95.0 GA

4.1.1 - New Features

69356 - Added a new 'Uninstaller' Application Type. This feature allows end users to uninstall applications from machines managed by Defendpoint.

4.1.2 - Bugs Fixed

74597 - The console now shows the status of the ePO audit settings.

74661 - You can now delete auditing scripts that are not assigned in the console.

74749 - Fixed an issue where inserting an event into the console and then closing it caused it to become unresponsive.

76747 - Fixed an issue that caused the MMC Policy Editor to become unresponsive when adding an application rule for the OS X policy.

76968 - Fixed an issue that occurred if the certificate snap-in was added after the iC3 snap-in.

4.2 - 5.0.102.0 GA

4.2.1 - New Features

61293 – 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.

67887 – Added the ability to show and hide Sandboxing specific controls in the Policy Editor.

67890, **68472** – 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.

4.2.2 - Enhancements

68711 – There have been several branding updates throughout the product.

68974 – Defendpoint works when Windows Control Flow Guard is enabled.

73648 – You can now match on the Avecto Zone Identifier in the policy editor.

4.2.3 - Bugs Fixed

12615 – A message is now displayed if the user accidentally sets the start date after the end date for filtering in the Defendpoint reporting node.

18113 – When you set the Action to **Block Execution** for a Windows Application Rule, the **Access Token** is now correctly removed from the interface.

23226 – The Description field is now correctly populated as "Any ActiveX Control" for inserting an ActiveX control and "Any Windows Store App" for Windows Store App if you leave the Codebase (URL) or the Package Name blank respectively.

3009, **47366**, **72825** – Events imported from a database are now correctly classified according to their type.

47697 – You can now add a binary to a policy with Command Line as the matching criteria for OS X configurations.

59583 – The Content Groups and URL Groups search bars now correctly state the name that is selected in the tree view.

68947 – Opening a local draft from iC3 now correctly interprets the encoding on matching criteria.

72816 – The Get-DefendpointFileInformation cmdlet now returns the full publisher name, even if it contains a comma.

4.2.4 - Known Limitations

There are two circumstances in which the Avecto Zone Identifier is not applied by Avecto when the user downloads a file from the browser:

- Files that are compressed in a zip file. The zip file itself is tagged with the Avecto Zone Identifier tag.
- Files that are downloaded directly to a mapped network drive. The Avecto Zone Identifier tag is applied when you save the file to your local drive first before moving it to a mapped network drive.

This means that you cannot match on the Avecto Zone Identifier tag in the above scenarios.