Defendpoint Management Console Release Notes

Software Version: 5.2.21.0 GA

Document Version: 1.0

Document Date: August 2018

Chapter 1 - Release Notes

1.1 - New Features

82504 - 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 - Enhancements

85297 - Updated the EULA in the product to reflect the recent acquisition of the business by Bomgar. As part of this change we have also removed out of date help documentation from the product. Please refer to Avecto Connect for the latest product documentation.

1.3 - Bugs

79289 - Fixed multiple issues for the OS X Controlling Workstyle:

- The default rule pre-selected for the combination of a **Blacklist** and **Present users with a challenge code** is now **Allow execution** rather than **Block Execution**.
- The default target Application is now **Apps that are allowed** rather than **Apps that are blocked**.
- The Detail and Summary view no longer states **Show Allow Message (with Challenge)** when the End User Message is set to **Off**.

79477 - Controlling workstyles created using the Workstyle wizard now correctly set the **Authorization Requests** column in the Workstyle Overview.

79575 - The **Names**, **Descriptions**, **Body** and **Header** for the Mac Message Templates have been updated and standardized with other Defendpoint management platforms.

80511 - You can now specify a value of '0' for Mac OS X Account filters. This is the root account for the Mac operating system.

82274 - All special characters are preserved when a Defendpoint policy is exported using the PowerShell API.

Chapter 2 - Prerequisites

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

2.1 - 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.

2.2 - Defendpoint Activity Viewer

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

Chapter 3 - Supported Operating Systems

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

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10 builds Enterprise 2015 LTSB, Enterprise 2016 LTSB, 1607, 1703, 1709, 1803
- Server 2008 R2
- Server 2012
- Server 2012 R2
- Server 2016

Chapter 4 - Version History

4.1 - 5.1.149.0 SR1

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

4.1.1 - 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

4.1.2 - 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.

4.2 - 5.1.91.0 GA

4.2.1 - New Features

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

4.2.2 - 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.

4.2.3 - Known Limitations

There are some known limitations with the new 'Uninstaller' Application Type that are listed here.

Adobe Air Uninstall
76098 - When you attempt to uninstall Adobe Air the interface remains open although the uninstall process succeeds. You need to terminate this interface process manually once you have uninstalled the product. Alternatively, when you initiate the uninstall you can select the option 'Do Not close application' when it pops up and this will complete the uninstall successfully without needing to force the termination of the process at the end.

Concurrent Uninstalls
76011 - As with standard Windows behavior, you can only run one uninstall at a time. Attempts to run a second concurrent uninstall will not be started but the Windows warning is not displayed to the end user.

Google Toolbar
75853 - The install of the Google Toolbar matches the uninstall rule as it does perform an uninstall action as part of its install process. You can click 'Yes' or 'No' on the Defendpoint prompt to proceed. The program is successfully installed irrespective of your choice.

Minimizing System Settings
76254 - When System Settings is minimized the process will be suspended. Any uninstall process, running as a child of System Settings, will also be suspended. Maximizing System Settings causes the process to be active again and the uninstall will continue.

On-Demand Child Process Matching for Uninstallers
76302 - This scenario may apply if you have an On-Demand rule with the 'Add Admin' token and 'Allow child processes to match this application definition' selected. If you use this On-Demand rule to elevate a command line tool and run MSIEXEC to uninstall an application, Application rules in your policy may be matched.

4.3 - 5.0.102.0 GA

4.3.1 - 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.

4.3.2 - 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.

4.3.3 - 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.

4.3.4 - 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.