

Defendpoint Management Console Release

Software Version: 5.3.217.0 SR1

Document Version: 1.0

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

- ["New Features" below](#)
- ["Enhancements" below](#)
- ["Bugs Fixed" below](#)

1.1 - New Features

76996 - 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.

77159 - 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.

86206 - There is a new macOS QuickStart Template available for use in the policy editor. Full details of this can be found in the Defendpoint Management Console Administration Guide for this release

1.2 - Enhancements

76998 - 'User' context is now available in addition to 'System' context when you add a PowerShell Audit Script.

80702 - 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)**.

1.3 - Bugs Fixed

72072 - Replaced the ellipsis with a red cross on the right-hand of the search box in the Defendpoint Management Console to clearly indicate that it clears the text.

72628 - The macOS template **Startup Disk** of type System Preference Pane now correctly matches.

72662 - 'N/A' is now correctly shown for the Token field in the HTML report where the rule is Block.

73127 - The access token now correctly updates in the interface when it was set to a **Custom Token** in the Application Rule dialog and subsequently altered to a built-in token type from the right-click menu.

74966 - The summary view for the Application Rule now shows if Audit to **iC3** is enabled.

76130 - You can no longer set the **Send Events to iC3** setting if the **Raise an Event** setting in the **Auditing** section is disabled.

79609 - Importing the **TAP (High Flexibility)** or **TAP (High Security)** no longer shows the hidden groups by default.

87672 - Updated the message templates in the macOS Quick Start Policy.

Chapter 2 - Prerequisites

- ["Defendpoint Management Console" below](#)
- ["Defendpoint Activity Viewer" below](#)

2.1 - Defendpoint Management Console

- Microsoft .NET Framework 4.0 (required for the PowerShell API)
- 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 Native Client

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 and 1809
- Server 2008 R2
- Server 2012
- Server 2012 R2
- Server 2016

Chapter 4 - Version History

4.1 - 5.2.2.0 SR1

- ["Bugs" below](#)

4.2 - Bugs

79664 - Updated the Windows Store application templates to match those provided in recent Windows 10 versions.

86133 - Activity Viewer 5.2 now correctly connects to an Enterprise Reporting 5.2 database.

Known issues for this release are listed on Connect: https://connect.avecto.com/community/articles/en_US/Support_KB_Article/Activity-viewer-Could-not-connect-error.

4.3 - 5.2.21.0 GA

- ["New Features" below](#)
- ["Enhancements" below](#)
- ["Bugs" above](#)

4.3.1 - 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.

4.3.2 - 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.

4.3.3 - 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.

4.4 - 5.1.149.0 SR1

- ["New Features" on the previous page](#)
- ["Bugs" on the previous page](#)

4.4.1 - 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

4.4.2 - 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.

4.5 - 5.1.91.0 GA

4.5.1 - New Features

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

4.5.2 - 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.

4.6 - 5.0.102.0 GA

4.6.1 - 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.

4.6.2 - 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.

4.6.3 - 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.

4.6.4 - 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.