



# Defendpoint Console Release Notes

**Software Version: 4.5.1.0 GA**

**Document Version: 1.0**

**Document Date: 31 May 2017**

## **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 - Defendpoint Console

- [Release Notes](#) detailed below
- [Supported Operating Systems](#) detailed below
- [Prerequisites](#) detailed below
- [Version History](#) detailed on page 4

### 1.1 - Release Notes

- [New Features](#) detailed below
- [Enhancements](#) detailed below
- [Bug Fixes](#) detailed below

#### 1.1.1 - New Features

**65161** – Added configuration to allow you to control the ability to run sudo commands. Please refer to the Defendpoint for Mac Administration Guide for more information.

**63530** – New Commands Only view in the Event Import.

#### 1.1.2 - Enhancements

**63310** – Binaries that trigger authorization requests can be managed by Defendpoint.

#### 1.1.3 - Bug Fixes

**65789** – The licensing banner correctly displays on the Windows or OS X node if the relevant license has not been added to Defendpoint.

## 1.2 - Supported Operating Systems

Both the 32-bit and 64-bit versions of these platforms are supported:

- Windows Vista Service Pack 2
- Windows 7 Service Pack 1
- Windows 8/8.1
- Windows 10
- Windows Server 2008 Service Pack 2
- Windows Server 2008 R2 Service Pack 1
- Windows Server 2012/R2
- Windows Server 2016

## 1.3 - Prerequisites

- [Defendpoint Management Console](#) detailed below

### 1.3.1 - Defendpoint Management Console

- Microsoft Visual C++ 2015 Redistributable
- Microsoft Group Policy Management Console (for Active Directory integration)

## Notes



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 2008 R2 Native Client is required for connectivity with Enterprise Reporting.

---

## Chapter 2 - Version History


### 2.1 - 4.4.92.0 Release

#### 2.1.1 - Enhancements

**33073** - Added policy editor support for the Modern UI in Windows 8 and 10 On-Demand feature. Please refer to the Admin Guide for more information.

Updated Defendpoint runtimes to use Microsoft Visual C++ 2015. Due to this update, the Defendpoint Management Console (MMC) is no longer supported on Microsoft Windows XP or Microsoft Windows Server 2003.

---

 This change only affects the Management Console. The Defendpoint Client version 4.4 is supported on Microsoft Windows XP and Microsoft Windows Server 2003.

---

#### 2.1.2 - Bugs Fixed

**3683** - Fixed an issue that caused a "Failed to Launch Help" message to appear when F1 was pressed in the PGChallengeResponseUI application.

**10078** - Fixed an issue where long workstyle descriptions in the Defendpoint management console would wrap onto a new line.

**11050** - Updated WMI templates to include versions for Windows 8.1, Windows 10, Windows Server 2012 R2 and Windows Server 2016.

**31669** - Fixed an issue in the Defendpoint management console where license expiry dates were not completely visible.

**49154, 51223, 54027** - Fixed an issue where events weren't being read correctly when imported from a 4.1 version of the database to a version 4.3 of the Console.

**49317** - Fixed an issue where the application properties for certain MSIs were not being returned in version 4.0 of the console and higher.

**53908** - Fixed an issue in assigning custom audit scripts to rules using the right-click functionality.

**56069** - Fixed an issue where negation of "publisher" matching criteria was not possible.

### 2.2 - 4.3.118 Release

#### 2.2.1 - Bug Fixes

- **29450** – Link to the correct Help page within content and URL dialogs.
- **10384, 28426, 28503, 29452, 28497, 29743, 29744, 29746, 29750, 29748, 48474, 29752, 29757, 29781, 47409, 7784** – Grammatical improvements in the Defendpoint Management Console.
- **10459** – Use consistent icons when creating workstyle on the toolbar and context menu.
- **29857** – Consistent language for Authorization Type in the option and the description.

- **10098** – Improved URL validation in the Defendpoint Management Console.
- **33008** – Prevent duplicate licenses when importing configuration.
- **32781** – HTML report now specifies On-Demand application rules.
- **5196** – Renamed application wizard headers to be appropriate to the application type.
- **1297** – Use consistent icons for control panel applets and batch files on the Application Groups context menu.
- **2992** – Disable Insert button when template list is empty.
- **10038** – Consistent use of tick icon on the Insert Application wizard.
- **11158** – Correct help link for On-Demand application rules.
- **10088** – Improved error message when URL validation fails.
- **3151** – Fix Inverse Outcome of this Filter context menu option in the Defendpoint Management Console.
- **18090** – Built in Application Groups are now available in controlling process and child process matches.
- **8166, 8168** – Fixed the Run Script context menu in the Defendpoint Management Console.
- **3152** – Added support for Cut/Copy/Paste for workstyle filters.

## 2.3 - 4.3.50 Release

### New Features

- Sandboxing of the Google Chrome browser.
- Defendpoint provides support for Google Chrome. Defendpoint will apply the same rules that are used for Internet Explorer, so that Google Chrome will automatically be sandboxed when users navigate to an untrusted website.
- All content downloaded from untrusted websites using Google Chrome is automatically classified as 'untrusted' and opens inside the sandbox.

### Enhancements

- Support for Windows 10 Anniversary Edition.

## 2.4 - 4.1.234 Release

### Enhancements

- Provide the ability to choose whether to use Designated User Authorization or Challenge/Response on the same custom message.

### Bug Fixes

- **28420, 28422** – Fixed spelling errors in template titles list.
- **29759, 29783, 29865, 31225** – Spelling, grammar and visual updates following brand and tone of voice review.
- **31278** – Custom templates no longer need to follow a specific naming convention.
- **31364** – Removed unnecessary scroll bar when creating rules.
- **32082, 34670** – Fixed spelling errors in EULA.
- **32014, 32125** – Fixed copy/paste for filters and rules.
- **32551** – Removed Match Case matching criteria for an OS X URI.

## 2.5 - 4.1.149 Release

### New Features

- Sandboxing of Outlook Email Attachments.
- Added ability to check out, edit and check in Defendpoint configurations from within IC3.
- Added support for creating Defendpoint workstyles for both Windows and Mac computers using the same configuration.

### Enhancements

- **29391** - All Avecto and Defendpoint binaries are now dual-signed with SHA-1 and SHA-256 certificates.
- **2629** - The 'Source URL' of a downloaded application added via the 'Add Application' wizard is now included as a matching criteria for that application.
- **16512, 22008** - Added Microsoft Office 2007/2016 rules for the Sandbox Content Handlers generated group.
- **19494** – Updated the Windows Store Applications templates to support Windows 10 applications.

### Bug Fixes

- **10101, 10618** - Optimized the generation of SHA-1 hashes, to improve performance when downloading, copying, editing or opening large (>1GB) files.
- **14127** - Fixed a bug in the Event Import Wizard, where COM Classes were being added as Executable types.
- **15852** – Fixed a bug in the Advanced UAC Replacement template, which was causing excessive message prompting for signed applications.
- **18375** – Fixed a bug in the Advanced UAC Replacement template, which was unnecessarily prompting users when the COM Surrogate process was launched.
- **21098** – Fix a bug in the MMC where using the 'Move to top' on a URL rule caused the rule to be deleted.
- **19003** – Fixed a bug in the MMC where Parent Process Group matching criteria were not being included when copying workstyles from one configuration to another.

## 2.6 - 4.0.387.0 SR5 Release

### Enhancements

- Added SHA-1/SHA-256 dual signed certificate for Defendpoint binaries and installation packages.

## 2.7 - 4.0.349.0 SR2 Release

### Enhancements

- Create the correct type of message when using the Create Workstyle wizard to create a blacklisting configuration
- Corrected the File Archivers entry in the Sandbox Content Handlers generated group.

## 2.8 - 4.0.247 SR1 Release

- Updated auto-generated Sandboxed Content Handler application group to cater for new version of Adobe Acrobat Reader.

## 2.9 - 4.0.191.0 Release

### New Features

- 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.
- Enhanced Enterprise Reporting
- User experience dashboard to expose blocks and requests for access
- Faster access to key application data
- Database admin dashboard with application purge and exclude

## **Enhancements**

- 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.
- Added ability to show/hide individual tabs in Workstyles, so that only feature tabs in use are shown.
- 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.