BeyondTrust

Windows Client Release Notes

5.3.229.0 SR2

Privilege Management

TC:3/4/2019

Release Notes

Note: *For this release, Microsoft Office 2016 should be at version 16.0.6001.1038 or later. Please see Avecto KB article https://connect.avecto.com/community/articles/en_US/Support_KB_Article/Required-Microsoft-Update-for-Office-2016-when-using-Defendpoint-v4-3-118-and-above and Microsoft KB article: https://support.microsoft.com/en-gb/kb/3104401 for more information.*

Enhancements

88775 - Added support for Windows Server 2019.

Bugs Fixed

74983, 87874, 88799 - Prohibit Privileged Account Management now enforces restrictions on the PowerShell cmdlets **Add-LocalGroupMember**, **Remove-LocalGroupMember** and **Set-LocalUser**.

87083, 87115 - Defendpoint now correctly matches when applications are run from a network share, and the matching criteria includes **Application Requires Elevation (UAC)** in addition to other matching criteria.

87275 - Added functionality to ensure that event files are only generated from the QuickStart policy for ePO and iC3 when the client is installed in those configurations.

88261, 88480 - Fixed a process-handle memory leak in Defendpoint that occurred in certain scenarios.

87280 - Fixed an issue to ensure that rules are matched correctly when the user is the PowerUsers group and matching criteria **Application Requires Elevation (UAC)** is applied.

88965 - Fixed an issue that caused the Defendpoint service to crash if it was stopped, and the **Collect host information** general rule was enabled.

Prerequisites

Defendpoint Client

- .NET Framework 4.0 (Required to use Power Rules, PowerShell audit scripts and PowerShell API)
- PowerShell 3.0 (Required to use Power Rules, PowerShell audit scripts and PowerShell API)
- Microsoft SQL Server Compact 4.0 (x86 & x64)
    - Required on the endpoint for Activity Viewer functionality. This prerequisite is included with the executable (EXE) of the Defendpoint Client. If you are using the Defendpoint Client Microsoft Installer (MSI) or the ePO Defendpoint Windows Client zip package you need to manually install this prerequisite.
- The McAfee Agent must be installed if you are installing the Defendpoint client with switch EPOMODE=1

Defendpoint Activity Viewer

- Microsoft SQL Server Compact 4.0
    - Required on the endpoint that will run the Activity Viewer Console. This prerequisite is included with the executable (EXE) of the utility.
- Microsoft .NET Framework 4.0 Client

Note: *The executable version of the client package includes all necessary prerequisites (excluding .NET Framework 4.0), and automatically installs them as necessary.*

Note: *The Defendpoint Client executable installer automatically installs Microsoft SQL Server Compact. If you do not wish to use the Activity Viewer, and do not wish for this prerequisite to be installed, we recommend you install the Defendpoint Client MSI installation.*

Compatibility

The Windows client compatibility is listed below:

BeyondTrust Products Compatibility

Defendpoint Group Policy Console

This release is compatible with the Defendpoint Console 4.5 or later.

Defendpoint ePO Extension

The following Defendpoint Extension versions are compatible with this version of the Defendpoint Client.

> ***Note:*** *Please use the latest Defendpoint ePO Extension at the time of release. If you use an older version of the Defendpoint ePO extension, some Windows client functionality may not be supported. Clients that are newer than the ePO extension may be tolerated depending on the internal product ID.*

- **Recommended**: 5.3 (all versions)
- 5.2 (all versions)
- 5.1 (all versions)
- 5.0 (all versions)

iC3 Windows Adapters

The following iC3 adapters are compatible with this version of the Defendpoint Windows client.

- 1.4 (all versions)
- 2.1 (all versions)

McAfee Products Compatibility

McAfee Agent

The following McAfee supported versions of these Agents are compatible with this version of the Defendpoint Client:

- **Recommended**: 5.6.x
- 5.5.x
- 5.0.x

> ***Note:*** *Version 4.8 and older of the McAfee agent are* ***not*** *supported with this release.*

McAfee ePO Server

The following McAfee supported ePO Server versions are compatible with this version of the Defendpoint Client:

- **Recommended**: 5.10 (all versions)
- 5.9 (all versions)
- 5.3 (all versions)

> ***Note:*** *Version 5.2.21.0 GA of the Defendpoint Windows Client is certified with ePO Server 5.9.*

> ***Note:*** *Version 5.2.28.0 SR1 of the Defendpoint Windows Client is certified with ePO Server 5.10.*

McAfee Endpoint Security (ENS)

The following McAfee supported Endpoint Security versions are compatible with this version of the Defendpoint Client:

- Endpoint Security (ENS) Adaptive Threat Protection (ATP) 10.x
    - With Generic Privilege Escalation Prevention (GPEP) enabled and disabled
- ENS Firewall 10.x
- ENS Threat Prevention 10.x
- ENS Web Control 10.x

McAfee MOVE Multi-Platform Client

The following McAfee supported versions of the MOVE Multi-Platform Client are compatible with this version of the Defendpoint Client:

- MOVE AV[Multi-Platform] SVA Manager 3.6.1.141
- MOVE AV[Multi-Platform] Client 3.6.1.141
- MOVE AV[Multi-Platform] License Extension 3.6.1.141
- MOVE AV[Multi-Platform] Offload Scan Server 3.6.1.141

> ***Note:*** *We do not support the agentless version of McAfee MOVE.*

If the version of McAfee MOVE is compatible with the McAfee Agent you're using then Defendpoint is also compatible.

Supported Operating Systems

Privilege Management/Application Control Support

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

- Windows 7
- Windows 8 and 8.1
- Windows 10 builds Enterprise 2015 LTSB, Enterprise 2016 LTSB, 1607, 1703, 1709, 1803 and 1809
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Content Isolation

Note: *Content Isolation is supported with Windows 10 1709 and lower.*

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

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

Primary Application Support

- Internet Explorer 8+
- Google Chrome
- Microsoft Office Word 2007/2010/2013/2016
- Microsoft Office Excel 2007/2010/2013/2016
- Microsoft Office PowerPoint 2007/2010/2013/2016
- Microsoft Office Outlook 2007/2010/2013/2016
- Adobe Reader 10+
- Zip Archivers (Winzip, WinRAR, Windows Compressed Folders)

Note: *If you are upgrading Defendpoint you may need to update your workstyles to incorporate newly supported features/applications.*

Version History

5.3.219.0 SR1

Enhancements

87832 - Updated the product EULA with the BeyondTrust license agreement.

Bugs Fixed

87754 - Fixed an issue with the version number display that is passed to the Defendpoint ePO Extension.

5.3.216.0 GA

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.

Enhancements

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)**.

Bugs Fixed

70125- Fixed an issue that caused navigation to be slow in the File Explorer when the files or folders were exceptionally large.

71445 - Fixed a crash so you can now download, and open, a Word document from Microsoft Edge.

84570, 84892, 85978, 87336 - The current working directory no longer defaults to `c:\windows\system32` when an application is launched using the on-demand functionality.

85442, 85443, 85445, 85631 - Fixed an issue that was causing delays in opening Microsoft Excel files from a network location when a policy containing Content Control was applied.

5.2.28.0 SR1

- "Bugs Fixed" on page 9

Bugs

75970 - Accounts that are members of the Windows BUILTIN\Guests group are now supported by Defendpoint.

84242, 84340, 84401, 85134, 85173, 85300, 85976, 85977, 86439 - Fixed an issue that caused the installation of some applications to fail when elevating them with Defendpoint.

85291 - The performance of opening files from a NAS share has been improved.

85442, 85398 - The Microsoft SQL Server Compact version required for the Defendpoint Activity Viewer has been updated to version 4.0. This is installed as part of the Defendpoint client executable.

85654 - Negated process matching for Content Control groups now works correctly.

85975 - Defendpoint now correctly sets the Windows integrity level for custom and built-in Drop Admin tokens.

86123, 86131, 86672 - You can now run executables (EXE) located on a network share that require elevation when specifying a UNC path.

5.2.21.0 GA

New Features

63750 - Updated the Defendpoint client to use the McAfee Message Bus API. Support for the older method of communication known as McAfee LPC has been removed.

> ***Note:*** *This version of the Defendpoint client is not compatible with McAfee ePO Server 4.8 and older.*

77951 - The generation of Challenge Response codes for Windows now takes into account the Defendpoint token being applied. This ensures that a different Challenge Response code is generated if Defendpoint applies a different token to the same application, for example an elevation rule versus a passive rule.

> ***Note:*** *Using two different custom tokens will still generate the same challenge code for the same application.*

Enhancements

85297 - Updated the EULA in the product to reflect the recent acquisition of the business by Bomgar.

Bugs

69866 - Fixed an issue that caused Windows explorer to crash when running shortcuts with target paths longer than 257 characters using on-demand application rules.

81174 - You can now install Visual Studio 2017 successfully when elevating the installer with Defendpoint.

81836 - The retention period you set for a **Challenge Response** message is correctly applied when you set both a **Designated User Must Authorize** and a **Challenge / Response** message where either is sufficient.

82101, 82693 - You can no longer use Defendpoint and an admin token to uninstall a Defendpoint client that has been installed from a network share using the MSI. A Windows UAC prompt is correctly displayed.

82227 - Negated parent process matching now works correctly in Defendpoint.

79457, 81817, 81812, 81821, 82130 - You can now install, repair and uninstall Microsoft Office Professional Plus 2013 and Microsoft Project Plus 2013 with Defendpoint.

84486 - You can now install, repair and uninstall Microsoft Visio 2016 with Defendpoint.

5.1.149.0 SR1

- "New Features" on page 11
- "Enhancements" on page 9
- "Bug Fixes" on page 11

> ***Note:*** *You need to restart all endpoints managed by Defendpoint after upgrading to this version of Defendpoint to ensure policy is correctly applied.*

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

80242 - Added support for Windows 10 version 1803.

Enhancements

83059 - Targeting a UNC path will also match any drives mapped to that UNC path.

Bug Fixes

77416 - Hardened the security for the Defendpoint hook load mechanism by removing the reliance on global mutexes. This does not affect the management of, or the user experience of, Defendpoint. This addresses CVE-2017-16245.

75951 - Hardened security by migrating the Defendpoint Application Control feature from user mode to kernel mode. This does not affect the management of, or the user experience of, Defendpoint. This addresses CVE-2017-16246.

54821 - Added support for Swedish in the on-demand options to 'Run as' and 'Run as administrator'.

72106, 72539, 74152 - Application rules are now correctly applied when an application is run from a network path.

73972 - Anti-tamper has been improved to protect the Defendpoint client from a WMIC uninstall.

76474 - All events are now correctly forwarded and displayed in iC3 irrespective of time-zone.

80880 - Improved the reliability of command line parsing for batch files. As part of this change we have hardened our approach to matching for batch files. When using the 'start' command line switch, Defendpoint does not match any rules for subsequent batch files. This is in line with the existing '\K' command line switch functionality.

81499 - Added a check to ensure computer level environment variables cannot be overridden by user defined environment variables. This addresses CVE-2018-10959 reported by the Lockheed Martin Red Team.

Known Issues

Note: *Known issues for this release are listed on Connect: https://connect.avecto.com/community/articles/en_US/Support_KB_Document/Released-known-issues*

5.1.95.0 GA

New Features

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

73305 - Added Support For Windows 10 version 1709.

Bug Fixes

37022, 51595, 70376, 76273 - You can now run applications as a different user when you have a policy in place to elevate applications that have generated a UAC prompt.

54257, 54734, 73099 - These bugs have been addressed by the new uninstall capability in this release using the native Windows Programs and Features functionality.

74360, 74387 - Compatibility issues between Docker for Windows and Defendpoint have been resolved.

74595, 74596, 74827 - Defendpoint now correctly elevates 'Windows PowerShell (Admin)' from the start menu when an application rule is in place that targets it.

74598 - Information is now correctly audited from files that have been run from a network share.

74659, 74660 - You can now use the on-demand rule to elevate Device Manager from the Control Panel.

74663, 74666 - MSIs with child processes are now correctly elevated according to Defendpoint policy when using the '/qn' command line switch.

74751 - Fixed an issue that caused attributes to be missing within MSI audit events.

76388 - Added an engineering setting to the Defendpoint Client that allows specific processes to be excluded in the event that incompatibilities with Defendpoint are encountered. For more information, please refer to Avecto Support.

76353 - Fixed an issue that caused the Windows Store application to crash if it was elevated using Defendpoint with Windows 10 build 1709.

76786 - Fixed an issue that caused Internet Explorer to open minimized on the task bar.

5.0.102.0 GA

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.

Enhancements

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

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

73544 – Defendpoint can now match on the Avecto Zone Identifier.

Bug Fixes

39857, 48539, 55970 – Defendpoint now correctly displays information in the event viewer when Media from Netflix or Amazon Video is blocked because 'mfpmp.exe' isn't allowed to execute due to policy.

69319 – Fixed signature verification checks for remote PowerShell scripts.

74642 - Conflicts between Defendpoint and Hyper-V have been resolved so that virtual machines start correctly.

71665 - Fixed an issue that caused Internet Explorer to fail to run sandboxed on a clean installation of Windows 10.

72815 – The SQL Server Express service now starts correctly.

61231, 72989, 67147 – Wildcards in the 'Does not match publisher' criteria are now correctly matched for applications.

Known Issues

Note: *Known issues for this release are listed on Connect: https://connect.avecto.com/community/articles/en_US/Support_KB_Document/Released-known-issues*