Defendpoint Windows Client Release Notes

Software Version: 4.4.267.0 SR6

Document Version: 1.2

Document Date: May 2018

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

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.

- **New Features** detailed below
- **Bug Fixes** detailed below

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

1.1 - New Features

80242 - Added support for Windows 10 version 1803.

1.2 - Bug Fixes

77418 - 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.

78453 - 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.

72879 - The ProductName field for MSI files is now audited correctly in events.

78628, 78629, 78630 - Application rules are now correctly applied when an application is run from a network path.

79212 - All events are now correctly forwarded and displayed in iC3 irrespective of time-zone.

79238 - Added support for Swedish in the on-demand options to 'Run as' and 'Run as administrator'.

81335 - 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.

81588 - 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.

1.3 - Known Issues

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

Chapter 2 - Supported Operating Systems

- **Privilege Management/Application Control Support** detailed below
- **Supported Operating Systems** detailed above

2.1 - Privilege Management/Application Control Support

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

Platforms

- Windows XP x86
- Windows 7
- Windows 8 and 8.1
- Windows 10 builds 1507, 1607, 1703, 1709, and 1803
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

2.2 - Content Isolation

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

Platforms

- Windows XP x86
- Windows 7
- Windows 8 and 8.1
- Windows 10 builds 1507, 1607, 1703, 1709, and 1803
- Windows Server 2003 R2
- Windows Server 2008
- 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)

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

Chapter 3 - Prerequisites

- **Defendpoint Client** detailed below
- **Defendpoint Activity Viewer** detailed below

3.1 - Defendpoint Client

- Microsoft Core XML Services 6.0 (XP SP3 only)
- Microsoft SQL Server Compact 3.5 SP2 (Required for using the Activity Viewer)
- .NET Framework 2.0 (Required to run PowerShell audit scripts)
- The McAfee Agent must be installed if you are installing the Defendpoint client with switch EPOMODE=1

3.2 - Defendpoint Activity Viewer

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

Notes

The executable version of the client package includes all necessary prerequisites (excluding .NET Framework 2.0), and automatically installs them as necessary.

The Defendpoint Client executable installer automatically installs Microsoft SQL Server Compact 3.5 SP2. 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.

Chapter 4 - Version History

4.1 - 4.4.233 (SR5) Release

4.1.1 - Bug Fixes

76060 - 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.

4.2 - 4.4.222.0 (SR4) Release

4.2.1 - New Features

74956 - Added Support For Windows 10 version 1709.

4.2.2 - Bug Fixes

29473 - SolidWorks Product Data Management now opens correctly when Content Control is enabled.

36188, **68083**, **71966** - Defendpoint now correctly elevates 'Windows PowerShell (Admin)' from the start menu when an application rule is in place that targets it.

37021 - Applications that are launched and trigger an On-Demand rule where the Message is configured to 'Run Application as Authorizing user' now start correctly.

39649, **64644** - MSIs with child processes are now correctly elevated according to Defendpoint policy when using the ‘/qn’ command line switch.

63873 - SQL Server 2008 service now starts correctly without a timeout.

67212 - The Get-DefendpointFileInformation cmdlet now correctly returns the full publisher name, even if it contains a comma.

69443 - Information is now correctly audited from files that have been run from a network share.

72890, **73017** - You can now use the on-demand rule to elevate Device Manager from the Control Panel.

73092 - Fixed an issue that caused a sporadic build error with Visual Studio when elevating the process 'devenv.exe' and associated child processes.

75208, **75211** - You can now successfully start the Docker container using the Docker for Windows application and the application remains stable throughout the period of execution.

74589, **74590**, **74591** - 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.

74786 - Defendpoint application rules now correctly intercept shortcuts that have been set to run as an administrator.

74957 - Conflicts between Defendpoint and Hyper-V on Windows 10 1709 have been resolved so that virtual machines start correctly.

75216 - Fixed an issue that caused On Demand rules to fail to match when using **Run As Admin** on Windows 10 1709.

4.3 - 4.4.199 (SR3) Release

4.3.1 - Bug Fixes

58096, 58144, 63405, 63501, 64001, 64643, 67209, 68127 – Improved the performance of wildcard matching.

59127, 59130 – Improved resilience of running command-line-based applications after running PowerShell audit scripts.

60401, 68233 – Added support for environment variables when applying on-demand application rules to the run as administrator option.

68595 – Increased file size limit for file hash matching when using Defendpoint's PowerShell API.

69235 – Added support for long argument paths in shortcuts when using on-demand elevation.

4.4 - 4.4.177 (SR2) Release

4.4.1 - New Features

63938 – Added support for Windows 10 Creators Update build 1703.

4.4.2 - Enhancements

67173 – Improvements to PGMessageHost and System Tray communications.

4.4.3 - Bug Fixes

13228, 35038 – A new Host Local SID field has been created and added to events so that the local SID can be included on events.

36465, 54820, 55637, 66801– Applications can now be sorted by date in PGProgramsUtil.

51022 – VMWare Workstation can now be uninstalled using PGProgramsUtil.

53955, 53956, 63739, 67146, 67533, 67703, 67738, 68546 – Added support for Microsoft Edge on Windows 10 Creators Update build 1703.

54819, 56388, 66462 – Processes elevated by Defendpoint can now be used to start or stop a service that is controlled by Defendpoint service control rules.

57989 – IPass Open Mobile can now be uninstalled using PGProgramsUtil.

63083, 65155 – Fixed an intermittent issue where applications elevated on-demand didn't always launch successfully.

63493, 63693 – Previous versions of folders created by VSS (Volume Snapshot Service) can now be opened on Windows 7.

64020 – The authorizing user details are now available in events for actions that requested authorization from a designated user.

64627, 67278 – Defendpoint can now parse the PowerShell call operator &.

65774 – When a child process is elevated, the Application Workstyle Description within the Event Viewer now displays the name of the workstyle that elevated the process.

66150, 66153 – New vector (.TIFF) files can now be loaded into ArcGIS Pro.

66463 – FileStream mode can now be enabled within an elevated instance of SQL Server Configuration Manager.

66469 – Printer drivers can now be installed using admin rights when there is an application rule that elevates the print spooler.

66907 – Public files that are located on a mapped network drive that has a file path of more than 105 characters now open successfully.

67485 – Services verify that the executable being run is the one that is expected by the service.

67505 – Child processes of a process run from a mapped network drive are now matched correctly.

67877 – Defendpoint can now parse and match on Chrome proxy host names.

68328 – Executables launched from a symlink location now match correctly on Publisher and Product Description.

68417 – One 100 event is now raised instead of two 100 events when a designated user authorizes a UAC prompt and the process is run as the authorizing user.

4.5 - 4.4.145.0 (SR1) Release

4.5.1 - Bug Fixes

31957, 59199, 59380, 59710, 59711, 60137, 64024 – The properties of network adapters can now be viewed using PGNetworkAdapterUtils on Windows 10.

56958, 63738, 65035 – Chrome extensions are no longer removed when Defendpoint is installed.

51002 – Debugging Web projects using Visual Studio no longer causes high CPU usage.

61894, 62864 – UAC prompts are correctly triggered when using shortcuts that have the Run As Administrator option selected in Advanced Properties.

53814, 56195 – The sandboxing extension for IE is removed when sandboxing is disabled.

55899 – The Defendpoint Outlook add-in is removed when sandboxing is disabled.

51358 – Applications with the MSI uninstall feature enabled can now be uninstalled.

59581 – Fixed an issue that was causing applications to incorrectly match as children of fast-running processes.

61646 – Anti-tamper rules are correctly enforced when a service rule is applied to the Defendpoint service.

62308 – Fixed a compatibility issue with NokiaMgr so that it doesn't require a hook exclusion to function correctly.

64073 – Fixed a compatibility issue with LogMeInToolkit.exe so that it doesn't require a hook exclusion to function correctly.

62320 – Using the Run as Administrator option correctly triggers a UAC prompt if a passive on-demand rule is applied.

60175 – Untrusted instances of Notepad only have read-only access to files located outside of the user's profile.

16277, 27021, 45938, 59855 – Removed support for privilege management of app containers, which are used by applications such as Cortana, Edge and Windows Store Apps.

65229 – Improved resiliency between PGMessageHost and the Defendpoint Service.

4.6 - 4.4.92.0 Release

4.6.1 - Enhancements

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

50714 – Added the ability to access a OneDrive folder from within a Sandbox when opening and saving untrusted content in Windows 10.

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.

4.6.2 - Bug Fixes

540 - Updated standard Defendpoint messages to follow best practices.

17639, **53954** – Fixed a compatibility issue with dbus-daemon.exe that previously required a hook exclusion for Kleopatra to function correctly.

21206, **54482** – Fixed a compatibility issue with procmon.exe that previously required a hook exclusion for ProcMon to function correctly.

22773 – Fixed a compatibility issue with baretailpro.exe that previously required a hook exclusion for BareTail to function correctly.

29927 – Fixed an issue with AutoCAD so you can save files in AutoCAD or copy/paste text/info into drawings.

34218 – Fixed a minor typo in Defendpoint ePO Interface events.

42931, **57970** -Fixed an issue to allow users to enter details into an Avecto message box using a touch screen keyboard.

44167 – Visual Studio tools crashing with Privilege Monitoring enabled.

45929– Fixed an issue with sandbox taskbar icons not grouping properly.

50833 – Fixed an issue where Notepad++ would remain open and display an error when re-launching in administrator mode with Defendpoint elevation.

51254 – Fixed a compatibility issue with sandboxing and UE- V that caused processes to terminate.

53181, **53182**, **55255**, **56411** – Fixed an issue that caused Defendpoint to repeatedly try to connect to Avec.to after upgrading to a 4.3 version when sandboxing was disabled.

54436 – Fixed an issue so EnCase Examiner can be installed successfully.

26762, **52885**, **44104**, **52802**, **47744**, **54853**, **54851**, **56391** , **60329** – Fixed cases where certain applications were falsely triggering the Defendpoint replacement User Account Control (UAC) prompts.

56506 – Improved the resilience of URL download tracking

57255 – Fixed a minor memory leak in the Defendpoint Service when using Windows Store Applications matching criteria.

4.7 - 4.3.138.0 (SR6) Release

4.7.1 - Bug Fixes

56759 – Fixed an issue affecting Internet Explorer and Chrome browsers that prevented certain secure https URLs from being loaded successfully in a sandbox.

4.8 - 4.3.136.0 (SR5) Release

4.8.1 - Bug Fixes

57048 – Fixed an issue with Windows XP that caused the Defendpoint client not to function after fix 55556 was applied.

57321 – Fixed an issue identified with Defendpoint versions 4.3 SR3 or 4.3 SR4 that prevented Windows 10 setup/upgrade from starting correctly.

57473 – Added a hook exclusion to allow DISM (Deployment Image Servicing and Management) to function correctly.

4.9 - 4.3.131.0 (SR4) Release

4.9.1 - Bug Fixes

- **55556** – Fixed a flaw that could allow an attacker to bypass Defendpoint rules.
- **54156** – Updated the PGDriver to fix a blue screen issue.

- **50003** – Added support for Chrome sandboxing with proxy configuration via a .pac file.
- **54387** – Resolved a compatibility issue when running LSASS as a protected process, and Defendpoint is configured to only accept signed configuration (CERT_MODE=2).
- **54497** – Fixed an issue to ensure configuration signing is correctly enforced.
- **54525** – Fixed a bug which caused fast running processes to crash sporadically.
- **55197** – Fixed a bug that caused authentication prompts to be shown regularly whilst in sandboxed applications, in environments with an authenticated internet proxy.

4.10 - 4.3.118 Release

4.10.1 - Bug Fixes

- **45105** – Resolved performance problem with Flash content in sandbox instances of IE.
- **47336** – Fixed the Application Group generated for Privilege Monitoring Exclusions so that Privilege Monitoring events are raised appropriately.
- **48533** – Resolved performance problem navigating folders in explorer when Egnyte Drive is installed.
- **36187** – Resolved issues rendering Defendpoint messages when the <alt> key is pressed.
- **47306**, **27017**, **20672**, **43616**, **50074** – Fixed sporadic application fault during process exit.
- **44357** – Resolved 4kb memory leak for applications launched using On-Demand.
- **38279**, **34365** – Resolved occasional problems loading videos in YouTube, Netflix and Amazon Prime in a sandbox instance of IE.
- **35108** – Resolved sporadic failure to launch IE on initial sandbox navigation.
- **36730** – Display the configured message when incorrect Authorizing User credentials are provided.
- **13178** – Can now control the Defendpoint service when there is a passive application rule for any service.
- **30283** – Resolved incompatibility between the ManageSystemProcess engineering key and COM application rules.
- **35638** – Prevent the Defendpoint Task Manager from stopping the Defendpoint service when elevated using Defendpoint.
- **47685** – Resolved application fault in VMWare Remote Console Plug-in 5.1.
- **31154**, **50243**, **19727** – Prevent Defendpoint elevated processes from taking ownership of Defendpoint files and registry keys.
- **49363** – Fixed problem resulting in the reclassify sandbox content context menu occasionally being greyed out.
- **49672** – Resolved occasional issue with installation of the Defendpoint Chrome extension.
- **30123** – Host Information events now report Windows 10 correctly.
- **41217** – Fixed use of mailto links from sandbox Chrome instance.
- **50278**, **51422** – Fixed rare application error in taskhostw.exe when changing user.
- **39221** – Do not show the LastPass extension welcome screen when a new sandbox Chrome instance is launched.
- **41091** – Trusteer Rapport extension is now available in sandbox Chrome instances.
- **45219** – Do not close chrome:// URLs when navigating to different sandbox contexts.
- **18226** – An administrator or logged on user can now end sandbox processes from cmd.exe.
- **12632** – Do not show the On-Demand context menu for non-application file types.
- **40602** – Resolved performance issue browsing network shares with Content Control rules enabled.

- **17164** – Resolved performance issue when extracting zip files with Content Control rules enabled.
- **15785** – Chrome slow to launch with specific application matching rules.
- **41229** – The PGDriver is now signed by Microsoft.
- **45885** – The PGDriver is now anti-tamper protected.
- **34267**, **42701**, **34623** – Service events are now shown correctly in iC3 reports.
- **35113**, **42144** – Sandbox URL events are now shown correctly in iC3 reports.
- **35152**, **42698** – User Logon events are now shown correctly in iC3 reports.
- **36409** – Improved Chrome visibility on navigation to a sandbox instance.
- **45248** – Do not launch new instance of explorer when a Google account is disconnected from a sandbox Chrome instance.
- **38208** – Fix sporadic “Server Error” when downloading a PDF from sandbox Chrome instance.
- **34138** – Do not allow initial loading of websites in prior to creating a sandbox Chrome instance.
- **42105**, **48586** – Fix “Chrome didn’t shut down correctly” message on initial launch of sandbox Chrome instance.

4.11 - 4.3.78 Release

- **49230** – Resolved a compatibility issue in Windows 10 Anniversary Update when running HookLoadMethod=0.

4.12 - 4.3.58 Release

- **47686** – Fixed an incompatibility with Microsoft App-V 5.0 that caused an exception in Windows Explorer.
- **46758** – Fixed a bug that caused source URL verification and auditing to fail when an application was opened from a UNC path.

4.13 - 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.

4.14 - 4.1.279 Release

Bug Fixes

- **49230** – Resolved a compatibility issue in Windows 10 Anniversary Update when running HookLoadMethod=0.

4.15 - 4.1.273 Release

- **32299** – Resolved a compatibility issue in Windows 8.1 and Windows 10 when running LSASS as a protected process.

4.16 - 4.1.271 Release

Bug Fixes

- **46718** – Fixed a bug which caused fast running processes to crash sporadically.

4.17 - 4.1.262 Release

Bug Fixes

- **44986** – Resolved a compatibility issue with Windows 10 “Redstone” anniversary edition, which caused the Edge browser to crash on startup.
- **45809** – Implemented a new version of Microsoft Detours, which resolves an ASLR security issue when hooking APIs.

4.18 - 4.1.255 Release

Enhancements

- Webserver configuration deployment now supports client certificate authentication, so that only authenticated endpoints can download a webserver hosted configuration. Refer to the section “Webserver Management” in the Defendpoint Administration Guide for details.

Bug Fixes

- **25126** – Resolved an incompatibility with VirtualBox version 4.3.20, which caused virtual machines to crash on startup.
- **31791** – Resolved an incompatibility with Kaspersky Enterprise Endpoint Security which caused 32bit application launches to fail on 64bit endpoints.

4.19 - 4.1.234 Release

Enhancements

- Specific applications can now be excluded from the “Prohibit privilege account management” general rule. For more information, refer to the Prohibit Privilege Account Management section in the Defendpoint Administration Guide.
- Provide the ability to choose whether to use Designated User Authorization or Challenge/Response on the same custom message.
- **25784** – Add support for Microsoft Outlook 2007 for the sandboxing of Outlook Email Attachments.
- **23445** – Minor performance improvements.

Bug Fixes

- **31368** - Resolved a compatibility issue with Windows Credential Guard, which caused excessive CPU usage.
- **34047** – Fixed sporadic problem that resulted in license errors being logged in the event log when a full Suite license is present.
- **33802** – Source URL matching criteria now works for files downloaded to CIFS file shares.

- **32519** – Fixed occasional memory leak for short lived processes.
- **12830**, **18158**, **19024**, **29671** – Windows upgrades are now supported.
- **23384** – The Programs and Features utility now shows the correct options for custom applications.
- **26050**, **38497** – Favourites that are redirected to a network share are now available within a sandbox.
- **20856** – Allow elevation of Chrome Update COM class.
- **35831** – Unlicensed events for IC3 are no longer generated when not installed in this mode.
- **32082**, **34670** – Fixed spelling errors in EULA.
- **32870**, **33064** – Fixed Source URL matching criteria within a Sandbox.
- **33114** – Fixed application error in task manager when setting “always on top”.
- **39639** – Fixed a bug that caused Intel McAfee ePO user policy updates to fail when deployed to endpoints with McAfee Agent version 5.0.3.
- **38102** – Support for Windows 10 LTSB with Cumulative update KB3147461.

If you are planning to deploy Defendpoint on Windows 10 LTSB Threshold 1, please refer to Avecto KB Article 1552 in connect.avecto.com.

4.20 - 4.1.149 Release

New Features

- Sandboxing of Outlook Email Attachments.

Enhancements

- Optimized the sandbox cleanup process.
- **29391** – All Avecto and Defendpoint binaries are now dual-signed with SHA-1 and SHA-256 certificates.

Bug Fixes

- **25098** – Fixed a bug in the Defendpoint hook DLL which occasionally caused processes with PID’s greater than 6 digits to crash.
- **23336** – Fixed a compatibility issue in Content Control which sporadically caused directory lookups to fail.
- **9823**, **23216** – Fixed a bug which caused private PDF files to fail to open if a public (sandboxed) PDF was already open.
- **286**, **1440** – The ‘Run Maximized’ and ‘Working Directory’ options on application shortcuts are now honoured when running applications On-Demand.
- **10101**, **10618** - Optimized the generation of SHA-1 hashes, to improve performance when downloading, copying, editing or opening large (>1GB) files.
- **10695**,**10844** - Fixed a bug which caused file classification to fail when saving files to UNC mapped paths.
- **6719** – Fixed a bug which caused batch files with commandline arguments to fail a SHA-1 matching rule.
- **6901**, **20449** – Fixed a compatibility issue with 3rd party products that use Shell Menu items (E.G., WinRAR, Tortoise CVS), which occasionally caused to the On-Demand shell menu option to fail to display, only partially display, or result in 3rd party shell menu items to be removed.
- **19079** – Fixed a bug where printing a public (sandboxed) PDF in Adobe Reader would fail, if no documents had ever been printed natively.
- **7815** – Fixed an issue where computers were failing to join or leave an Active Directory domain, when the ‘Prohibit Privileged Account Management’ general rule was enabled.
- **14947** - Fixed a bug where the on-demand shell menu option was being displayed twice, when the ‘Hide Run As Administrator…’ option is disabled.

- **24127** – Fixed a bug which caused on-demand elevations to fail with a “System cannot file the path specified” error, when no message was configured for the on-demand rule.
- **8742** - Fixed a bug where Internet Explorer browser extensions were not being automatically enabled in the sandbox, causing users to be prompted to re-enable them.
- **22006** – Fixed a bug which caused the Windows 10 application store to fail to open.
- **18164**, **23548** – Adobe Reader DC no longer displays the ‘Welcome’ splash screen when first launching in a fresh sandbox, and now honors any previously dismissed start-up prompts.
- **21140** – PGProgramsUtil now respects the “NoRemove” and “NoRepair” registry values for installed applications, and prevents these applications from being uninstalled or repaired.
- **21209** – The “AutoConfigURL” registry setting for Internet Explorer is now applied to sandboxes.
- **22815** – Fixed a sporadic crash when using MSBuild in an elevated Microsoft Visual Studio instance.
- **26930** – Fixed a bug which sometimes caused Microsoft Office applications to crash when trying to open public (sandboxed) documents from Forwarded mapped network drives on remote desktop sessions.
- **10967** – Fixed a bug where MSI’s with long file paths/command lines would fail to match.
- **30683** – Fixed incompatibility with Windows 10 Account Control
- **32950** – Fixed a bug that sometimes prevented sandboxed documents being saved via the Desktop Quick Link on Windows 10

4.21 - 4.0.387.0 SR5 Release

Enhancements

- Added support for applications that specify the UIAccess flag in an external manifest file. This behaviour is enabled using a Defendpoint engineering setting via the Registry:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Avecto\Privilege Guard Client\
  - DWORD “ReadManifestMode” = 1 ; Attempts to read external manifest if embedded manifest is not present. When set to 0, will only check for embedded manifest.
  - This engineering setting can be implemented via the Defendpoint configuration as an Advanced Agent Setting. For more information, please contact Avecto Support.
- Added SHA-1/SHA-256 dual signed certificate for Defendpoint binaries and installation packages.

4.22 - 4.0.375.0 SR4 Release

Bug Fixes

- Fixed a bug in PGProgramsUtil where the ‘Repair’ option was not always displayed.
- Fixed a bug in PGProgramsUtil where multiple installations of the same application were only displayed once.

4.23 - 4.0.369.0 SR3 Release

Bug Fixes

- Fixed an incompatibility when building solutions in Microsoft Visual Studio.

4.24 - 4.0.349.0 SR2 Release

Enhancements

- Added support for Windows 10
- Implemented secure sandbox printing mechanism. Refer to the Defendpoint Administration Guide for details.
- Improved content blocking experience:
    - Defendpoint messaging now more consistent
    - Removed erroneous Windows error messages
- Improved Internet Explorer launch when homepage has been sandboxed
- Resolved memory leak when running a large number of processes
- Improved initial rendering time for sandboxed Internet Explorer
- Resolved problems starting Java applications with a large Java Memory Pool
- Passive application rules no longer require an Application Control license
- Fixed problem with child matching logic when using the parent process matching criteria
- Fixed duplicated on-demand options on context menu for shortcuts
- Resolved issues installing Autocad App Manager updates
- Resolved delays the first time Internet Explorer is sandboxed, following a machine reboot
- UiAccess applications no longer incorrectly match UAC rules
- No longer proceed when “No” is selected on custom messages for Content Rules
- Resolved memory and process handle leaks in the Defendpoint Service
- Resolved focus issues when navigating in between sandboxed Internet Explorer instances
- Correctly close tabs when navigating to a sandboxed URL
- Enabled Internet Explorer extensions within a sandbox
- Resolved intermittent issues accessing network locations with passive content rules
- Resolved issues passing command line options in shortcuts for on-demand elevation
- Resolved problems running applications that require elevation from the command prompt
- Improved creation of local accounts for sandboxing to stop large numbers of accounts being created
- Fixed problems matching MSI installers using a location-based whitelisting policy
- Resolved problems accessing sandboxed documents on the network from within a sandbox on Windows XP
- Restricted scope of content rules to machines where the feature is in use
- Resolved Windows Security Event Log errors for PGHook.

4.25 - 4.0.247 SR1 Release

- Resolved exceptions in AddInUtil.exe on Windows 8 with Office 2013 32-bit and .NET 3.5, when Windows Updates are applied.
- Resolved incompatibility with McAfee HIPS shown on Windows 7 during machine shutdown.
- Resolved licensing errors in Office 2013 on Windows 8 when using VLK/KMS licensing.
- Resolved issues opening classified content via a shortcut.
- Performance improvements to the Defendpoint service.
- Fixed intermittent failure to stop password change with Prohibit Account Management general rule enabled.
- Fixed errors when modifying the “Log on as” property of a service.
- Resolved application timeouts when the WMI provider stops when using WMI filters.

- Resolved “Configuration error” message when launching a PDF in sandboxed Adobe Acrobat XI Professional.
- Fixed a security issue when using custom messaging
- Fixed event compatibility with McAfee ePO.
- When there are a large number of existing IE tabs, ensure a new window is not opened as well as a new tab.
- Resolved sandboxing compatibility issues with Excel 2010 and certain types of spreadsheet.
- Resolved application matching failures for PS1 files when using a 32 bit version of PowerShell on a 64 bit system.
- Fixed problem encountered when “Force standard rights on File Open/Save common dialogs” option is enabled for notepad.
- Audit events are now generated for content control rules using a custom token.
- Fixed publisher matching on mapped network drives.
- Fixed problem with Cygwin (mintty) failing to launch.

4.26 - 4.0.191.0 Release

New Features

- New Module – Sandboxing
- Defendpoint sandbxing 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 – 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

- Added support for %APPDATA%, %LOCALAPPDATA%, %PROGRAMDATA%, %ALLUSERSPROFILE% environment variables
- Optimized License event auditing so that ‘No License’ events are only issued once.
- Added several built-in application groups for common application types.
- 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 arguments to the Defendpoint Client installer to allow override of the default Hook method.
- Added new ‘Avecto Task Manager’ utility to Defendpoint Client that provides contextual information on running processes managed by Defendpoint.
- Implemented several improvements to the PGCaptureConfig utility.
    - Now uses SFTP for secure transfer of system information.

Bug Fixes

- Resolved occasional unhandled exception observed when installing a specific ActiveX control
- Resolved COM Class elevation errors for power users and administrators.
- Resolved system hang during reboot after installation/upgrade caused by PGDriver.sys.
- Resolved issue elevating Flash Player 12 installer.
- Resolved various DPI issues in message prompt.
- Anti-tamper is now disabled on domain controllers.
- Resolved incompatibility with Cygwin