Avecto

Release Notes

Defendpoint Windows Client 4.3.136.0 SR5

3 January 2017

Avecto

Chapter 2 - Windows Client 4.3.136.0 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.

2.1 - Release Notes 4.3.136.0

2.1.1 - 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.

2.2 - Supported ePO Extension Versions

This Defendpoint client is compatible with the following combination of ePO extensions and Enterprise Reporting databases:

- ePO extension 4.1.205.0 and Enterprise Reporting database 4.1.160
- ePO extension 4.1.8544.0 SR1 and Enterprise Reporting database 4.1.160

- ePO extension 4.3.11275.0 and Enterprise Reporting database 4.1.160 and higher

2.3 - Supported Operating Systems

- **privilege management / application control Support** detailed below
- **sandboxing** detailed below

2.3.1 - privilege management / application control Support

Platforms

- Windows XP SP3+
- Windows Vista
- Windows 7 SP1+
- Windows 8 / 8.1
- Windows 10
- Windows Server 2003
- Windows Server 2008 / R2
- Windows Server 2012 / R2
- Windows Server 2016

2.3.2 - sandboxing

Platforms

- Windows XP SP3 x86
- Windows Vista[1]
- Windows 7 SP1+
- Windows 8 / 8.1
- Windows 10
- Windows Server 2003 (32bit)

[1]The new Printing from a Sandbox feature is not supported on these platforms.

- Windows Server 2008 / R2[1]
- Windows Server 2012 / R2
- Windows Server 2016

Primary Application Support

- Internet Explorer 8+
- 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: Note: If you are upgrading from Defendpoint 4.0 to 4.1 you may need to update your workstyles to incorporate newly supported features/applications.

2.4 - Prerequisites

- **Defendpoint Client** detailed below
- **Defendpoint Management Console** detailed on the next page
- **Defendpoint Activity Viewer** detailed on the next page

2.4.1 - 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)

[1]The new Printing from a Sandbox feature is not supported on these platforms.

2.4.2 - Defendpoint Management Console

- Microsoft Core XML Services 6.0 (XP SP3 only)
- Microsoft Visual C++ 2013 Redistributable
- Microsoft Group Policy Management Console (for Active Directory integration)

2.4.3 - Defendpoint Activity Viewer

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

Notes

Note: The executable version of the installation package includes all necessary prerequisites (excluding the Group Policy Management Console), and will automatically install them as necessary.

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

Note: The Defendpoint Client executable installer will automatically install 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, it is recommended that you install the Defendpoint Client MSI installation.

Note: Microsoft SQL Server 2008 R2 Native Client is required for connectivity with Enterprise Reporting.

Chapter 3 - Version History

3.1 - 4.3.131 Release

3.1.1 - 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.

3.2 - 4.3.118 Release

3.2.1 - 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.
- **29450** – Link to the correct Help page within content and URL dialogs.
- **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.
- **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.
- **35108** – Resolved sporadic failure to launch IE on initial sandbox navigation.
- **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.
- **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.
- **5196** – Renamed application wizard headers to be appropriate to the application type.
- **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.
- **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.
- **21073** – Only write the ShellExtension element to configuration once.
- **8166**, **8168** – Fixed the Run Script context menu in the Defendpoint Management Console.
- **3152** – Added support for Cut/Copy/Paste for workstyle filters.
- **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.

3.3 - 4.3.78 Release

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

3.4 - 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.

3.5 - 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.

3.6 - 4.1.279 Release

Bug Fixes

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

3.7 - 4.1.273 Release

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

3.8 - 4.1.271 Release

Bug Fixes

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

3.9 - 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.

3.10 - 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.

3.11 - 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.

- **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.
- **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.

3.12 - 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

- Optimized the sandbox cleanup process.
- **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

- **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.
- **14127** - Fixed a bug in the Event Import Wizard, where COM Classes were being added as Executable types.
- **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.
- **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.
- **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.
- **21098** – Fix a bug in the MMC where using the ‘Move to top’ on a URL rule caused the rule to be deleted.
- **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.
- **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.
- **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

3.13 - 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.

3.14 - 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.

3.15 - 4.0.369.0 SR3 Release

Bug Fixes

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

3.16 - 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
- Create the correct type of message when using the Create Workstyle wizard to create a blacklisting configuration
- 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
- Corrected the File Archivers entry in the Sandbox Content Handlers generated group
- 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.

3.17 - 4.0.247 SR1 Release

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

3.18 - 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 - 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.
- Optimized License event auditing so that ‘No License’ events are only issued once.
- 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.
- 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