

Privilege Management for Windows 5.4 SR3 Release Notes

October 4, 2019

New Features and Enhancements:


- The software has been rebranded with the new company logo and colors, and some products have been renamed.
- Privilege Management for Windows has improved compatibility with other BeyondTrust software offerings.
- Privilege Management for Windows integrates with BeyondInsight.
 - Apply all changes to machine policy which can be received from BeyondInsight, including lists of policies to be applied or deleted.
 - Retrieve and display the list of BeyondInsight policies which the user or asset can edit.
 - Apply changes to the last machine policy in any lists received from BeyondInsight, including policies to be applied or deleted.
 - Raise an Application Launched with No Change event into BeyondInsight, which represents the launch of an application where the privileges were not modified.
 - Send heartbeat events to BeyondInsight to mark new and existing assets for management.
 - Create a new policy in BeyondInsight for the Privilege Management for Windows client.
 - Push a valid policy from BeyondInsight into the Privilege Management for Windows client.
 - Using the Advanced Agent Settings feature in Privilege Management for Windows, BeyondInsight settings can be pushed down to the endpoint.
 - Configure the settings required to communicate with BeyondInsight using command line arguments and a page in the installer.
 - Configure events to be forwarded to BeyondInsight as an audit destination.
 - Policies assigned to users in BeyondInsight can be applied to Privilege Management for Windows.
 - Create matching criteria from events which have been raised to BeyondInsight.
- When logging into the client, a user is prompted for their username and password only once per session. The data is stored securely within the session state so that it can be reused for every policy management message.
- Raise an Application Launch Denied message using data mapped from the Privilege Management for Windows block message.
- Raise an Application Launched with Modified Privileges event using data mapped from an Add Admin, Drop Admin, or Custom Token application event.
- Raise an Application Launched with Shell Rule event using data mapped from an application event:
 - Add Admin Rights - Shell
 - Drop Admin Rights - Shell
 - Passive - Shell - No Change
 - User Defaults - Shell
 - Custom Token - Shell
- QuickStart has been updated.
- Create application definitions which allow the location of installation or deletion to be undefined.

Issues Resolved:

- Resolved an issue where the client could be uninstalled using an elevated PowerShell, bypassing anti-tamper.
- Resolved an issue with processes invisible to Task Manager were being created but never closed.
- Corrected an issue with the Mac Quick Start Policy containing ampersands within messages.
- Resolved an issue with "Check Min Version" and "Check Max Version" showing an error even when configured correctly when checking Mac application types.
- Resolved an issue with the QuickStart Policy not forwarding events to iC3 automatically.
- Resolved an issue with the On Demand Rule matching the App Rule intermittently.
- Resolved an issue with the client not handling Cyrillic text in some menus.
- Corrected an issue with Mac console message templates containing Windows-specific reasons.
- Resolved an issue with a process handle not being closed when intercepting apps that require UAC.
- Resolved an issue where the Policy Validation message would fail due to an incorrect install identifier.
- Resolved an issue with a code integrity being flagged on the PGHook.DLL.
- Resolved an issue with Microsoft Word displaying an error on startup when Code Integrity Guide was enabled.
- Resolved an issue with a policy being lost if group policy update failed.
- Resolved an issue where Windows Updates would fail to install when Privilege Management for Windows and VMWare Horizon were installed.
- Resolved an issue with the ManageSystemProcesses registry key no longer working.
- Resolved an issue where upgrading an environment with more than one policy would result in only one policy being applied to an endpoint. This issue applied only to the GPO delivery method.
- Updated the EULA.
- Improved validation and error handling around applications launched via context menu.
- Resolved an issue with accessing UNC pipe network shares, which were matching content control rules unexpectedly.
- Made performance improvements to reduce the number of required UAC checks performed when starting processes.
- Resolved an issue where system crashes were possible in a race condition during installation and/or upgrade of the client.
- Resolved a compatibility issue with Windows Additional LSA Protection.

Requirements:

- Microsoft .NET Framework 4.0 (required to use Activity Viewer, 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 (required on the endpoint that will run the Activity Viewer console)
- McAfee Agent (required if you are installing the Privilege Management client with switch EPOMODE=1)

 **Note:** The executable version of the client package includes all necessary prerequisites (excluding .NET Framework 4.0) and automatically installs them as necessary. If you use the MSI or ZIP package, you must manually install any necessary prerequisites.

Compatibility:

- Privilege Management Console 4.5 or later
- Privilege Management ePO Extension 5.4 (recommended), 5.0+
- Privilege Management Console Adapter 2.1 and 1.4

- McAfee Agent 5.6 (recommended), 5.0+
- McAfee ePO Server 5.10 (recommended), 5.9
- McAfee Endpoint Security (ENS)
 - 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



Note: *If the version of McAfee MOVE is compatible with the McAfee Agent you are using, then Privilege Management is also compatible. The following McAfee supported versions of the MOVE Multi-Platform Client are compatible with this version of the Privilege Management client. The agentless version of McAfee MOVE is not supported.*

- 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

Supported Operating Systems:

- Privilege Management/Application Control Support
 - Windows 7
 - Windows 8 and 8.1
 - Windows 10 builds Enterprise 2015 LTSC, Enterprise 2016 LTSC, 1607, 1703, 1709, 1803, 1809, 1903, 1909
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016
 - Windows Server 2019
- 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)