Privilege Management for Windows 21.6 Release Notes

November 4, 2021

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.*

New Features and Enhancements:

- **Client**
  - An additional Multifactor Authentication protocol, RADIUS, is now supported by Privilege Management for Windows. This can be used as a means of user authentication on messages to allow the user to perform a requested action and can be used in combination with other existing authentication and authorization methods.
  - Password Safe Cloud customers can now use the Account Rotation and Run As Password Safe User features with any of the supported BeyondTrust policy management platforms (e.g., Privilege Management Cloud).
  - New IDs are added to events that enable them to be uniquely identified and related to the specific configuration that generated them when that information is present in the configuration file.
  - Added support for Microsoft Windows 11 operating system.
- **Privilege Management Policy Editor:**
  - Added additional security capabilities to the TAP policy that enable increased protection from *living off the land binaries* (LOLBINS). To take advantage of this you must import/re-import the TAP policy once you have updated your Policy editor to version 21.6.
  - An additional Multifactor Authentication protocol, RADIUS, is now supported by Privilege Management for Windows. This can be used as a means of user authentication on messages to allow the user to perform a requested action and can be used in combination with other existing authentication and authorization methods.
  - Password Safe Cloud customers can now use the Account Rotation and Run As Password Safe User features with any of the supported BeyondTrust policy management platforms (e.g., Privilege Management Cloud).

Issues Resolved:

- Resolved issue in which GUIDs where being shown in Windows events when using PM for Windows to uninstall the McAfee Agent (v5.6.x) from **AppWiz.cpl**.
- Resolved issue in which invalid message array size crashed service.

- Resolved issue in which nothing happened when answering **Yes** to a message.
- Resolved issue in which an additional Event Log entry is entered when the DefendpointService starts when none is expected.
- Resolved issue in which IdP GlobalOptionsSet was retrieved from config instead of policy.
- Resolved UAC prompt issue with Visual Studio 2017 and 2019.
- Resolved issue in which a UAC message displayed when launching apps from the **On-Demand** menu when Quickstart Workstyles were applied.
- Resolved issue in which a UAC message displayed when clicking on **Rename** within **Settings** when Quickstart Workstyles were applied.
- Resolved issue in which Windows Subsystem for Linux (WSL) was aborting commands with the Content Rule in place.
- Resolved issue in which a PM rule was not completing a installation with a custom script.
- Resolved issue in which an invalid XML message array size crashed service.

Compatibility:

- Privilege Management Policy Editor **21.6 (recommended)**, 5.2+
- Privilege Management ePO Extension **21.1 (recommended)**, 5.2+
- Privilege Management Console Windows Adapter **21.7 (recommended)**, 21.1
- BeyondInsight/Password Safe **21.2 (recommended)**, 7.2
- McAfee Agent **5.7 (recommended)**, 5.6+
- McAfee ePO Server **5.10 (recommended)**, 5.9

Supported Operating Systems:

- Windows 11
  - 21H2
- Windows 10
  - 21H1
  - 20H2
  - 2004
  - 1909
  - 1809
  - LTSB 2015
  - LTSB 2016
  - LTSC 2019
- Windows 8 / 8.1
- Windows 7
- Server
  - 2019
  - 2016
  - 2012R2

- 2012

For more information about compatibility, please see Privilege Management for Windows and Mac: Supported Versions and Operating System Compatibility at https://beyondtrustcorp.service-now.com/csm?id=kb_article_view&sysparm_article=KB0017101.

Notes:

- Privilege Management for Windows 21.6 supports upgrades from Privilege Management for Windows 5.2+.

IMPORTANT!

*Starting with Windows 8 and the introduction of Secure Boot, **AppInit** has been disabled in scenarios where Secure Boot is in use. Since that time, Secure Boot has become standard and best practice for our customers and thus AppInit has increasingly become irrelevant. Further, due to some recent code signing changes implemented by Microsoft, EPMfW cannot continue to support this method of injection. For these reasons, AppInit injection will stop working on Microsoft Server Operating Systems as of EPMfW 21.6, with the injection method being removed entirely in a future release across ALL supported Microsoft Operating Systems. Please see KB0016341 for information regarding if you are affected by this.*

IMPORTANT!

An update to our code signing certificate used from version 21.6 has introduced a dependency on the DigiCert Trusted Root G4 certificate. This certificate will be present on all operating systems back to Windows 7, provided automatic updating of root certificates is enabled (the default). If your organization manages trusted root certificates manually, you may need to install this trusted root certificate.