

Privilege Management for Windows 5.5 Release Notes

November 5, 2019

New Features and Enhancements:

- Common Dialog Launch Protection:
 - Now applies standard user rights to processes launched from within the dialog as well as to content accessed from within it.
 - Extended the range of dialogs covered by the **Force Standard User Rights on File Open/Save common dialogs** checkbox in Application Definitions.
- Updated Authenticode Certificate to sign software as the publisher **BeyondTrust Corporation**, and to no longer dual sign with SHA11 and SHA256 algorithms, but with SHA256 only.

Policy Editor

- New **Script** Application Type under the Mac policy node allows targeting the execution of scripts to aid end users to develop and install their own applications.
- The Mac QuickStart policy includes rules to allow install to and delete from **/Applications**.
- Improved publisher matching in the QuickStart policy by always matching the exact publisher name.
- The QuickStart policy will now also elevate the **Bomgar Support Customer Client** by its new name, **Remote Support Customer Client**.
- TAP Policy has been updated to include additional common attack vectors.
- Updated Authenticode Certificate to sign software as the publisher **BeyondTrust Corporation**, and to no longer dual sign with SHA11 and SHA256 algorithms, but with SHA256 only.

Issues Resolved:

- Resolved a compatibility issue in which Windows Explorer would fail to launch on some systems with Veriato installed.
- Resolved an issue in which Windows OS upgrades could cause Resultant Set of Policy (RSOP) errors with GPUupdate referencing our Group Policy Extension.
- Corrected an issue in which a restart was required to get new policy changes after upgrading McAfee Agent.
- Resolved an issue in which a poorly configured PGDriver service key could cause persistent BSODs on shutdown.

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)
 - Must be installed after the .NET Framework
- 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 Policy Editor 4.5 or later
- Privilege Management ePO Extension 5.4 (recommended), 5.0+
- Privilege Management Console Adapter 2.1 or later
- 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