



Privilege Management for Windows & Mac 21.6

New and Updated Features – November 4, 2021

BeyondTrust Privilege Management for Windows & Mac pairs powerful least privilege management and pragmatic application control capabilities, delivering fast, unmatched preventative endpoint security. Grant the right privilege to the right application – not user – only when needed and create a single audit trail. Prebuilt policy templates stop attacks involving trusted apps, addressing bad scripts and infected email attachments immediately. Application control, allow lists, and exception handling granular control over what users can install or run, and what applications can execute. Operationalize quickly with our QuickStart feature and simplified deployment models, for fast time-to-value and streamlined compliance.

This release provides improved templates for Trusted Application Protection, Windows 10 support, plus more usability enhancements.

Please see the [release notes](#) for additional details on these important enhancements.

New Feature Highlights – Privilege Management for Windows & Mac (PMWM)

Improved Templates for Trusted Application Control

Trusted Application Protection (TAP) helps organizations defend their users from the threat of malware and ransomware attacks by locking down email attachments, blocking malicious activity, and securing business applications like Microsoft Office, Adobe Reader, and other applications typically exploited by threat actors.

In Privilege Management for Windows 21.6, we have increased the coverage of TAP by introducing new rules that provide further mitigation against the use of "Living off the Land" binaries (or LOLBins) commonly used as part of a cyberattack on end users.

LOLBins are applications natively installed with Windows and are an easy way for threat actors to bypass other security controls like Antivirus (AV) and EDR. Attackers leverage LOLBins to exploit and compromise endpoints without having to run custom code that can be detected.

These new rules mitigate the following:

- Use of native compilers to build, obfuscate, and execute malicious code
- Use of native tools to download scripts and payloads
- Execution of code and common application control bypasses, for example, the use of a tool to execute a DLL
- Known malware execution techniques, such as WMI, COM, and chaining Explorer launches
- Misuse of Alternate Data Streams to hide executables

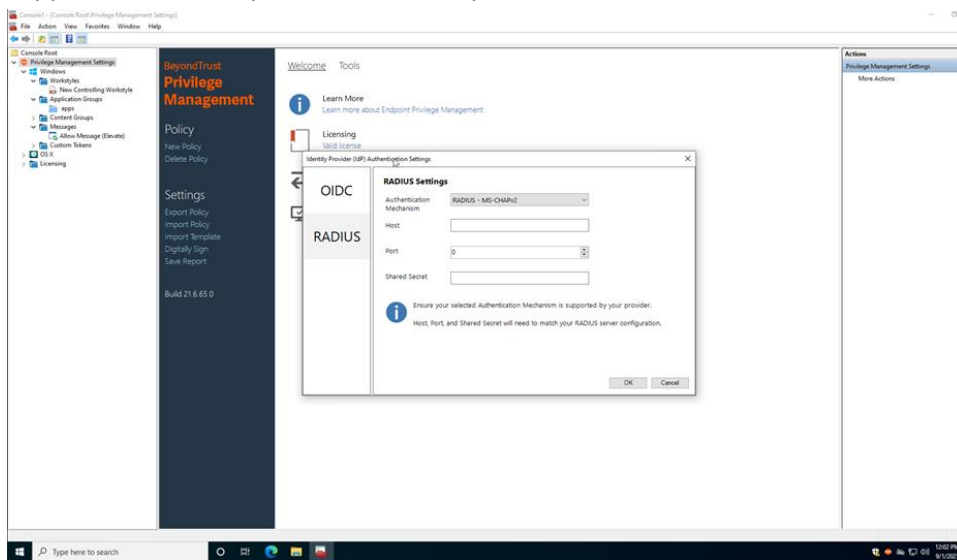
The new TAP rules are designed to block many LOLBins from being executed by trusted applications. This reduces the attack surface by further limiting an attacker's ability to execute code or execute remote commands through the exploitation of malicious websites and malicious email attachments.

Windows 11 Support

Version 21.6 of Privilege Management for Windows ensures full feature support on Windows 11. We recommend taking this version of Privilege Management for Windows before upgrading to Windows 11.

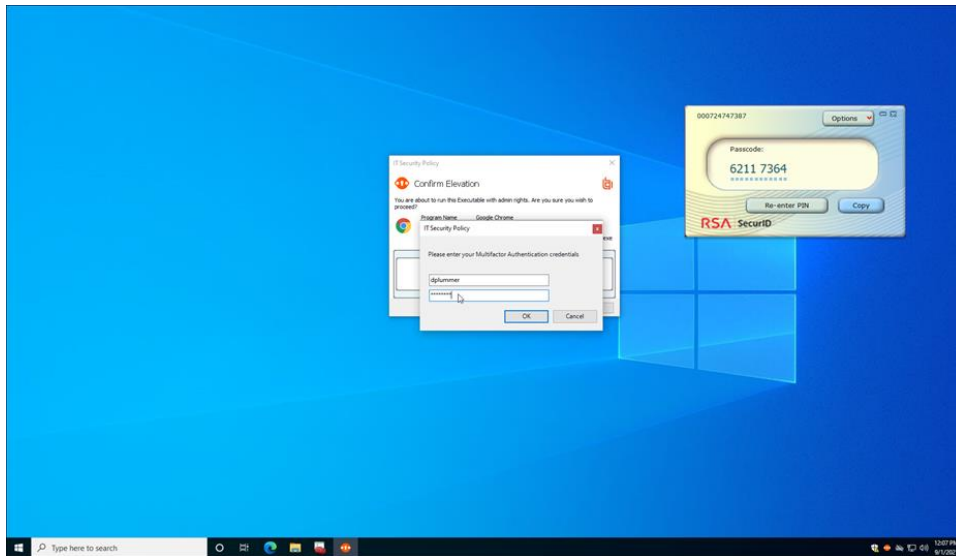
RADIUS Support

Privilege Management for Windows (PMW) 21.6 allows authentication via identity providers that support the RADIUS protocol, for example, RSA SecurID.



Setting Up RADIUS Connection

Adding another protocol (alongside the existing OIDC integration) extends the capability of PMW to integrate with your existing authentication infrastructure to ensure that the right people receive the right privileges.



A RADIUS (RSA SecurID) authentication step in PMW message, with a server-driven challenge

Password Safe Integration

Privilege Management for Windows and Mac (PMWM) 21.6+ integrates with PS Cloud 21.2+. The agents can rotate passwords for Password Safe Cloud managed accounts. PMW Run as Password Safe account rules can utilize PS Cloud managed accounts.

This functionality previously was available only to on-premises customers; now it is available on all PMWM management platforms, including our increasingly popular PM Cloud offering.

Other Enhancements

- Additional support for VirusTotal and McAfee GTI reputation services for Mac applications



About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network. Learn more at www.beyondtrust.com.