

# Privilege Management for Windows & Mac 21.3

## PM Cloud 21.4

New and Updated Features – May 27, 2021

BeyondTrust Privilege Management for Windows & Mac (PMWM) is a preventative endpoint security solution that removes excessive admin rights, applies modern application control, enables passwordless administration, and gives users just enough privileges to do their jobs and be productive. Available on-premises or SaaS, the solution blocks malware and ransomware and protects against both external and internal threats. Utilizing QuickStart policies, organizations receive rapid time-to-value.

This release introduces new multi-factor authentication options for end user messages, Reputation scoring of audited applications and processes in PM Cloud Analytics, improves user experience on the Cloud platform (v21.4) and provides further feature enhancements for both Cloud and on-premises versions.

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

### New Feature Highlights – Privilege Management for Windows & Mac (all deployment options)

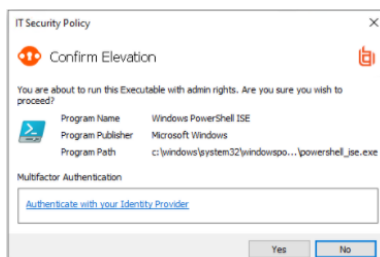
#### Multi-Factor Authentication Using Identity Providers

---

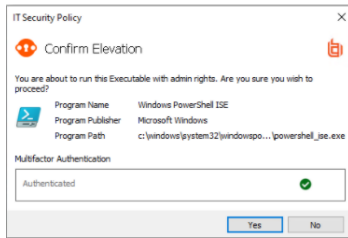
This feature for Windows and Mac introduces the ability to integrate End User Messages with any identity provider (IdP) that support OpenID Connect (OIDC). As a more secure, and more user-friendly alternative to using passwords, it brings the familiarity, simplicity, and flexibility usually associated with web-based identity products to Windows and Mac applications in organizations.

Adopting the widely used OIDC protocol means that customers can use their existing IdP infrastructure and use multi-factor authentication (MFA) for users operating in higher flex roles.

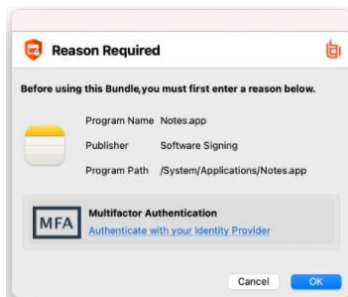
The feature is highly configurable and can be combined with other existing types of authentications offered by BeyondTrust, to ensure the usability users require to be productive is balanced with security. It is ideal as an added layer of security for privileged applications as well as sensitive and higher risk tasks, to ensure that the user is validated with an additional factor.



*Privilege Management for Windows – Message Requesting MFA*



*Privilege Management for Windows – Message Showing Successful Authentication*



*Privilege Management for Mac – Message Requesting MFA*



*Privilege Management for Mac – Message Showing Successful Authentication*

## Advanced Parent Tracking

---

Privilege Management for Windows now includes new enhancements to Trusted Application Protection and Application Control, called Advanced Parent Tracking, that tracks the use of COM and WMI as a method of creating child processes.

Increasingly used as a way of evading traditional App Control and EDR solutions, malware use surrogate processes like COM and WMI to spawn processes in a way that evades detection through Windows parent and child process hierarchies. With Advanced Parent Tracking, Privilege Management for Windows detects this form of process creation and ensures that parent/child relationships are tracked through TAP and App Control rules.

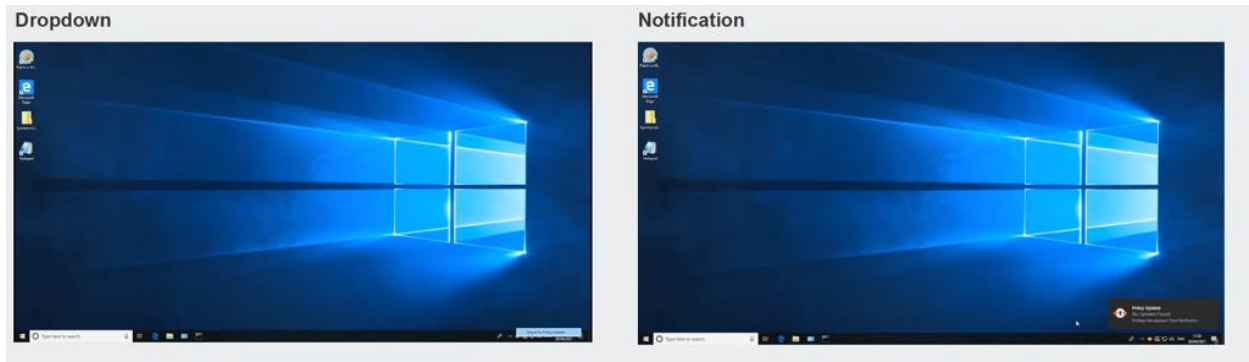
## Allow Users to Check for Policy Updates

---

When a policy change is required to cater to the needs of one of your end users, this new feature gives those users a quick and easy way to force an immediate check for new policies, rather than having to

wait for the next scheduled check. Found as a new option on the EPM systray icon, a single click is all that is required to ensure users are on the latest policy, vital for ongoing security and productivity.

The extra information provided to the service desk, including Client Version Number, Computer Name and Last Updated, provides valuable information for diagnosing and fixing an issue on the user's machine.



## New Feature Highlights – Privilege Management for Windows & Mac Cloud

### Reputation-Based Analytics

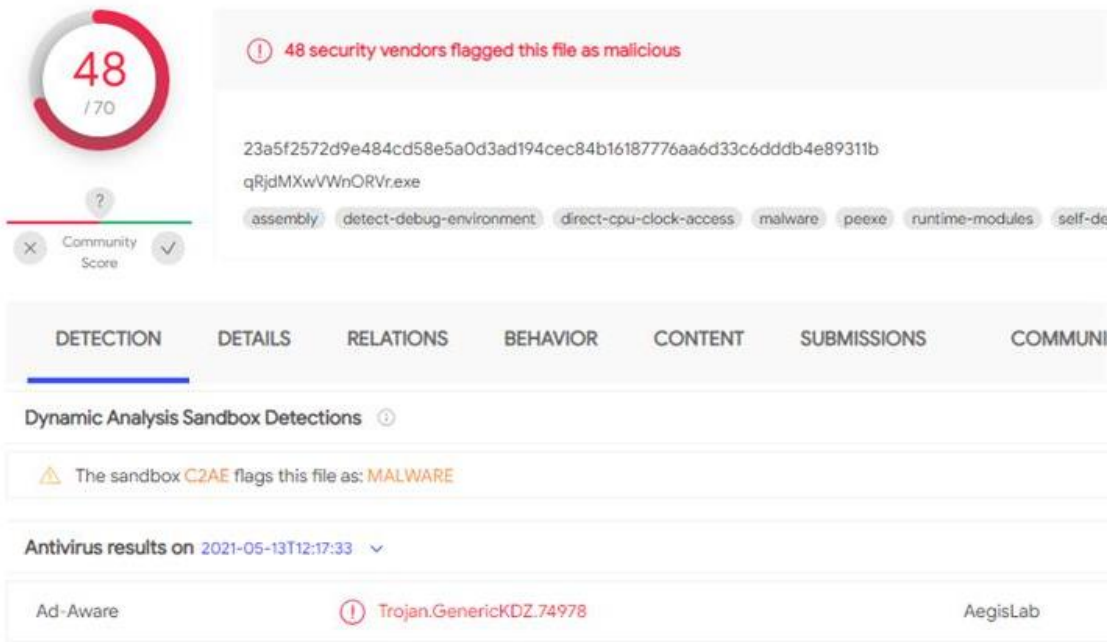
---

Whether you are reviewing the applications being installed and accessed by your users, handling exception requests, or performing security audits on your endpoint estate – reputation plays a vital role in establishing the risk associated with unknown apps and processes.

BeyondTrust Privilege Management for Windows and Mac Cloud 21.4 introduces reputation into Analytics and Reporting, providing a simple and convenient method of checking for, and validating the reputation of any application or process that has been audited on endpoints managed with PM Cloud.

Leveraging the powerful VirusTotal database, this feature removes the burden of having to run manual checks on apps. Using your own VirusTotal Premium subscription, scores are pulled directly into the EPM Analytics platform, and persisted alongside other application and environment metadata; providing an additional and valuable data point for faster and more secure decisions around whether to allow – or block – unknown apps, or exceptions that fall outside of your corporate policies.

The integration with VirusTotal brings new insights and information about application risk directly into PM Cloud analytics.



48 / 70

Community Score

48 security vendors flagged this file as malicious

23a5f2572d9e484cd58e5a0d3ad194cec84b16187776aa6d33c6dddb4e89311b  
qRjdMXwVWnORVr.exe

assembly detect-debug-environment direct-cpu-clock-access malware peexe runtime-modules self-de

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNI

Dynamic Analysis Sandbox Detections ⓘ

The sandbox C2AE flags this file as: MALWARE

Antivirus results on 2021-05-13T12:17:33 ▾

Ad-Aware	Trojan.GenericKDZ.74978	AegisLab
----------	-------------------------	----------

*View vendors that are flagged as malicious.*

'Cancel Lists the current running tasks' Windows Event Details

Application	Workstyle	Process	Session	Rule Script	COM	Windows Store
Description	Lists the current running tasks					
VirusTotal Reputation	1 / 66 engines detected this					
Publisher	Microsoft Windows					
Application Type	Executable					
File Name / Codebase	c:\windows\syswow64\tasklist.exe					
Command Line	tasklist /FI "PID eq 9604"					

*Cancel lists the current running tasks in Windows Event Details.*

## Web Policy Updates

To further improve user experience, several updates have been created, including:

- The ability to create and add/delete your own messaging, allowing further personalization for end users
- Updated Challenge/Response key configuration for easier setup and management
- Added applications via template, making it easier to add new rules to policies

## MESSAGES

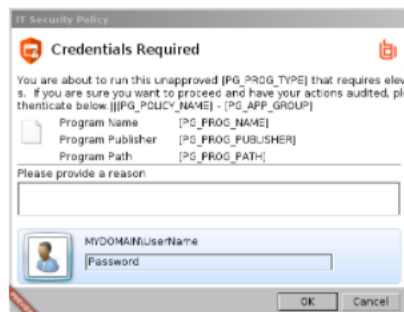
Filter by

The Challenge / Response Key must be set for Challenge / Response Messages to work. Select the 'Challenge / Response Keys' button to set this.

+ Create New Message

Challenge/Response Keys

### Allow Message (Authentication & Reason)



Confirmation before elevating privileges, with reason and re-authentication

- Allow Message
- Will be shown on secure desktop
- Challenge / Response: Not enabled
- User must authorize

Allow messaging for authentication and reason.

## APPLICATION TEMPLATES

Filter by

100 items			
<input type="checkbox"/>	Description	Type	File Name / Code Base
<input type="checkbox"/>	Microsoft - Windows Update	ActiveX Control	http://update.microsoft.com/
<input type="checkbox"/>	Microsoft - MSDN Download Manager	ActiveX Control	https://transfers.ds.microsoft.com/FTM/Trans...
<input type="checkbox"/>	Microsoft - Windows Genuine Advantage	ActiveX Control	http://go.microsoft.com/fwlink/?linkid=39204
<input type="checkbox"/>	Adobe - Flash Player (All Locations)	ActiveX Control	http://((platformdl.adobe\com)  (fpdownload\macromedia\com)  (download\macromedia\com)).*
<input type="checkbox"/>	Microsoft - Office Genuine Advantage	ActiveX Control	http://go.microsoft.com/fwlink/?linkid=58813
<input type="checkbox"/>	Cisco - WebEx	ActiveX Control	http://*.webex.com

Application templates.

## Export to CSV

It is important for administrators to be able to view, manage, and share data in a number of ways. Following the launch of the SIEM integration, we have added CSV export capabilities within the Privilege



Management Cloud console making export of all data for subsequent manipulation and sharing easier than ever across Computers, Groups, Policies, Users, and Audit Activity.



## 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](http://www.beyondtrust.com).