Privilege Management for Windows & Mac 22.3

Privilege Management Cloud 22.3

Release Date – May 5, 2022

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 provide 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.

Please see the release notes for additional details on these important enhancements.

New in Privilege Management for Windows

Enhancement: Remote Capture Config

In earlier versions of the Privilege Management for Windows solution, running diagnostic tools on an end-user machine meant that an admin had to be physically present at the machine or have the ability to remote in. This can be challenging to arrange/set up, it delays diagnostics and presents a disruption to the end-user.

In 22.3 we have introduced the ability to use the BeyondTrust Capture Config tool remotely from cmdline. This enables admins to remotely get details from machines without interrupting the end-user or having to be present at the user machine. This enhancement helps customers be more efficient with their troubleshooting efforts and minimize end-user loss of productivity.

Enhancement: Accessibility Improvement

The tasktray icon menu can now be accessed and interacted with entirely with keyboard shortcuts. This enhancement removes the need to use a mouse to interact with the tasktray, improving accessibility and compliance with Section 508 (Federal Electronic and Information Technology) of the Rehabilitation Act of 1973.

Enhancement: New Admin Token

Privilege Management for Windows enables customers to remove admin rights with a policy-based privilege elevation process. As part of this process, the solution assigns a token (usually the default elevation token) to the application being elevated so it can function as intended. This default token contains privileges which can be abused by an attacker. While we only apply this token to applications specified in the policy, still there are several security challenges that exist. To mitigate these challenges, 22.3 introduces a new “Add Basic Admin Rights” admin token. This token becomes the default Admin token as of 22.3.

This feature was built to mitigate the risks associated with an elevated process having the SeDegubPrivilege and SeLoadDriverPrivilege enabled. Prior to 22.3, this could be achieved using a custom token; however with 22.3, this is now a prebuilt and default option, increasing security and customer productivity.

New in Privilege Management Cloud

Enhancement: New Admin Token: Add Basic Admin Rights

Privilege Management for Windows enables customers to remove admin rights with a policy-based privilege elevation process. As part of this process, the solution assigns a token (usually the default elevation token) to the application being elevated so it can function as intended. This default token contains privileges which can be abused by an attacker. While we only apply this token to applications specified in the policy, still there are several security challenges that exist. To mitigate these challenges, 22.3 introduces a new “Add Basic Admin Rights” admin token. This token becomes the default Admin token as of 22.3.

This feature was built to mitigate the risks associated with an elevated process having the SeDegubPrivilege and SeLoadDriverPrivilege enabled. Prior to 22.3, this could be achieved using a custom token; however with 22.3, this is now a prebuilt and default option, increasing security and customer productivity.
In 22.3 users are now able to utilize a new token “Add Basic Admin Rights” to create application rules within their policy via Web Policy Editor (WPE). The previous add Admin token is now “Add Full Admin Rights”. When an event is triggered with a new token applied, it will be reportable to customers via ‘Analytics’ on the ‘Process Detail’ report within PM Cloud.

Enhancement: Privilege Management Reporting Update

The User, Host, and Privilege Account Management reports are now available within ‘Analytics’ in 22.3. In addition, Add to Policy has been added to the Process Detail report. These reports have been re-added to Privilege Management Cloud following work completed to migrate the reporting feature from Angular JS to Angular 3.

Enhancement: Increased Messaging Flexibility in Web Policy Editor

Users will now be able to add and edit designated users for Windows Messages, manage Audit Scripts and configure Advanced Agent Settings via the Web Policy Editor.

New: Ping Identity as an Open ID Connect (OIDC) Authentication Provider

In 22.3. BeyondTrust expanded support of OIDC authentication providers into the PM Cloud portal, to include Ping Identity.

Enhancements: Policy Flows

In 22.3, BeyondTrust has made enhancements to Policy Flows to improve ease of use of the solution. Some of these enhancements include:

- Clicking Policy Name now launches Web Policy Editor (WPE) instead of staying in PMC in a Policy Detail screen
- The Policy Detail section above Revisions and Drafts has been removed
- Policy Properties can now be viewed for a locked policy
- Revert & Discard Changes icon was changed

New in Privilege Management for MAC

Enhanced Product Security: Anti-Tamper Control for MAC

In 22.3, BeyondTrust has introduced new controls to further strengthen the security of the Privilege Management for Mac Solution. This anti-tamper control safeguards the PM for Mac agent from being exposed to savvy users who could seek to change it or disable it.
The introduction of this safety mechanism into the PM Mac agent automatically blocks any attempts to modify or disable any footprint of the agent or policies, without the need to have explicit blocking rules in place. This feature strengthens the security of the agent and the overall solution.

About BeyondTrust

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

BeyondTrust protects all privileged identities, access, and endpoints across your IT environment from security threats, while creating a superior user experience and operational efficiencies. 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 75 of the Fortune 100, and a global partner network. Learn more at www.beyondtrust.com.