

Privilege Management for Windows & Mac 22.9

Privilege Management Cloud 22.9

What's New Documentation

Release Date – November 29th, 2022

BeyondTrust Privilege Management for Windows and 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.

Release Highlights

New Feature: Windows Hello Support for Privilege Management Prompts

Windows Hello is a feature that organizations can enable to allow their end users to access their Windows endpoints in a more personal, secure way using a PIN, facial recognition, or fingerprint. With release 22.9, organizations that have enabled Windows Hello can allow their end users to use their PIN or biometric data instead of their username and password when authenticating in response to a Privilege Management pop-up prompt. This new feature will improve your end user's day-to-day experience with Privilege Management while also providing an added layer of security to the authentication process.

Enhancement: Agent Protection – Core File and Driver Protection

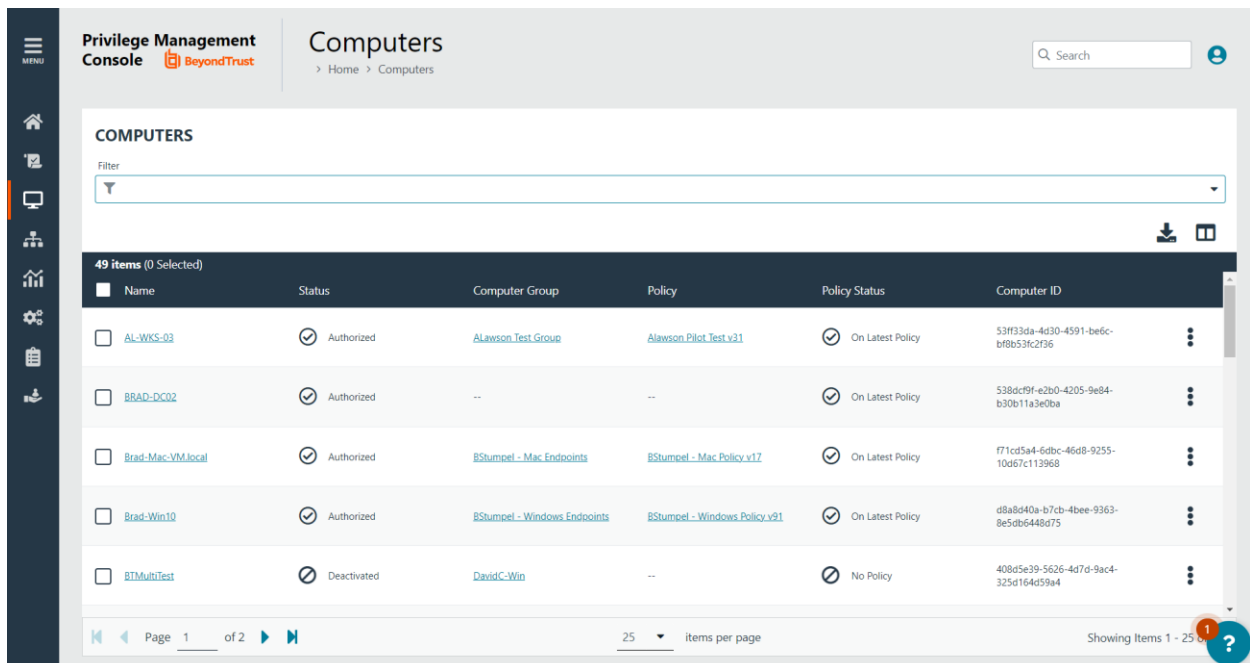
Agent Protection is a series of feature enhancements designed to prevent admins (real or rogue) from getting around the Privilege Management agent to threaten an endpoint. Initially launched in release 22.5, the first Agent Protection feature requires an admin to use a predefined secret to uninstall the Privilege Management agent. In release 22.7 we added a further layer of protection to the feature by protecting the registry keys used by the Privilege Management agent.

In release 22.9, we're adding even more functionality to Agent Protection. Admins are now prevented from tampering with or deleting the core files that are responsible for installation of the Privilege Management agent on an endpoint. We've also increased protection of the Privilege Management driver, which is responsible for critical actions like intercepting processes and running rules. Admins are no longer able to make changes to the driver that could make it stop running and restrict Privilege Management performance. These new features round out Agent Protection to provide even more protection for your estate.

New Feature: De-Duplication via Unique Endpoint IDs

Managing an estate of diverse endpoints can be a complex job. Some organizations have experienced an issue where PM Cloud would mistakenly identify multiple endpoints within their estate as duplicates. This problem would cause a headache for IT and security managers, bringing more complexity to managing their estates. In the worst case, this resulted in machines being disconnected from PM Cloud, with manual intervention being the only remediation path.

With release 22.9, we've fixed the problem of mistaken duplication by introducing unique identifiers for endpoints. Now every endpoint within your estate will automatically be assigned a unique ID. This new feature simplifies the experience of managing your estate and eliminates errors that could cause problems for your organization. Unique identifier data can be seen in the computers grid via the addition of a Computer ID column that can be optionally added to the view.



The screenshot displays the 'Computers' section of the Privilege Management Console. The interface includes a search bar, a filter dropdown, and a table with 49 items. The table columns are: Name, Status, Computer Group, Policy, Policy Status, and Computer ID. The 'Computer ID' column shows unique identifiers for each endpoint.

Name	Status	Computer Group	Policy	Policy Status	Computer ID
AL-WKS-03	Authorized	Alawson_Test_Group	Alawson_Pilot_Test_v31	On Latest Policy	53ff33da-4d30-4591-be6c-bf8b53fc2f36
BRAD-DC02	Authorized	--	--	On Latest Policy	538dc9f-e2b0-4205-9e84-b30b11a3e0ba
Brad-Mac-VM.local	Authorized	BStumpel - Mac Endpoints	BStumpel - Mac Policy v17	On Latest Policy	f71cd544-6dbc-46d8-9255-10d67c113968
Brad-Win10	Authorized	BStumpel - Windows Endpoints	BStumpel - Windows Policy v21	On Latest Policy	d8a8d40a-b7cb-4bee-9363-8e5db6448d75
BTMultiTest	Deactivated	DavidC-Win	--	No Policy	408d5e39-5626-4d7d-9ac4-325d164d59a4

Figure 1 – The Computer ID column can be added to the computer grid and shows each endpoint's unique identifier

Enhancement: Add to Policy UX Improvements

Previously, if a user selected a single event to add to policy from Analytics, they would be directed to the Applications Group. The Applications Group can be long, making it difficult to find and edit the application they needed.

With release 22.9, we've introduced enhancements to the Add to Policy user experience that make it easier and more efficient to use. Now, if a user selects a single event to Add to Policy, upon clicking 'Add and Edit' from the Add Applications to Policy panel, they will be directed to the application matcher edit panel in the Web Policy Editor based on the application added to policy via the selected event in Analytics. With this update, we're streamlining the process of adding applications to policy and making day-to-day management simpler.

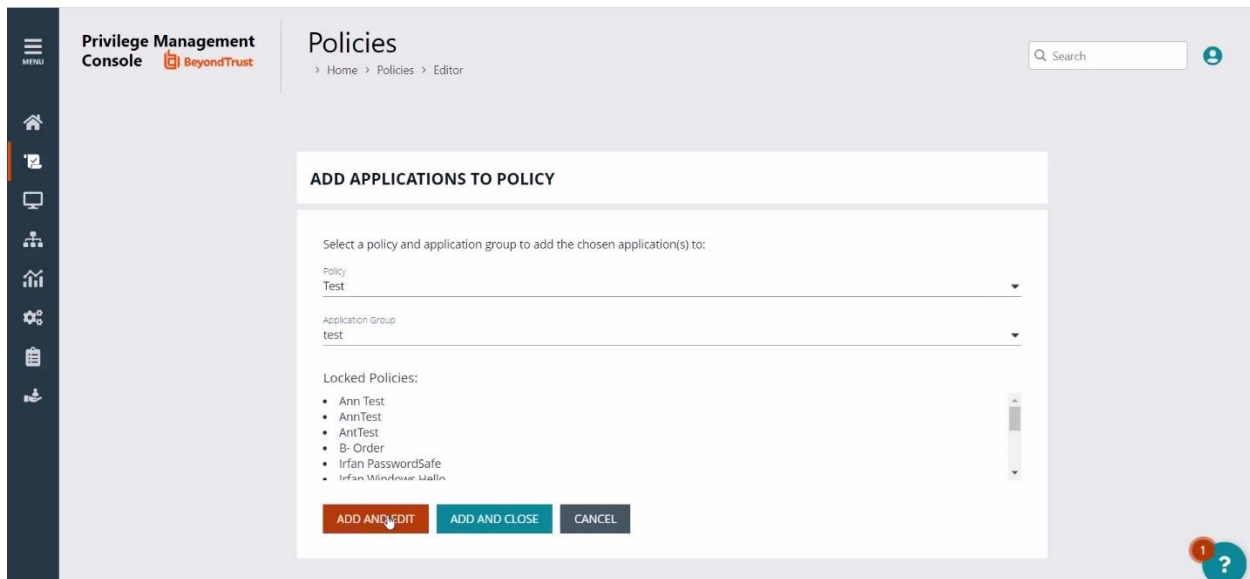


Figure 2 – When a user selects a single event to Add to Policy, they will be directed to the Add Applications to Policy panel

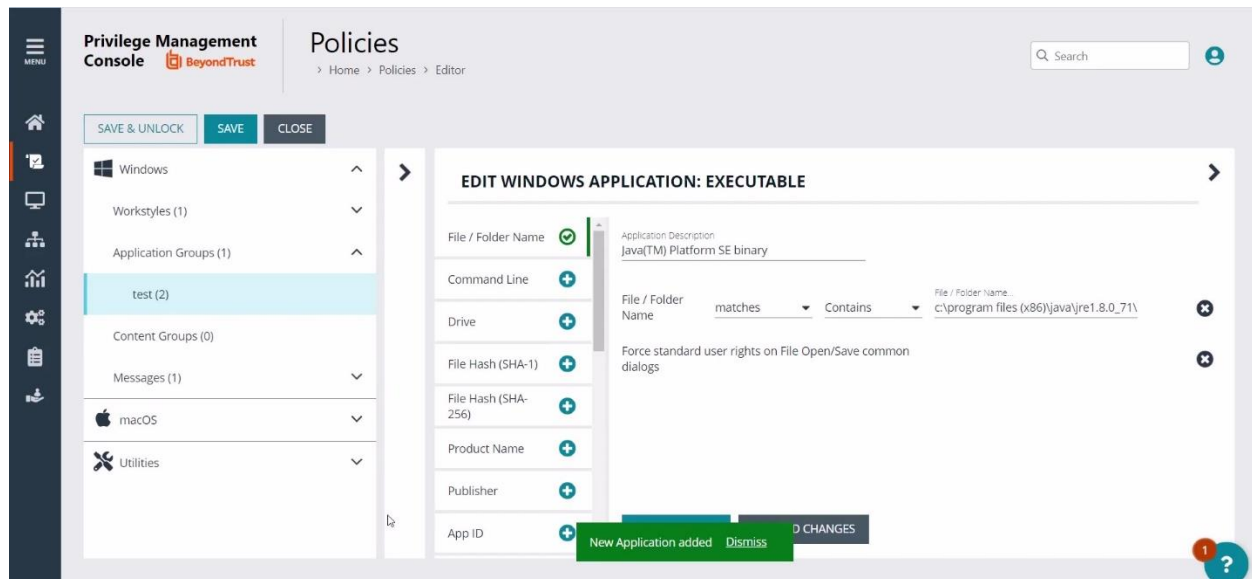


Figure 3 – After selecting Add and Edit, the user will be directed straight to the application matcher edit panel based on the application added to policy

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.