



Privilege Management for Windows & Mac 23.1

Privilege Management Cloud 23.1

What's New Documentation

Release Date – February 28th, 2023

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

Enhancement: Role-Based Access for Settings and Analytics

Release 22.8 introduced Role-Based Access, a feature that gives you granular control over the access and permissions your users have within the Privilege Management Console. Since release 22.8, you've been able to utilize Role-Based Access to quickly and easily define roles and permissions for your users, governing which computer groups and policies they can edit, analyze, view, or assign policy to.

With release 23.1, we've enhanced Role-Based Access to give you even more control over your users' access and permissions. In addition to defining your users' permissions to view and make changes to policies and computer groups, you can now set their permissions to view and edit Settings and Analytics within the Privilege Management Console. With this enhancement, you can now give your users permission to view or edit settings like Adapter Installation, Computer Settings, Azure AD Settings, or SIEM Settings. In addition, you can also govern their ability to view and make changes to the **Analytics** section of the Privilege Management Console.

These enhancements to Role-Based Access give you even more granular control over the access your users have to the Privilege Management Console, providing your organization with enhanced flexibility and adapting to how your teams work, regardless of the size or complexity.

Settings

13 items		
Setting	<input type="checkbox"/> Edit Setting ?	<input type="checkbox"/> View Setting ?
Privilege Management Installation	<input type="checkbox"/>	<input type="checkbox"/>
Adapter Installation	<input type="checkbox"/>	<input type="checkbox"/>
MMC Snap-In Installation	<input type="checkbox"/>	<input type="checkbox"/>
Computer Settings	<input type="checkbox"/>	<input type="checkbox"/>
Domain Settings	<input type="checkbox"/>	<input type="checkbox"/>
Azure AD Settings	<input type="checkbox"/>	<input type="checkbox"/>
SIEM Settings	<input type="checkbox"/>	<input type="checkbox"/>
Authorization Request Settings	<input type="checkbox"/>	<input type="checkbox"/>
Reputation Settings	<input type="checkbox"/>	<input type="checkbox"/>

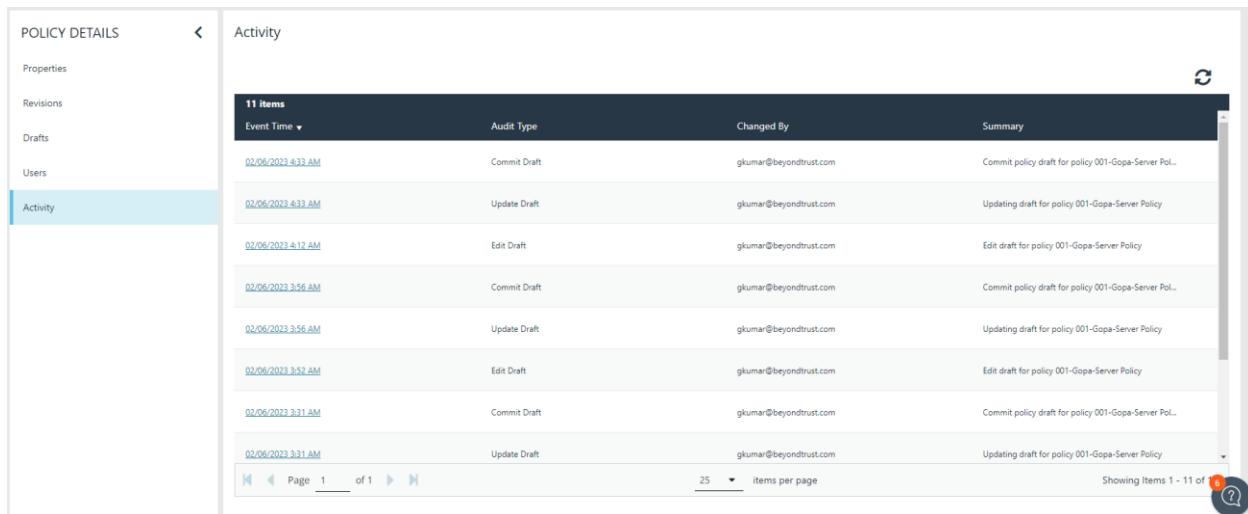
Page 1 of 1 | 25 items per page | Showing Items 1 - 13 of 13

Figure 1 – When you create a new user in the Privilege Management Console, you’re now able to set that user’s permissions to view and edit different settings.

New Feature: Activity Tracking for Policies, Users, Computers, and Groups

In complex, fast-moving organizations, changes to policies, users, computers, and computer groups happen often. As a result, those changes frequently aren’t clearly communicated across security and IT teams. This can lead to confusion about the source of changes and difficulty collaborating among teams.

In release 23.1, we’ve added functionality that can help communicate changes by adding an **Activity** tab to the **View Details** page for policies, users, computers, and computer groups. Now Privilege Management users can easily view the changes made to any policy, user, computer, or computer group that they have permissions to view. This includes the time the change took place, the type of change (including edit, assign, update, and more), who the change was made by, and a summary of the change. These changes will also flow through to the Activity Auditing feature within Privilege Management, which acts as the centralized location for all auditing. With Activity Tracking, security and IT teams of all sizes now have a clear source of activity information that make collaboration easier.



Event Time	Audit Type	Changed By	Summary
02/06/2023 4:33 AM	Commit Draft	gkumar@beyondtrust.com	Commit policy draft for policy 001-Gopa-Server Pol...
02/06/2023 4:33 AM	Update Draft	gkumar@beyondtrust.com	Updating draft for policy 001-Gopa-Server Policy
02/06/2023 4:12 AM	Edit Draft	gkumar@beyondtrust.com	Edit draft for policy 001-Gopa-Server Policy
02/06/2023 3:56 AM	Commit Draft	gkumar@beyondtrust.com	Commit policy draft for policy 001-Gopa-Server Pol...
02/06/2023 3:56 AM	Update Draft	gkumar@beyondtrust.com	Updating draft for policy 001-Gopa-Server Policy
02/06/2023 3:52 AM	Edit Draft	gkumar@beyondtrust.com	Edit draft for policy 001-Gopa-Server Policy
02/06/2023 3:31 AM	Commit Draft	gkumar@beyondtrust.com	Commit policy draft for policy 001-Gopa-Server Pol...
02/06/2023 3:31 AM	Update Draft	gkumar@beyondtrust.com	Updating draft for policy 001-Gopa-Server Policy

Figure 2 – The Activity tab can be found in the View Details page of any policy, user, computer, or computer group.

Enhancement: All Data Available for SIEM Integration via New ECS Format

In order to fully protect your organization, it's critical that your key security tools work together seamlessly to give you a full and detailed view of your estate and any incoming threats. Previously, if you had enabled the Privilege Management integration with your SIEM tool, only a small subset of the events data that Privilege Management captures was visible to the tool.

In release 23.1, we have introduced a new way to connect Privilege Management to your SIEM tool via a new Elastic Common Schema (ECS) format. This makes all of the event data captured by Privilege Management as well as all fields within each event visible through your SIEM tool.

This enhancement will help you stay on top of what is happening in your estate by comprehensively integrating Privilege Management with your SIEM tool and providing you with greater data fidelity.

New Feature: Enable or Disable Application Rules and Definitions Within a Policy

Your estate and your end users are constantly changing. New applications are being used, new business requirements are being set, new roles and teams are being created, and more. Nothing is static about your organization, so your policies can't be static either.

In release 23.1, we've introduced the ability to enable or disable application rules and definitions within a policy. This new feature will give you a fast, flexible way to add and test new application rules and definitions as you refine your policies to meet the change in your organization. Instead of having to delete an application rule within a policy, test it, and manually add it back if the test fails, you can now disable the application rule, test it, and if the test fails, enable it again.

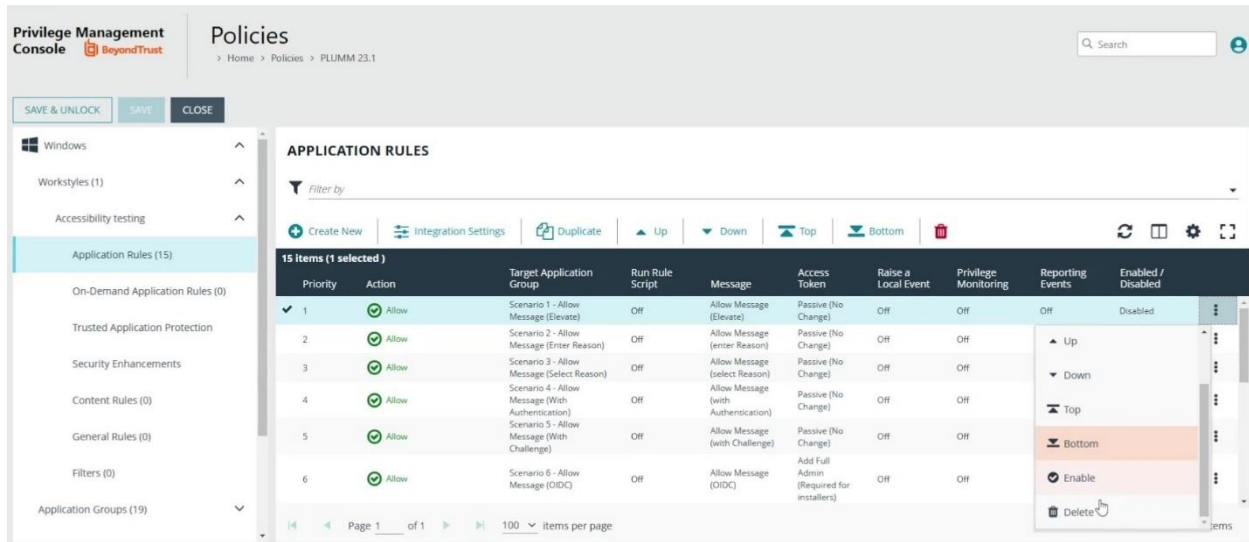


Figure 3 – You can now quickly enable or disable application rules within a policy.

New Feature: TouchID Support in macOS

With release 23.1, end users on macOS endpoints can now use TouchID instead of their username and password to authenticate in response to a Privilege Management pop-up. This new feature improves the day-to-day experience of end users, seamlessly embedding Privilege Management into their everyday workflows and providing an added layer of security for the organization.

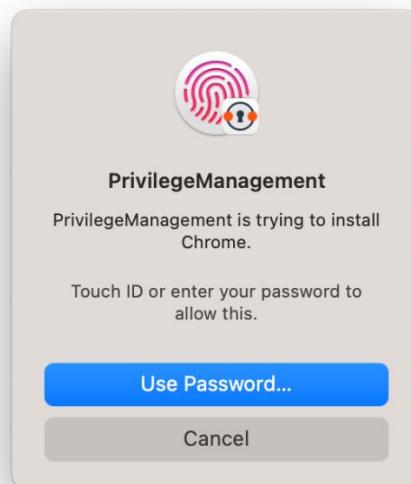
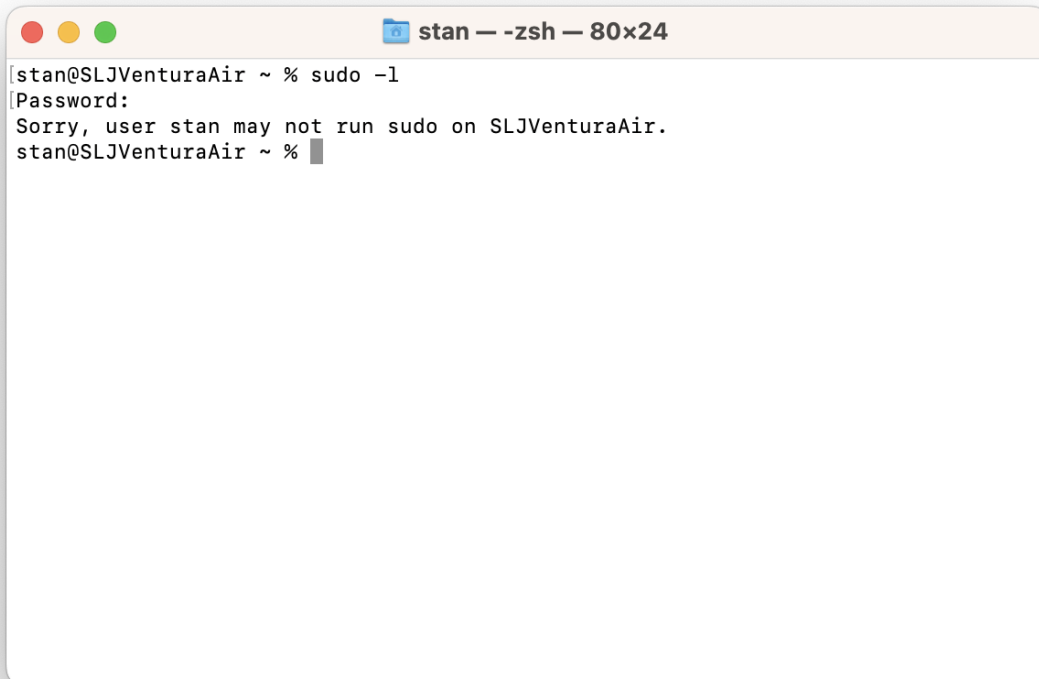


Figure 4 – End users can now use TouchID to authenticate in response to a Privilege Management pop-up.

New Feature: macOS Sudo -l or Sudo -list Query

To improve the day-to-day experience of technical macOS users, we've introduced the ability for end users to query the Privilege Management policy applied to their endpoint using the **sudo -l** or **sudo -list** commands to know what commands they are allowed to run with sudo (root) privileges. This new feature removes roadblocks for technical macOS end users, especially those using Homebrew.

A screenshot of a macOS terminal window titled 'stan -- -zsh -- 80x24'. The terminal shows the user 'stan' at 'SLJVenturaAir' running the command 'sudo -l'. The prompt asks for a password, and the user enters it. The output is 'Sorry, user stan may not run sudo on SLJVenturaAir.' followed by the prompt 'stan@SLJVenturaAir ~ %' and a cursor.

```
[stan@SLJVenturaAir ~ % sudo -l ]
[Password: ]
Sorry, user stan may not run sudo on SLJVenturaAir.
stan@SLJVenturaAir ~ % █
```

Figure 5 – macOS end users can now use sudo -l or sudo -list commands to know what commands are allowed to run with sudo (root) privileges.

New Feature: Live Message Preview in Web Policy Editor

Previously, when editing messages that would be shown to end users, you would need to save your updates to the message in order to see a preview of them. Now, with release 23.1, you can see a live preview of the updates you're making to a message with no need to save before you're finished.

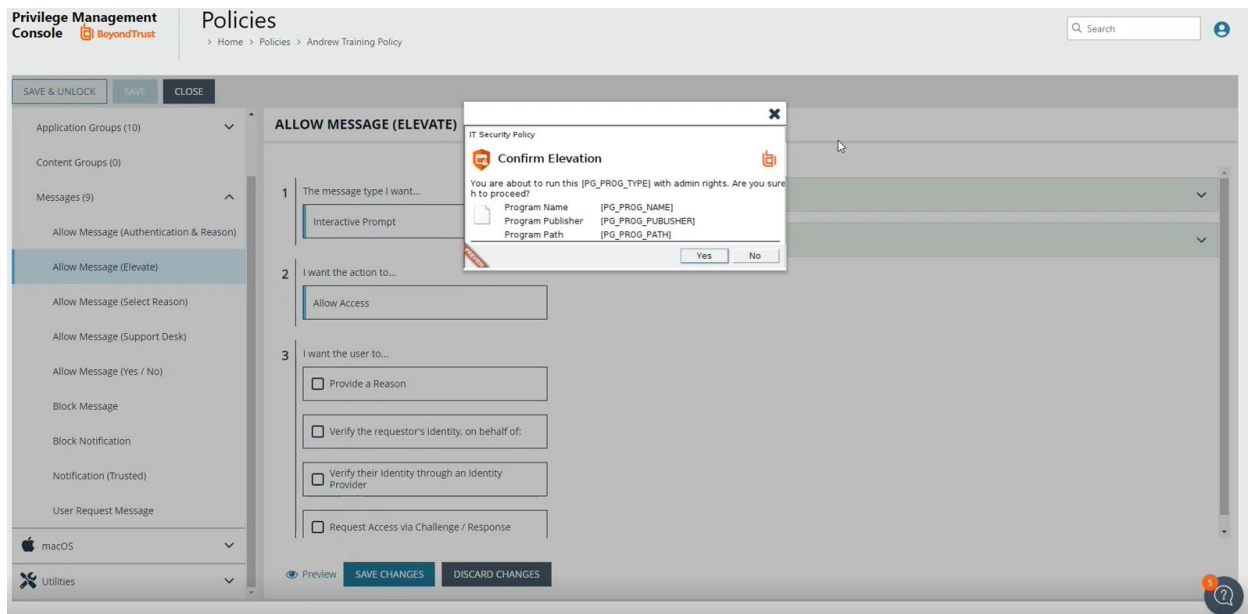


Figure 6 – A live preview of the message that's being edited can be seen by clicking the Preview button to the left of the Save Changes button.

Enhancement: Windows System Tray Menu

With release 23.1, end users can see more information about Privilege Management on their endpoint by clicking the BeyondTrust Privilege Management logo in their Windows System Tray. The new pop-up menu shows active policies on the user's endpoint, system info including client version, computer name, and adapter version, and provides the ability to refresh all policies and copy all of the details shown. These updates give end users more information about their system and the policies it's running and acts as an important source of information for IT service desk or support workers when troubleshooting problems.

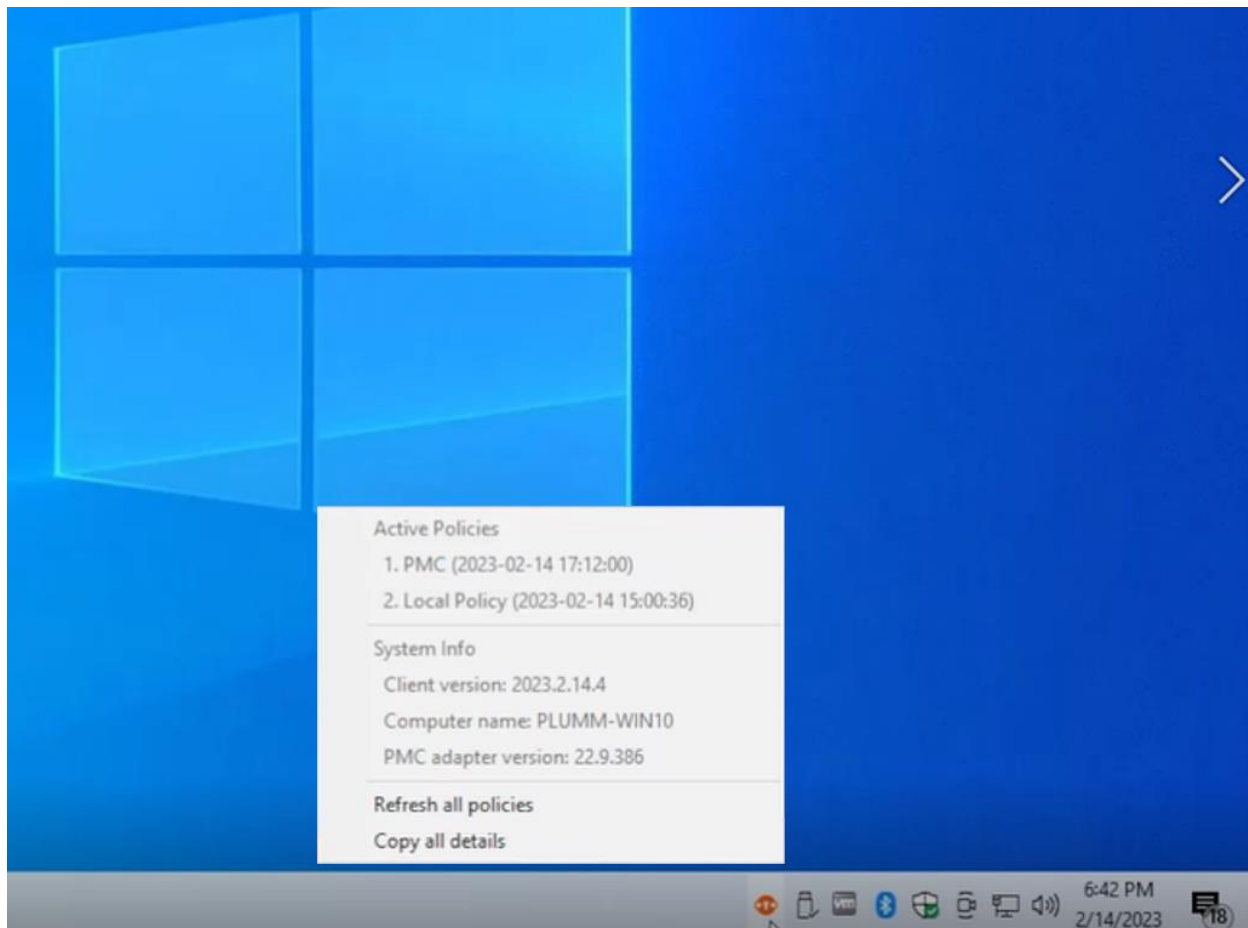


Figure 7 – End users as well as IT service or support workers can now see important information about the endpoint in the Windows System Tray pop-up menu.

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.