

Privilege Management for Windows & Mac Cloud

23.3

What's New Documentation

Release Date – April 20th, 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

New Feature: Role-Based Access for APIs

In release 22.8 we introduced role-based access, a feature that gives you granular control over the access and permissions your users have within the Privilege Management Console. In release 23.3, we're introducing role-based access for APIs, which allows you to apply that same granular control over access and permissions to the APIs you use in Privilege Management.

Now, when you create a new API account in the **API Settings** page of the **Configuration** section of the Privilege Management Console, you can select which endpoints you want the API account to have access to. This ensures that each API only has the access and permissions it requires, reducing risk and protecting your organization against potential vulnerabilities.

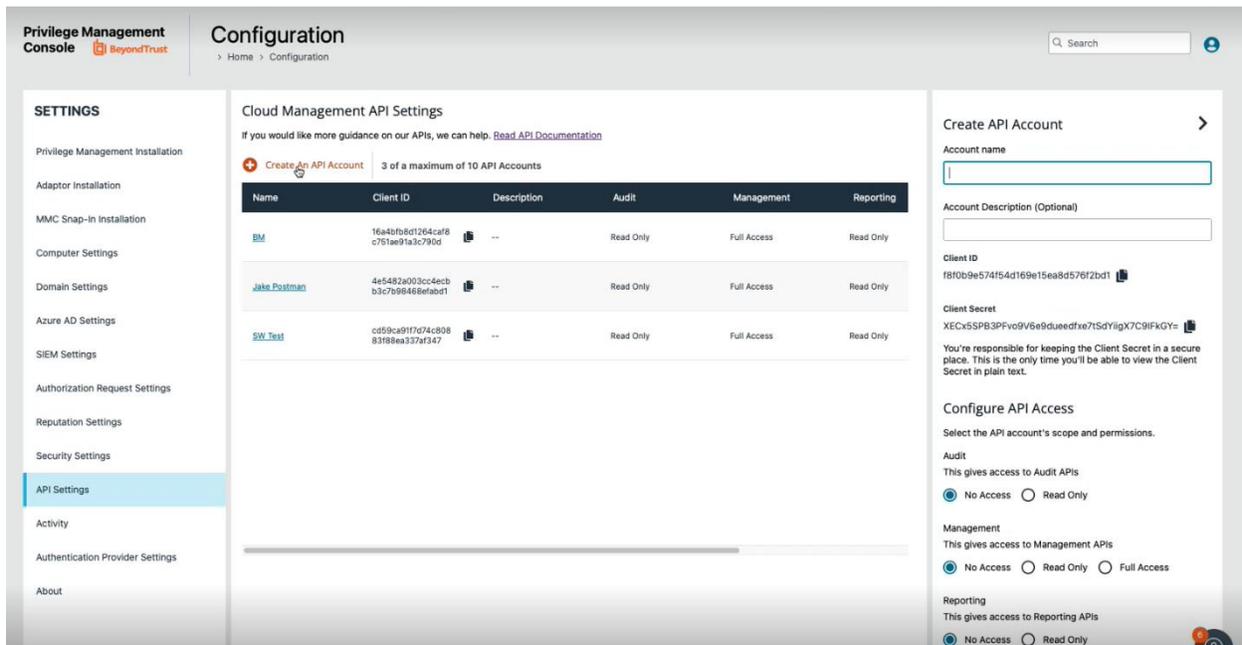


Figure 1 – You can now configure API access through the API Settings page

New Feature: Elevation of Store Applications

Today, many end users rely on app stores such as the Microsoft Store or the Apple App Store to download the applications they need in order to do their jobs. Many of these applications require elevation – such as Windows Terminal, Windows Notepad, WinDbg, Dell SupportAssist, and others – and until now Privilege Management did not offer a seamless way to elevate them.

With release 23.3, Privilege Management can now seamlessly elevate applications downloaded from app stores. This streamlines the elevation process and reduces service desk tickets for IT and security teams. It also provides end users with more flexibility to download applications from the trusted source of their choosing.

Beta Feature: Add to Policy in Analytics v2

Last year, in release 22.10, we unveiled the first stage of Analytics v2, an upgraded beta version of the analytics functionality within Privilege Management. Since that initial release, we've been introducing more and more functionality to the Analytics v2 beta. In release 23.3, we're launching a new feature in Analytics v2 that enables you to refine your policies more efficiently.

Users can now action policy changes directly from Analytics v2 thanks to the introduction of the Add to Policy functionality in release 23.3. This means that instead of navigating between Analytics and the Web Policy Editor to implement a change to policy based on Analytics data, that policy change can be actioned directly from Analytics v2, streamlining the process for IT and security teams as they refine policies and react to user behavior.

Analytics v2 is built on entirely new technology, which provides improved scale and performance so you can get the data and insights you need to monitor your estate and improve your least privilege posture fast. You can enable the Analytics v2 beta via the **Analytics v2** switch in the top-right corner of the **Analytics** page. The full release of Analytics v2 is on the roadmap for mid-2023.

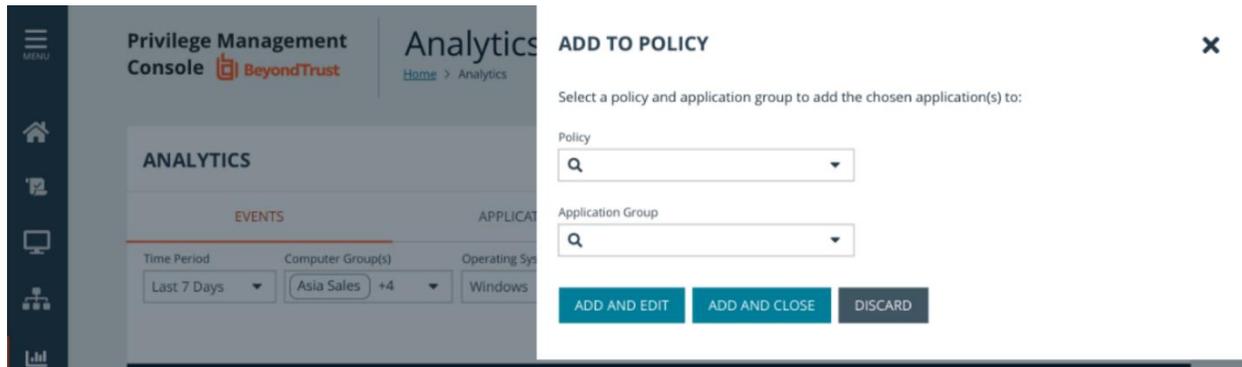


Figure 2 – Policy changes can now be actioned directly from Analytics v2 with the Add to Policy functionality

New Feature: DLL Control

DLLs (Dynamic Link Libraries) are files that contain code and data that can be used by multiple programs at the same time. They are commonly used by Windows operating systems and applications to improve performance and reduce disk space usage. However, DLLs can also be used by attackers to inject malicious code into legitimate programs, leading to a range of security threats.

With release 23.3, you can now block six DLLs from Microsoft’s recommended block list with the click of a button in the Web Policy Editor. If you navigate to the **Policies** section in the Privilege Management Console and then choose the policy in which you’d like to block DLLs, you can then select **Security Enhancements** from the dropdown menu. You’ll then click a toggle to enable blocking the six DLLs Microsoft recommends that you block. If you’d like to customize your approach further, you can use the table below to change the allow/block status of each individual DLL.

The Essential Eight, a set of eight security strategies recommended by the Australian Cyber Security Centre (ASCS) to help organizations protect against cyberthreats, states that application control should be one of the eight key pillars of an organization’s security posture, and that control of software libraries (including DLLs) is vital to achieving effective application control. With DLL Control, you can now enhance your organization’s security posture by blocking six risky DLLs at the click of a button.

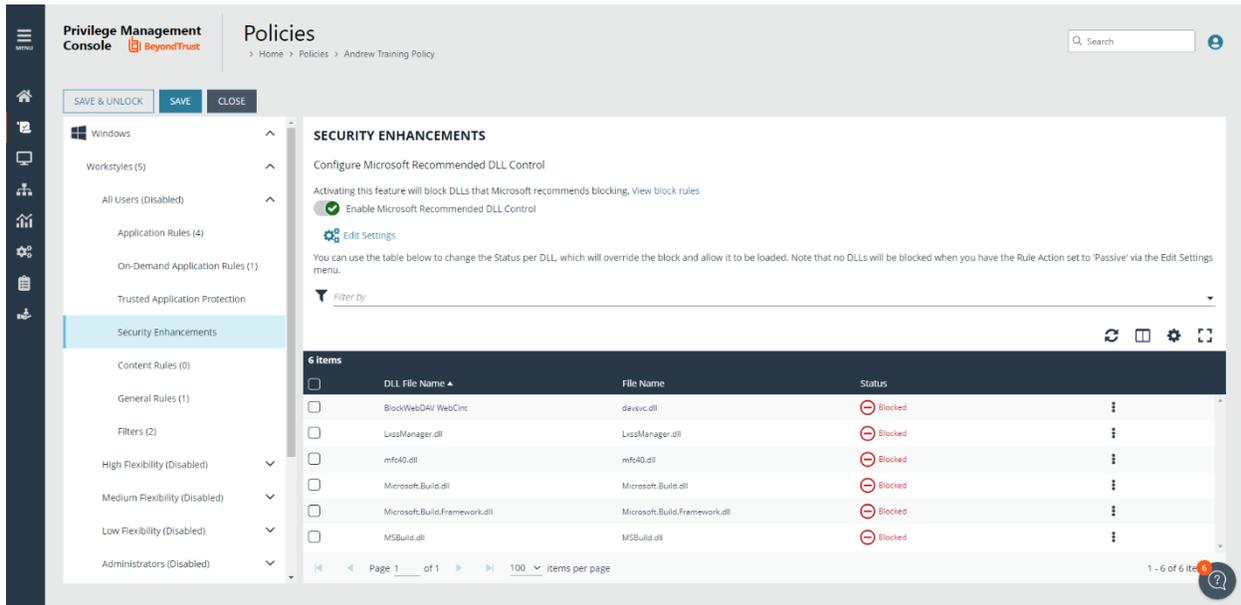


Figure 3 – You can now block the six DLLs that Microsoft recommends blocking by clicking the toggle in the Security Enhancements section

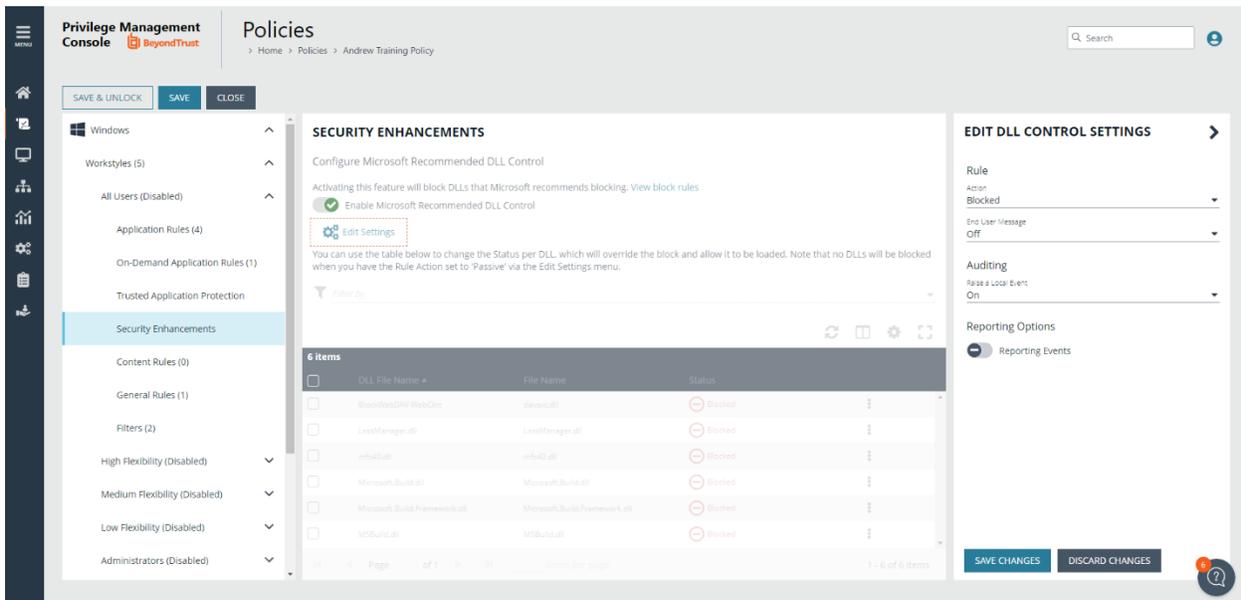


Figure 4 – If you'd like to customize your approach to blocking DLLs, you can choose to allow or block each DLL from within the table as well as set end user messaging, auditing, and reporting choices.

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.