BeyondTrust

Privilege Management for Windows & Mac Cloud 23.2

What's New Documentation

Release Date – March 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.

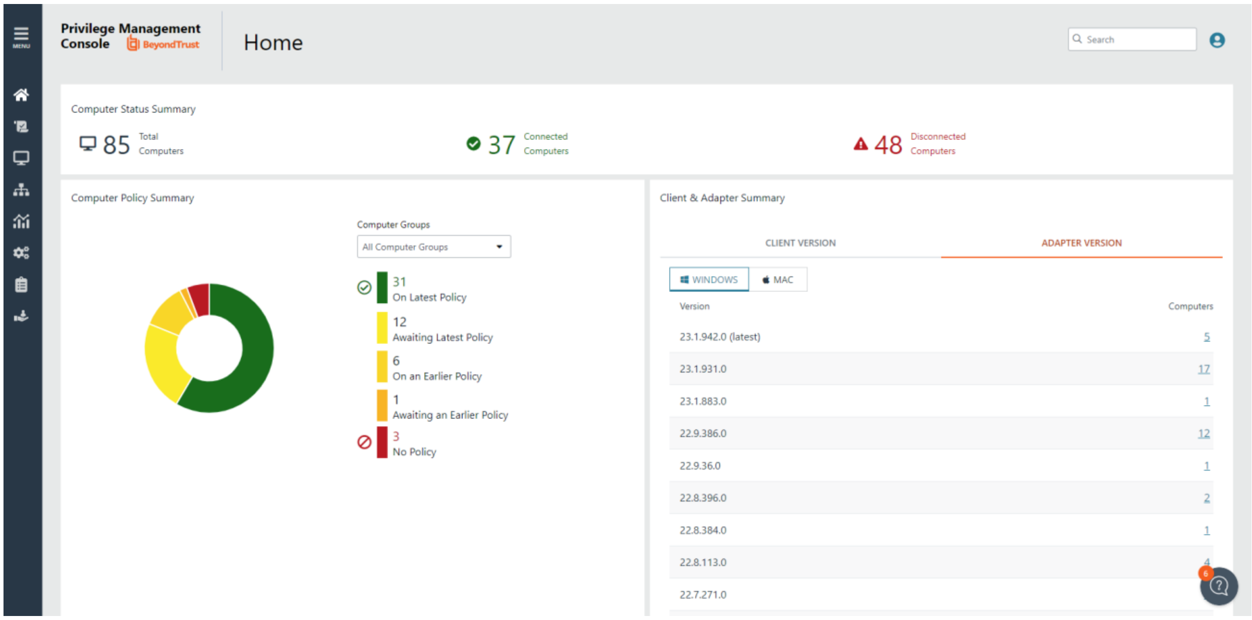
Release Highlights

New Feature: Endpoint Connection Status

When managing a complex estate, it's vital to understand the connection status of your endpoints to Privilege Management. If an endpoint becomes disconnected from Privilege Management, it cannot receive policy updates, and its activity will not be visible in the Analytics or Auditing functionalities. This can cause a headache for IT and security teams as well as jeopardize the protection and compliance of the organization.

In release 23.2, we've introduced endpoint connection statuses. Now, on the homepage of the Privilege Management Console, you'll see a Computer Status Summary section. This shows the total number of computers in your estate, the number of those computers that are connected to Privilege Management, and the number that are disconnected. The connection status of each individual computer can be seen in the Computers tab along with the number of days disconnected for those computers that are disconnected from Privilege Management. In the Computer Settings section of the Settings tab, you can customize the number of days that a computer needs to be disconnected from Privilege Management in order for its status to change to disconnected.

With endpoint connection statuses, organizations now have a convenient, real-time way to monitor the connection status of all the endpoints in their estates, enabling quick detection of disconnected endpoints and a fast path to remediation.



Privilege Management Console BeyondTrust

Home

Computer Status Summary

85 Total Computers	37 Connected Computers	48 Disconnected Computers

Computer Policy Summary

Computer Groups: All Computer Groups

- 31 On Latest Policy
- 12 Awaiting Latest Policy
- 6 On an Earlier Policy
- 1 Awaiting an Earlier Policy
- 3 No Policy

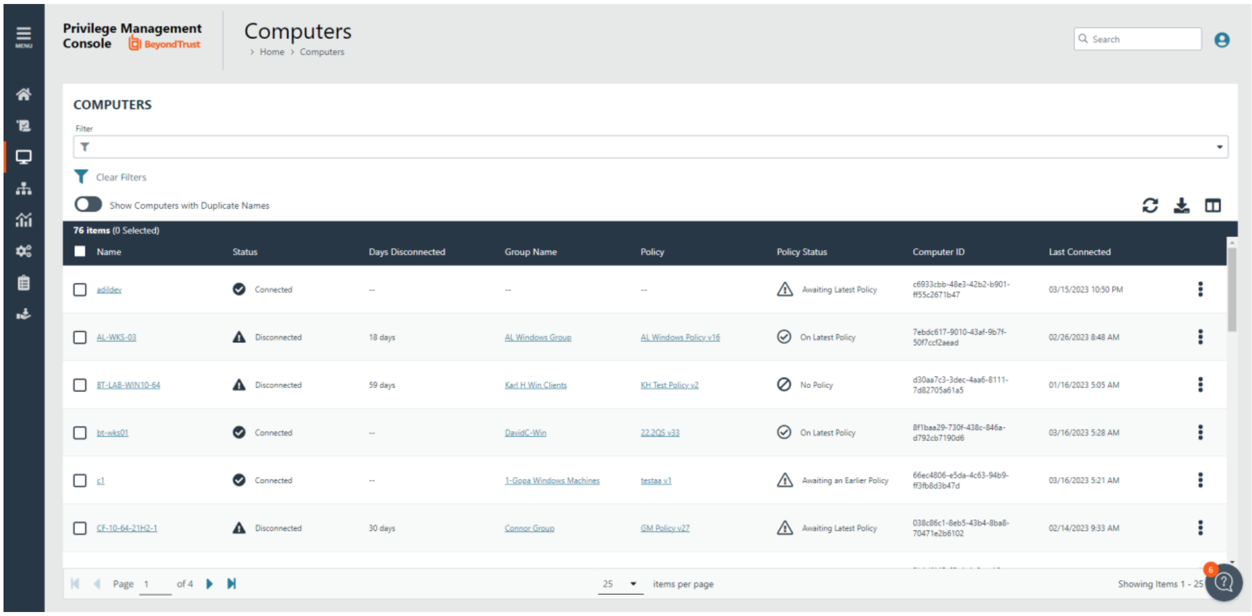
Client & Adapter Summary

CLIENT VERSION | ADAPTER VERSION

WINDOWS | MAC

Version	Computers
23.1.942.0 (latest)	5
23.1.931.0	17
23.1.883.0	1
22.9.386.0	12
22.9.36.0	1
22.8.396.0	2
22.8.384.0	1
22.8.113.0	4
22.7.271.0	

Figure 1 – The homepage of the Privilege Management Console now includes a Computer Status Summary, where you can see how many computers are connected and disconnected within your estate



Privilege Management Console BeyondTrust

Computers

> Home > Computers

COMPUTERS

Filter

Clear Filters

Show Computers with Duplicate Names

76 items (0 Selected)

Name	Status	Days Disconnected	Group Name	Policy	Policy Status	Computer ID	Last Connected
adildev	Connected	--	--	--	Awaiting Latest Policy	c6933cbb-48e3-42b2-b901-ff55c2671b47	03/15/2023 10:50 PM
AL-WKS-03	Disconnected	18 days	AL Windows Group	AL Windows Policy v16	On Latest Policy	7ebdc617-9010-43af-9b7f-50f7ccf2aead	02/26/2023 8:48 AM
BT-LAB-WIN10-64	Disconnected	59 days	Karl H Win Clients	KH Test Policy v2	No Policy	d30aa7c3-3dec-4aa6-8111-7d82705a61a5	01/16/2023 5:05 AM
bt-wks01	Connected	--	DavidC-Win	22.2QS v33	On Latest Policy	8f1baa29-730f-438c-846a-d792cb7190d6	03/16/2023 5:28 AM
c1	Connected	--	1-Gopa Windows Machines	testaa v1	Awaiting an Earlier Policy	66ec4806-e5da-4c63-94b9-ff3fb8d3b47d	03/16/2023 5:21 AM
CF-10-64-21H2-1	Disconnected	30 days	Connor Group	GM Policy v27	Awaiting Latest Policy	038c86c1-8eb5-43b4-8ba8-70471e2b6102	02/14/2023 9:33 AM

Page 1 of 4 | 25 items per page | Showing Items 1 - 25

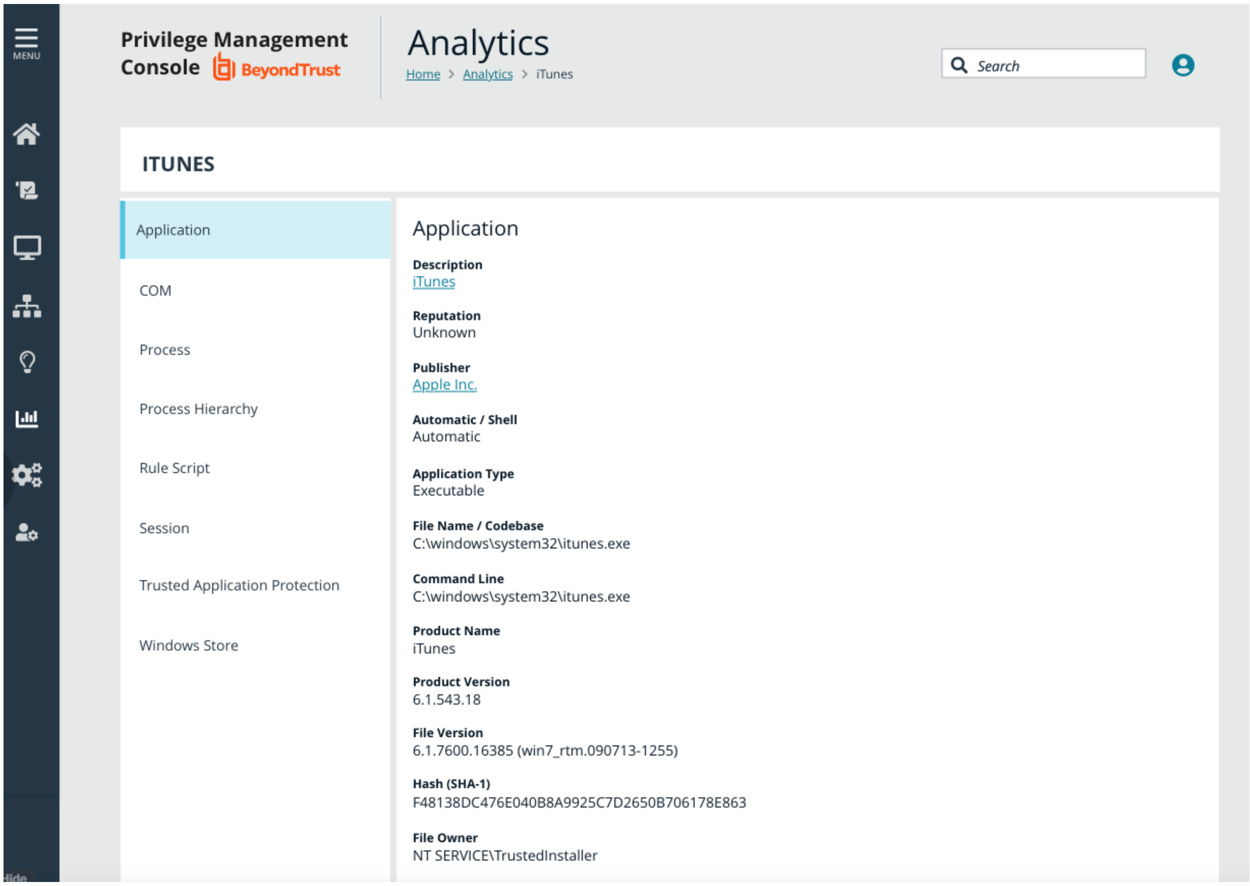
Figure 2 – The connection status of each computer can be seen in the Computers tab along with the number of days disconnected for those computers that are disconnected from Privilege Management

Beta Feature: Event Details in Analytics v2

Last year, in release 22.10, we introduced the first stage of Analytics v2, an upgraded beta version of the analytics functionality within Privilege Management. In release 23.2, we're introducing new functionality that will enable you to dig deeper into the details of each event captured by Privilege Management.

Now, when viewing the events list in Analytics v2, you can select an event to view its details. This will show all of the information that Privilege Management has captured for that individual event, including things like application, publisher, version, hash (SHA-1), and much more. This new feature will give you easy access to the fine-grained details of your users' privileged events, allowing you to monitor your estate more closely.

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.



ITUNES

Application

Description
iTunes

Reputation
Unknown

Publisher
Apple Inc.

Automatic / Shell
Automatic

Application Type
Executable

File Name / Codebase
C:\windows\system32\itunes.exe

Command Line
C:\windows\system32\itunes.exe

Product Name
iTunes

Product Version
6.1.543.18

File Version
6.1.7600.16385 (win7_rtm.090713-1255)

Hash (SHA-1)
F48138DC476E040B8A9925C7D2650B706178E863

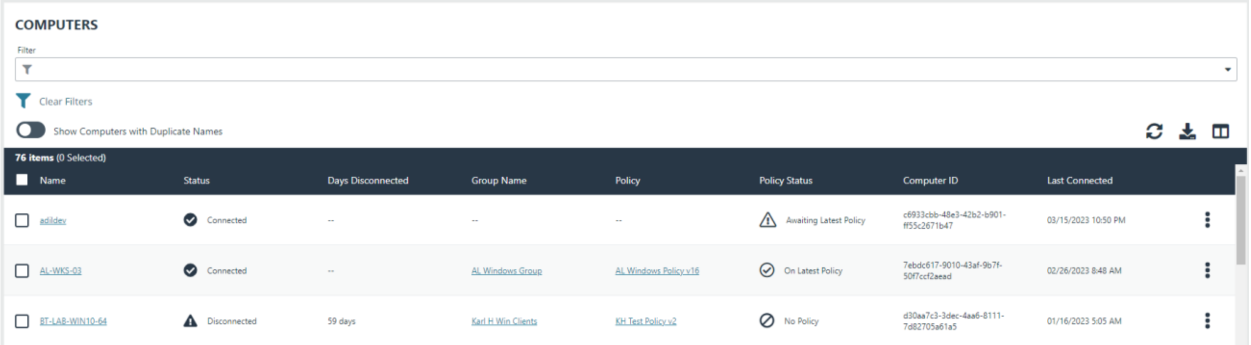
File Owner
NT SERVICE\TrustedInstaller

Figure 3 – You can now see all of the information that Privilege Management captures for each event through the Event Details page.

New Feature: Computer Duplication Filtering

When managing a complex organization, the list of computers in your estate can get complicated fast. Duplicate computer names make it difficult to find recently created computers. In release 23.2, we're introducing a **Show Computers with Duplicate Names** switch at the top of the computer list. By default, this switch will be set to **OFF** and duplicate computer names will be removed from the computer list, showing you only the computers that were most recently connected in the case of a duplicate. When switched **ON**, you will be able to see all computers, including duplicates.

This new feature will help to clean up your computer list, filtering out duplicates and allowing you to find the computers you need quickly.



COMPUTERS

Filter

○ Show Computers with Duplicate Names

76 items (0 Selected)

□	Name	Status	Days Disconnected	Group Name	Policy	Policy Status	Computer ID	Last Connected
□	adildev	Connected	--	--	--	Awaiting Latest Policy	c6933cbb-48e3-42b2-b901-ff55c2671b47	03/15/2023 10:50 PM
□	AL-WKS-03	Connected	--	AL Windows Group	AL Windows Policy v16	On Latest Policy	7ebdc617-9010-43af-9b7f-50f7ccf2aead	02/26/2023 8:48 AM
□	BT-LAB-WIN10-64	Disconnected	59 days	Karl H Win Clients	KH Test Policy v2	No Policy	d30aa7c3-3dec-4aa6-8111-7d82705a61a5	01/16/2023 5:05 AM

Figure 4 – A Show Computers with Duplicate Names switch has now been added to the computers list, filtering out duplicate computer names.

Enhancement: Windows Server Core Support

With release 23.2, Privilege Management now fully supports Windows Server Core operating system. By expanding the list of supported operating systems, organizations will now be able to fully achieve least privilege across their Windows server deployments and have the flexibility to run the operating system of their choice.

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.