

Tenable Security Center and BeyondTrust Password Safe Integration Guide

Last Revised: August 14, 2023

Table of Contents

Welcome to Tenable Security Center for BeyondTrust	
Integrations	
Windows Integration	5
SSH Integration	
Add the BeyondTrust Credential to a Scan	
API Configuration	
API Keys Setup	
Enable API Access	17
Additional Information	
Elevation	
Customized Report	
About Tenable	

- Ø

Welcome to Tenable Security Center for BeyondTrust

This document describes how to configure Tenable Security Center for integration with the BeyondTrust Password Safe and BeyondTrust Password Safe Cloud.

Security administrators know that conducting network vulnerability assessments means getting access to and navigating an ever-changing sea of usernames, passwords, and privileges. By integrating BeyondTrust with Tenable Security Center, customers have more choice and flexibility.

The benefits of integrating Tenable Security Center with BeyondTrust include:

- Credential updates directly in Tenable Security Center, requiring less management.
- Reduced time and effort documenting where credentials are stored in the organizational environment.
- Automatic enforcement of security policies in specific departments or business unit requirements, simplifying compliance.
- Reduced risk of unsecured privileged accounts and credentials across the enterprise.

Integrations

Configure BeyondTrust with either Windows or SSH. Click the corresponding link to view the configuration steps.

Ø

Windows Integration

SSH Integration

Add Credential to a Scan

Windows Integration

To configure a **Windows** credentialed network scan with BeyondTrust:

- 1. Log in to Tenable Security Center.
- 2. In the top navigation bar, click **Scans**.

A drop-down appears.

3. Click **Credentials**.

The **Credentials** window opens.

4. Click the **+ Add** button.

Interset Interset <th< th=""><th>SecurityCenter 😒 👘</th><th>Dashboard ▼ Analysis ▼ Scans</th><th>✓ Reporting</th><th>Users -</th><th></th><th>🛔 qahead 🕶</th></th<>	SecurityCenter 😒 👘	Dashboard ▼ Analysis ▼ Scans	✓ Reporting	Users -		🛔 qahead 🕶
Active Scans Agent Scans Scan Results Policies Audit Files Blackout Windows Image Image Tage Tage <th>Credentials</th> <th></th> <th></th> <th></th> <th></th> <th>+ Add</th>	Credentials					+ Add
Name Tag Type Group Owner Last Modified testoracle Database Full Access qahead 4 hours ago Image: Compare to the standard tot t	Active Scans Agent Scans	Scan Results Policies Audit F	iles Credentials Blackout Windows			< T 0
testoracleDatabaseFull Accessqahead4 hours agoImporttestinfomixDatabaseFull Accessqahead4 hours agoImporttestinDatabaseFull Accessqahead3 hours agoImporttestinSSHFull Accessqahead3 hours agoImport	Name	Tag Type	Group	Owner	Last Modified	
tesinformix Database Full Access qahead 4 hours ago I w tesin Database Full Access qahead 3 hours ago I w tesin SH Full Access qahead 3 hours ago I w	testoracle	Database	Full Access	qahead	4 hours ago	0 -
tesinDatabaseFull Accessqahead3 hours agotestSSHFull Accessqahead3 hours ago\$ *	testinfomix	Database	Full Access	qahead	4 hours ago	0 -
test SSH Full Access gahead 3 hours ago I or solutions ago	testin	Database	Full Access	qahead	3 hours ago	0 -
	test	SSH	Full Access	qahead	3 hours ago	Q ~
testcred SSH Full Access qahead 1 hour ago 💠 🛩	testcred	SSH	Full Access	qahead	1 hour ago	0 ×

O

The **Add Credential** window opens.

5. In the **Windows** section, click **BeyondTrust**.

ecurityCenter sc	Dashboard 🗸	Analysis 👻 Scans 👻	Reporting - Assets	s Workflow -	Users -			💄 qahead •
Add Credentia	al							← Bac
Database								
IBM DB2	Informix/DRDA	MySQL	Oracle Database	PostgreSQL	SQL Server			
SNMP								
SNMP								
SSH								
BeyondTrust	Certificate	CyberArk Vault	Kerberos	Lieberman	Password	Public Key	Thycotic Secret Server	
Windows								
BeyondTrust	CyberArk Vault	Kerberos	Lieberman	LM Hash	NTLM Hash	Password	Thycotic Secret Server	

0 -

The **Add Credential** configuration page appears.

SecurityCenter sc	Dashboard - Analysis -	Scans 🗸	Reporting -	Assets	Workflow -	Users v	4
Add Credential							♦ Back
	General						
	Name*						
	Description						
	Tag			<i>"</i>			
	BeyondTrust Cre	dential					
	Username*						
	Domain						
	BeyondTrust host*						
	BeyondTrust port*	443					
	BeyondTrust API key*						
	Checkout duration*						
	Use SSL						
	Verify SSL Certificate						
Inn	Submit Cancel						

- 6. In the top section, enter a descriptive **Name** (required) , **Description** (optional), and **Tag** (optional).
- 7. Configure each field for **Windows** authentication. See the <u>Tenable Security Center User Guide</u> to get detailed descriptions for each option.

Ø

- 8. Click Save.
- 9. Next, follow the steps for adding the credential to a scan.

SSH Integration

To configure an **SSH** credentialed network scan with BeyondTrust:

- 1. Log in to Tenable Security Center.
- 2. In the top navigation bar, click **Scans**.

A drop-down appears.

3. Click **Credentials**.

The **Credentials** window appears.

4. Click the **+ Add** button.

		g Assets Workilow Users •			🐣 qahead 🔫
Credentials					+ Add
Active Scans Agent Scans Scan Results	Policies Audit Files Crede	entials Blackout Windows			< T 0
Name Tag	Туре	Group	Owner	Last Modified	
testoracle	Database	Full Access	qahead	4 hours ago	0 ×
testinfomix	Database	Full Access	qahead	4 hours ago	۰
testin	Database	Full Access	qahead	3 hours ago	۵.×
test	SSH	Full Access	qahead	3 hours ago	Q
testcred	SSH	Full Access	qahead	1 hour ago	۵ ×

O

The **Add Credential** window appears.

5. In the SSH section, click **BeyondTrust**.

SecurityCent <u>er</u> so	Dashboard -	Analysis 👻 Scans 👻	Reporting - Assets	Workflow -	Users -			🚨 qahead 🕇
Add Credenti	al							← Back
Database								
IBM DB2	Informix/DRDA	MySQL	Oracle Database	PostgreSQL	SQL Server			
SNMP								
SNMP								
SSH								
BeyondTrust	Certificate	CyberArk Vault	Kerberos	Lieberman	Password	Public Key	Thycotic Secret Server	
Windows								
BeyondTrust	CyberArk Vault	Kerberos	Lieberman	LM Hash	NTLM Hash	Password	Thycotic Secret Server	

0 -

The **Add Credential** configuration page appears.

SecurityCenter 😒	Dashboard ▼ Analysis ▼ Scans ▼ Reporting ▼ Assets Workflow ♥ Users ♥	🚨 qahead 🗸
Add Credential		♦ Back
	General	
	Name" BeyondTrust	
	Description	
	Tag	
	BeyondTrust Credential	
	Username*	
	BeyondTrust host*	
	BeyondTrust port* 443	
	BeyondTrust API key*	
	Checkout duration*	
	Use SSL	
	Verify SSL Certificate	
	Use Private Key	
	Use Privilege Escalations	
	Submit Cancel	

- In the top section, enter a descriptive Name (required), Description (optional), and Tag (optional).
- 7. Configure each field for **SSH** authentication. See the <u>Tenable Security Center User Guide</u> to get detailed descriptions for each option.

Ø

- 8. Click Save.
- 9. Next, follow the steps for adding the credential to a scan.

Add the BeyondTrust Credential to a Scan

To add the BeyondTrust credential to the scan:

1. In the top navigation bar of Tenable Security Center, click **Scans**.

A drop-down appears.

2. Select Active Scans.

SecurityCenter 🔊 Dashboard - Analysis -	Scans ▼ Reporting ▼ Assets Workflow ▼ Users ▼	🛓 qahead 🕶
Executive 7 Day	Active Scans Agent Scans	Switch Dashboard 👻 🍄 Options 👻
Executive 7 Day - Current Vulnerability Type Matrix	Scan Results Policies Day - Exploitable Vulnerability Type Matrix Vulnerability Type Matrix Exploit % Metasoloit Core Impact Canvas Malware	Executive 7 Day - Mitigated Vulnerability Type Matrix
Critical O O O N/A O High 0 <	Addit Files Central Addit	Critical 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1<
Last Updated: 33 minutes ago	Last Updated: 32 minutes ago	Last Updated: 32 minutes ago
	Severity	
Last Updated: 34 minutes ago	Last Updated: 34 minutes ago	Last Updated: 33 minutes ago
Executive 7 Day - Current Vulnerability Trending by Severity	Executive 7 Day - Exploitable Vulnerability Trending by Severity	Executive 7 Day - Previously Mitigated Vulnerability Trend

 \bigcirc

The Active Scans window appears.

3. In the top right corner, click **+Add**.

SecurityCenter 😒	Dashboard	Reporting - Assets Workflo	ow ▼ Users ▼			🚢 qahead 🔫
Active Scans						+ Add
Active Scans Agent Scans	Scan Results Policies Audit File	s Credentials Blackout Wind	ows			< T 0
Name	Policy	Start Time 🕶	Schedule	Group	Owner	
Basic	BNS	Never	On Demand	Full Access	qahead	▶ ۞ -
Host Discovery	Host Discovery	Never	On Demand	Full Access	qahead	► 0 -

O

The **Add Active Scan** window appears.

4. In the left column, click **Credentials**.

The **Scan Credentials** section appears.

SecurityCenter	SC Dashboard -	Analysis 🔻	Scans 🔻	Reporting -	Assets	Workflow -	Users -	📤 qahead 👻
Add Active S	Scan							♦ Back
	General Settings Targets		Scan Ci	redentials				
	Credentials Post Scan							
	Submit Cancel							
https://172.26.36.163/#								

5. In the **Scan Credentials** section, click **+Add Credential**.

SecurityCenter sc Dashboard -	Analysis 👻 🗧	Scans - Reporting -	Assets Workflow -	Users →	🚢 qahead 🔫
Add Active Scan					← Back
Add Active Scan General Settings Targets Credentials Post Scan Submt Cancel	S	Can Credentials			▲ Back

0 -

A drop-down appears.

ecurityCenter 😒 Dashboard - Analysis	▼ Scans ▼ Reporting ▼ Assets Workflow ▼ Users ▼	🐣 qahead -
Add Active Scan		♦ Back
General	Scan Credentials	
Settings	Nothing Selected Select a credential type.	¢
Targets	Windows SSH	
Credentials Post Scan	SNMP Database	
Submit Cancel		

6. Select the system type.

The **Select Credential** option appears.

7. Click Select Credential.

Add Active Scan General General Settings Targets Credentials Post Scan
General Scan Credentials Settings Windows Targets BeyondTrust Credentials CyberArk Windows
Settings Targets Credentials Post Scan
Targets BeyondTrust Credentials CyberArk Windows
Post Scan
Submit Cancel

O

A drop-down appears.

- 8. Select the previously created credential.
- 9. Enter information for the **General**, **Settings**, **Targets**, and **Post Scan** sections.
- 10. Click **Submit**.

API Configuration

API Keys Setup

Enable API Access

Ø

API Keys Setup

To set up your API keys:

- 1. Log in to **BeyondInsight**.
- 2. Click Configuration.

The general configuration menu appears.

3. Click **API Registrations**.

The API configuration menu appears.

4. Click Create New API Registration.

The Create New API Registration menu appears.

- 5. In the API Registration name box, enter a name.
- 6. Click Create API Registration.
- 7. Add your account details for the API registration in the **Details** section.

Caution: Do not select any **Authentication Rule Options** when using the API with Tenable integrations, otherwise the integration fails.

- 8. Click **SAVE CHANGES**.
- 9. Configure Authentication Rules. This allows the Tenable IP ranges to pull credentials.
- 10. Click **CREATE RULE**.
- 11. Click **SAVE**.

Note: Once saved, the API Key is available for future requests.

Enable API Access

To enable **API Access**:

- 1. Log in to BeyondInsight.
- 2. Go to Managed Accounts.

MENU	BeyondInsight BeyondTrust			\$ 0
* •	View and manage assets and Smart Rules			
* * ô	Schedule a discovery or vulnerability scan.	Execute password requests and approvals.	View reports, manage subscriptions, and interactively explore data.	
¢\$ ≢ €	JOBS	MANAGED ACCOUNTS		

Ø

3. Click Edit Account.

Image: Protocol (1) Qa-ssh-staging Linux Q2/15/2018 11:35 AM Success No Delete Account Delete Account Delete Account Delete Account Delete Account Delete Account	E	root	qa-ssh-staging	Linux	02/07/2018 12:57 PM	Failed	03/01/2018 12:00 AM	Yes	; ⇒
	E	not-root	qa-ssh-staging	Linux	02/15/2018 11:35 AM	Success		No	Delete Account

4. Click Enable for API Access.

Managed Acco	ount Settings			
Settings	Synced Accounts			
			· · · · · · · · · · · · · · · · · · ·	
		System Name:	qa-ssh-staging	
		Account Name:	root	
		Authentication Type:	DSS 🛛 🗸 Edit Remove	
		Password:	****	Reset Password
		Confirm Password:	****	
		Allow Fallback to Password:		
		Password Rule:	Default Password Rule	
		Account Description:		
		Workgroup:	Any	
		Enable Login Account For SSH Sessions:		
		Enable for API access:	\checkmark	
	Use this account	's current password to change the password:		
		Cond Dolonco Notification Email to:	[
		Save	Cancel	

Ø

Additional Information

Elevation

Customized Report

About Tenable

0 -

Elevation

Elevation is used in BeyondInsight to handle privilege escalation for SSH accounts when performing scans. This option is used because some rules won't allow server login using root. The **Elevation** can be enforced on BeyondInsight at system level or account level.

O

Customized Report

You can build a customized report in BeyondInsight to import hosts from a CSV to scan in Tenable Security Center. The customized report defines the information needed for Tenable Security Center uploads.

To build the report:

- 1. Log in to BeyondInsight .
- 2. Navigate to Assets > Scan > Customize Report.
- 3. Select the **Parameters**.
- 4. Click **Run Report**.

Note: This report can be run on any of your previous discovery scans, exported as a CSV, and uploaded as scan targets in Tenable Security Center.

About Tenable

Tenable transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organ-izations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting <u>tenable.com</u>.