



Tenable Security Center and BeyondTrust Password Safe Integration Guide

Last Revised: December 04, 2023



Table of Contents

Welcome to Tenable Security Center for BeyondTrust	3
Integrations	4
Windows Integration	5
SSH Integration	8
Add the BeyondTrust Credential to a Scan	11
API Configuration	15
API Keys Setup	16
Enable API Access	17
Additional Information	21
Elevation	22
Customized Report	23
About Tenable	24



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.

[Windows Integration](#)

[SSH Integration](#)

[Add Credential to a Scan](#)



Windows Integration

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

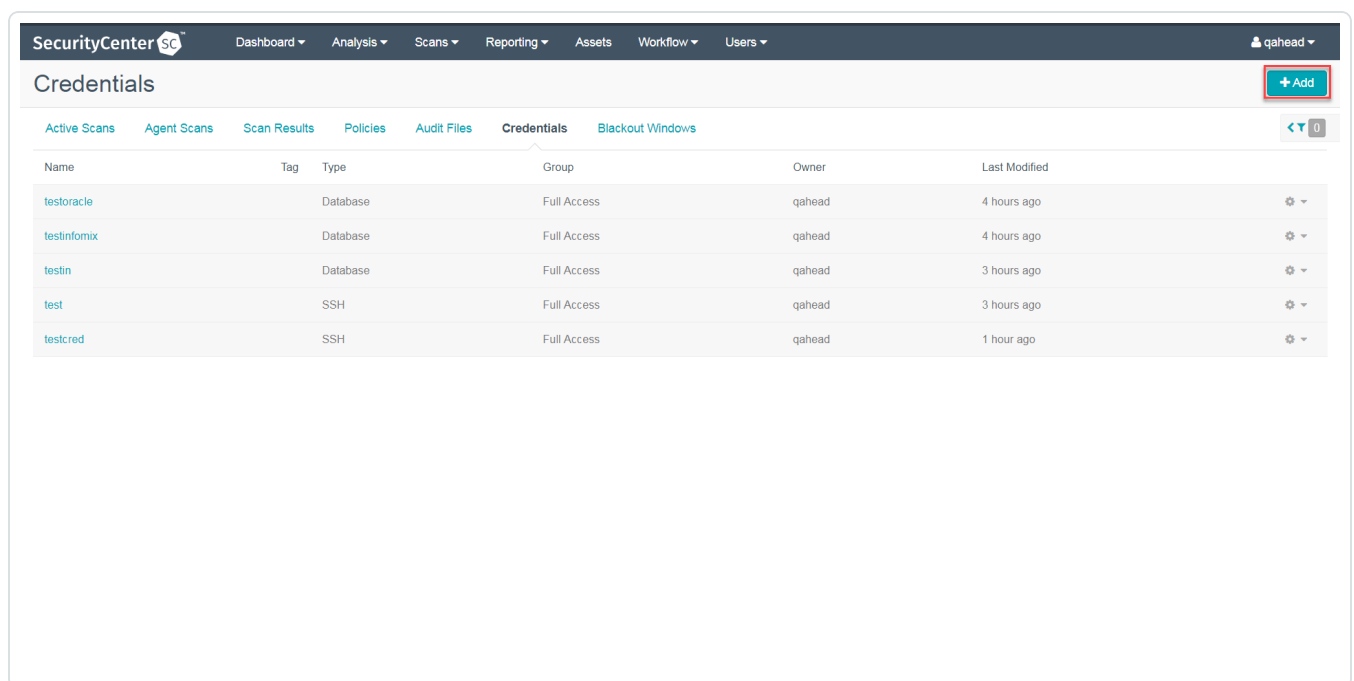
1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scans**.

A drop-down appears.

3. Click **Credentials**.


The **Credentials** window opens.


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



The **Add Credential** window opens.

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



SecurityCenter  Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets ▾ Workflow ▾ Users ▾ qahead ▾

Add Credential ← 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

The **Add Credential** configuration page appears.

SecurityCenter  Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets ▾ Workflow ▾ Users ▾ qahead ▾

Add Credential ← Back

General

Name*

Description

Tag

BeyondTrust Credential

Username*

Domain

BeyondTrust host*


BeyondTrust port*

BeyondTrust API key*

Checkout duration*

Use SSL ☐

Verify SSL Certificate ☐

 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 [Tenable Security Center User Guide](#) to get detailed descriptions for each option.
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:

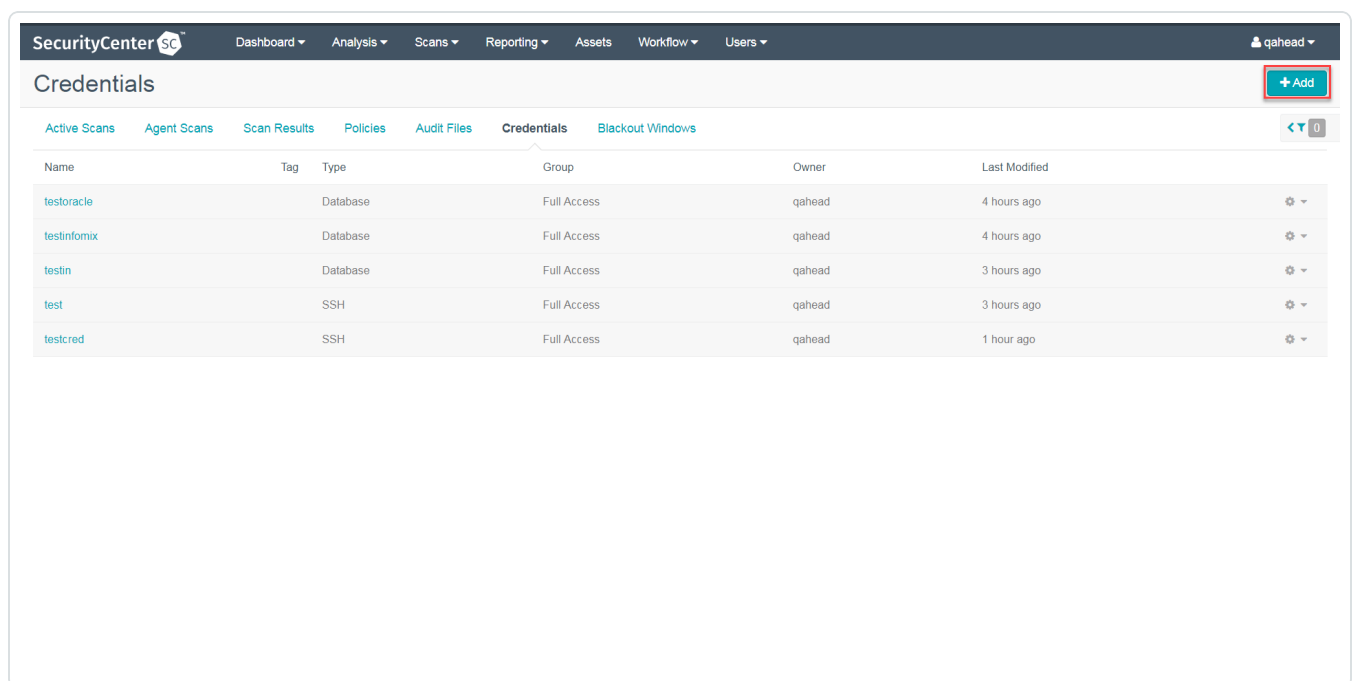
1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scans**.

A drop-down appears.

3. Click **Credentials**.


The **Credentials** window appears.

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



The **Add Credential** window appears.

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



SecurityCenterSM Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾ qahead ▾

Add Credential ← 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

The **Add Credential** configuration page appears.

SecurityCenterSM 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 ☐



6. In the top section, enter a descriptive **Name** (required), **Description** (optional), and **Tag** (optional).
7. Configure each field for **SSH** authentication. See the [Tenable Security Center User Guide](#) to get detailed descriptions for each option.
8. Click **Save**.
9. Next, follow the steps for [adding the credential to a scan](#).



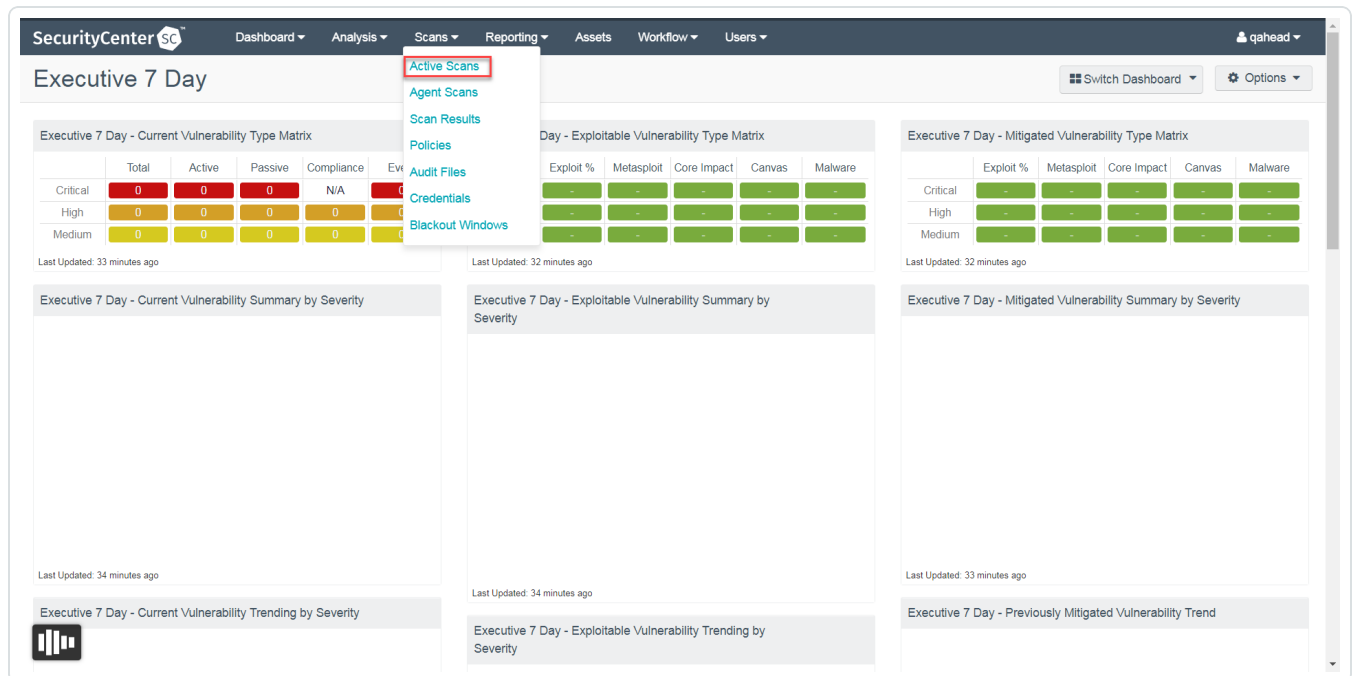
Add the BeyondTrust Credential to a Scan

To add the BeyondTrust credential to the scan:

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

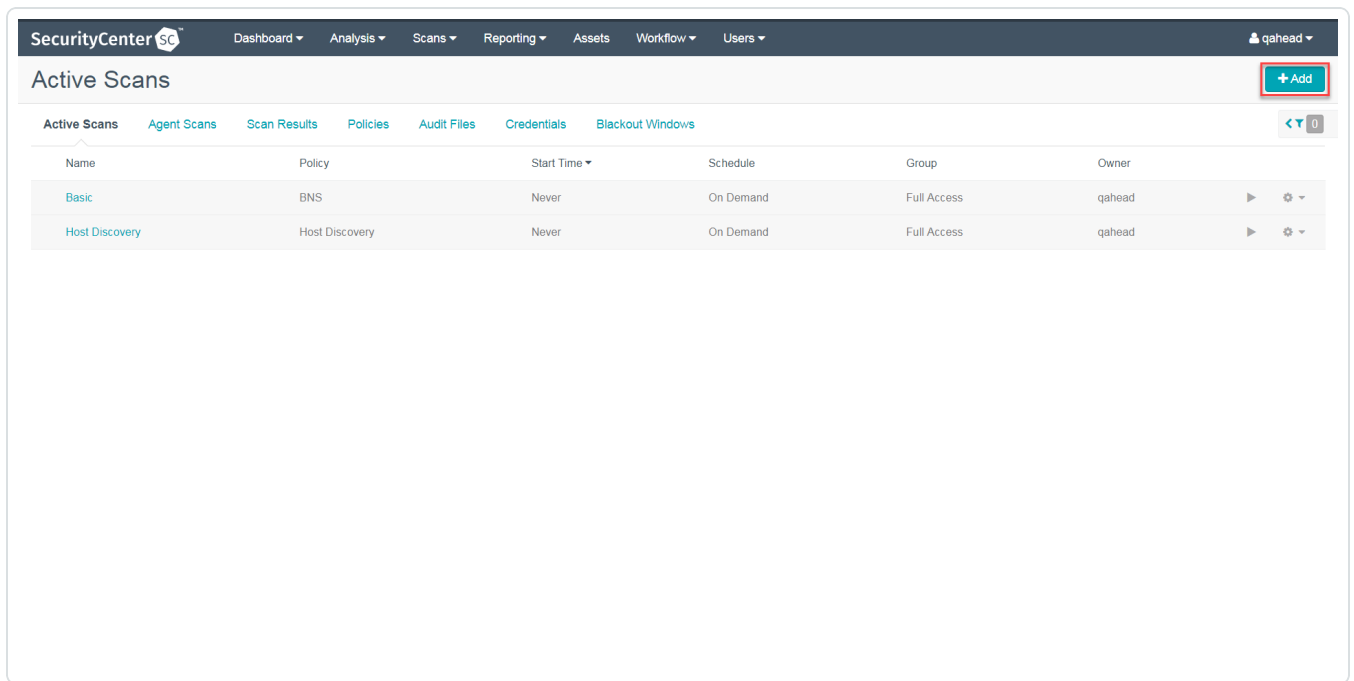
A drop-down appears.

2. Select **Active Scans**.



The **Active Scans** window appears.

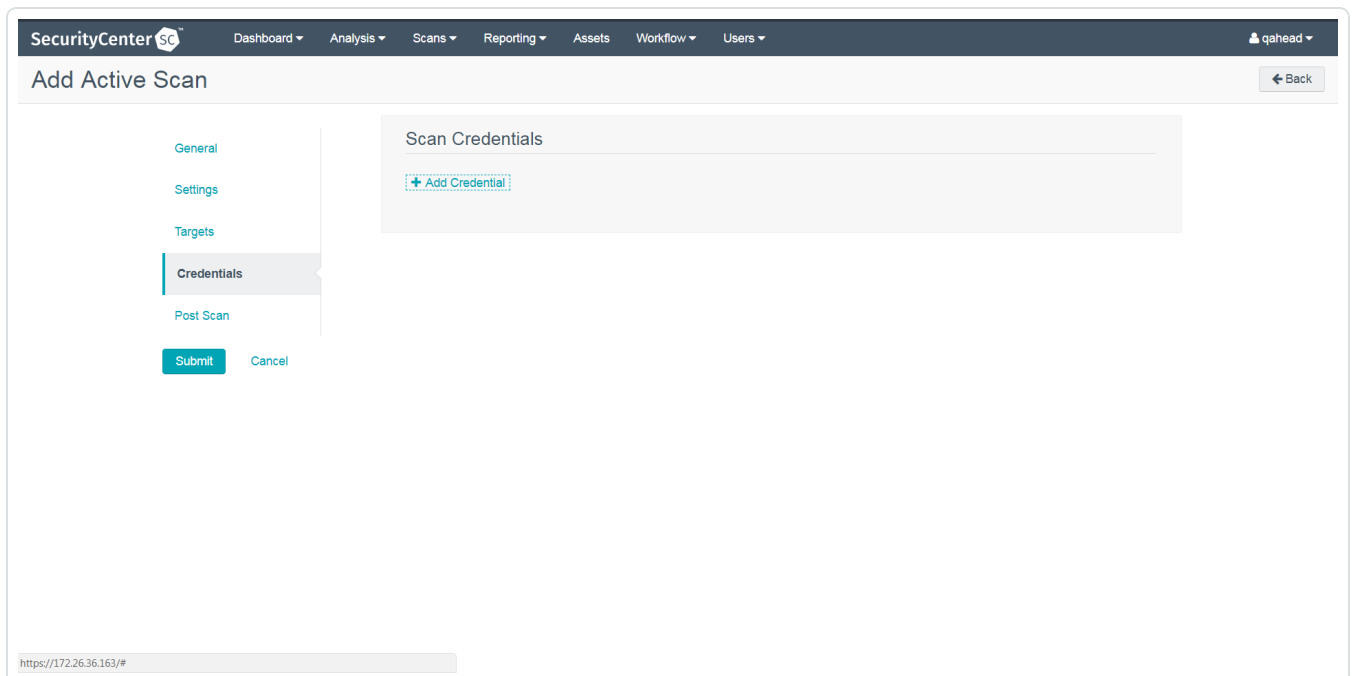
3. In the top-right corner, click **+Add**.



The **Add Active Scan** window appears.

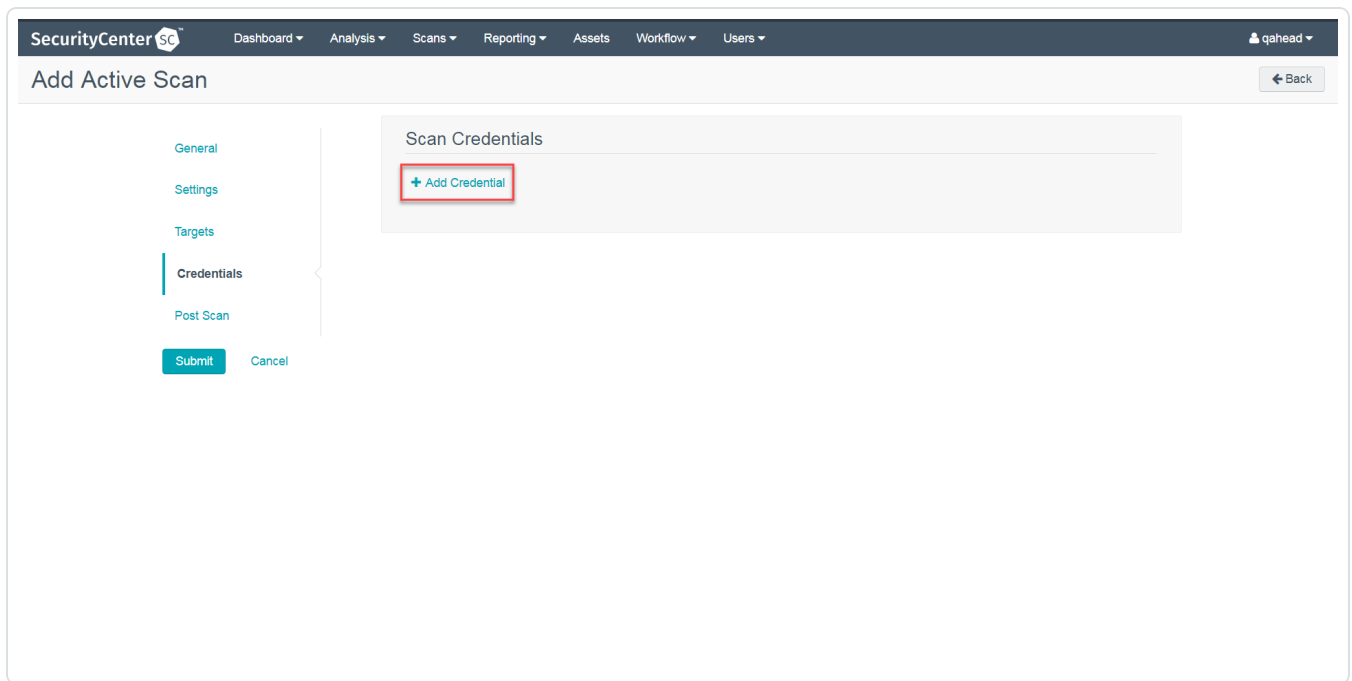
4. In the left column, click **Credentials**.

The **Scan Credentials** section appears.

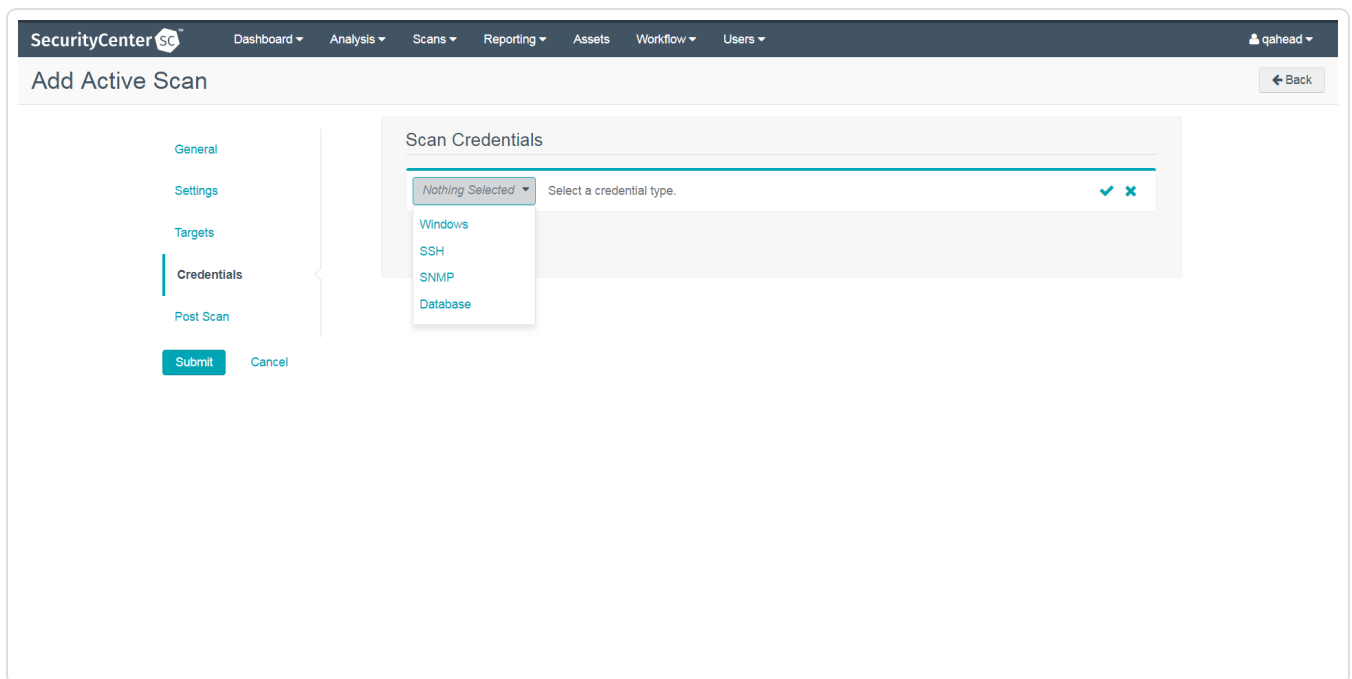




5. In the **Scan Credentials** section, click **+Add Credential**.



A drop-down appears.



6. Select the system type.

The **Select Credential** option appears.



7. Click **Select Credential**.

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](#)



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 API Registration**.
5. Select **API Key Policy**.
6. Enter a name for the API Registration.

Note: This name does not need to match your username. You do not need to enter anything under **Key**, it is automatically generated.

Caution: Do not select any **Authentication Rule Options** when using the API with Tenable integrations. This may cause the integration to fail.

7. Configure **Authentication Rules** by clicking **Add Authentication Rule**. Configure an IP address or range of IP addresses of one or more scanners.
8. Click **Create Registration**.

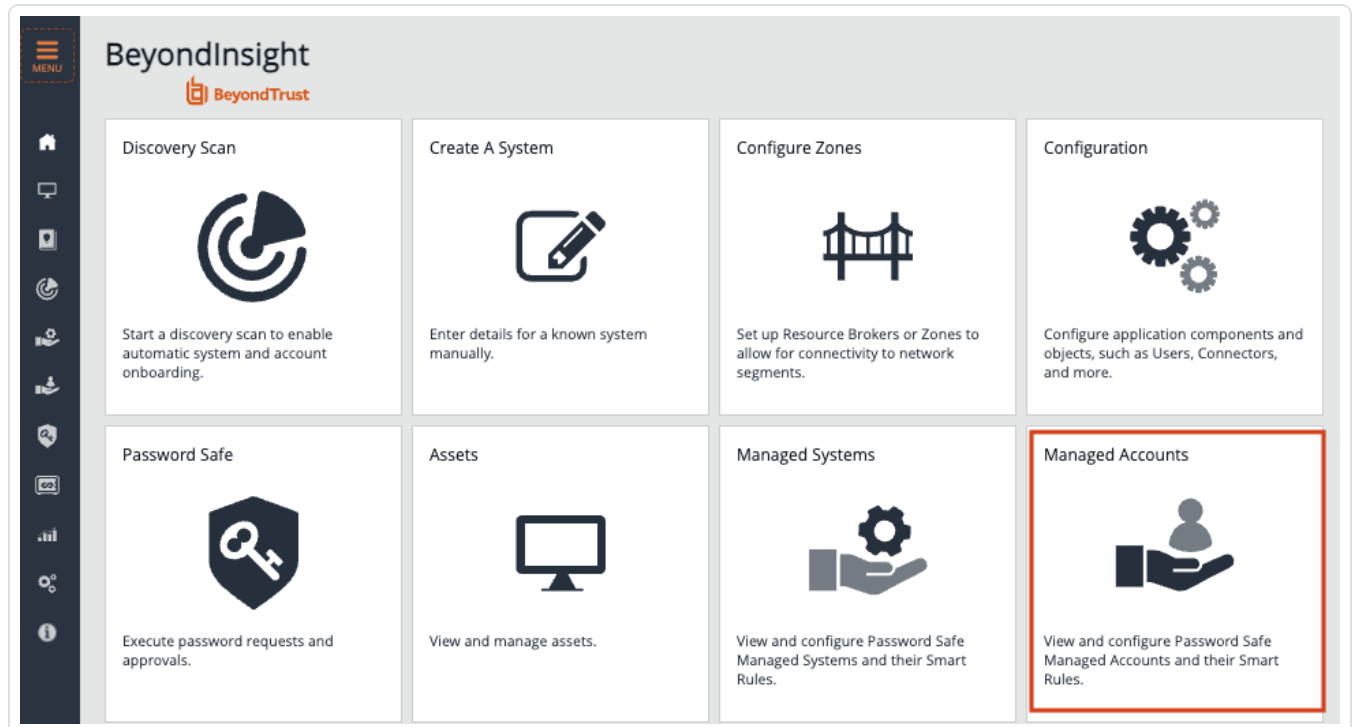
Once saved, the API Key is available for future requests.



Enable API Access

To enable **API Access**:

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



3. Click **Edit Account**.



1 item (0 selected | [Select all 1 rows](#))

<input type="checkbox"/>	Account	Description	System	Domain	Platform	Last Char
<input type="checkbox"/>	sample-account	--	Ubuntu SSH Key w/ Pass...	--	Linux	Nov 13, 20

Go to Advanced Details...

Edit Account...

Delete Account

Test Password

Password History...

Public Key

4. Click the **API Enabled** option.



Edit Sample-Account



[View Advanced Details...](#)

Managed System

Ubuntu SSH Key w/ Password

Entity Type

Asset

Platform

Linux



Collapse All



Expand All

Identification

Name

sample-account

Description

Workgroup

Inherit from Managed System

Credentials

Automatic Password Change Options

Account Settings





5. Click **Save**.



Additional Information

[Elevation](#)

[Customized Report](#)

[About Tenable](#)



Elevation

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



Customized Report

You can build a customized report in BeyondInsight to import hosts from a .csv file 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 file, 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, organizations 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 Tenable Nessus and leaders in continuous monitoring, by visiting tenable.com.