



Tenable Security Center and BeyondTrust Password Safe Integration Guide

Last Revised: August 14, 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	19
Elevation	20
Customized Report	21
About Tenable	22



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:

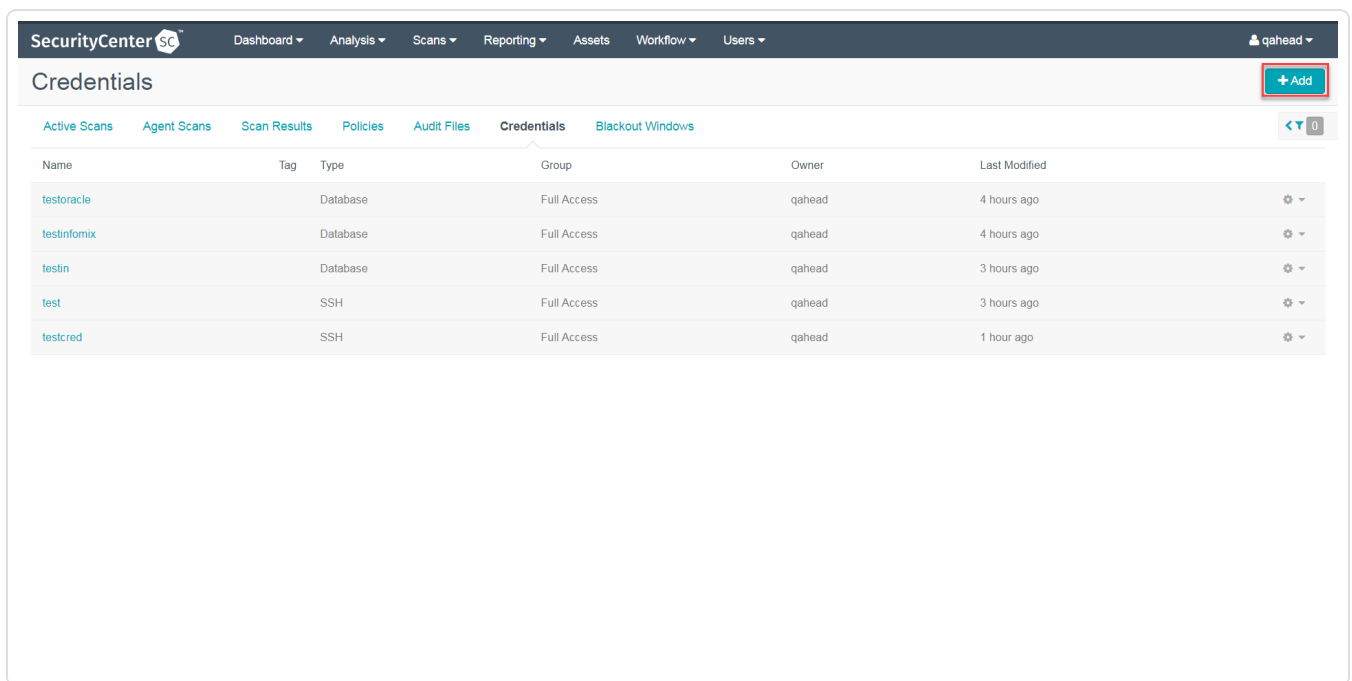
1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scans**.

A drop-down appears.

3. Click **Credentials**.

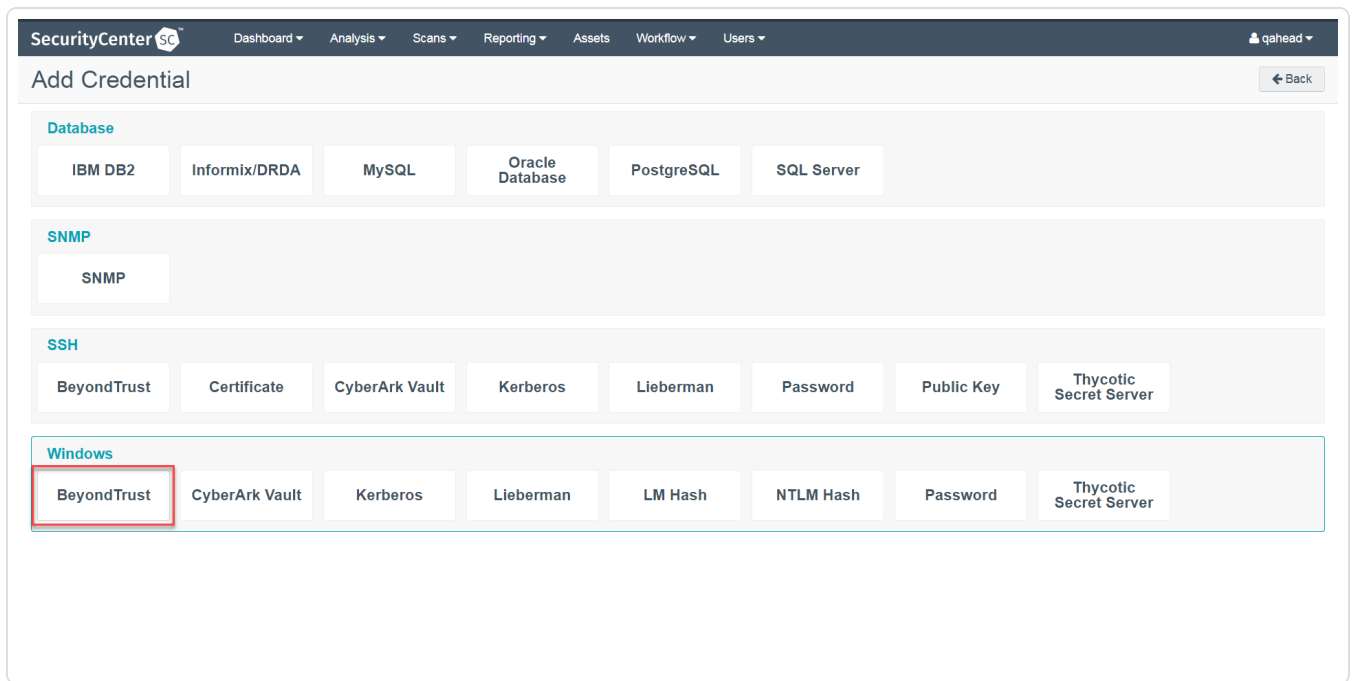
The **Credentials** window opens.

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

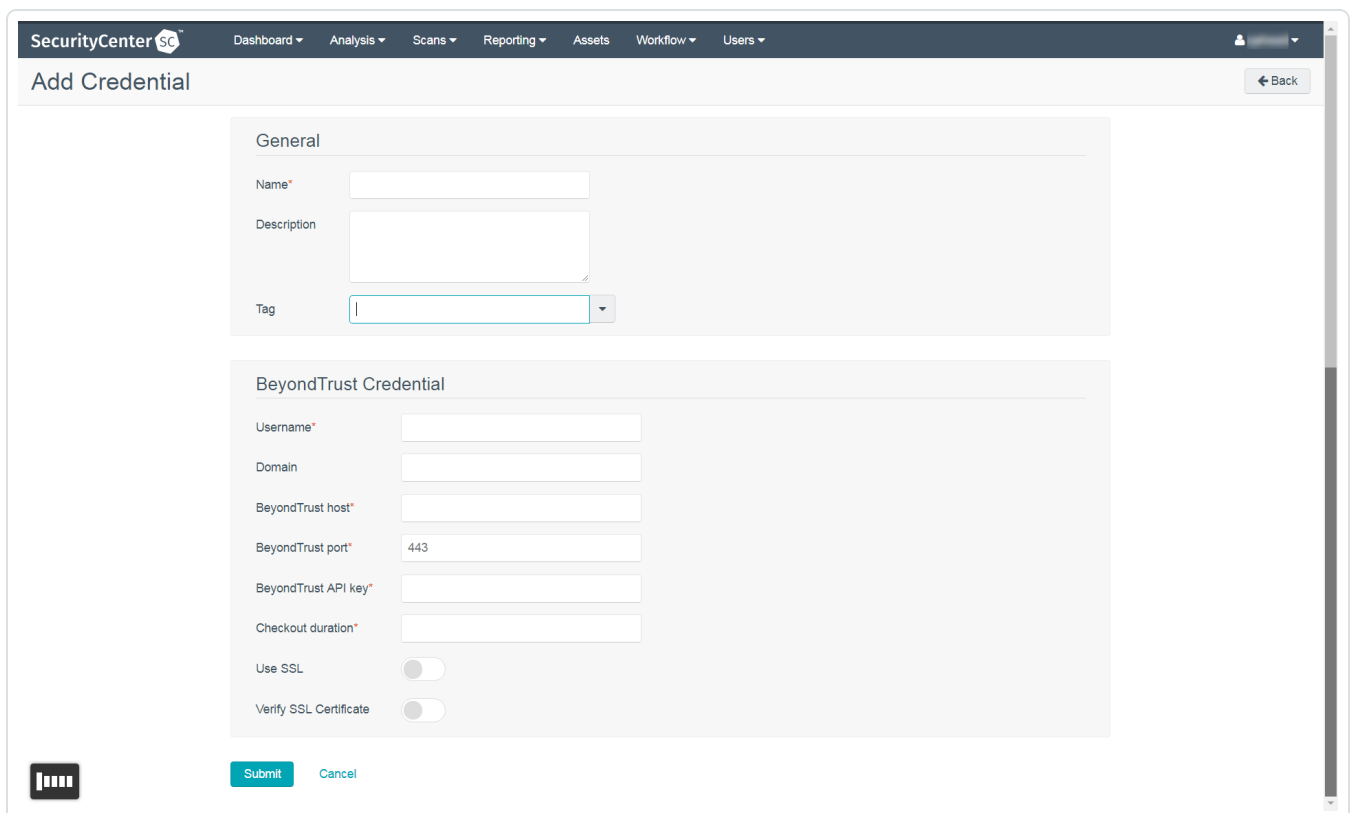


The **Add Credential** window opens.

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



The **Add Credential** configuration page appears.





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.

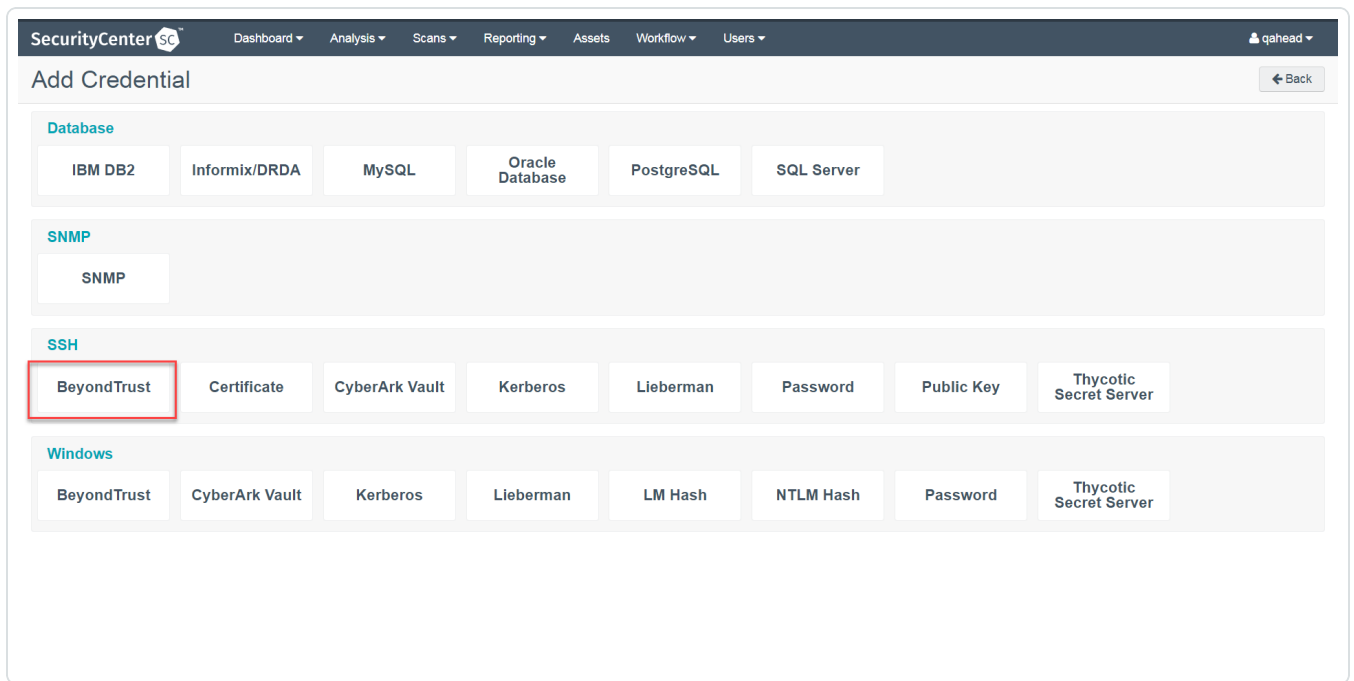
4. Click the **+ Add** button.

The screenshot shows the Tenable Security Center interface. The top navigation bar includes 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', 'Workflow', and 'Users'. The user 'qahead' is logged in. The main content area is titled 'Credentials' and has a '+ Add' button highlighted with a red box. Below the title are tabs for 'Active Scans', 'Agent Scans', 'Scan Results', 'Policies', 'Audit Files', 'Credentials', and 'Blackout Windows'. A table lists the following credentials:

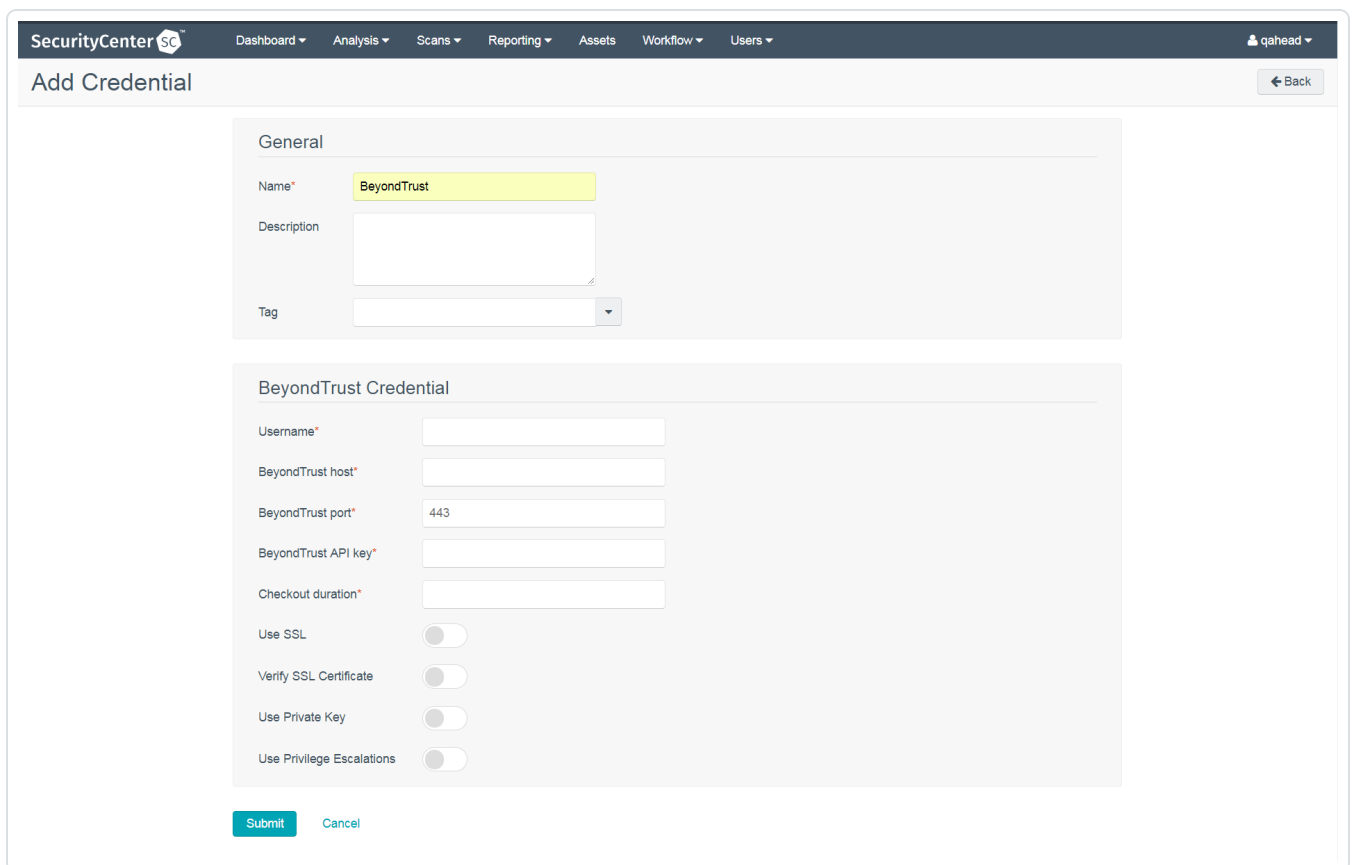
Name	Tag	Type	Group	Owner	Last Modified
testoracle		Database	Full Access	qahead	4 hours ago
testinfomix		Database	Full Access	qahead	4 hours ago
testin		Database	Full Access	qahead	3 hours ago
test		SSH	Full Access	qahead	3 hours ago
testcred		SSH	Full Access	qahead	1 hour ago

The **Add Credential** window appears.

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



The **Add Credential** configuration page appears.





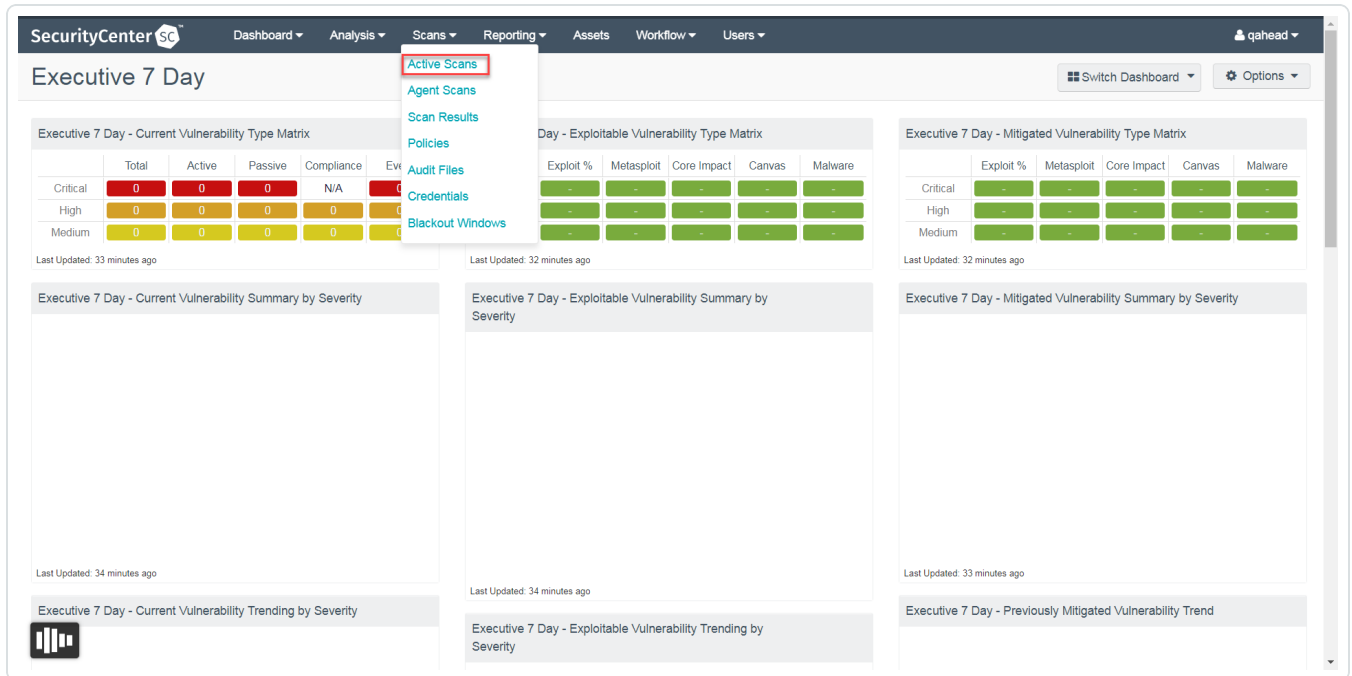
6. In the top section, enter a descriptive **Name** (required), **Description** (optional), and **Tag** (optional).
7. Configure each field for **SSH** authentication. See the [Tenable Security Center User Guide](#) to get detailed descriptions for each option.
8. Click **Save**.
9. Next, follow the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



Add the BeyondTrust Credential to a Scan

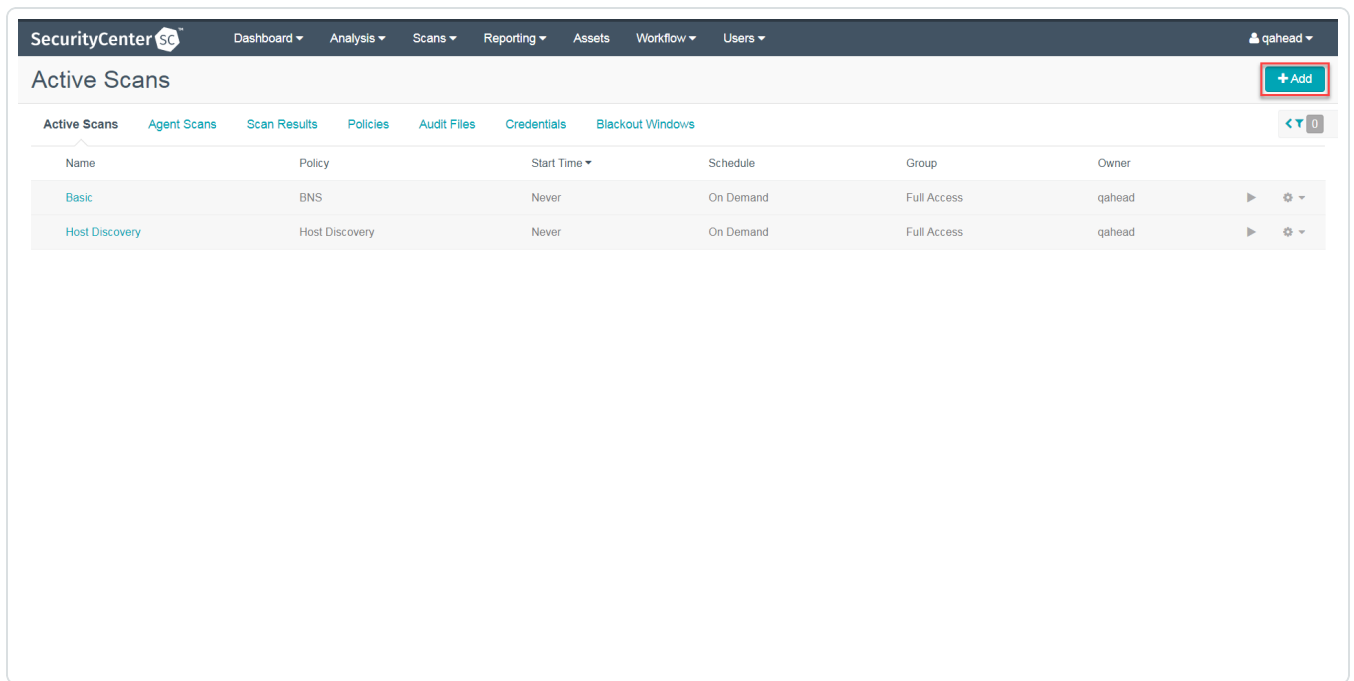
To add the BeyondTrust credential to the scan:

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.

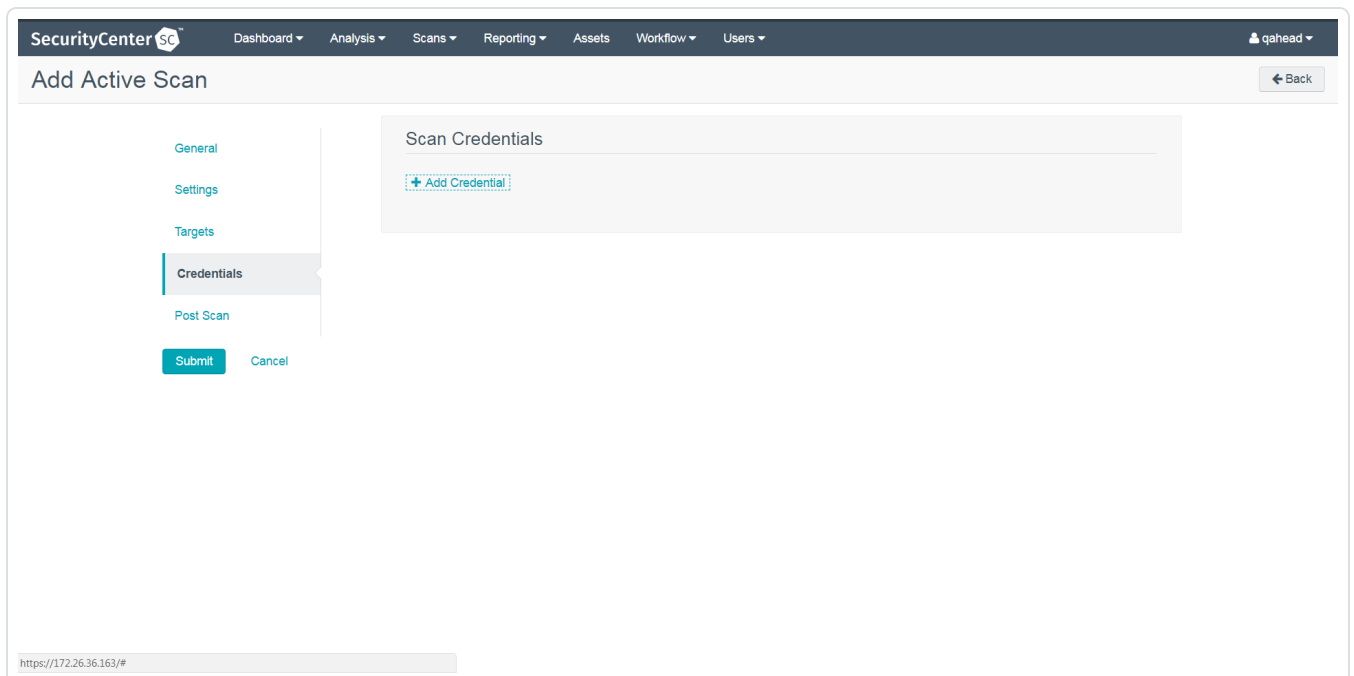
3. In the top right corner, click **+Add**.



The **Add Active Scan** window appears.

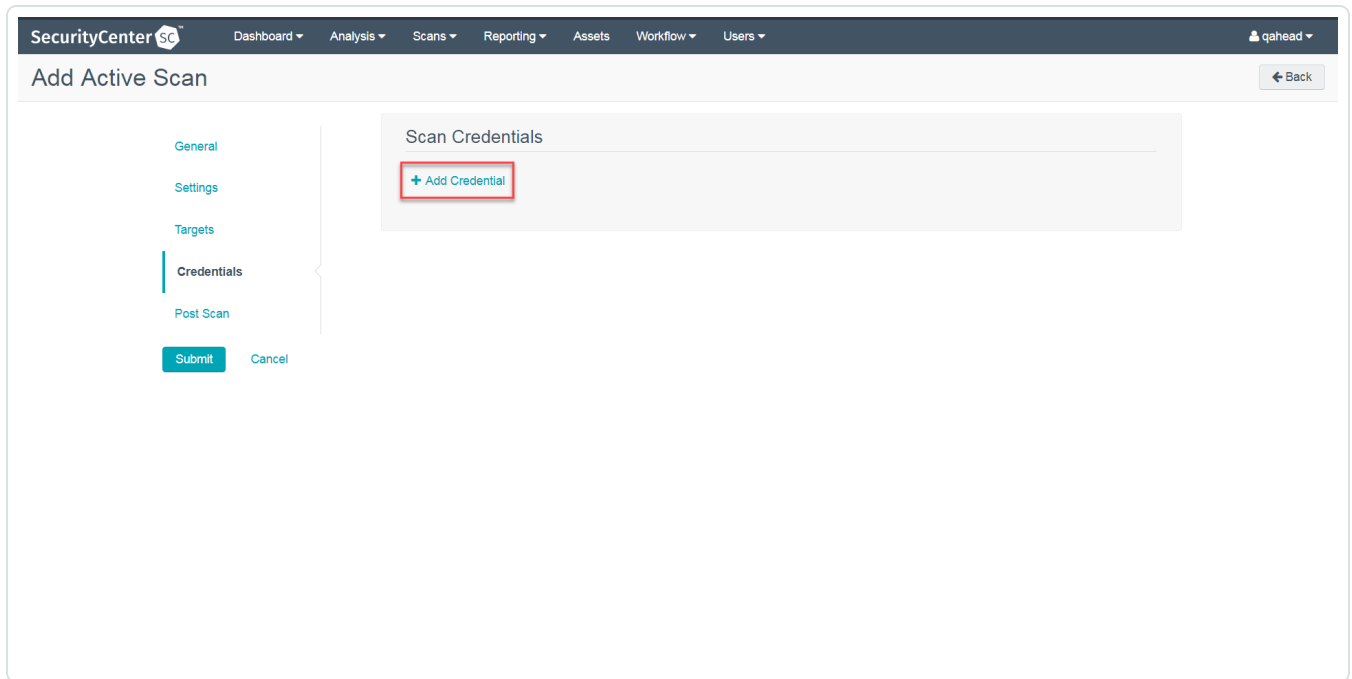
4. In the left column, click **Credentials**.

The **Scan Credentials** section appears.

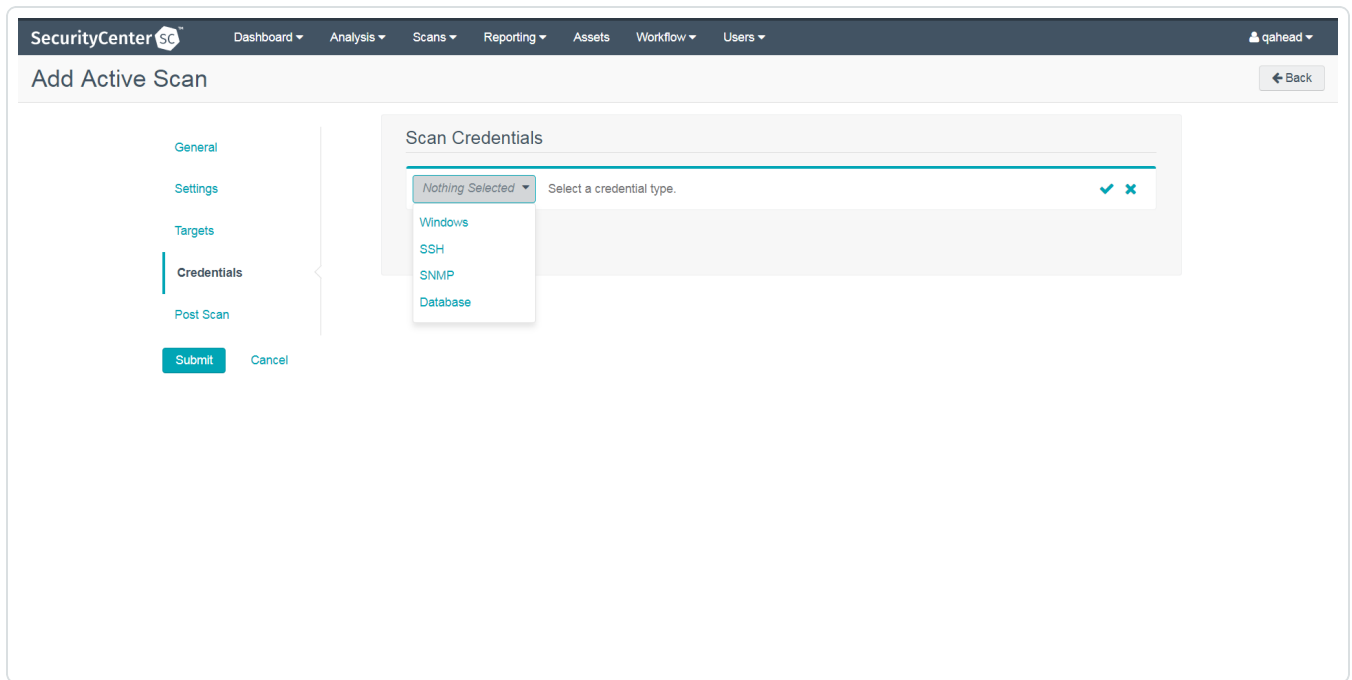




5. In the **Scan Credentials** section, click **+Add Credential**.



A drop-down appears.

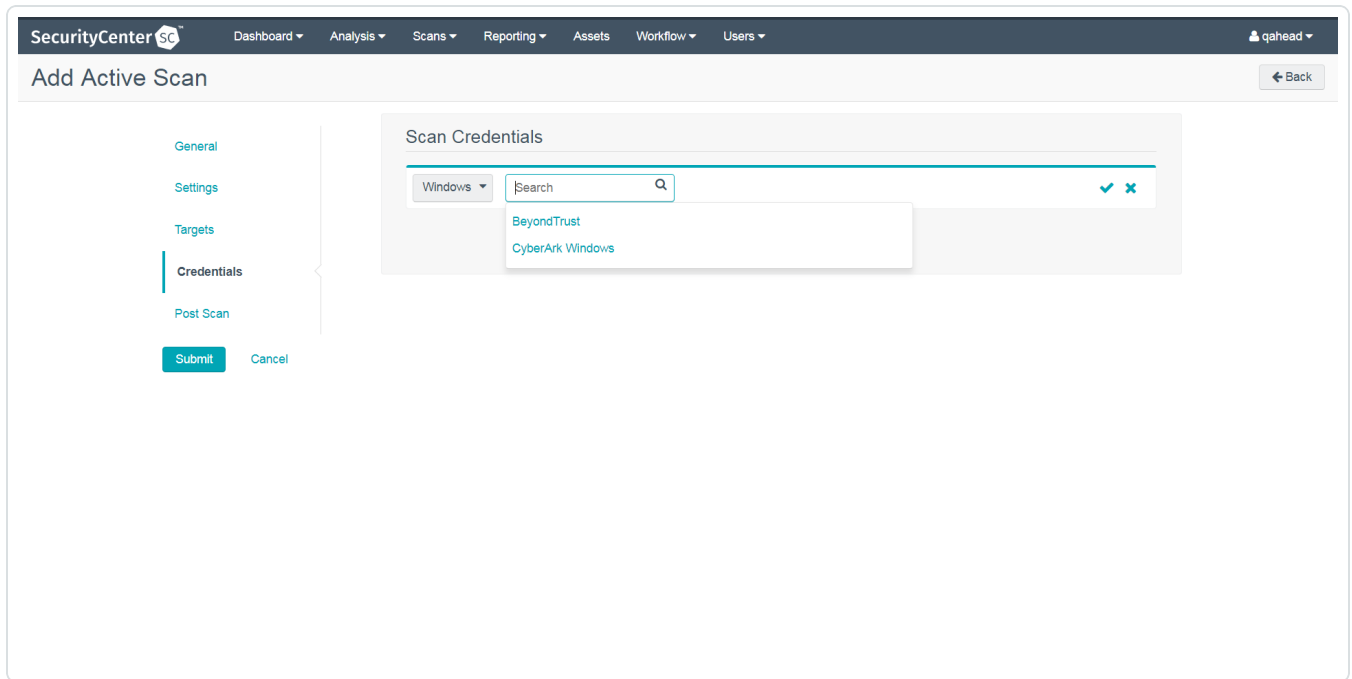


6. Select the system type.

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 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**.

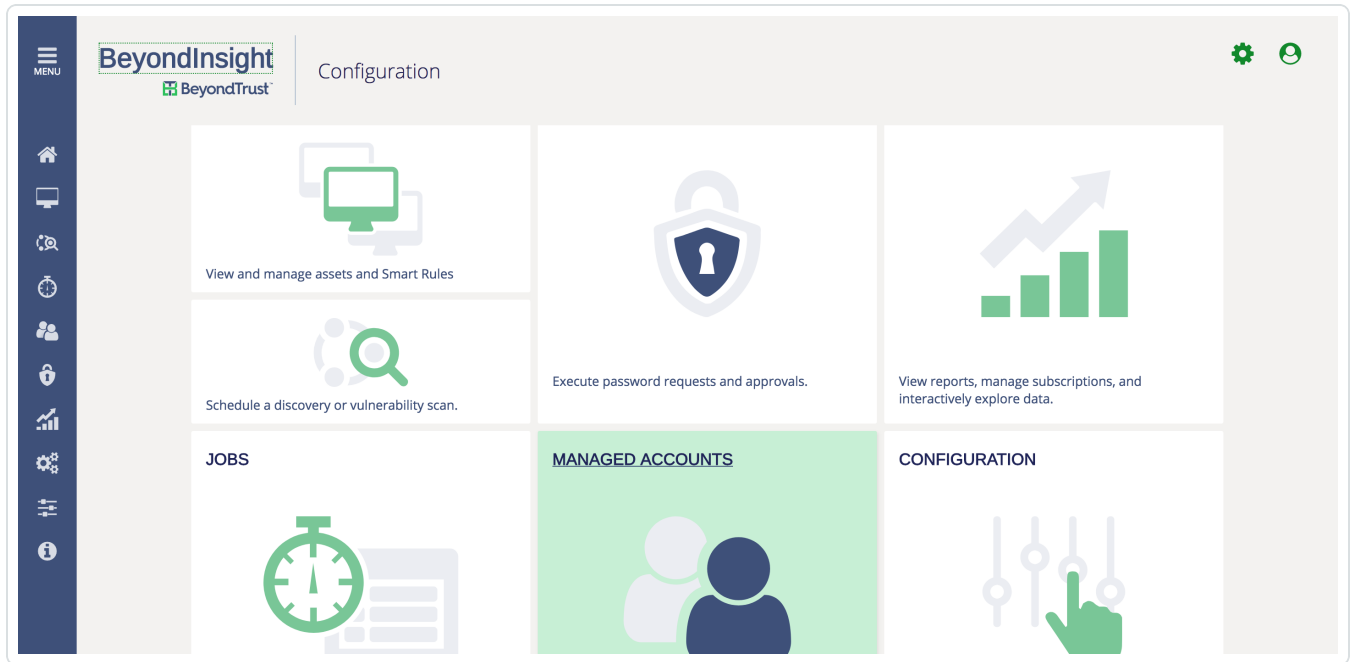
Note: Once saved, the API Key is available for future requests.



Enable API Access

To enable **API Access**:

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



3. Click **Edit Account**.

<input type="checkbox"/>	root	qa-ssh-staging	Linux	02/07/2018 12:57 PM	Failed	03/01/2018 12:00 AM	Yes	
<input type="checkbox"/>	not-root	qa-ssh-staging	Linux	02/15/2018 11:35 AM	Success		No	Edit Account Delete Account



4. Click **Enable for API Access**.

Managed Account Settings

Settings Synced Accounts

System Name:

Account Name:

Authentication Type: **DSS**

Password:

Confirm Password:

Allow Fallback to Password:

Password Rule:

Account Description:

Workgroup:

Enable Login Account For SSH Sessions:

Enable for API access:

Use this account's current password to change the password:

Send Release Notification Email to:



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 won't 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 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, 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 Nessus and leaders in continuous monitoring, by visiting tenable.com.