



How-to Guide: Tenable SecurityCenter for BeyondTrust

Last Revised: November 16, 2018

Table of Contents

Welcome to SecurityCenter 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	18
Additional Information	20
Elevation	21
Customized Report	22
About Tenable	23

Welcome to SecurityCenter for BeyondTrust

This document describes how to configure SecurityCenter for integration with the BeyondTrust PowerBroker Password Safe (BeyondTrust).

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 SecurityCenter, customers have more choice and flexibility.

The benefits of integrating SecurityCenter with BeyondTrust include:

- Credential updates directly in SecurityCenter, 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:

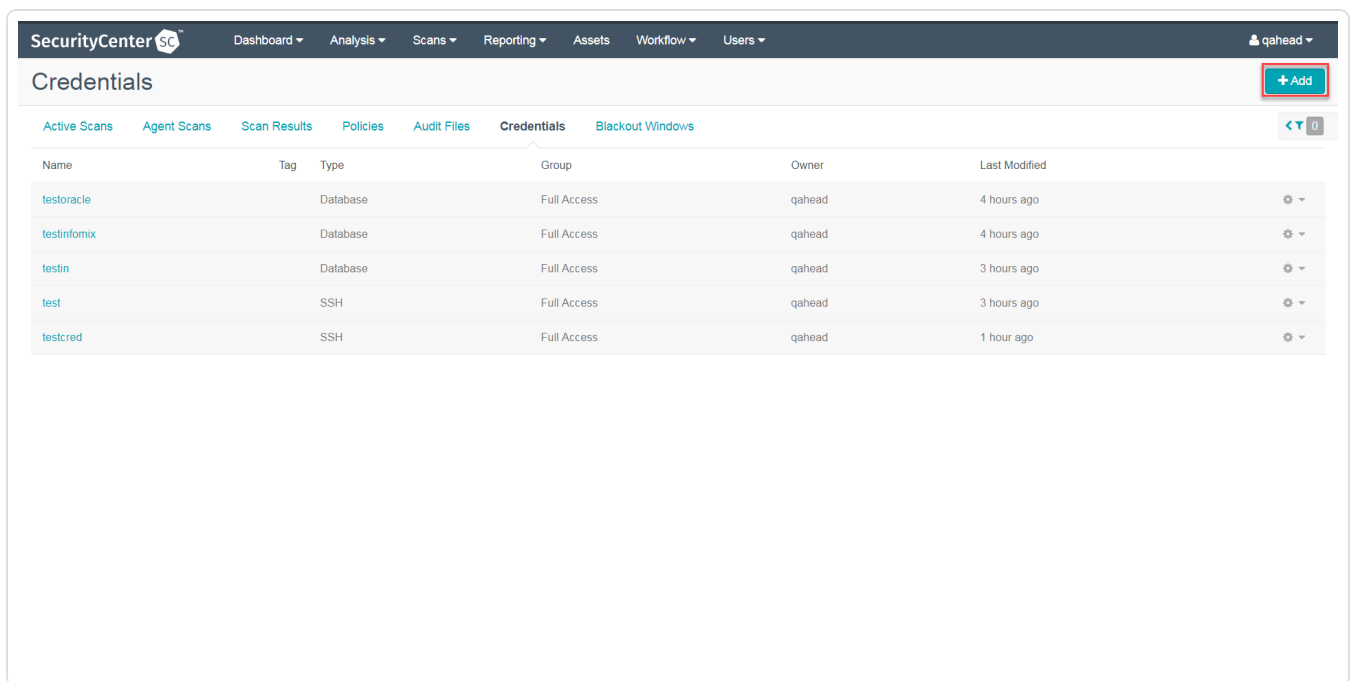
1. Log in to SecurityCenter.
2. In the top navigation bar, click **Scans**.

A drop-down appears.

3. Click **Credentials**.

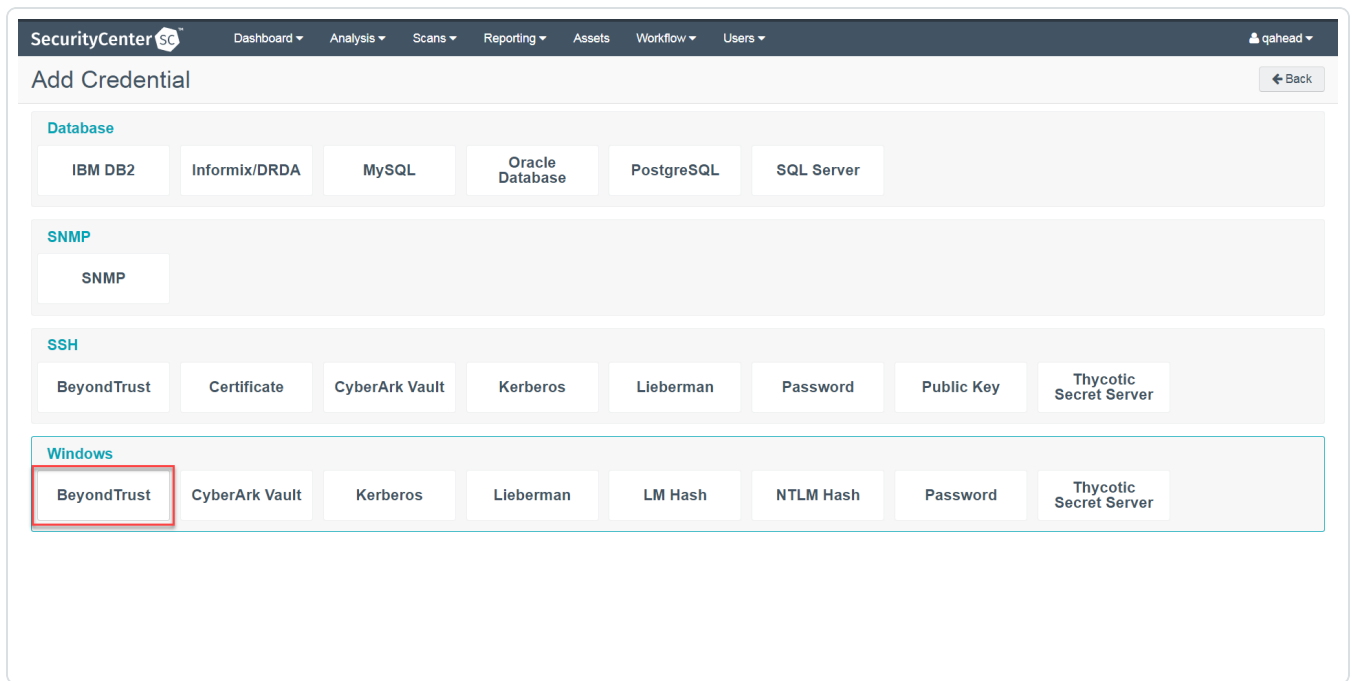
The **Credentials** window opens.

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

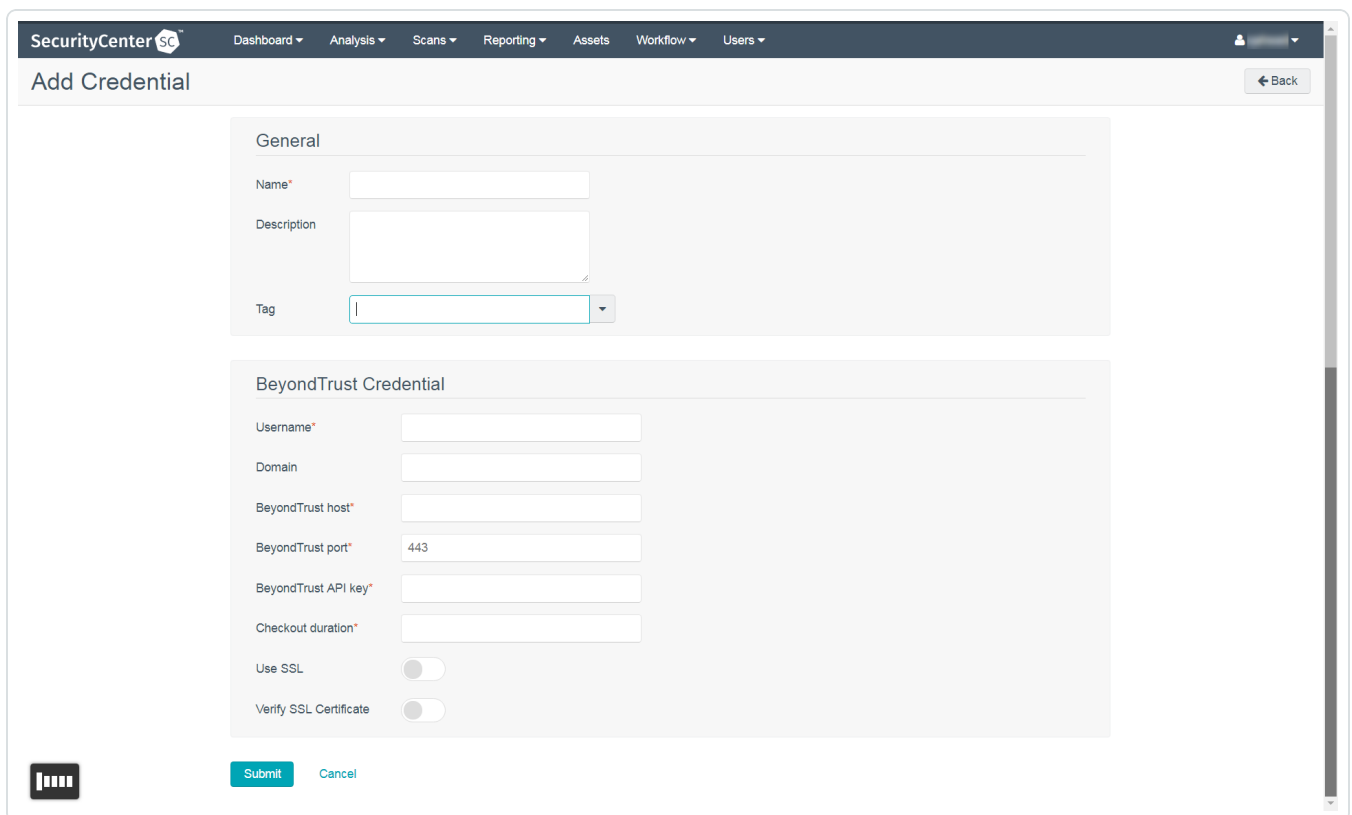


The **Add Credential** window opens.

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 [SecurityCenter 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:

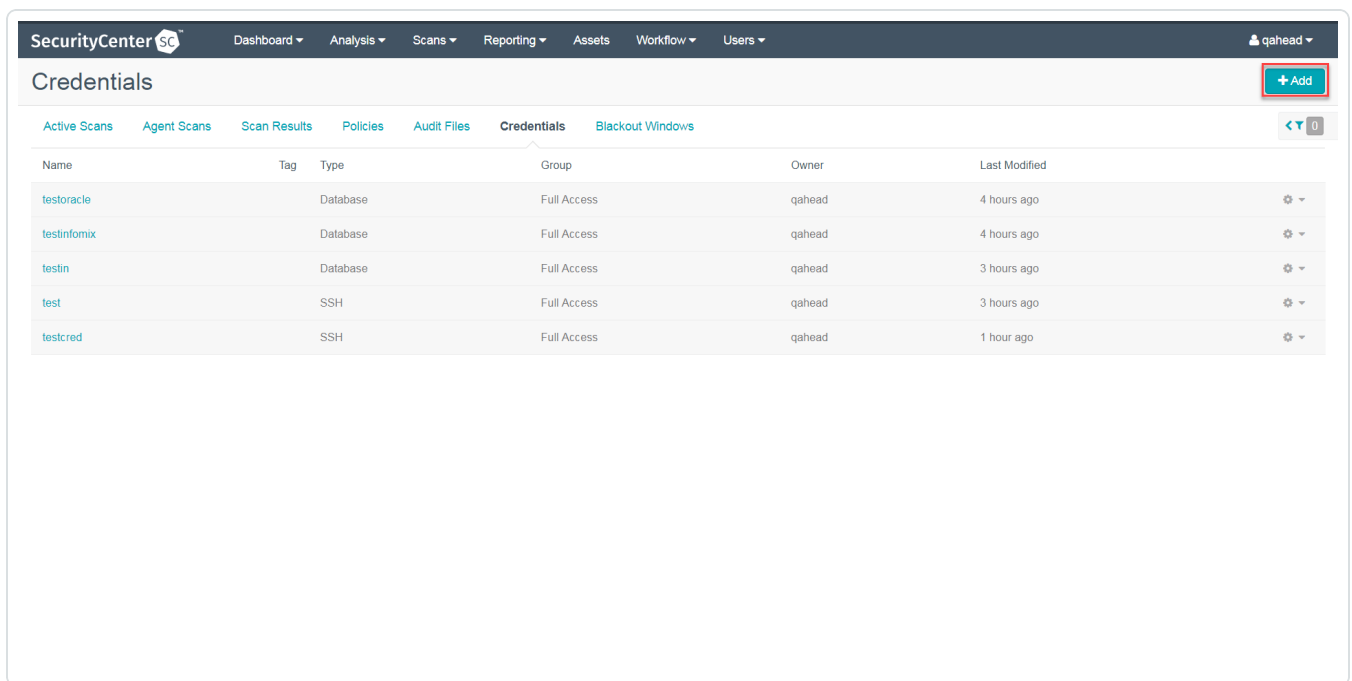
1. Log in to SecurityCenter.
2. In the top navigation bar, click **Scans**.

A drop-down appears.

3. Click **Credentials**.

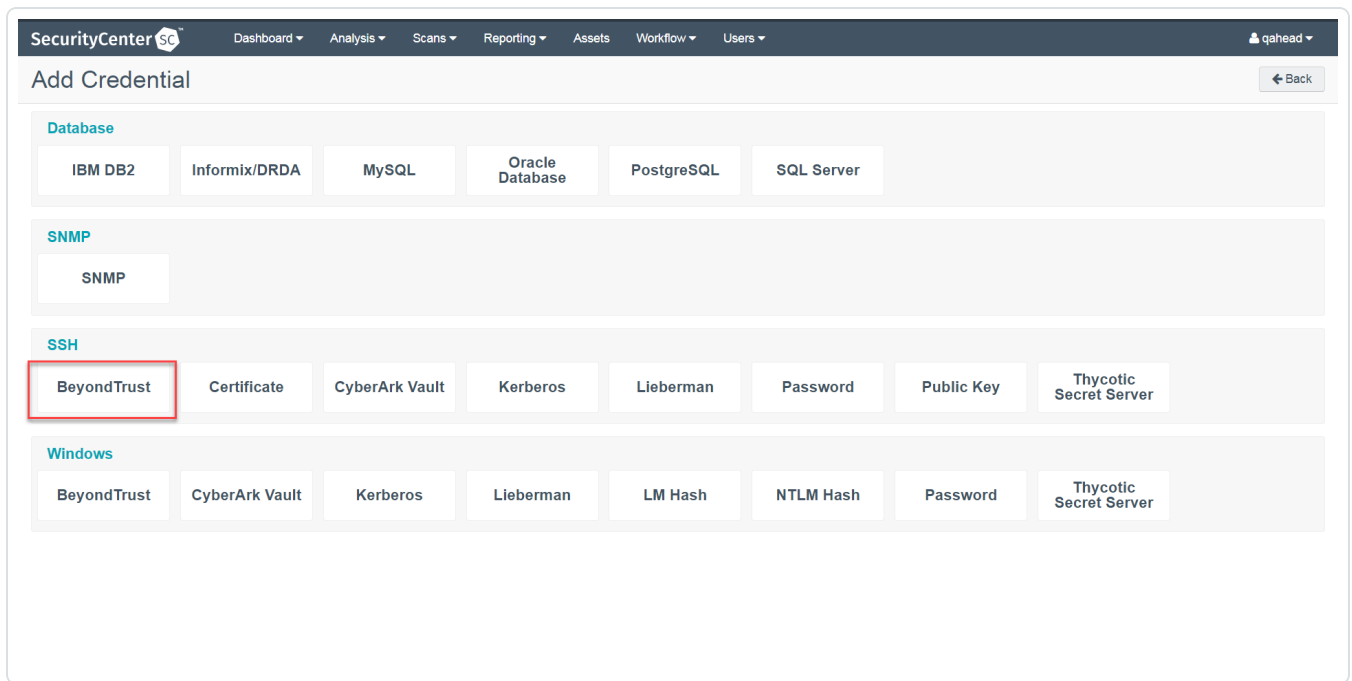
The **Credentials** window appears.

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

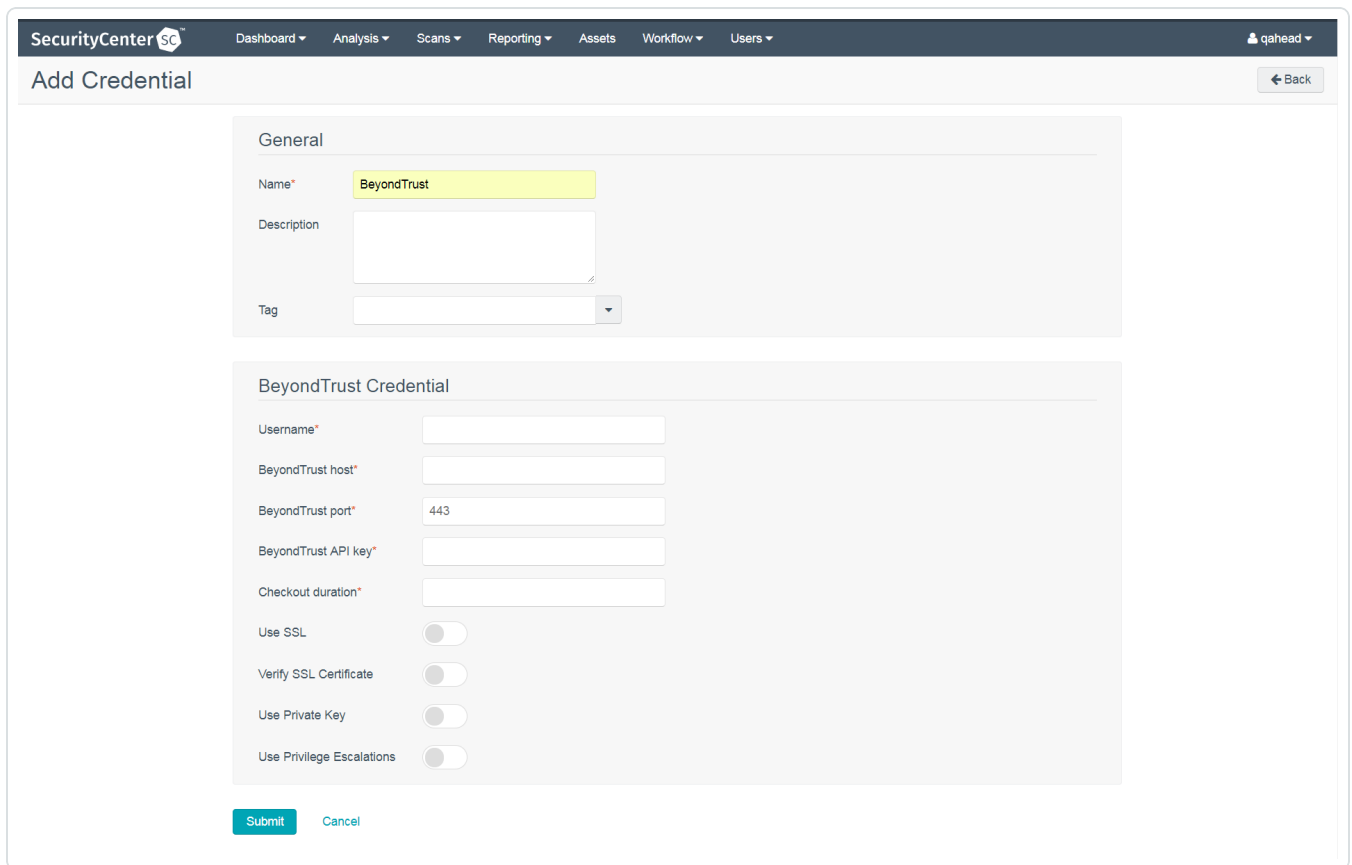


The **Add Credential** window appears.

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



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 [SecurityCenter User Guide](#) to get detailed descriptions for each option.
8. Click **Save**.
9. Next, follow the steps for [adding the credential to a scan](#).

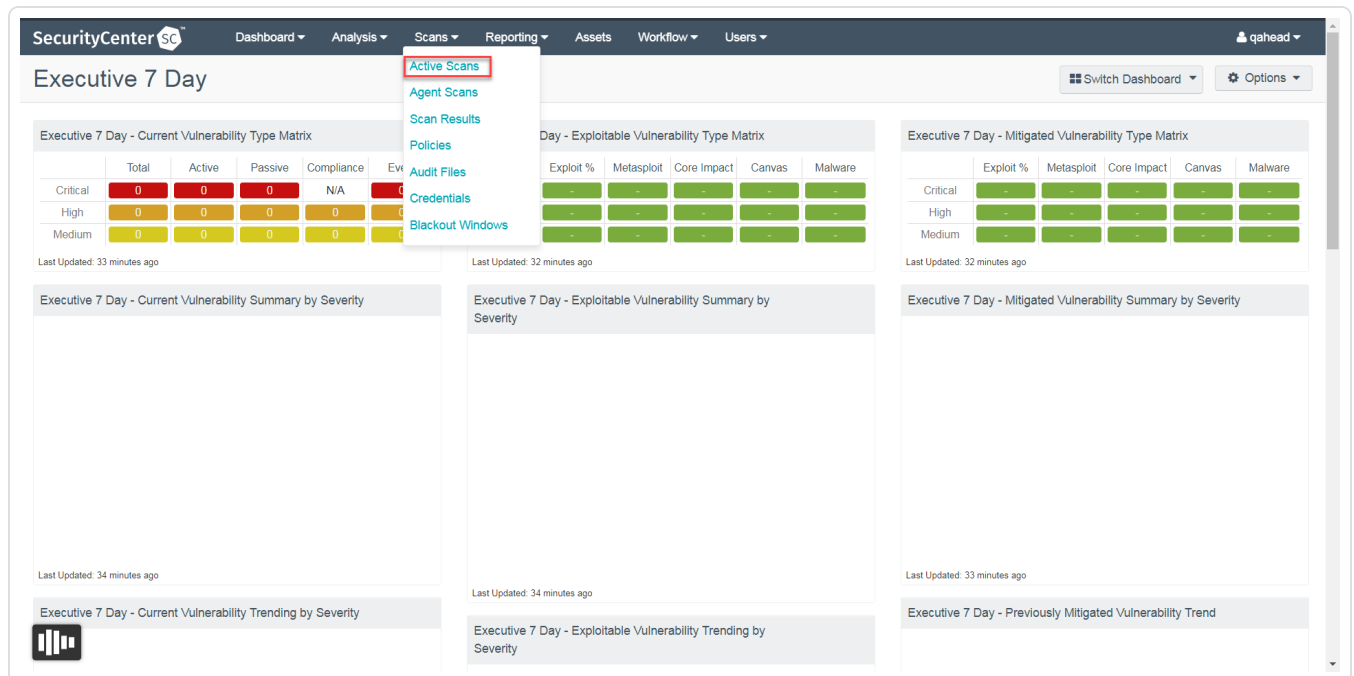
Add the BeyondTrust Credential to a Scan

To add the BeyondTrust credential to the scan:

1. In the top navigation bar, click **Scans**.

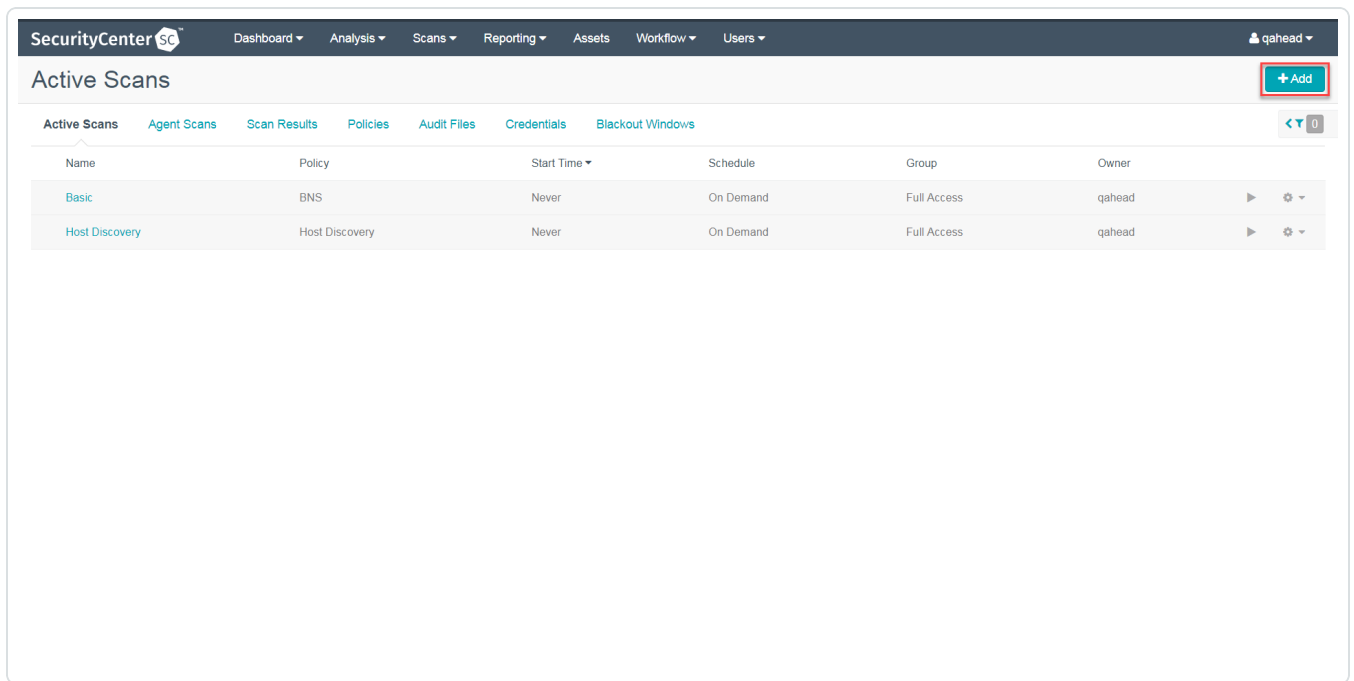
A drop-down appears.

2. Select **Active Scans**.



The **Active Scans** window appears.

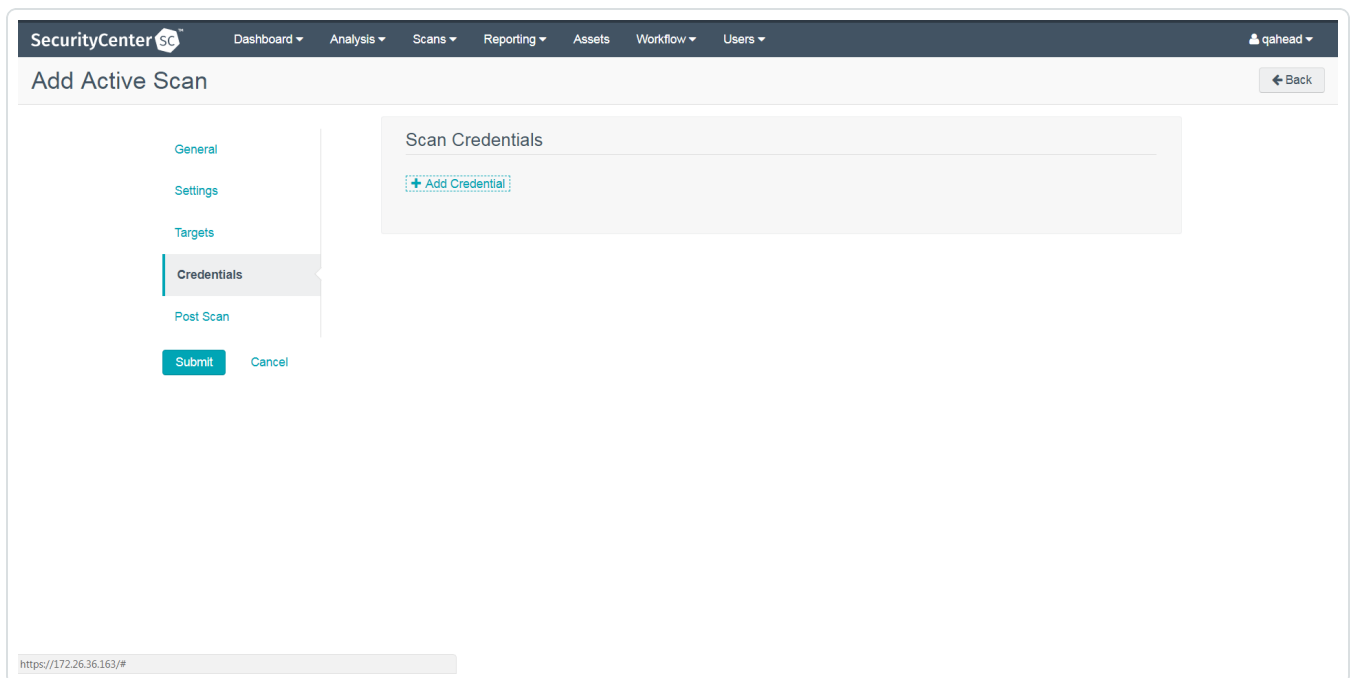
3. In the top right corner, click **+Add**.



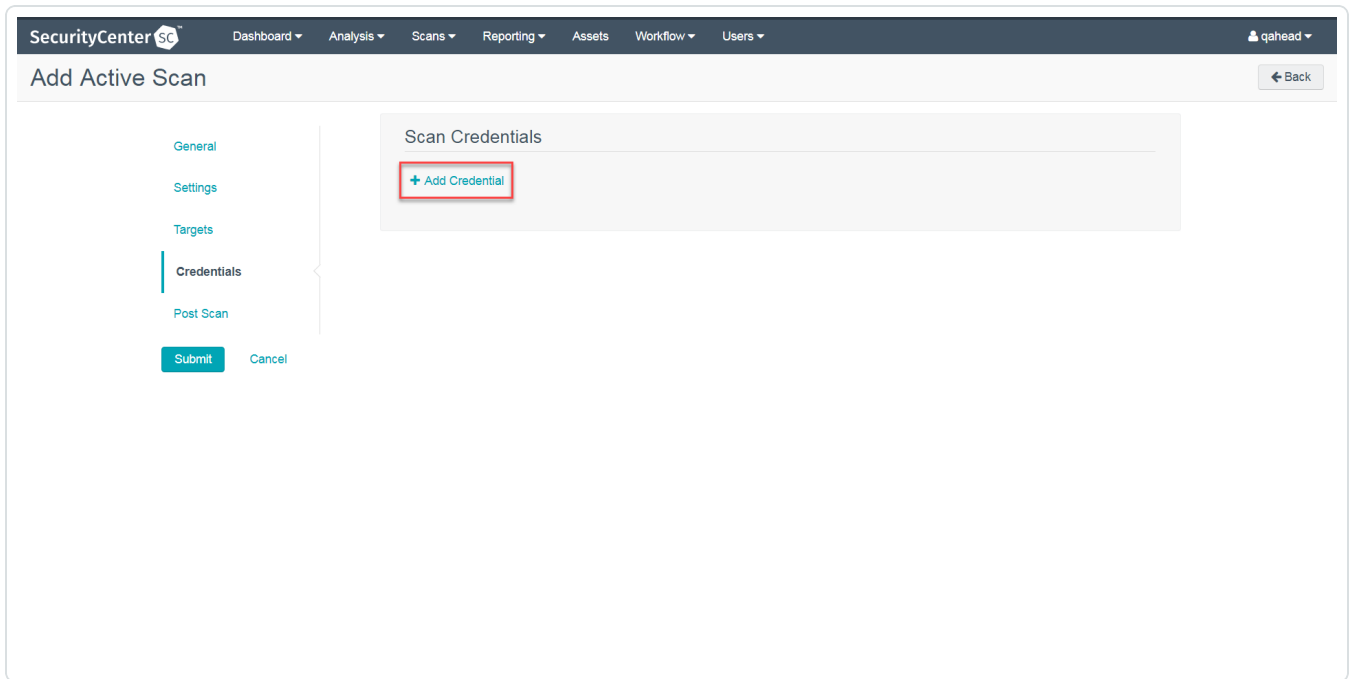
The **Add Active Scan** window appears.

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

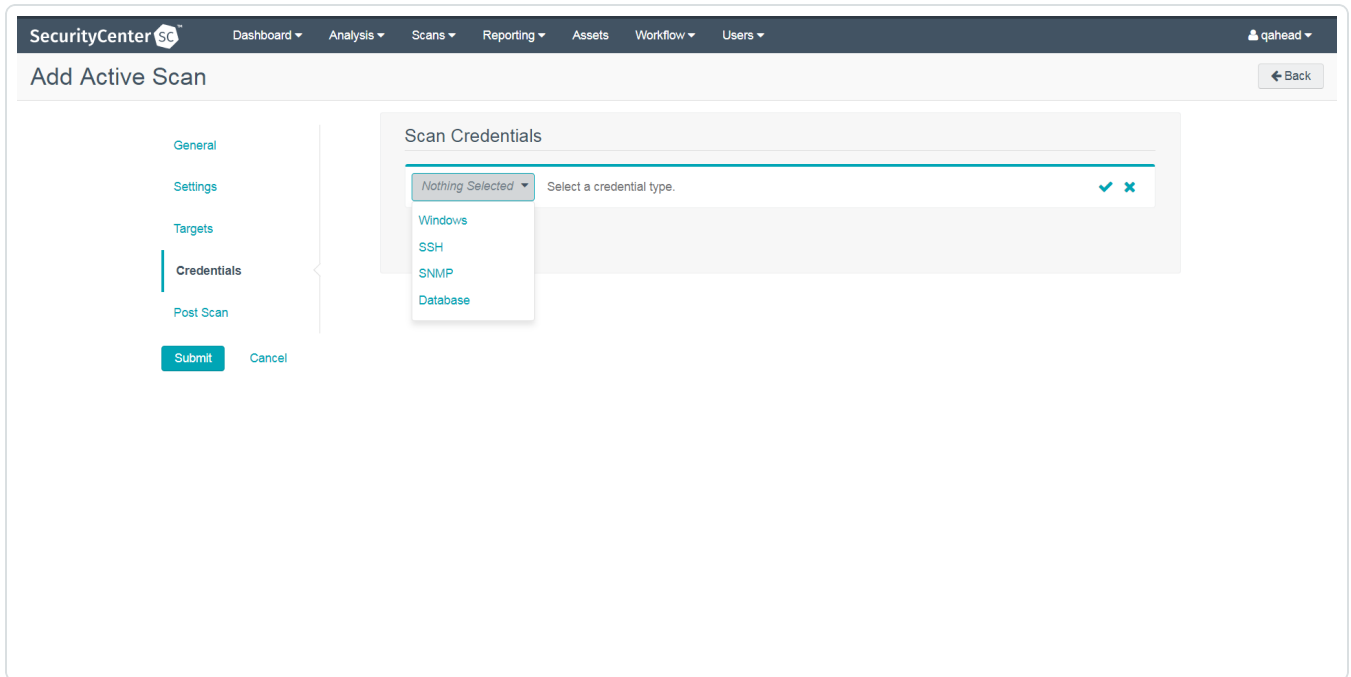
The **Scan Credentials** section appears.



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



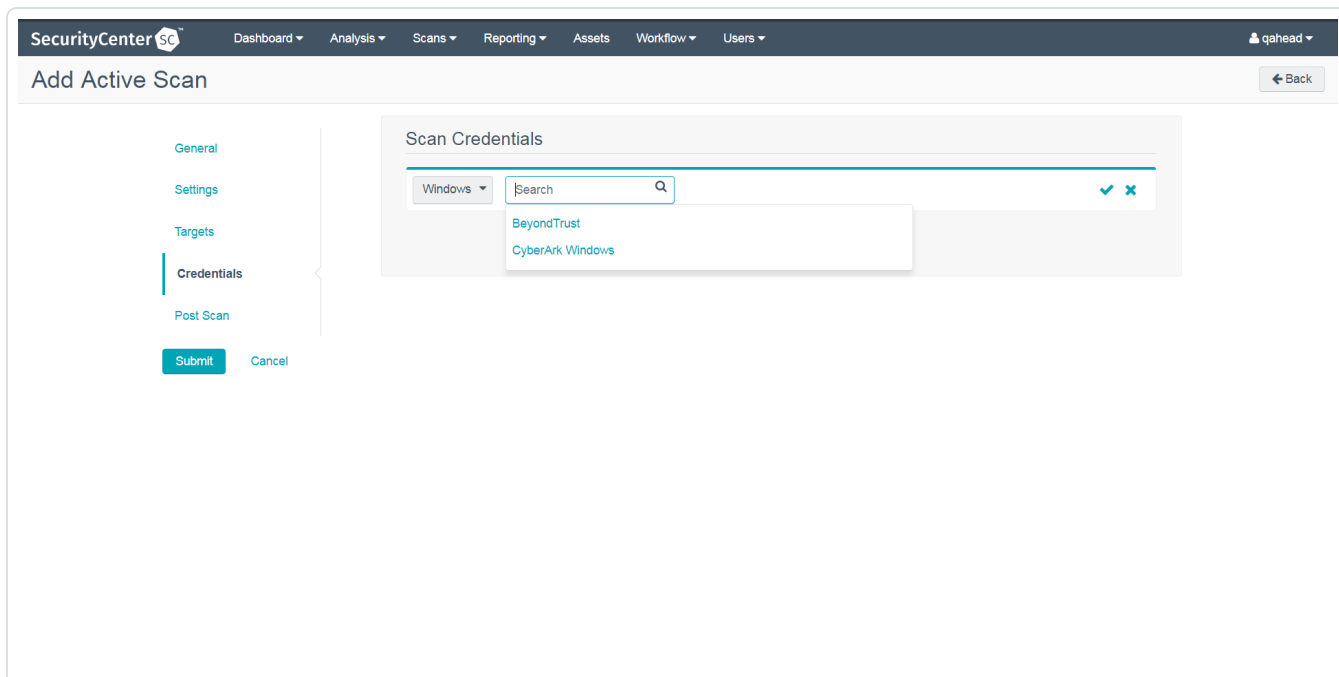
A drop-down appears.



6. Select the system type.

The **Select Credential** option appears.

7. Click **Select Credential**.



The screenshot shows the 'Add Active Scan' page in the SecurityCenter interface. The page has a dark header with the 'SecurityCenter' logo and navigation menus for Dashboard, Analysis, Scans, Reporting, Assets, Workflow, and Users. A user profile 'qahead' is visible in the top right. The main content area is titled 'Add Active Scan' and includes a 'Back' button. On the left, there is a sidebar with navigation options: General, Settings, Targets, Credentials (which is highlighted), and Post Scan. Below the sidebar are 'Submit' and 'Cancel' buttons. The main area displays a 'Scan Credentials' section with a dropdown menu set to 'Windows'. A search bar is present, and a dropdown list shows two options: 'BeyondTrust' and 'CyberArk Windows'. The 'BeyondTrust' option is currently selected.

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

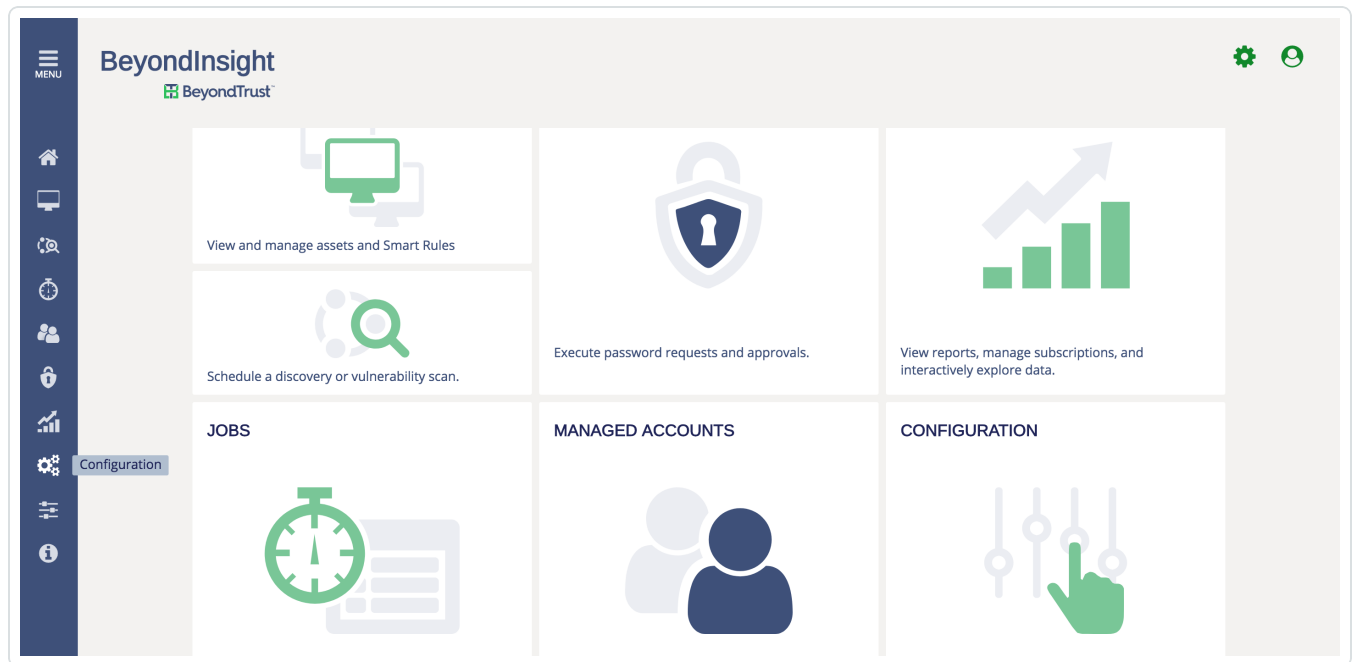
[API Keys Setup](#)

[Enable API Access](#)

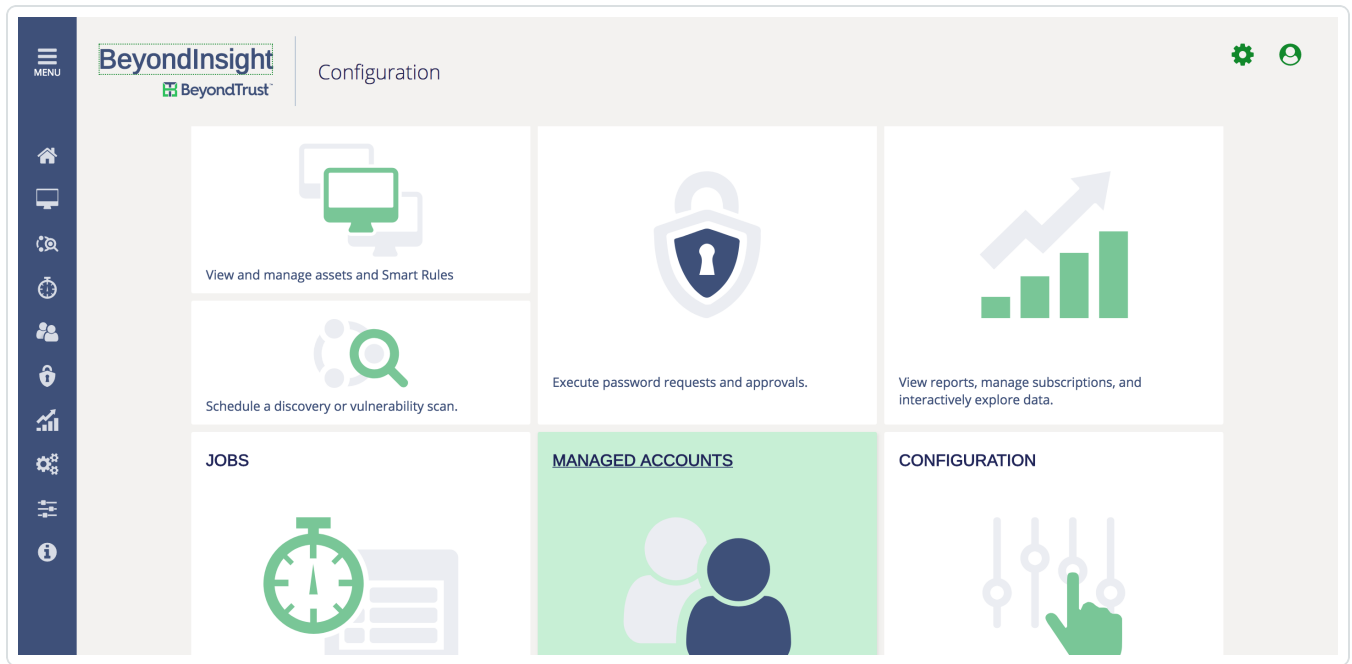
API Keys Setup

Steps

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



3. Click **API Registration**.



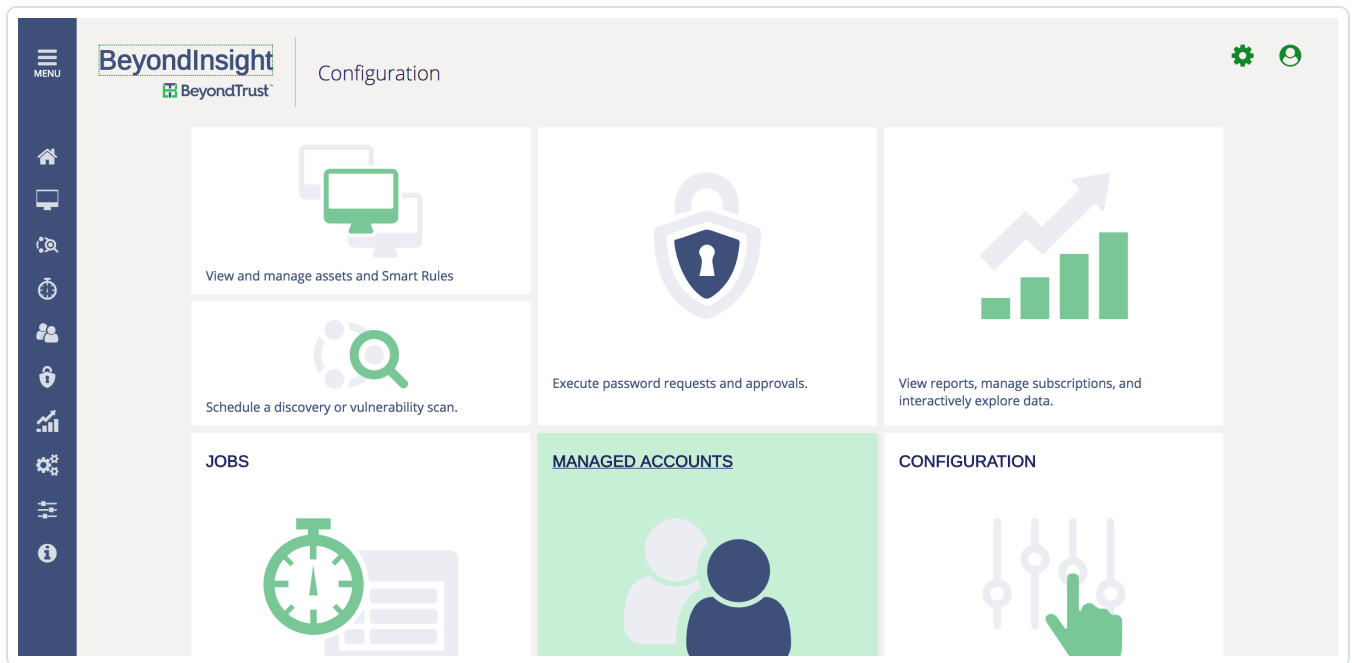
4. Configure the **source addresses** that are white listed requests.
5. Click **Save**.

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	Edit Account
<input type="checkbox"/>	not-root	qa-ssh-staging	Linux	02/15/2018 11:35 AM	Success		No	Delete Account

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

Managed Account Settings [X]

Settings | Synced Accounts

System Name:

Account Name:

Authentication Type: **DSS** [v]

Password:

Confirm Password:

Allow Fallback to Password:

Password Rule: [v]

Account Description:

Workgroup: [v]

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 SecurityCenter. The customized report defines the information needed for SecurityCenter 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 SecurityCenter .

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.