How-to Guide: Tenable SecurityCenter for BeyondTrust

Last Revised: August 06, 2018

Table of Contents

Introduction

This document describes how to configure Tenable SecurityCenter for integration with the BeyondTrust PowerBroker Password Safe. Please email comments or suggestions to support@tenable.com.

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 the BeyondTrust PowerBroker Password Safe with Tenable's solutions, customers are now granted even more choice and flexibility for reducing the credentials headache.

Benefits of integrating Tenable SecurityCenter with the BeyondTrust PowerBroker Password Safe include:

- Credentials stored in the BeyondTrust PowerBroker Password Safe do not need to be managed and updated directly within Tenable SecurityCenter.
- Reduce the time and effort needed to document where credentials are stored within the entire organizational environment.
- Automatically enforce security policies within specific departments or for specific business unit requirements, which simplifies compliance.
- Reduce the 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

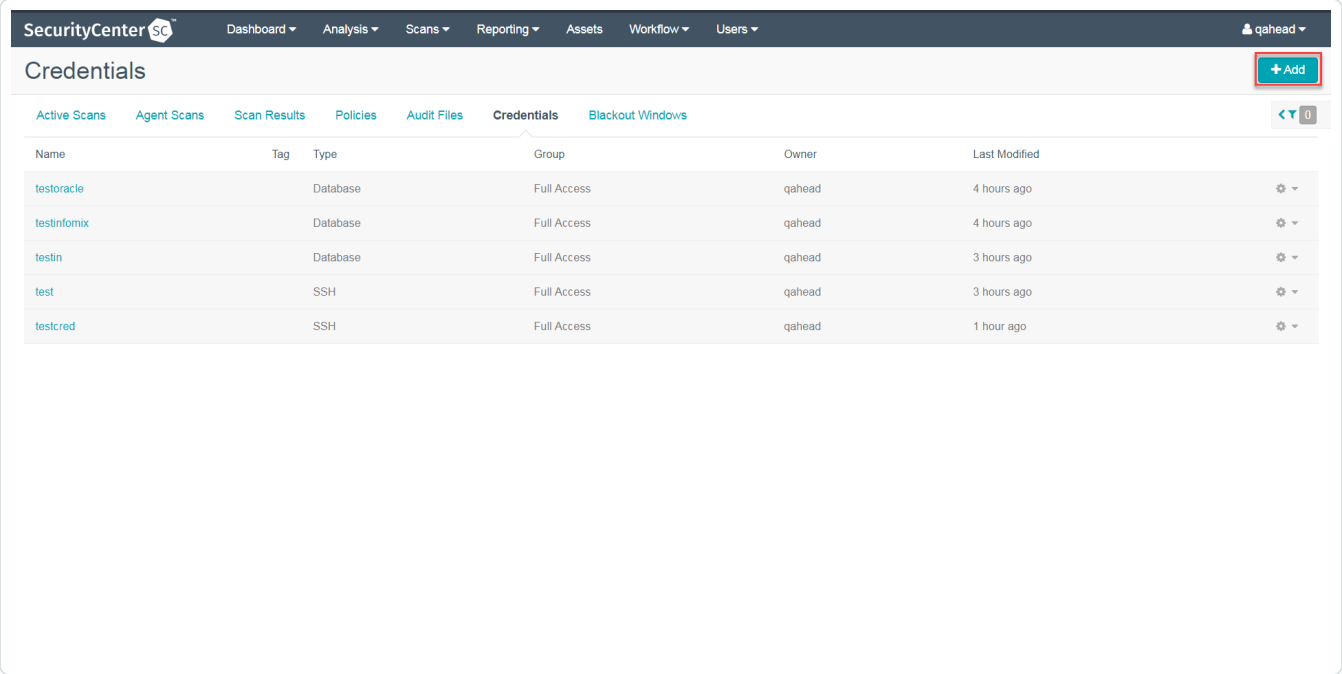
Windows Integration

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

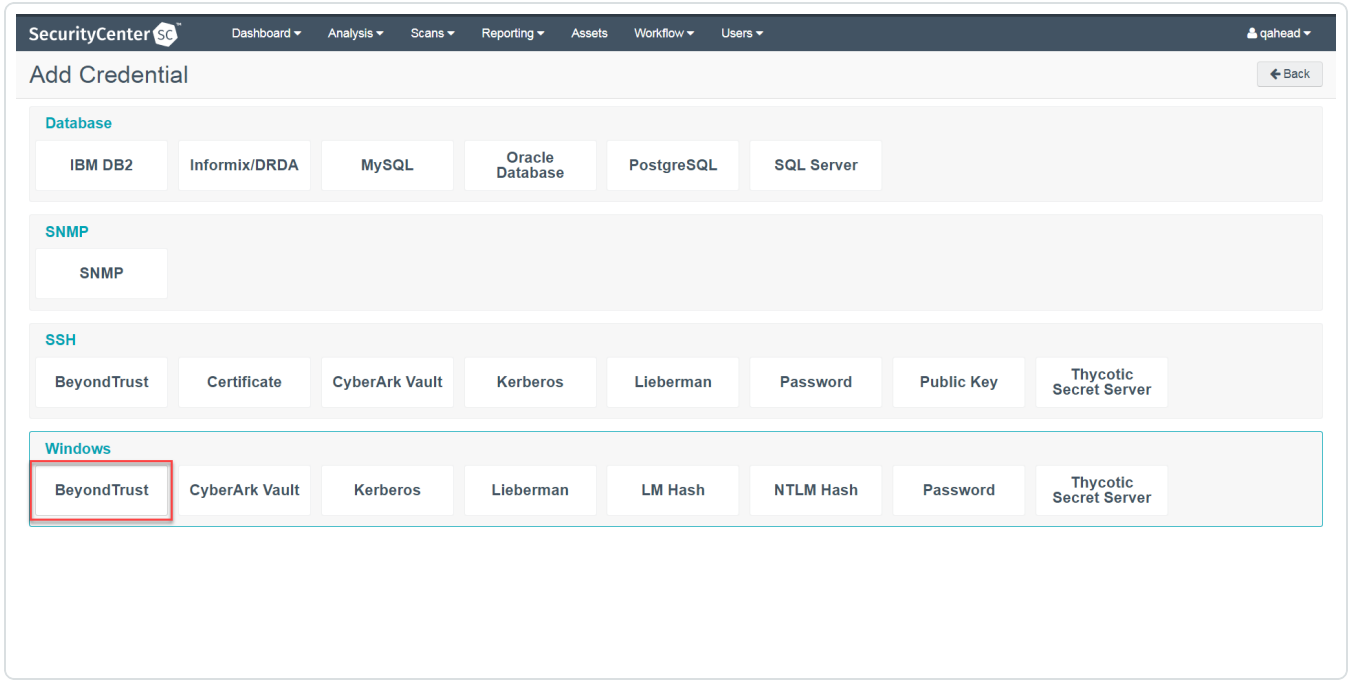
1. Log in to SecurityCenter.
2. In the top navigation bar, click **Scans**.

   A drop-down appears.
3. Click **Credentials**.

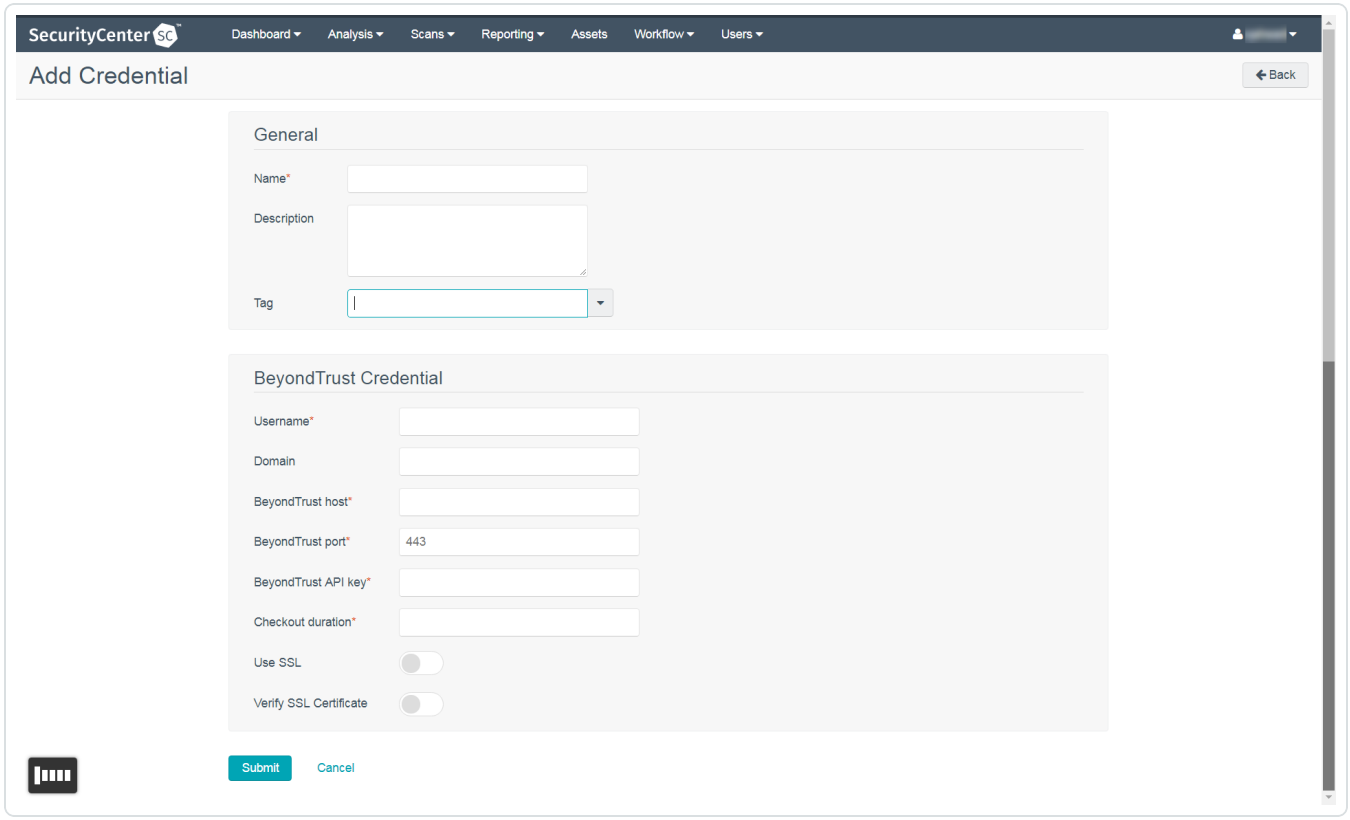
   The **Credentials** window opens.
4. Click the **+ Add** button.



   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.

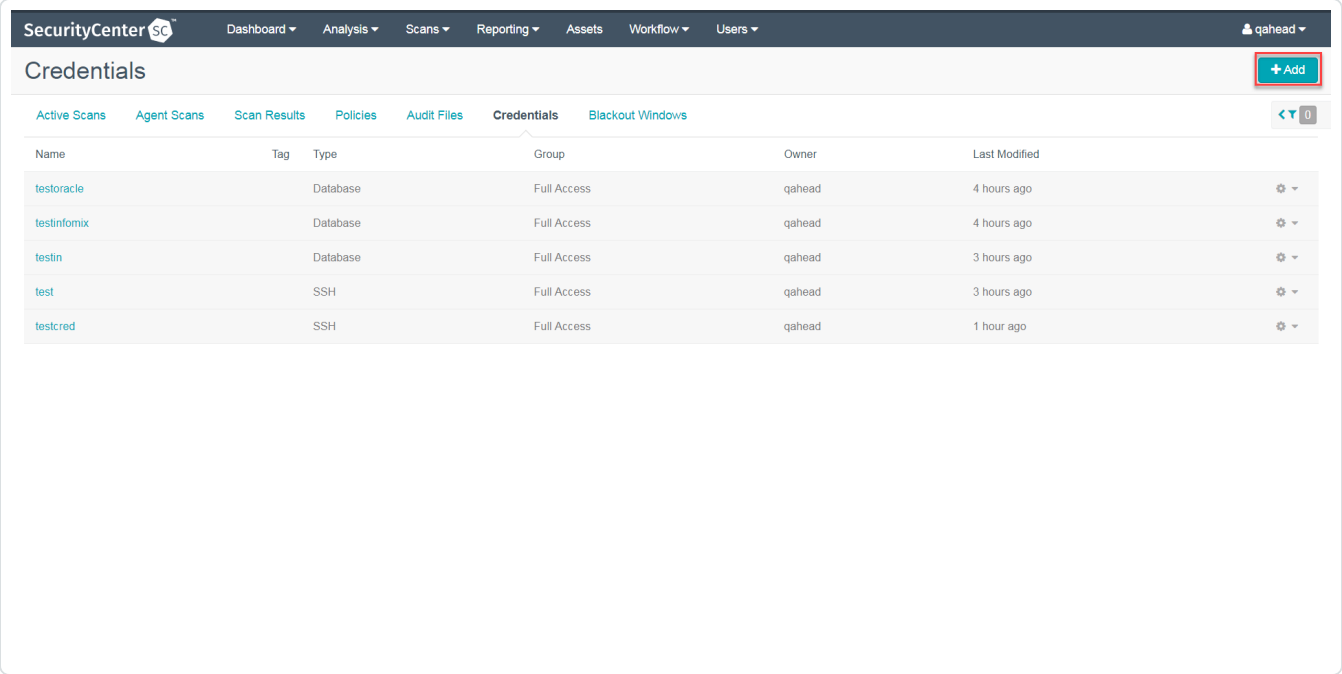
SSH Integration

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

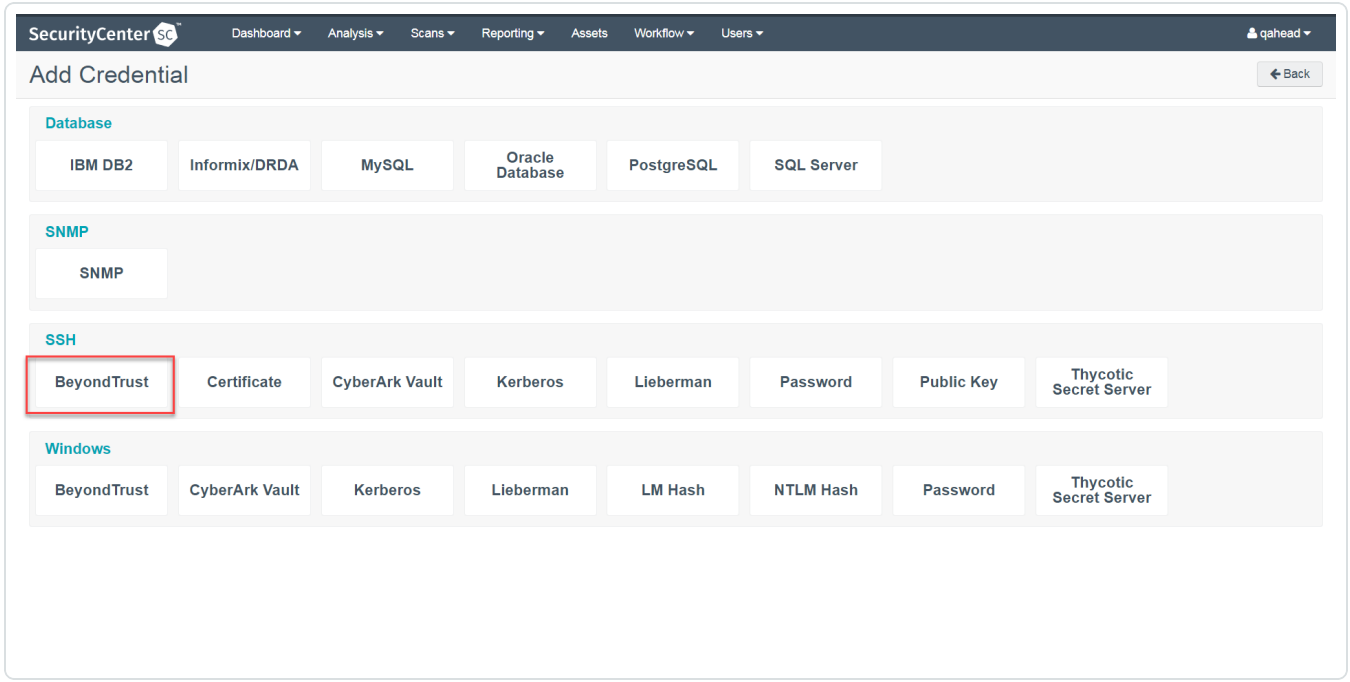
1. Log in to SecurityCenter.
2. In the top navigation bar, click **Scans**.

   A drop-down appears.
3. Click **Credentials**.

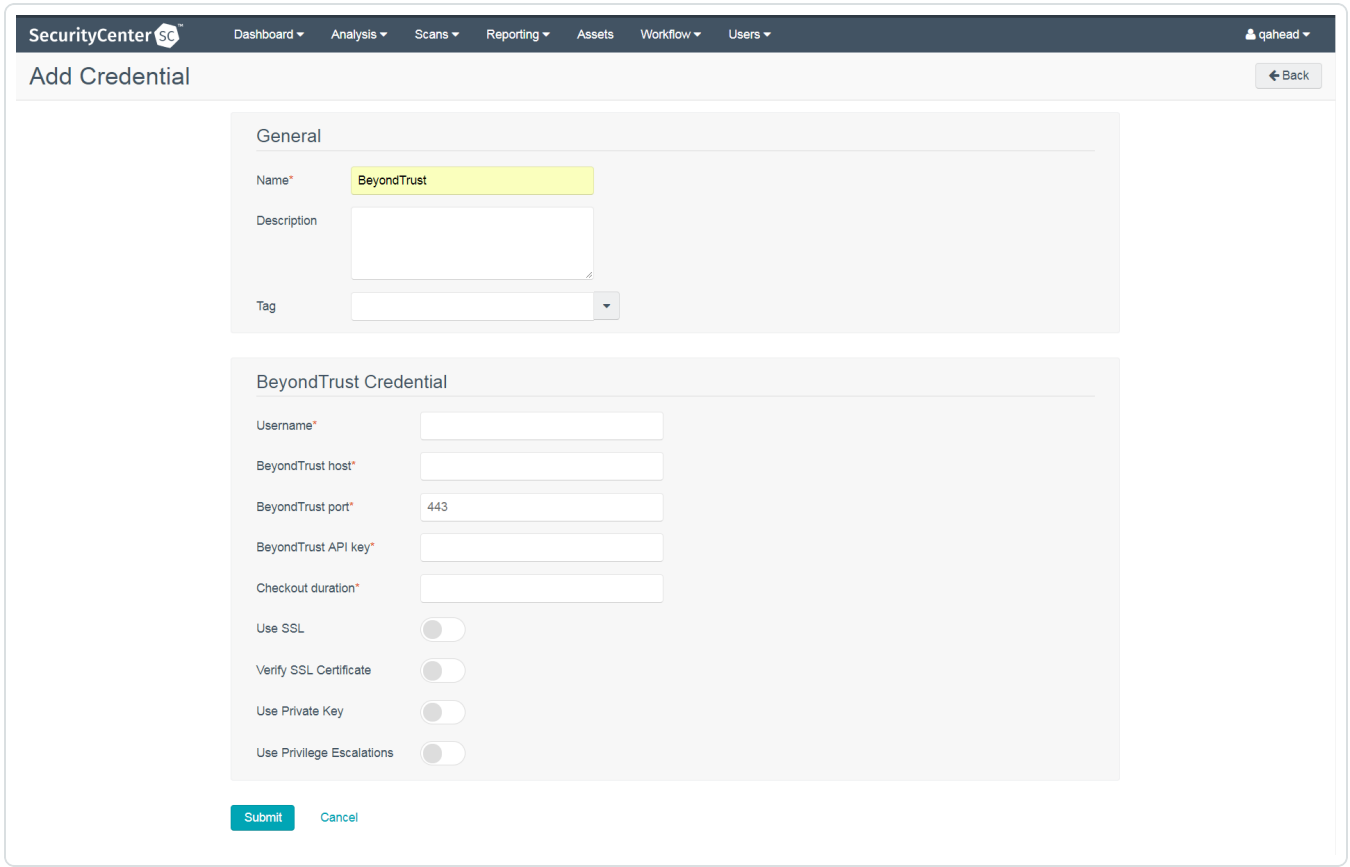
   The **Credentials** window appears.
4. Click the **+ Add** button.



   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.

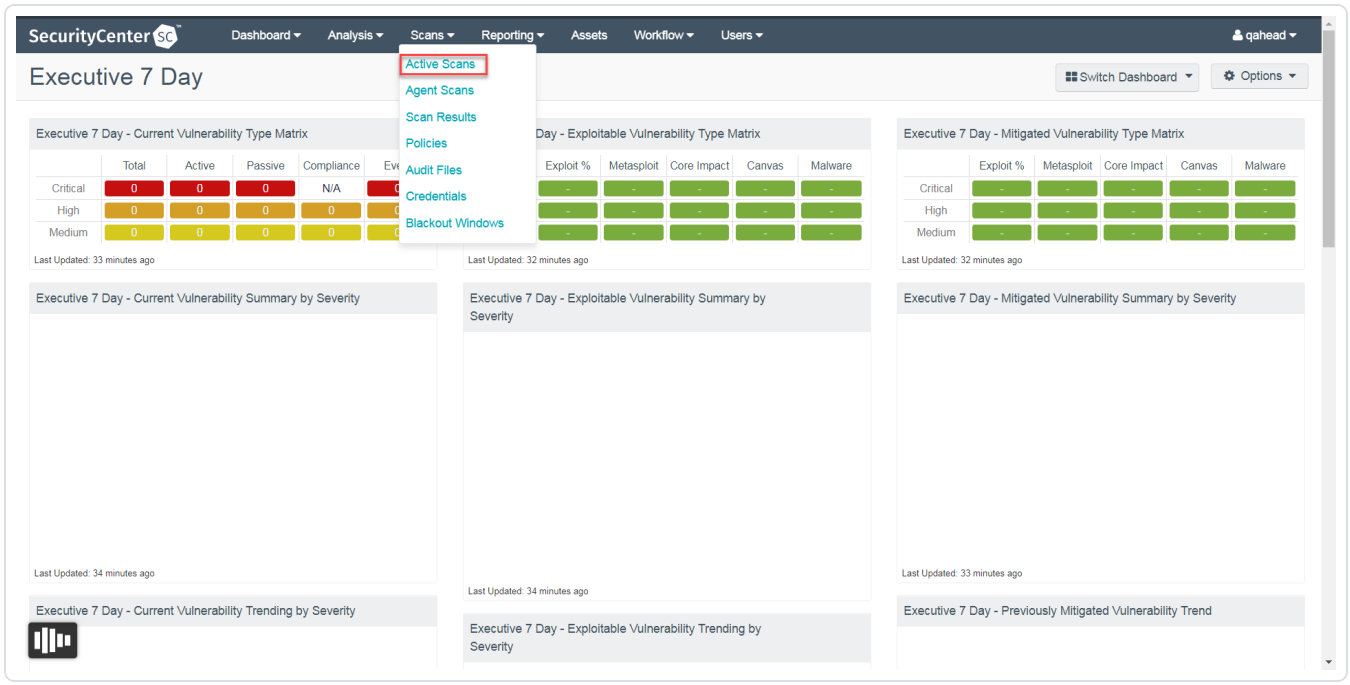
Add the BeyondTrust Credential to a Scan

To add the BeyondTrust credential to the scan:

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

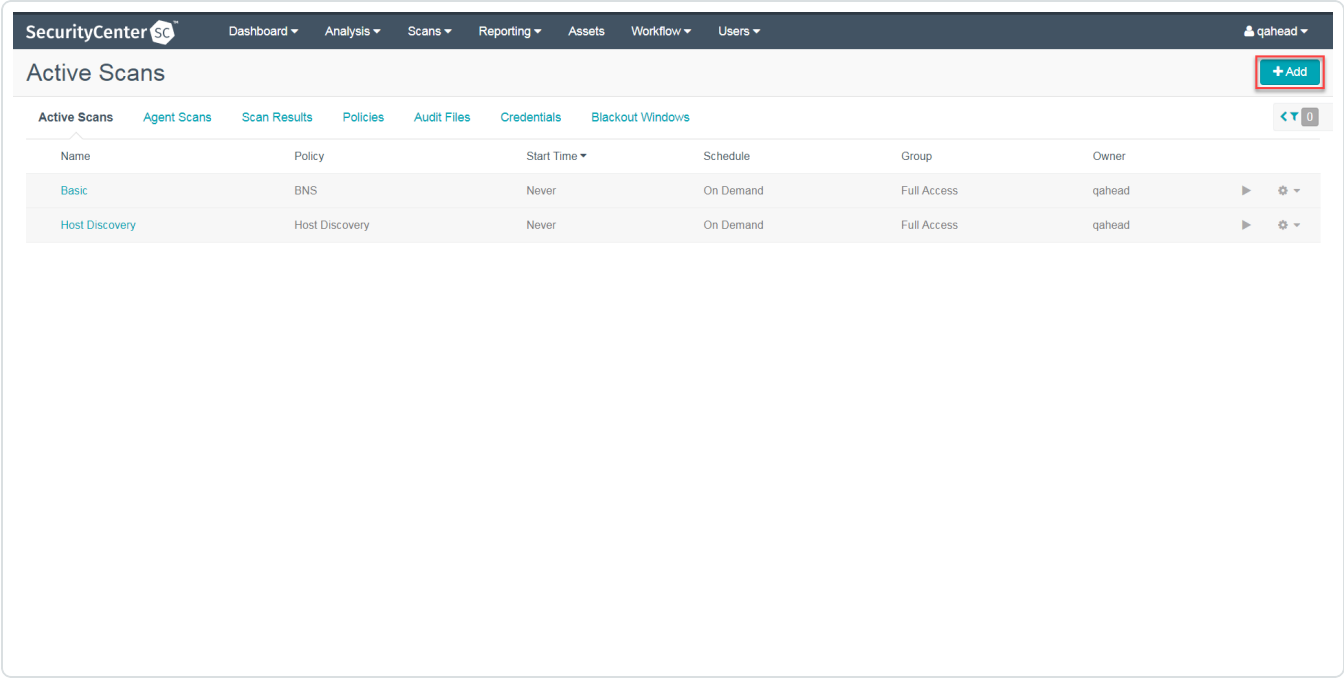
   A drop-down appears.

2. Select **Active Scans**.



   The **Active Scans** window appears.

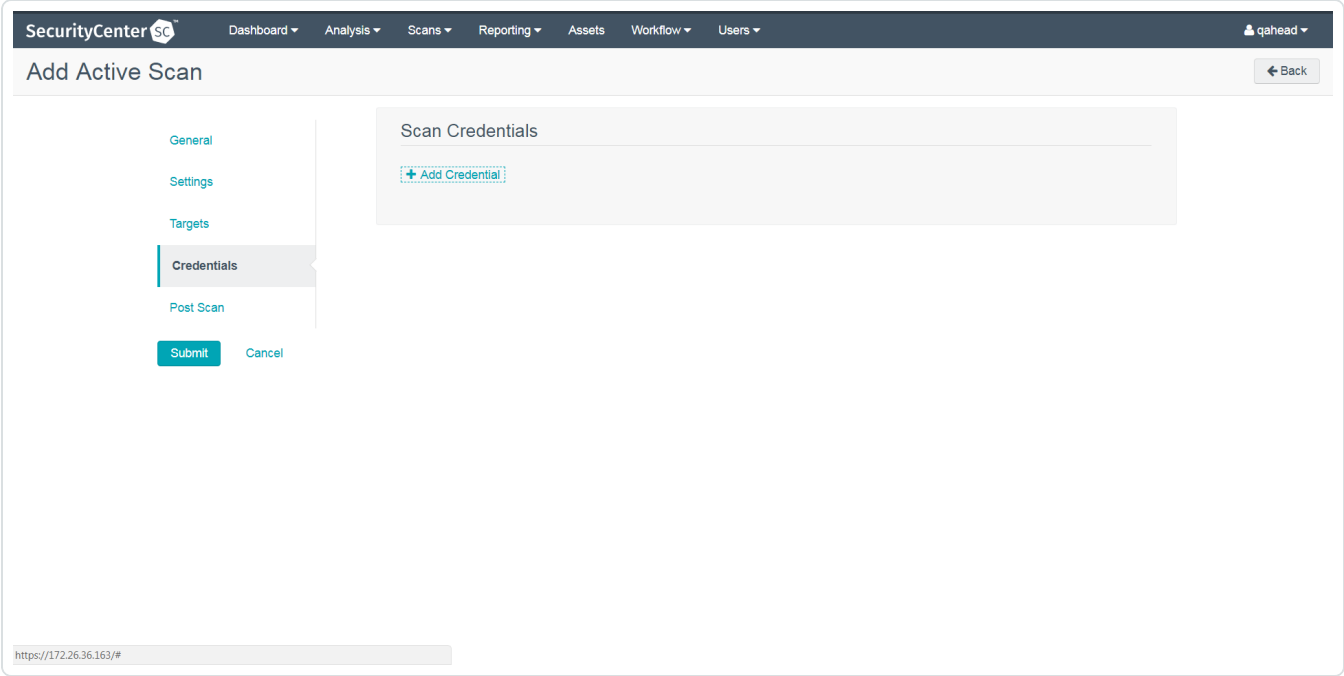
3. In the top right corner, click **+Add**.



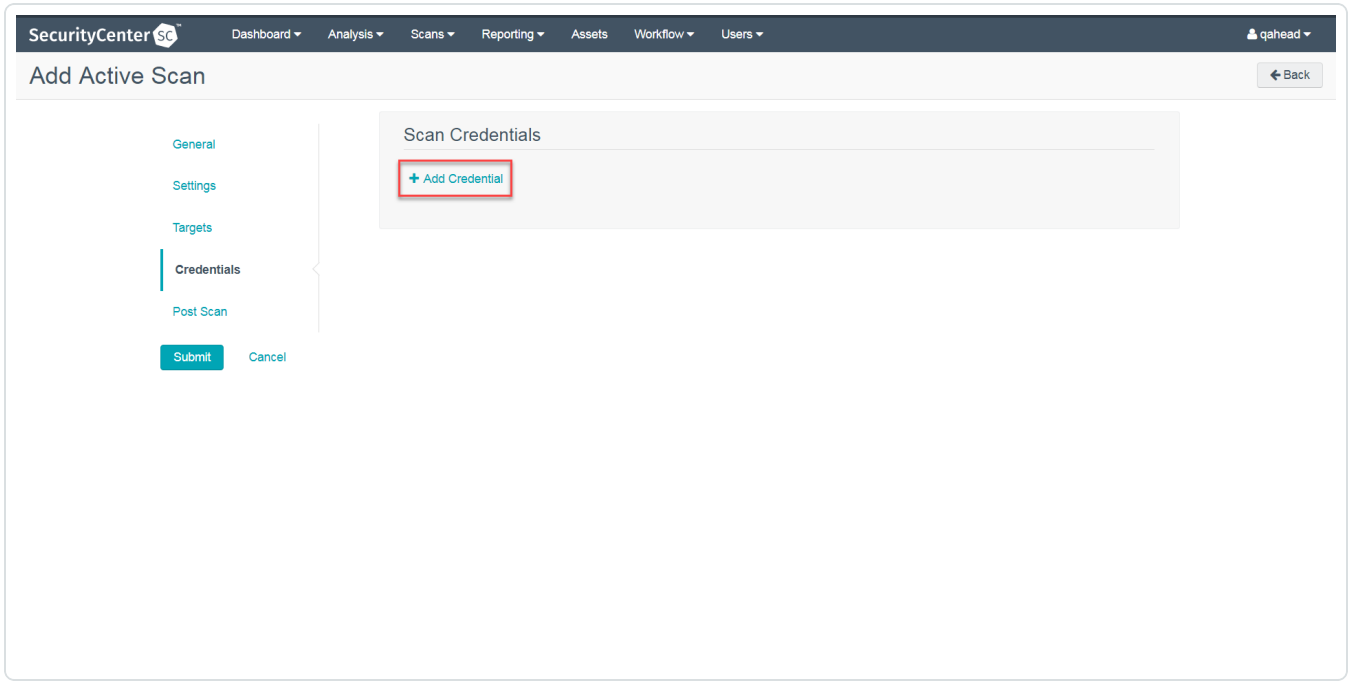
The **Add Active Scan** window appears.

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

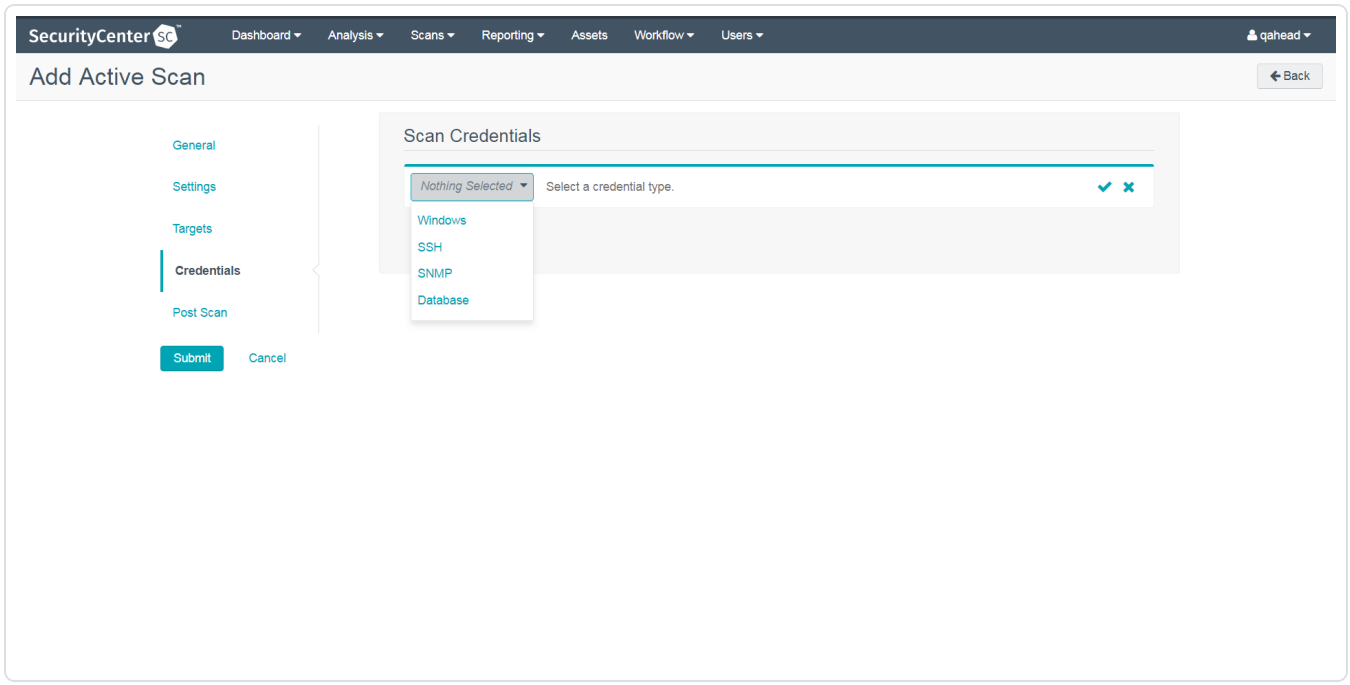
   The **Scan Credentials** section appears.



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



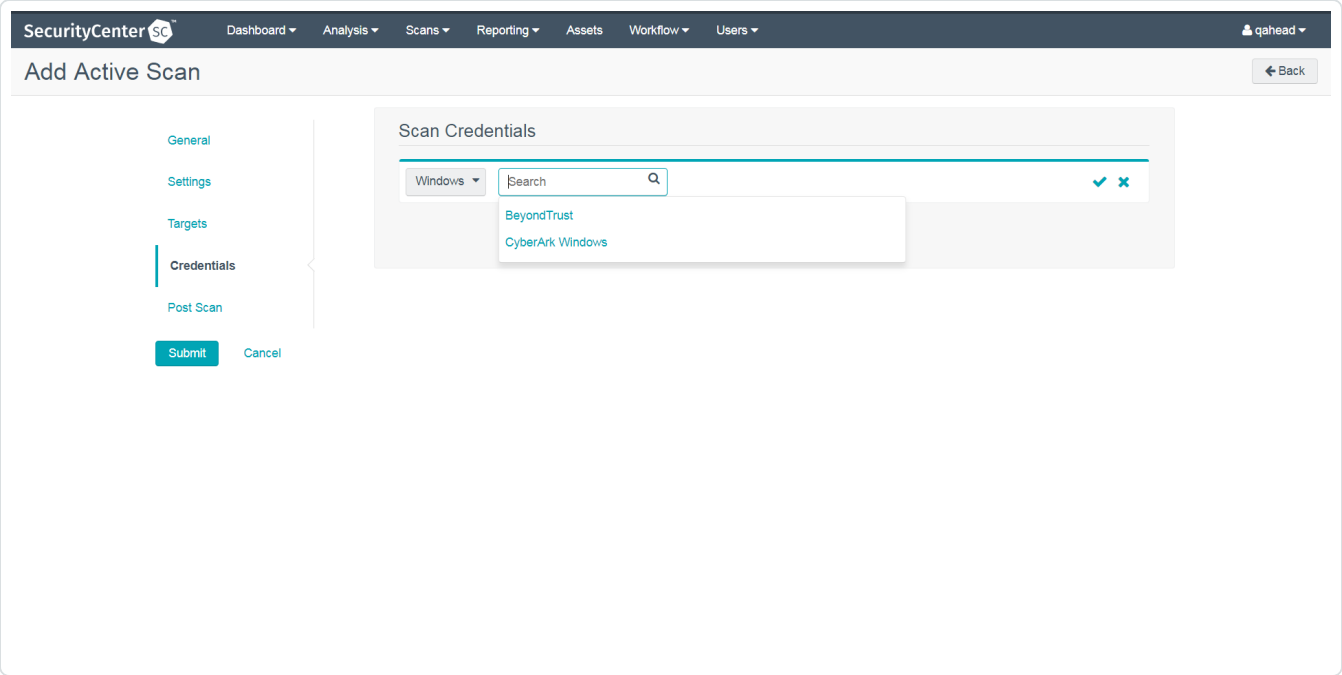
A drop-down appears.



6. Select the system type.

   The **Select Credential** option appears.

7. Click **Select Credential**.



A drop-down appears.

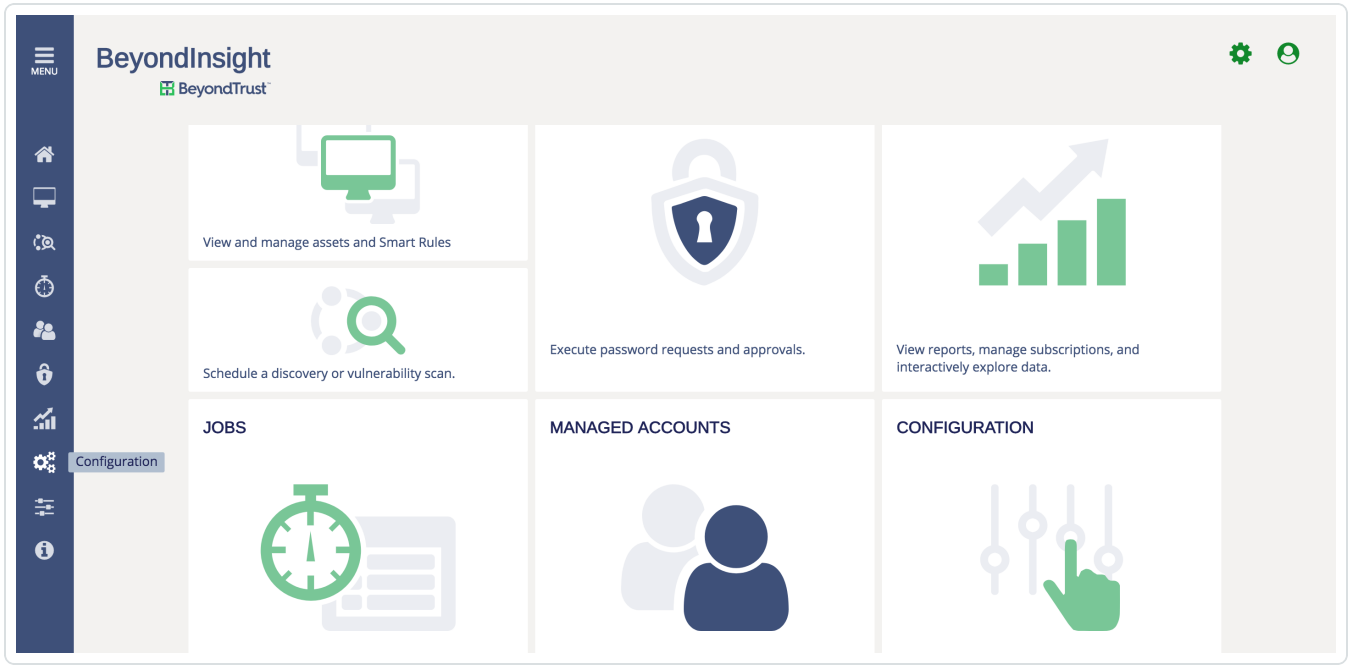
8. Select the previously created credential.
9. Enter information for the **General**, **Settings**, **Targets**, and **Post Scan** sections.
10. Click **Submit**.

API Configuration

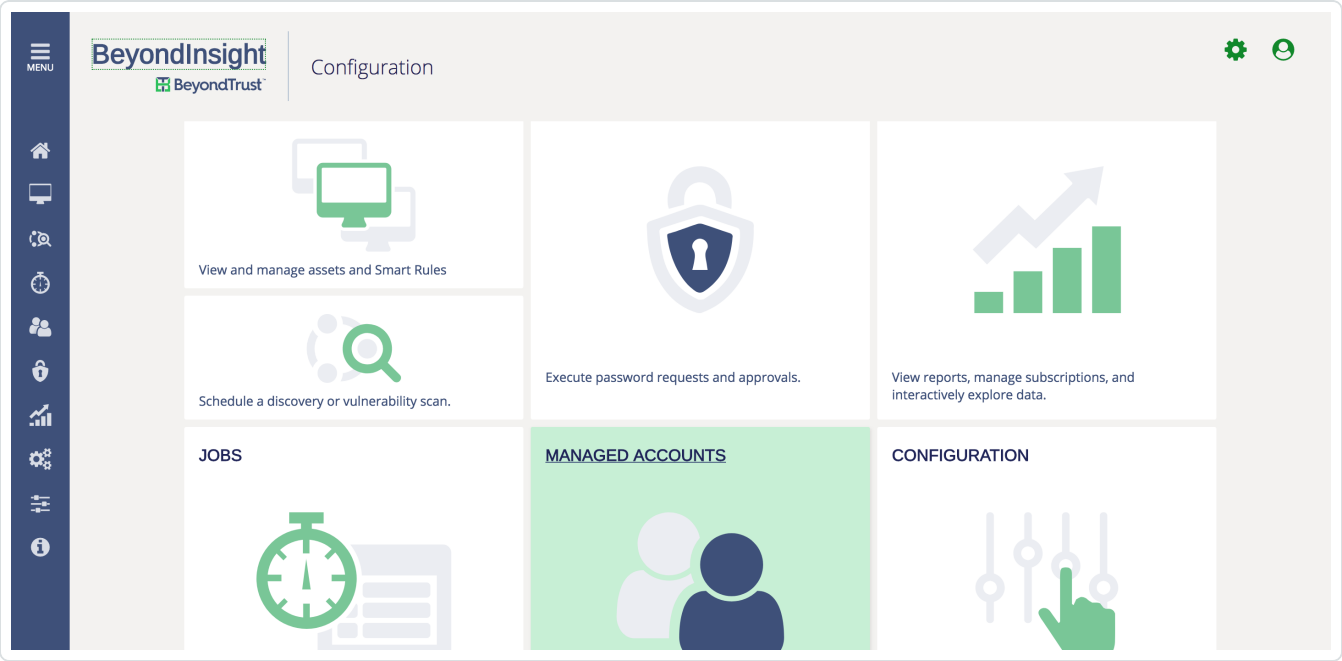
API Keys Setup

Steps

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



3. Click **API Registration**.



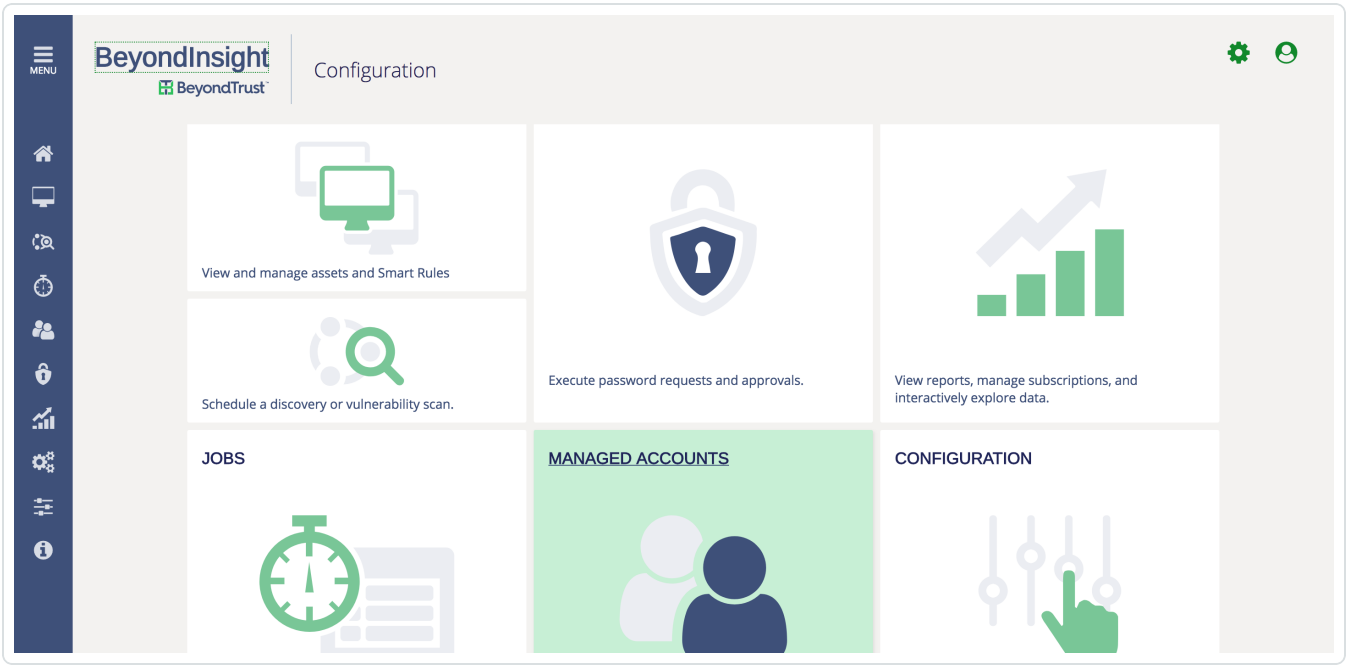
4. Configure the **source addresses** that are white listed requests.
5. Click **Save**.

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

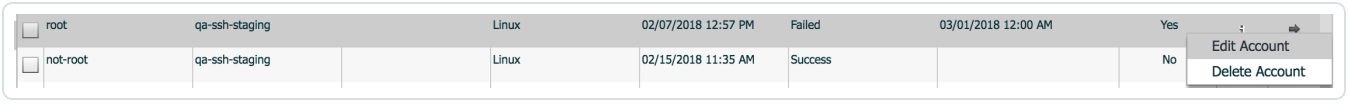
Enable API Access

To enable **API Access**:

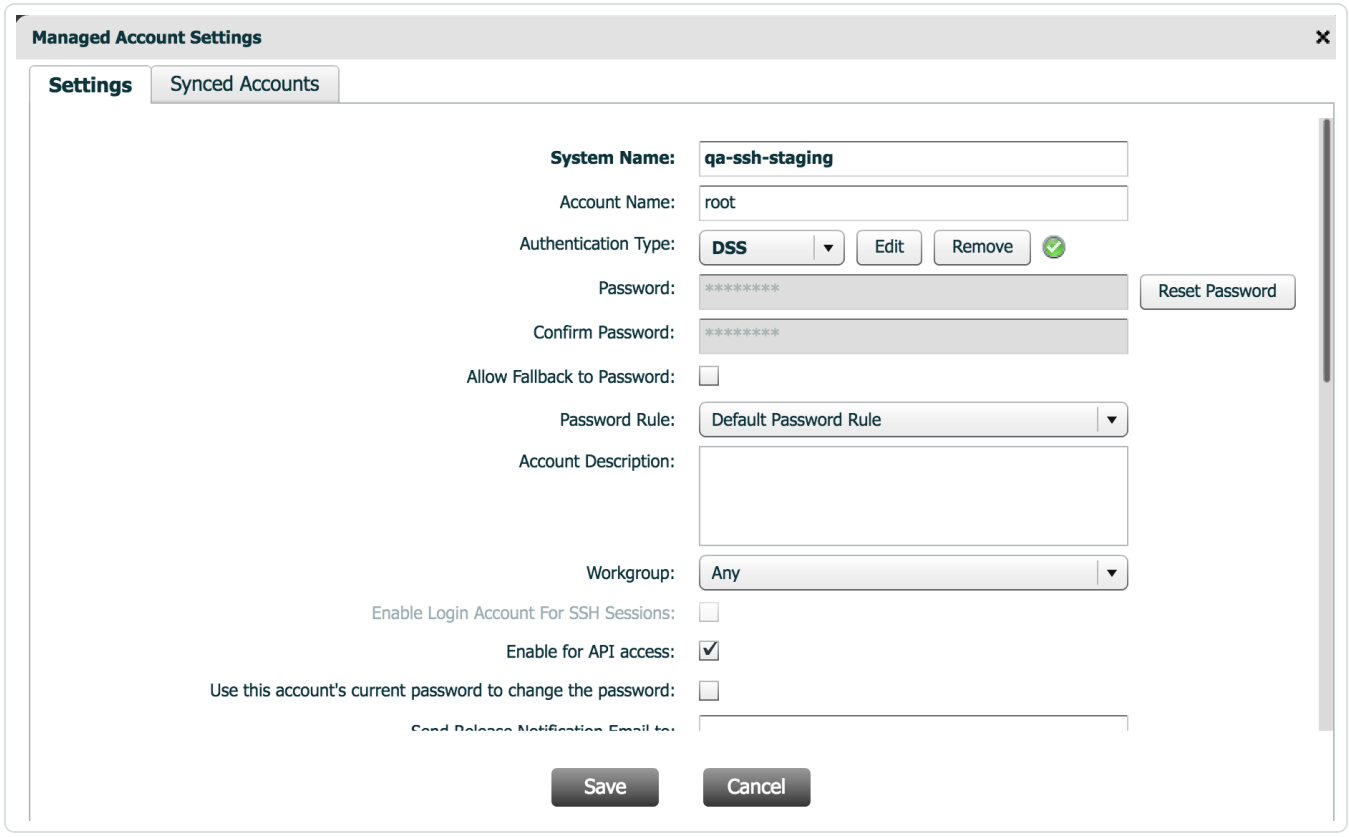
1. Log in to BeyondInsight.
2. Go to **Managed Accounts**.



3. Click **Edit Account**.



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



Additional Information

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.