Tenable Security Center and BeyondTrust Password Safe Integration Guide

Last Revised: July 15, 2025

Table of Contents

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. Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.
3. Click **Add**.

   The **Credential Templates** page appears.
4. In the **Miscellaneous**, **API Gateway**, **Database**, **SNMP**, **SSH**, or **Windows**, or **Web Authentication** sections, click the tile for the specific method you want to configure.

   The **Add Credentials** configuration page appears.
5. In the **Name** box, type a name for the credentials.
6. In the **Description** box, type a description for the credentials.
7. (Optional) Type or select a **Tag**. For more information, see Tags in the *Tenable Security Center User Guide*.
8. Configure each option for the **Windows** authentication.

Option	Description
Username	The username to log in to the host you want to scan.
Domain	The domain of the username, if required by BeyondTrust.
BeyondTrust Host	The BeyondTrust IP address or DNS address.
BeyondTrust Port	The port BeyondTrust is listening on.
BeyondTrust API User	The API user provided by BeyondTrust.
BeyondTrust API Key	The API key provided by BeyondTrust.Tenable Security Center
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the **Checkout duration** to exceed the typical duration of your Tenable Security Center scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Tip:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable Security Center scans. If BeyondTrust changes a password during a scan, the scan fails.
Use SSL	If enabled, uses SSL through IIS for secure communications. Configure SSL through IIS in BeyondTrust before enabling this option. **Caution:** If you do not enable this option the traffic that is sent is http and will not be accepted by the Beyond Trust server.
Verify SSL Certificate	If enabled, Tenable Security Center validates the SSL certificate. Configure SSL through IIS in BeyondTrust before enabling this option.

9. Click **Submit**.

   Tenable Security Center saves your configuration.

SSH Integration

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

1. Log in to Tenable Security Center.
2. Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.
3. Click **Add**.

   The **Credential Templates** page appears.
4. In the **Miscellaneous**, **API Gateway**, **Database**, **SNMP**, **SSH**, or **Windows**, or **Web Authentication** sections, click the tile for the specific method you want to configure.

   The **Add Credentials** configuration page appears.
5. In the **Name** box, type a name for the credentials.
6. In the **Description** box, type a description for the credentials.
7. (Optional) Type or select a **Tag**. For more information, see Tags in the *Tenable Security Center User Guide*.
8. Configure each option for the **SSH** authentication.

Option	Description
Username	The username to log in to the host you want to scan.
BeyondTrust Host	The BeyondTrust IP address or DNS address.
BeyondTrust Port	The port BeyondTrust is listening on.
BeyondTrust API User	The API user provided by BeyondTrust.
BeyondTrust API Key	The API key provided by BeyondTrust.

Option	Description
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the **Checkout duration** to exceed the typical duration of your Tenable Security Center scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Tip:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable Security Center scans. If BeyondTrust changes a password during a scan, the scan fails.
Use SSL	If enabled, Tenable Security Center uses SSL through IIS for secure communications. Configure SSL through IIS in BeyondTrust before enabling this option. **Caution:** If you do not enable this option the traffic that is sent is http and will not be accepted by the Beyond Trust server.
Verify SSL Certificate	If enabled, Tenable Security Center validates the SSL certificate. Configure SSL through IIS in BeyondTrust before enabling this option.
Use Private Key	If enabled, Tenable Security Center uses key-based authentication for SSH connections instead of password authentication.
Use Privilege Escalations	If enabled, Tenable Security Center uses BeyondTrust for privilege escalation.

9. Click **Submit**.

   Tenable Security Center saves your configuration.

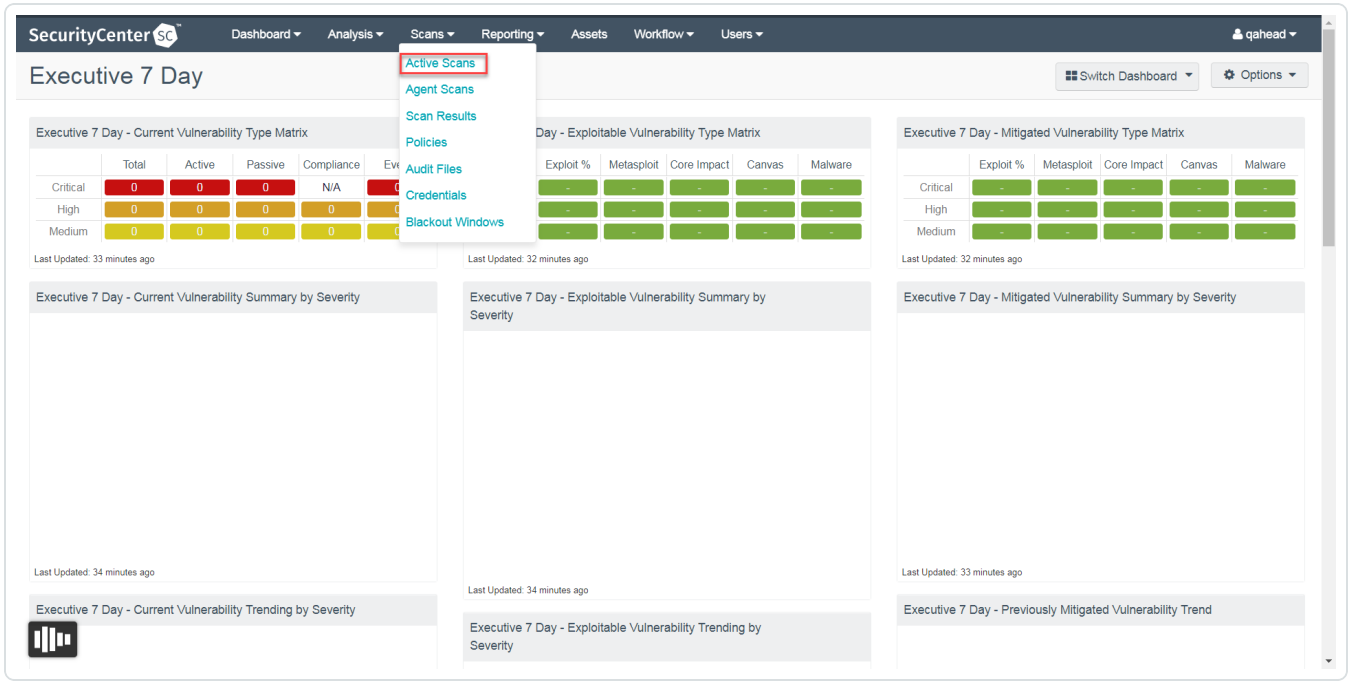
Add the BeyondTrust Credential to a Scan

To add the BeyondTrust credential to the scan:

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

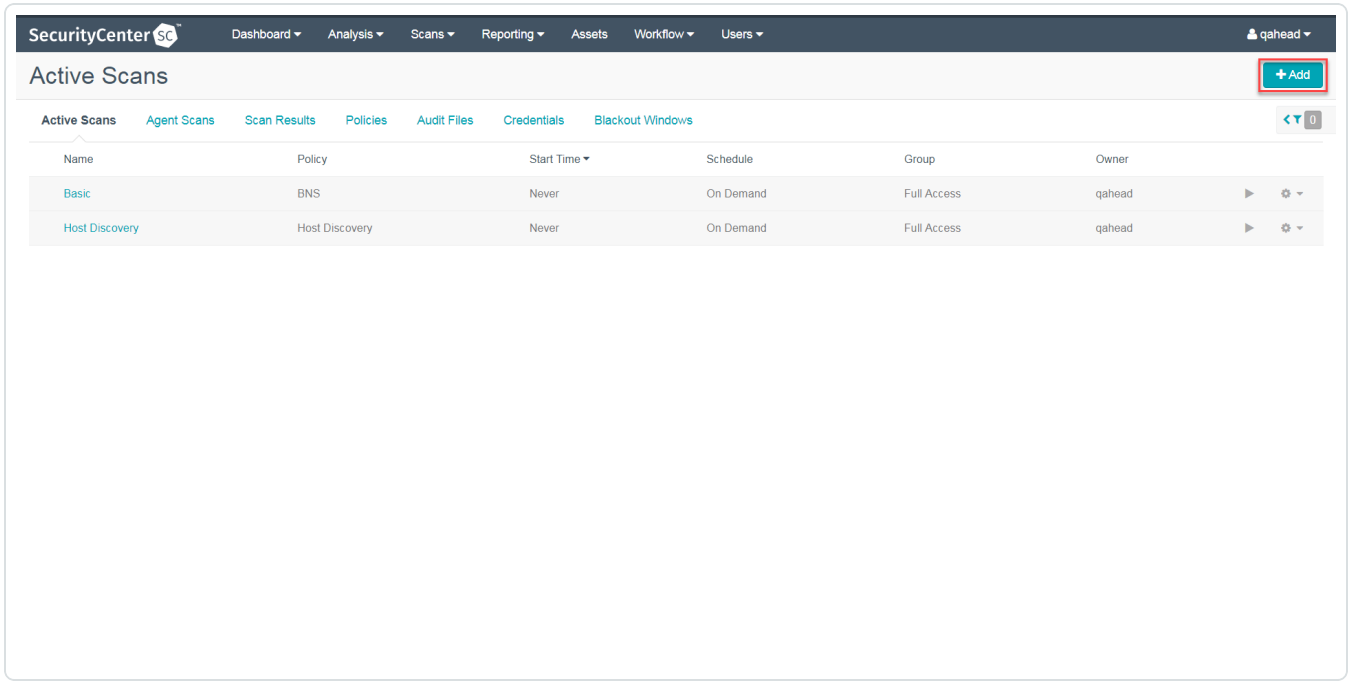
   A drop-down appears.

2. Select **Active Scans**.



The **Active Scans** window appears.

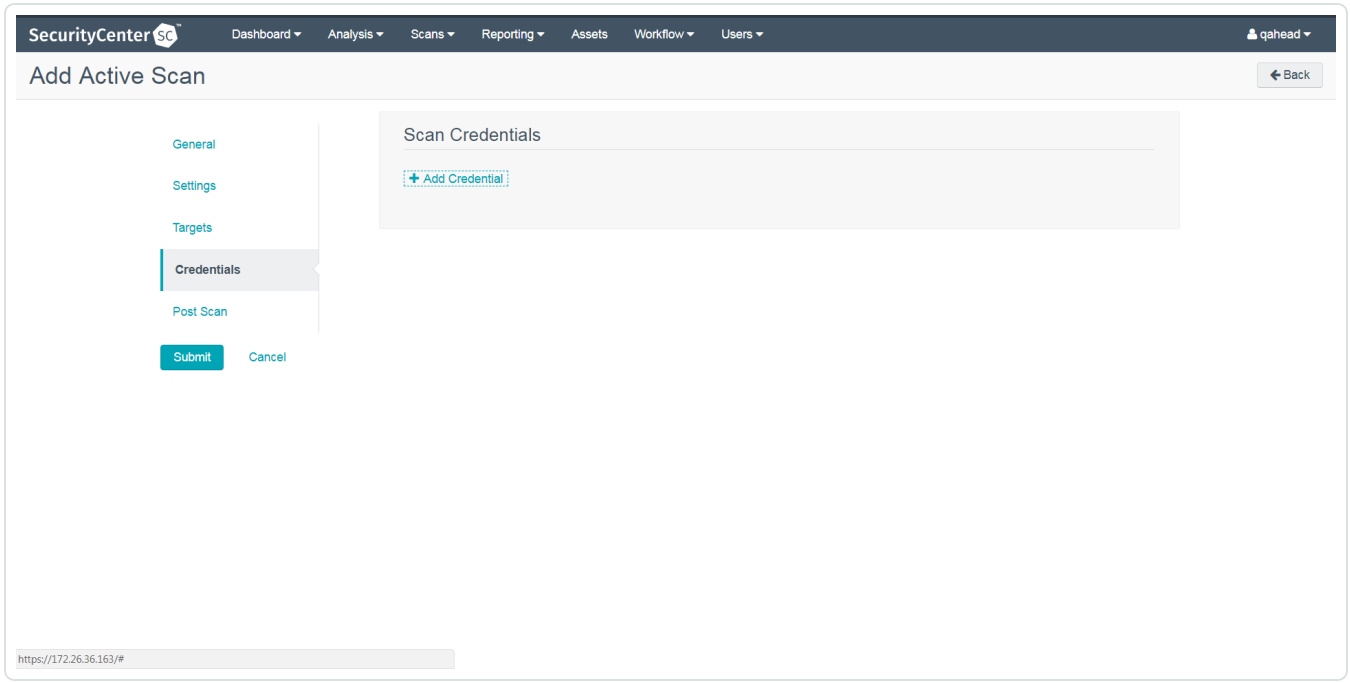
3. In the top-right corner, click **+Add**.



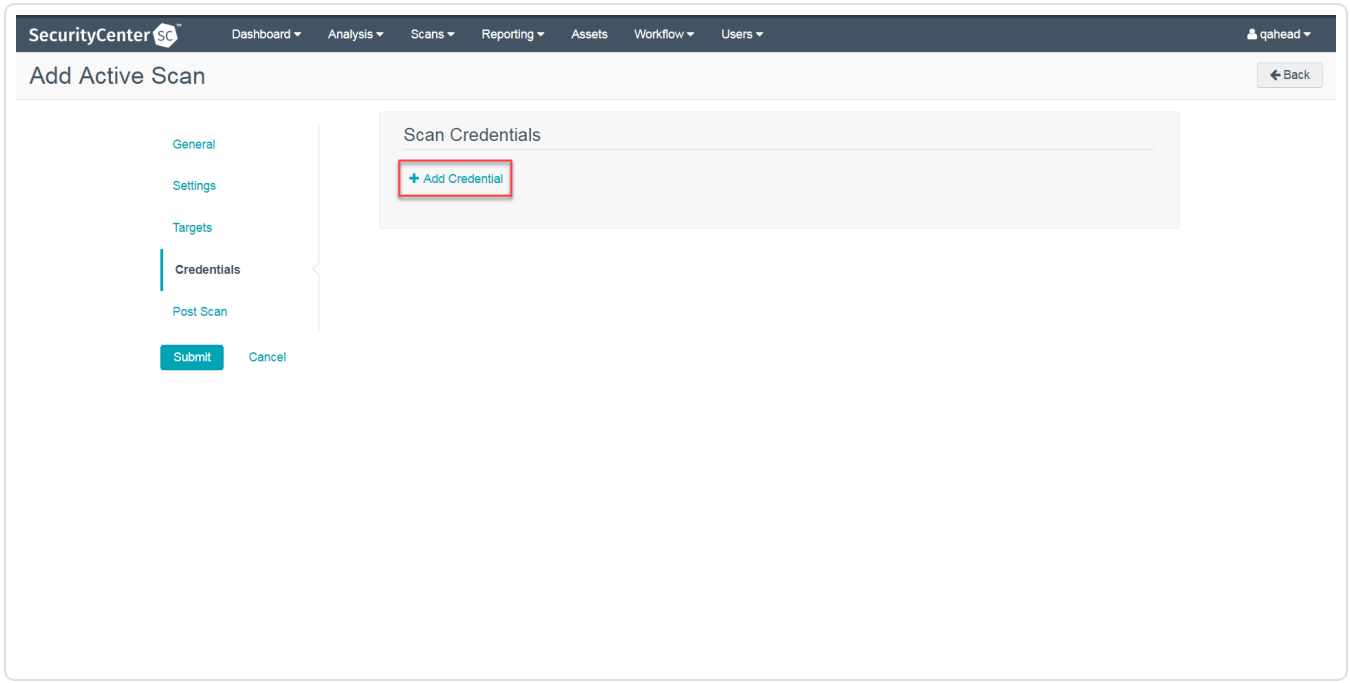
The **Add Active Scan** window appears.

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

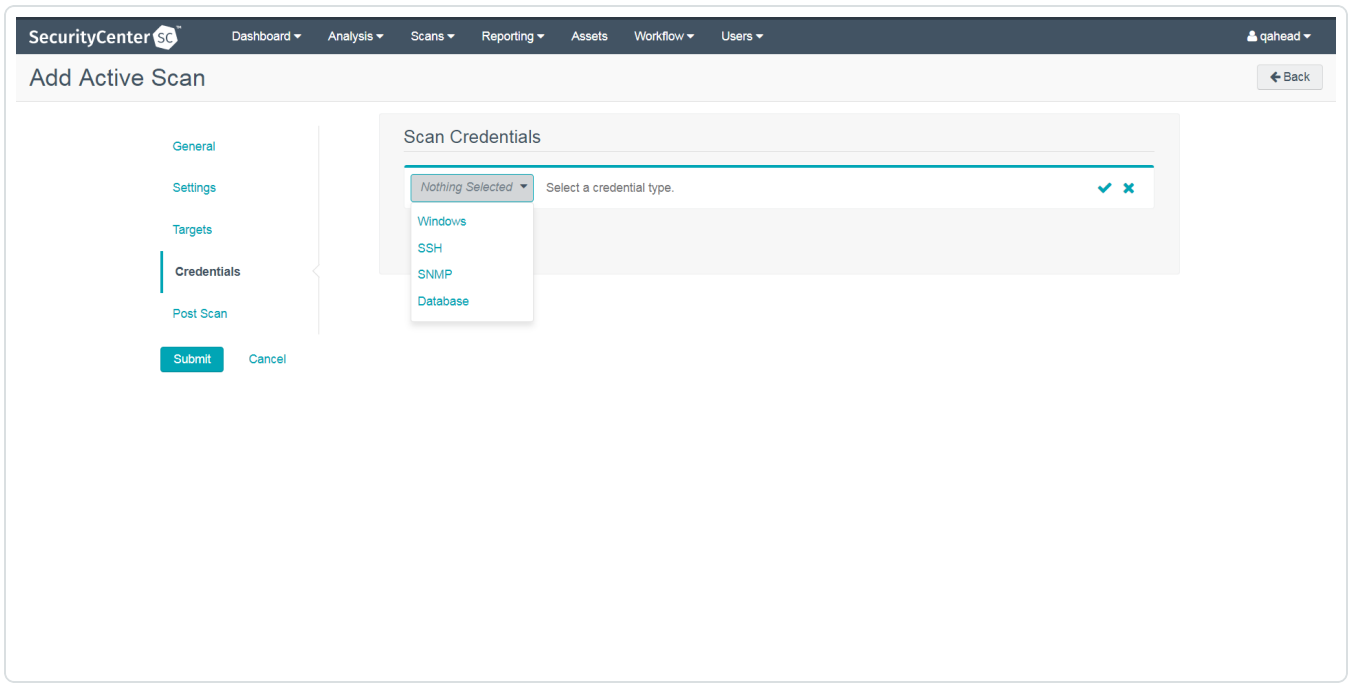
   The **Scan Credentials** section appears.



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



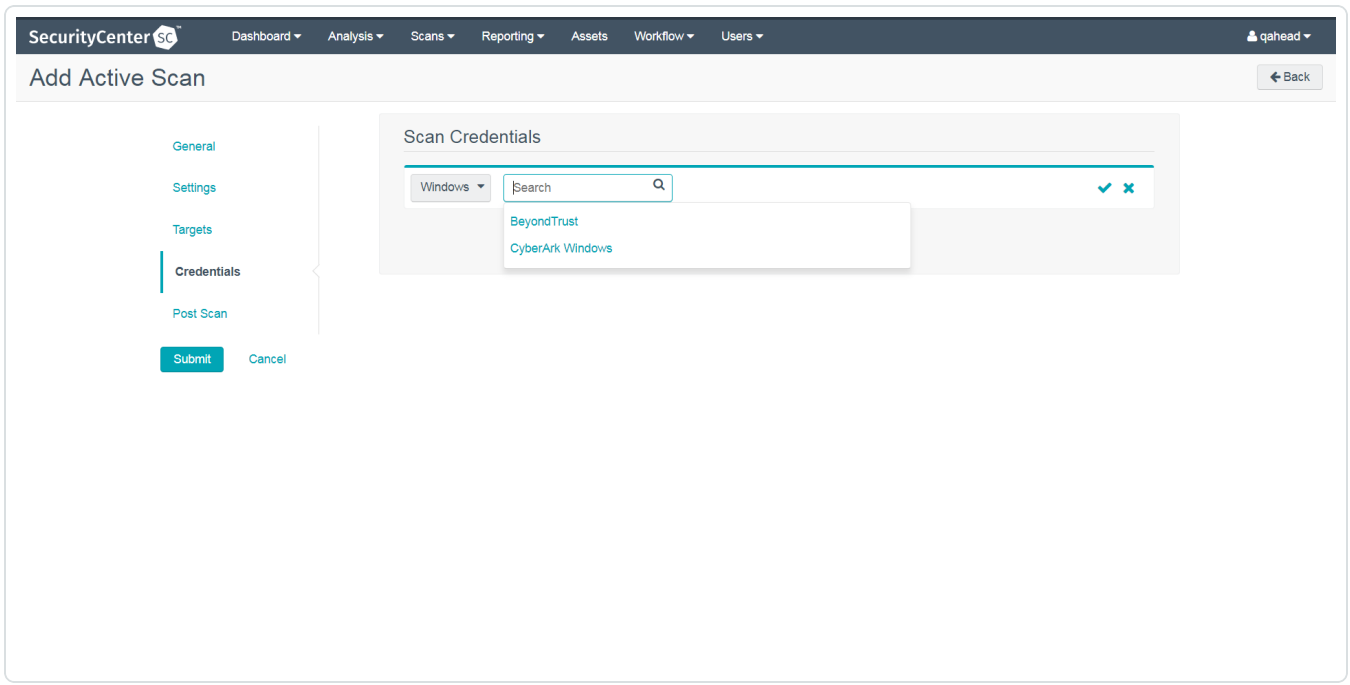
   A drop-down appears.



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

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.

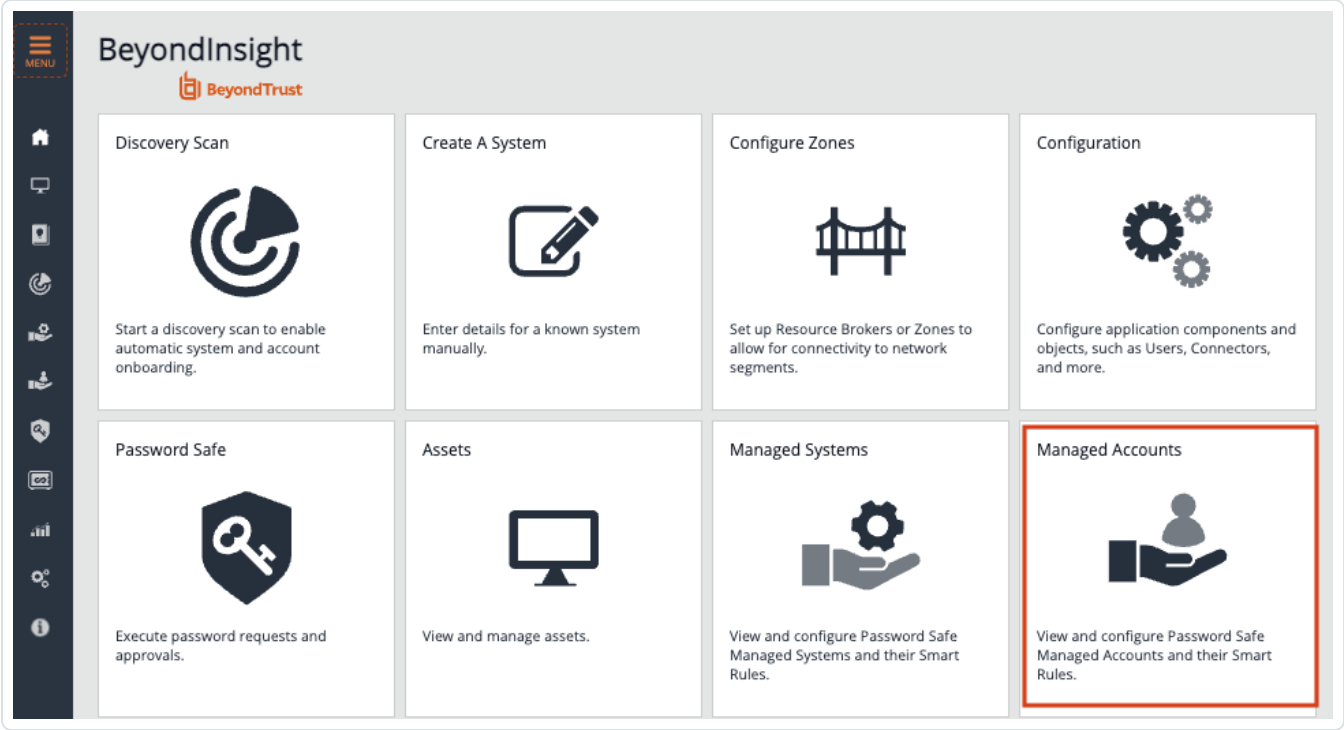
   Caution: Do not select any **Authentication Rule Options** when using the API with Tenable integrations. This may cause the integration to fail.
7. Configure **Authentication Rules** by clicking **Add Authentication Rule**. Configure an IP address or range of IP addresses of one or more scanners.
8. Click **Create Registration**.

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

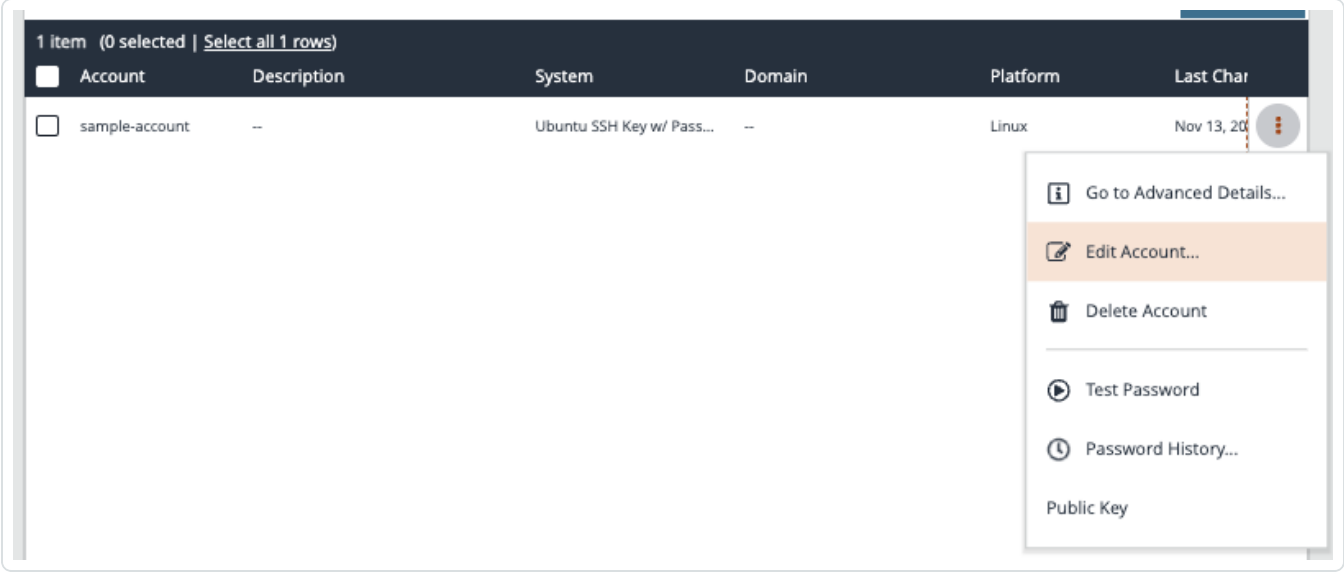
Enable API Access

To enable **API Access**:

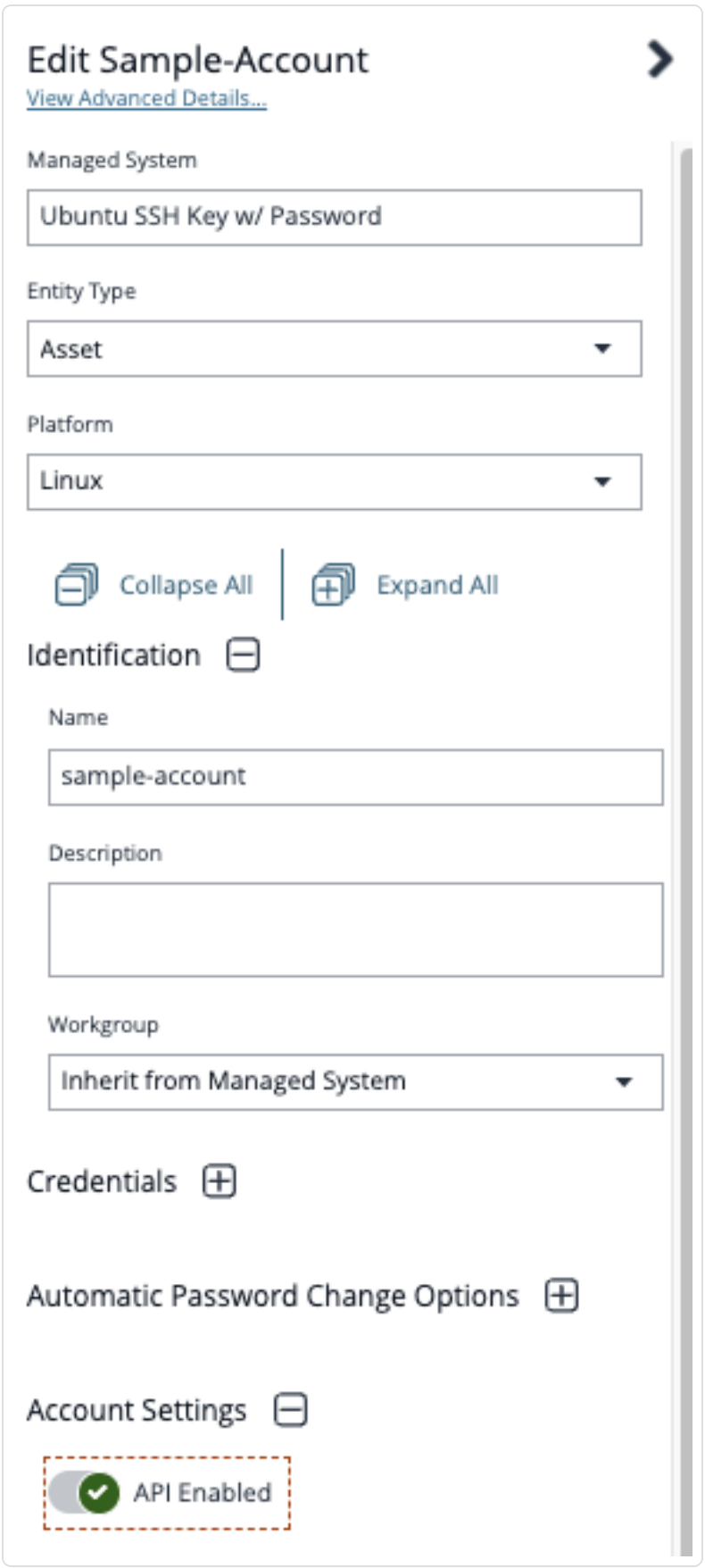
1. Log in to BeyondInsight.
2. Go to **Managed Accounts**.



3. Click **Edit Account**.



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
API Enabled

5. Click **Save**.

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 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.