Tenable Tenable Nessus and BeyondTrust Password Safe Integration Guide

Last Revised: February 15, 2024

Table of Contents

Welcome to Tenable Nessus for BeyondTrust

This document describes how to configure Tenable Tenable Nessus Manager for integration with 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 Nessus, customers have more choice and flexibility.

The benefits of integrating Tenable Nessus Manager with BeyondTrust include:

- Credential updates directly in Tenable Nessus, requiring less management.
- Reduced time and effort to document credential storage locations 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.

Database Integration

Tenable provides full database support for Nessus for BeyondTrust.

Requirements

- Tenable Nessus account
- Nessus for BeyondTrust account

Required User Role: Standard, Scan Manager, or Administrator

To configure Tenable for Nessus for BeyondTrust database:

1. Log in to Tenable Nessus.
2. Click **Scans**.

   The **My Scans** page appears.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.
4. Select a scan template.

   The selected scan template **Settings** page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   The **Credentials** pane appears.
9. Click the **Database** option.

   The **Database** options appear.
10. In the **Database Type** drop-down box, select **Cassandra**, **Oracle**, **DB2**, **MongoDB**, **PostgreSQL**, **MySQL**, **SQL Server**, or **Sybase ASE**.

11. In the **Auth Type** drop-down box, click **Nessus for BeyondTrust**.

    The Nessus for BeyondTrust options appear.

12. Configure each option for the **Database** authentication.

Option	Description	Required
Username	The username to log in to the host you want to scan.	yes
Domain	The domain of the username, which is recommended if using domain-linked accounts (managed accounts of a domain that are linked to a managed system).	no
BeyondTrust host	The Nessus for BeyondTrust IP address or DNS address.	yes
BeyondTrust port	The port on which Nessus for BeyondTrust listens.	yes
BeyondTrust API user	The API user provided by Nessus for BeyondTrust.	yes
BeyondTrust API key	The API key provided by Nessus for BeyondTrust.	yes
Checkout duration	The length of time, in minutes, that you want to keep credentials checked out in Nessus for BeyondTrust. Configure the checkout duration to exceed the typical duration of your Tenable Nessus scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Nessus for BeyondTrust so that password changes do not disrupt your Tenable Nessus	yes

	scans. If BeyondTrust changes a password during a scan, the scan fails.	
Use SSL	When enabled, Tenable Nessus uses SSL through IIS for secure communications. Configure SSL through IIS in Nessus for BeyondTrust before enabling this option.	no
Verify SSL certificate	When enabled, Tenable Nessus validates the SSL certificate. Configure SSL through IIS in Nessus for BeyondTrust before enabling this option.	no

13. Click **Save**.

SSH Integration

Complete the following steps to configure SSH credentialed network scans using BeyondTrust.

> **Note:** BeyondTrust is only compatible with Tenable Nessus Manager. It is not compatible with Tenable Nessus Professional.

To integrate Tenable Nessus with BeyondTrust using Windows:

1. Log in to Tenable Nessus Manager
2. Click **Scans**.

   The **My Scans** page appears.
3. Click **+New Scan**.

   The **Scan Templates** page appears.
4. Select a scan template.

   The selected scan template **Settings** page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a **Description**, **Folder location**, **Scanner location**, and specify **Target groups**.
8. Click the **Credentials** tab.

   The **Credentials** options appear. By default, the **Categories** drop-down box displays **Host**.
9. In the **Categories** drop-down, click **Host**.
10. In the **Categories** list, click **Windows** configuration.

    The selected configuration options appear.
11. In the selected configuration window, click the **Authentication method** drop-down box.

    The **Authentication method** options appear.
12. Select **BeyondTrust**.

The **BeyondTrust** options appear.

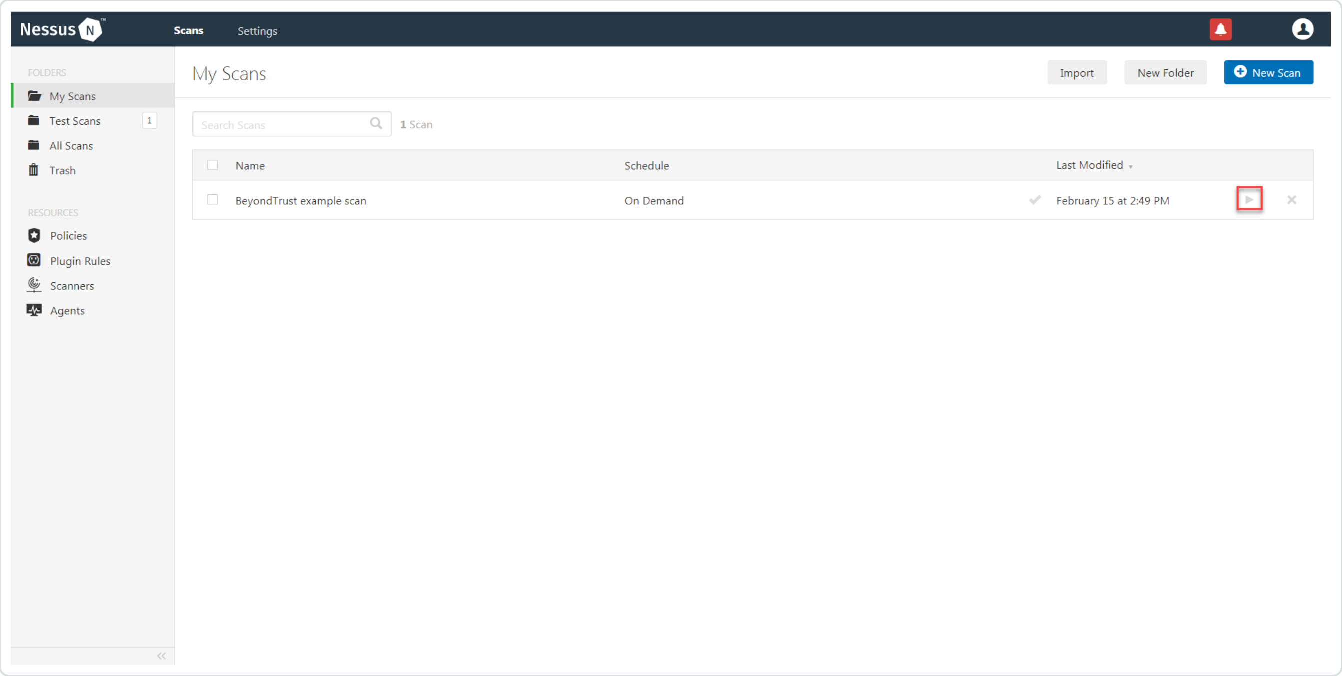
13. Configure the credentials.

Option	Description	Required
Username	The username to log in to the hosts you want to scan.	yes
Domain	The domain of the username, which is recommended if using domain-linked accounts (managed accounts of a domain that are linked to a managed system).	no
BeyondTrust host	The BeyondTrust IP address or DNS address.	yes
BeyondTrust port	The port on which BeyondTrust listens.	yes
BeyondTrust API user	The API user provided by BeyondTrust.	yes
BeyondTrust API key	The API key provided by BeyondTrust.	yes
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 Nessus scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable Nessus scans. If BeyondTrust changes a password during a scan, the scan fails.	yes
Use SSL	When enabled, Tenable Nessus uses SSL through	no

	IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.	
Verify SSL certificate	When enabled, Tenable Nessus validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.	no

14. Click **Save**.

15. To verify the integration is working, click the **Launch** button to initiate an on-demand scan.



My Scans

Name	Schedule	Last Modified
BeyondTrust example scan	On Demand	February 15 at 2:49 PM

16. Once the scan is complete, select the completed scan and look for the corresponding message - *OS Identification and Installed Software Enumeration over SSH: 97993*. This validates that authentication was successful.

Tenable Tenable Nessus for BeyondTrust (Windows)

Complete the following steps to configure Windows credentialed network scans using BeyondTrust.

> **Note:** BeyondTrust is only compatible with Tenable Nessus Manager.

To integrate Tenable Nessus with BeyondTrust using Windows:

1. Log in to Tenable Nessus Manager
2. Click **Scans**.

   The **My Scans** page appears.
3. Click **+New Scan**.

   The **Scan Templates** page appears.
4. Select a scan template.

   The selected scan template **Settings** page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a **Description**, **Folder location**, **Scanner location**, and specify **Target groups**.
8. Click the **Credentials** tab.

   The **Credentials** options appear. By default, the **Categories** drop-down box displays **Host**.
9. In the **Categories** drop-down, click **Host**.
10. In the **Categories** list, click **Windows** configuration.

    The selected configuration options appear.
11. In the selected configuration window, click the **Authentication method** drop-down box.

    The **Authentication method** options appear.
12. Select **BeyondTrust**.

The **BeyondTrust** options appear.

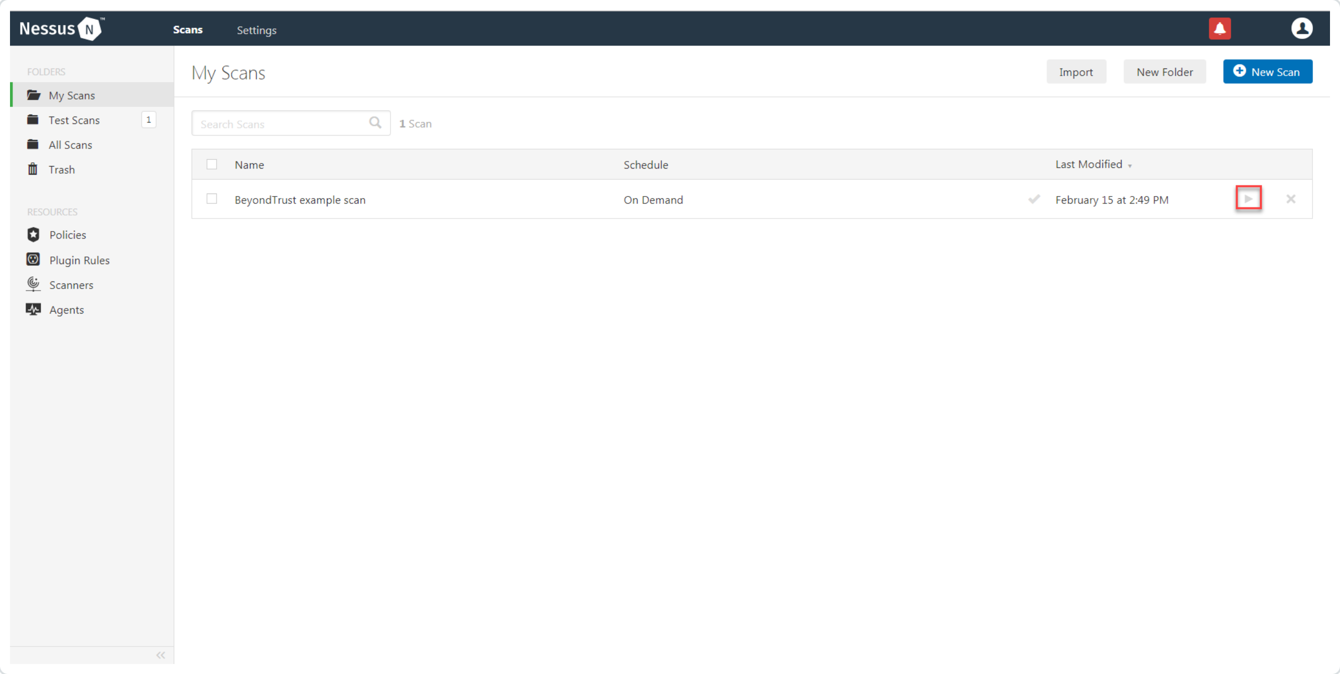
13. Configure the credentials.

Option	Description	Required
Username	The username to log in to the hosts you want to scan.	yes
Domain	The domain of the username, which is recommended if using domain-linked accounts (managed accounts of a domain that are linked to a managed system).	no
BeyondTrust host	The BeyondTrust IP address or DNS address.	yes
BeyondTrust port	The port on which BeyondTrust listens.	yes
BeyondTrust API user	The API user provided by BeyondTrust.	yes
BeyondTrust API key	The API key provided by BeyondTrust.	yes
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 Nessus scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable Nessus scans. If BeyondTrust changes a password during a scan, the scan fails.	yes
Use SSL	When enabled, Tenable Nessus uses SSL through	no

	IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.	
Verify SSL certificate	When enabled, Tenable Nessus validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.	no

13. Click **Save**.

14. To verify the integration is working, click **Launch** to initiate an on-demand scan.



Name	Schedule	Last Modified
BeyondTrust example scan	On Demand	February 15 at 2:49 PM

15. Once the scan is complete, select the completed scan and look for the corresponding message - *Microsoft Windows SMB Log In Possible: 10394*. This validates that authentication was successful.

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.

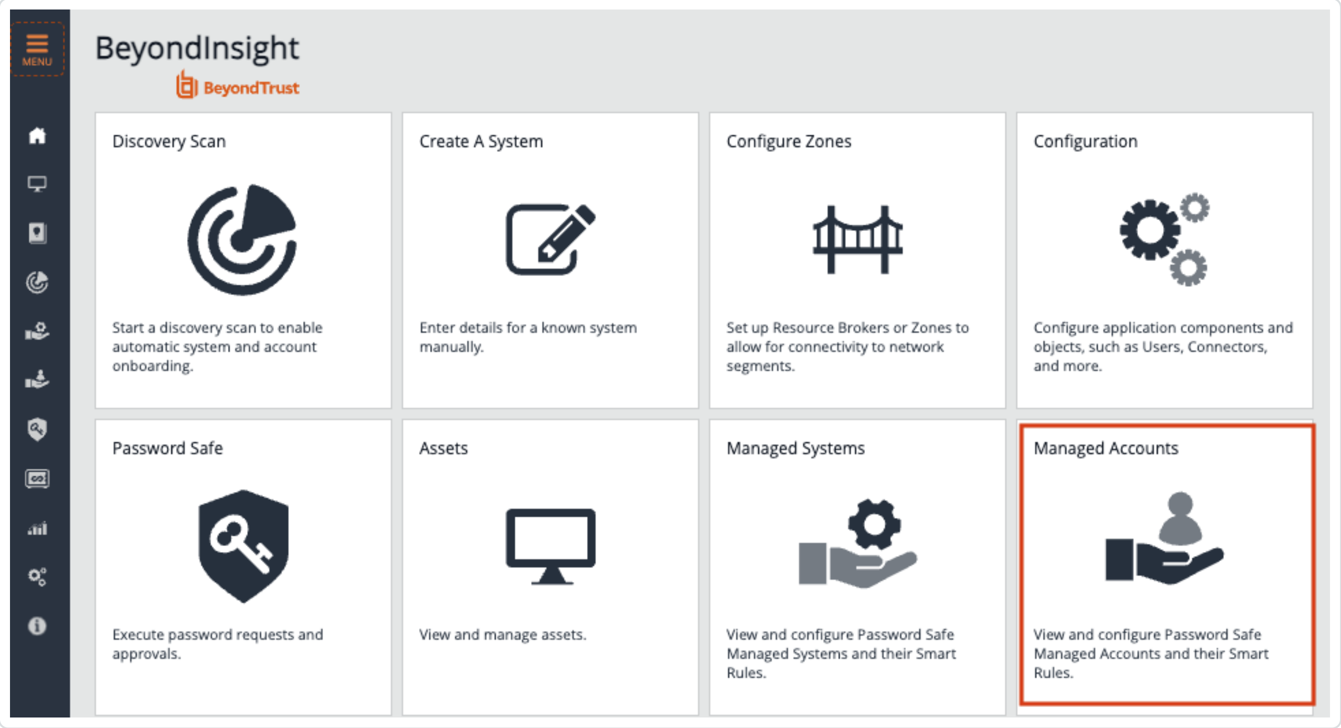
   > **Caution:** Do not select any **Authentication Rule Options** when using the API with Tenable integrations. This may cause the integration to fail.
7. Configure **Authentication Rules** by clicking **Add Authentication Rule**. Configure an IP address or range of IP addresses of one or more scanners.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

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

Enable API Access

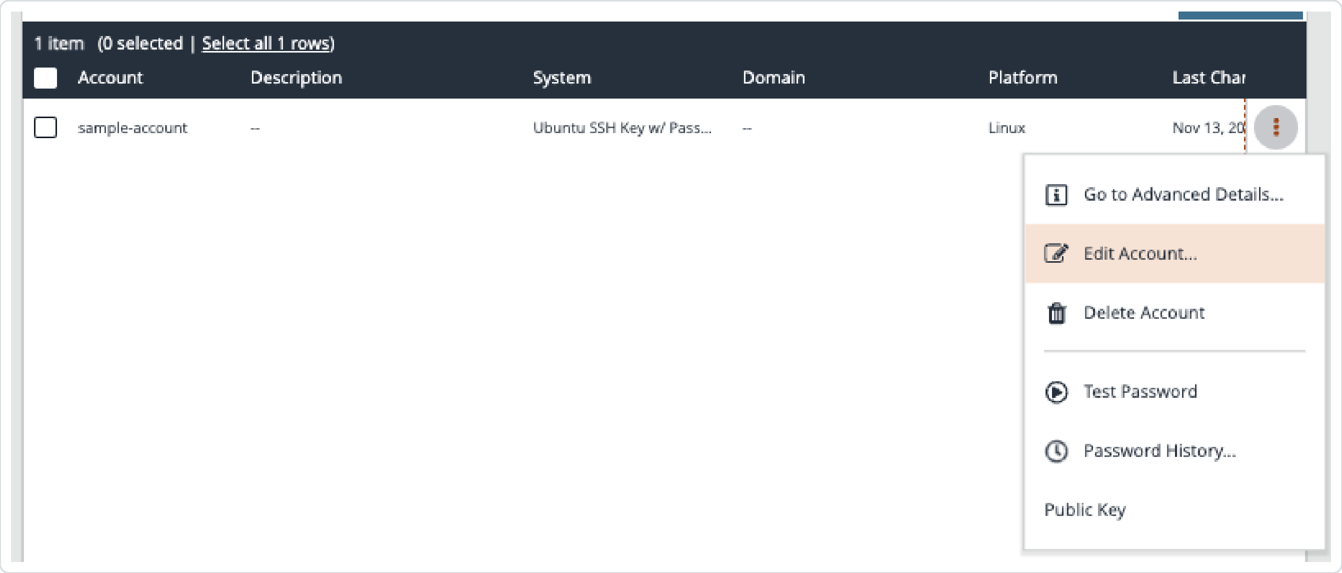
Note: Each **Managed Account** that you use for scanning must have **API Access** enabled. To enable API access:

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



MENU
BeyondInsight
BeyondTrust
Discovery Scan
Start a discovery scan to enable automatic system and account onboarding.
Create A System
Enter details for a known system manually.
Configure Zones
Set up Resource Brokers or Zones to allow for connectivity to network segments.
Configuration
Configure application components and objects, such as Users, Connectors, and more.
Password Safe
Execute password requests and approvals.
Assets
View and manage assets.
Managed Systems
View and configure Password Safe Managed Systems and their Smart Rules.
Managed Accounts
View and configure Password Safe Managed Accounts and their Smart Rules.

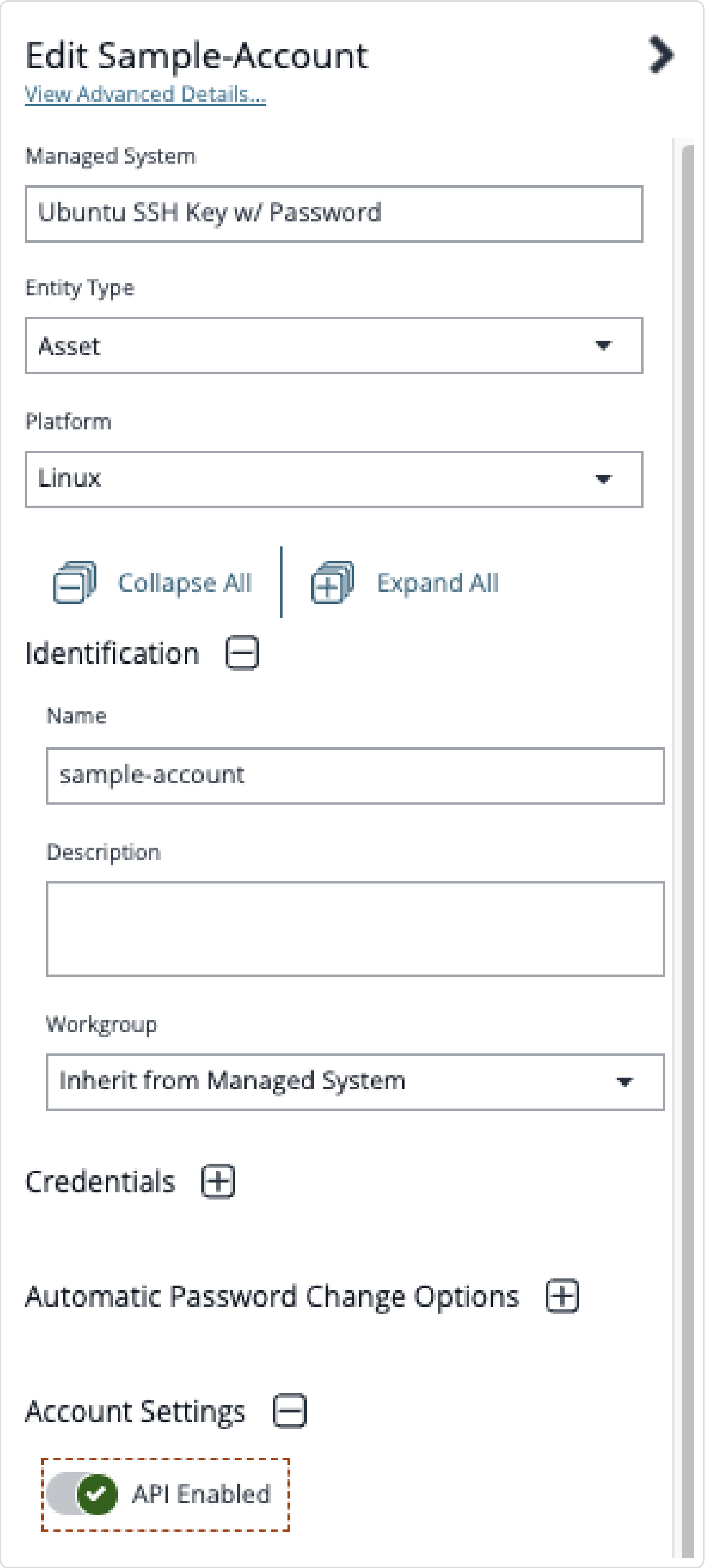
3. Click **Edit Account**.



1 item (0 selected | Select all 1 rows)

□	Account	Description	System	Domain	Platform	Last Char
□	sample-account	--	Ubuntu SSH Key w/ Pass...	--	Linux	Nov 13, 20

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



Edit Sample-Account

Managed System

Ubuntu SSH Key w/ Password

Entity Type

Asset

Platform

Linux

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

Customized Report

About Tenable

Elevation

BeyondInsight uses **Elevation** to handle privilege escalation for SSH accounts when performing scans. The **Elevation** option is used because some rules do not allow server login using `root`. **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 Nessus. The customized report defines the information needed for Tenable Nessus uploads.

To build the report:

1. Log in to BeyondInsight.
2. Go to - **Assets** > **Scan** > **Customize Report**.
3. Select the **Parameters**.
4. Click **Run Report**.

Note: You can run this report on any of your previous discovery scans, exported as a .csv file, and uploaded as scan targets in Tenable Nessus.

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 uncertainty, 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 vulnerability discovery, by visiting tenable.com.