Tenable Nessus and BeyondTrust PowerBroker Password Safe Integration Guide

Last Revised: May 22, 2021

Table of Contents

Welcome to Nessus for BeyondTrust

This document describes how to configure Tenable Nessus Manager for integration with the BeyondTrust PowerBroker Password Safe.

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

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 Nessus, customers have more choice and flexibility.

The benefits of integrating Nessus Manager with BeyondTrust include:

- Credential updates directly in Nessus, 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

The BeyondTrust Powerbroker Password Safe can be configured using either Windows or SSH. Click the corresponding link to view the configuration steps.

Windows Integration

SSH Integration

Tenable Nessus for BeyondTrust (Windows)

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

Note: BeyondTrust is only compatible with Nessus Manager.

To integrate Nessus with BeyondTrust using Windows:

1. Log in to 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.

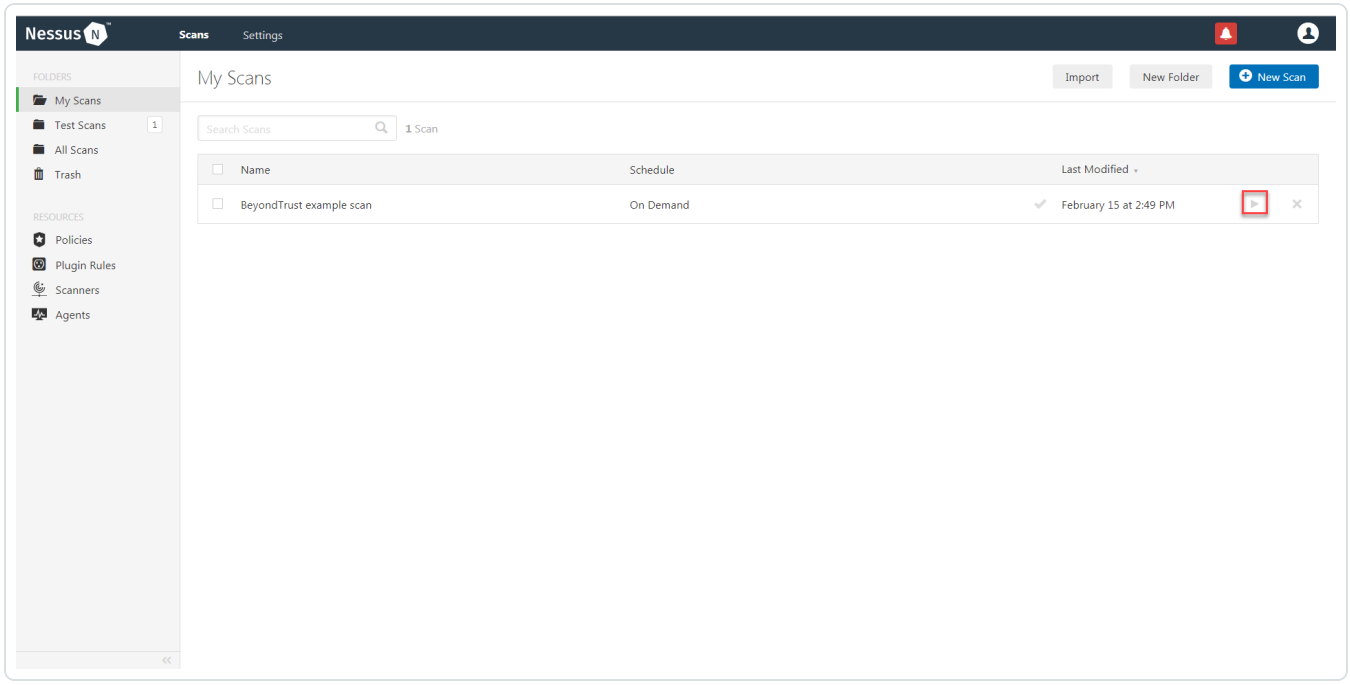
13. Configure the credentials.

Option	Description	Required
Username	The username to log in to the hosts you want to scan.	yes
Domain	The domain of the username, if required by BeyondTrust.	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 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 Nessus scans. If BeyondTrust changes a password during a scan, the scan fails.	yes
Use SSL	When enabled, Nessus uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.	no
Verify SSL cer-	When enabled, Nessus validates the SSL certificate.	no

tificate	You must configure SSL through IIS in BeyondTrust before enabling this option.	

13. Click **Save**.

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



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

SSH Integration

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

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

To integrate Nessus with BeyondTrust using Windows:

1. Log in to 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.

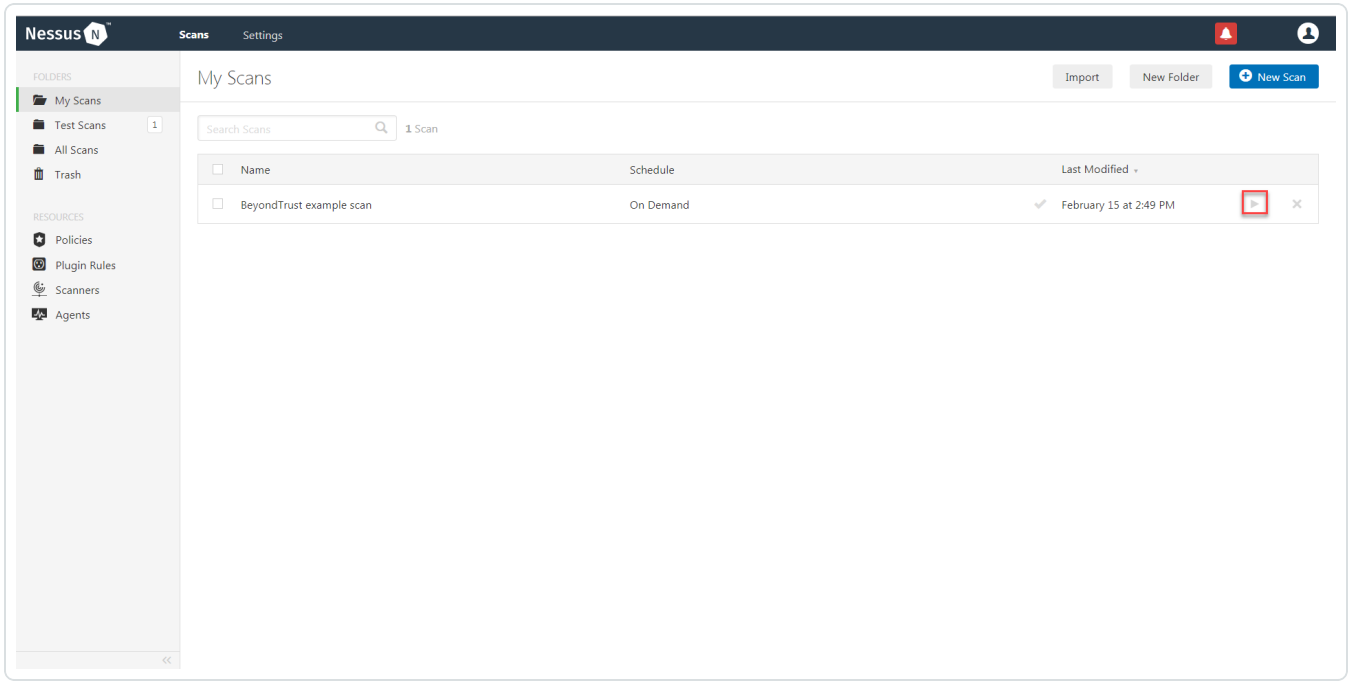
13. Configure the credentials.

Option	Description	Required
Username	The username to log in to the hosts you want to scan.	yes
Domain	The domain of the username, if required by BeyondTrust.	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 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 Nessus scans. If BeyondTrust changes a password during a scan, the scan fails.	yes
Use SSL	When enabled, Nessus uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.	no
Verify SSL cer-	When enabled, Nessus validates the SSL certificate.	no

tificate	You must configure SSL through IIS in BeyondTrust before enabling this option.	

14. Click **Save**.

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



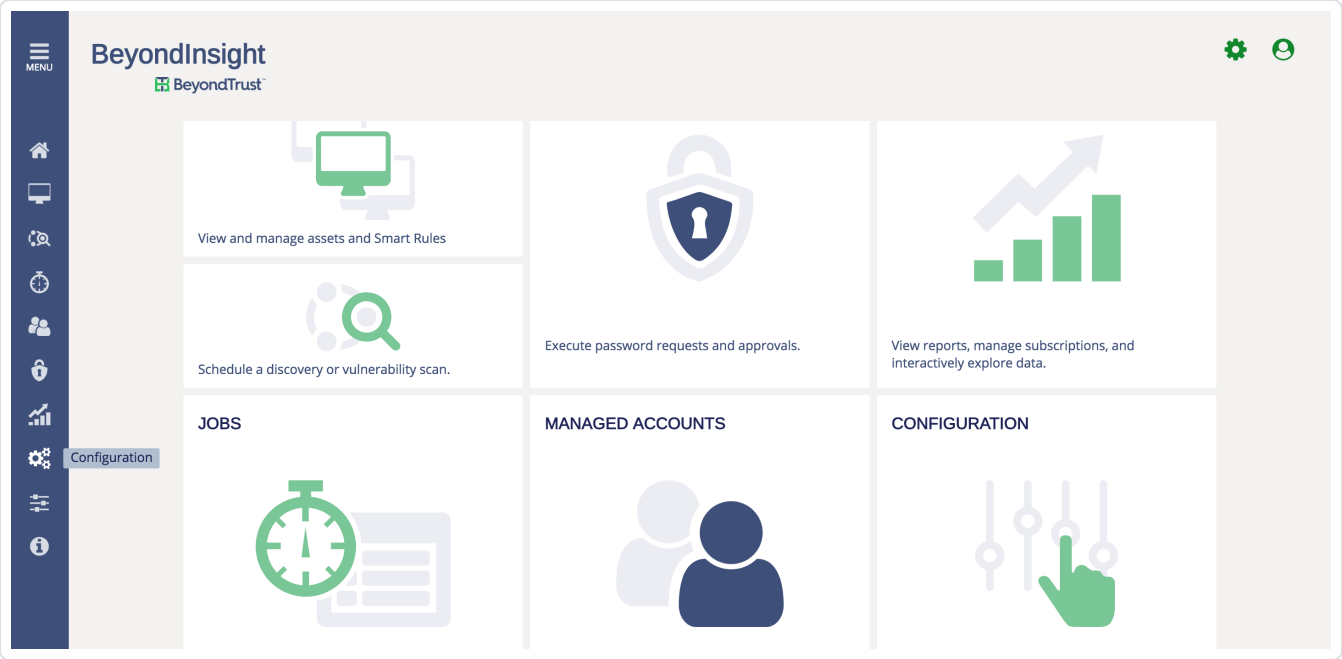
16. Once the scan has completed, select the completed scan and look for the corresponding message - *OS Identification and Installed Software Enumeration over SSH: 97993*. This validates that authentication was successful.

API Configuration

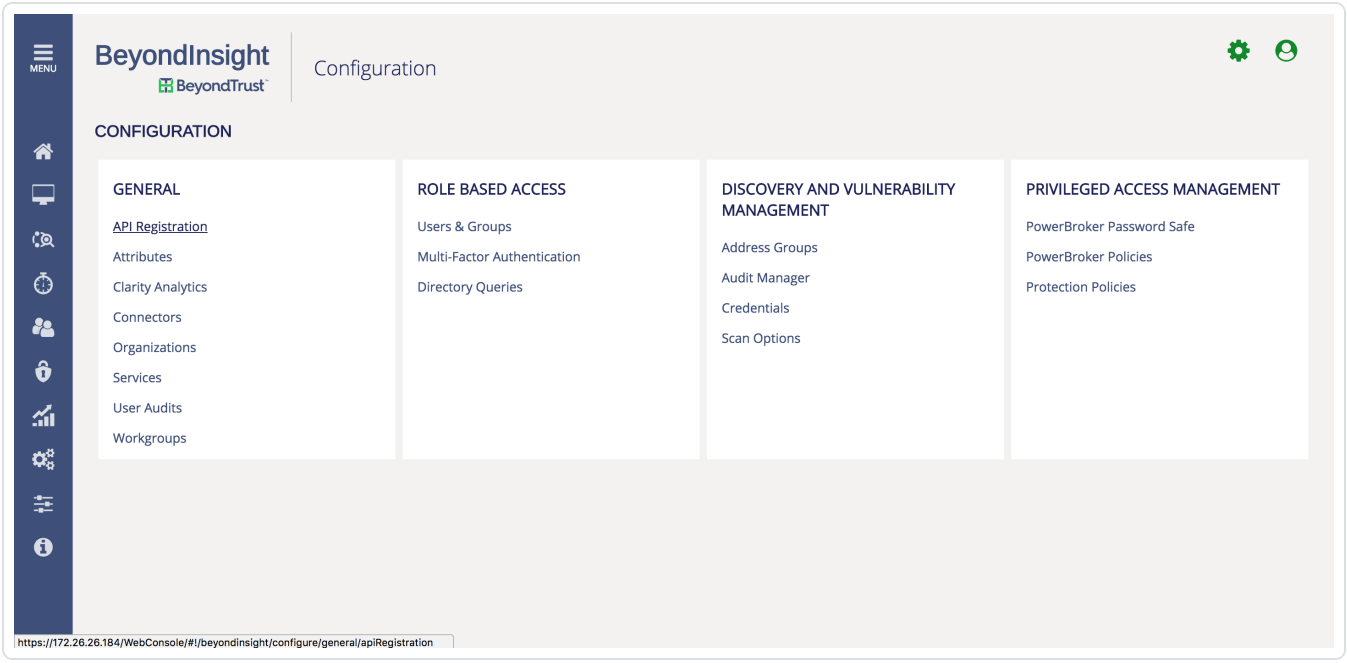
API Keys Setup

To setup your API keys:

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**.

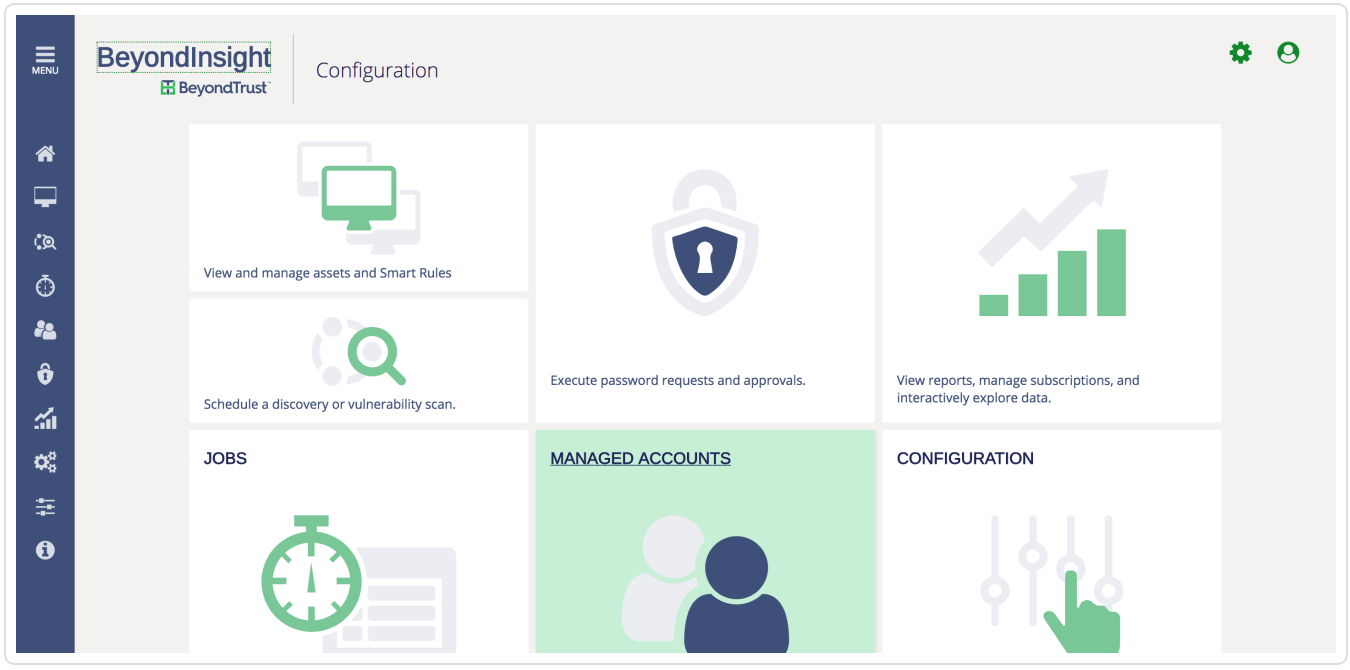
   Once saved, the API Key is available for future requests.

Enable API Access

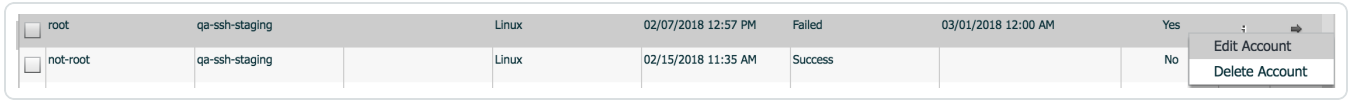
Each **Managed Account** that you use for scanning must have **API Access** enabled.

To Enable API Access:

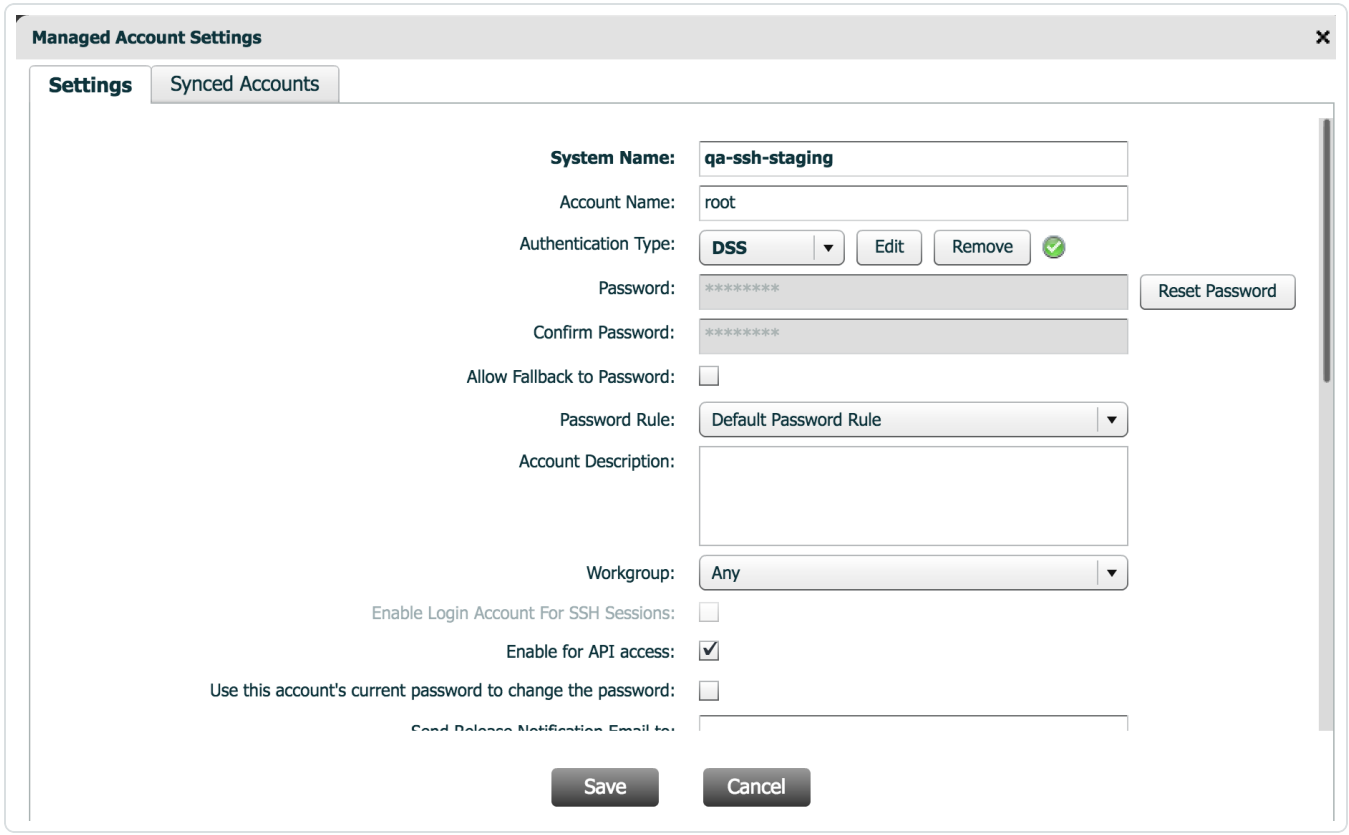
1. Log in to BeyondInsight.
2. Go to **Managed Accounts**.



3. Click **Edit Account**.



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



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 Nessus. The customized report defines the information needed for 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: This report can be run on any of your previous discovery scans, exported as an CSV, and uploaded as scan targets in 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 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.