# Table of Contents

- **Welcome to Tenable Vulnerability Management for BeyondTrust** ........................................ 3
- **Integrations** .................................................................................................................. 4
  - Windows Integration ........................................................................................................ 5
  - SSH Integration ............................................................................................................... 8
- **API Configuration** ........................................................................................................ 12
  - API Keys Setup .............................................................................................................. 13
  - Enable API Access ........................................................................................................ 14
- **Additional Information** ................................................................................................. 18
  - Elevation ......................................................................................................................... 19
  - Customized Report ......................................................................................................... 20
  - About Tenable ................................................................................................................. 21
Welcome to Tenable Vulnerability Management for BeyondTrust

This document provides information and steps for integrating Tenable 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 Tenable applications with BeyondTrust, customers have more choice and flexibility.

The benefits of integrating Tenable with BeyondTrust include:

- Credential updates directly in Tenable applications, 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 Password Safe integration can be configured using either Windows or SSH. Click the corresponding link to view the configuration steps.

- [Windows Integration](#)
- [SSH Integration](#)
Windows Integration

Tenable Vulnerability Management provides an option for BeyondTrust Windows integration. Complete the following steps to configure Tenable Vulnerability Management with BeyondTrust in Windows.

To integrate with Windows:

1. Log in to Tenable Vulnerability Management.
2. In the upper-left corner, click the button.
   The left navigation plane appears.
3. In the left navigation plane, click Settings.
   The Settings page appears.
4. Click the Credentials widget.
   The Credentials page appears. The credentials table lists the managed credentials you have permission to view.
5. Click the button next to the Credentials title.
   The credential form plane appears.
6. In the Host section, click Windows.
   The selected credential options appear.
7. In the Authentication Method drop-down, select BeyondTrust.
   The BeyondTrust options appear.
8. Configure the BeyondTrust credentials.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username to log in to the hosts you want to scan.</td>
<td>yes</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain of the username, which is recommended</td>
<td>no</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>BeyondTrust host</td>
<td>The BeyondTrust IP address or DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust port</td>
<td>The port on which BeyondTrust listens.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust API user</td>
<td>The API user provided by BeyondTrust.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust API key</td>
<td>The API key provided by BeyondTrust.</td>
<td>yes</td>
</tr>
<tr>
<td>Checkout duration</td>
<td>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 Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.</td>
<td>yes</td>
</tr>
<tr>
<td>Use SSL</td>
<td>When enabled, Tenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL certificate</td>
<td>When enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.</td>
<td>no</td>
</tr>
</tbody>
</table>

**Note:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable Vulnerability Management scans. If BeyondTrust changes a password during a scan, the scan fails.

What to do next:
Verify the integration is working.

1. On the **My Scans** page, click the **Launch** button to initiate an on-demand scan.

![Image of My Scans page](image)

2. Once the scan completes, click the scan.

   The scan details appear.

   Look for the following message - *Microsoft Windows SMB Log In Possible: 10394*. This validates that authentication was successful.
SSH Integration

Tenable Vulnerability Management provides an option for BeyondTrust Windows integration. Complete the following steps to configure Tenable Vulnerability Management with BeyondTrust in SSH.

Requirements

- Tenable Vulnerability Management account
- BeyondTrust account

**Required User Role:** Standard, Scan Manager, or Administrator

To configure Tenable Vulnerability Management for BeyondTrust SSH:

1. Log in to Tenable Vulnerability Management.
2. In the upper-left corner, click the button.

   The left navigation plane appears.
3. In the left navigation plane, click Settings.

   The Settings page appears.
4. Click the Credentials widget.

   The Credentials page appears. The credentials table lists the managed credentials you have permission to view.
5. Click the button next to the Credentials title.

   The credential form plane appears.
6. In the Host section, click SSH.

   The selected credential options appear.
7. In the Authentication Method drop-down, select BeyondTrust.

   The BeyondTrust options appear.
8. Configure the BeyondTrust credentials.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username to log in to the hosts you want to scan.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust host</td>
<td>The BeyondTrust IP address or DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust port</td>
<td>The port on which BeyondTrust listens.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust API user</td>
<td>The API user provided by BeyondTrust.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust API key</td>
<td>The API key provided by BeyondTrust.</td>
<td>yes</td>
</tr>
<tr>
<td>Checkout duration</td>
<td>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 Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable Vulnerability Management scans. If BeyondTrust changes a password during a scan, the scan fails.</td>
<td></td>
</tr>
<tr>
<td>Use SSL</td>
<td>When enabled, Tenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL certificate</td>
<td>When enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.</td>
<td>no</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Enable?</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Use private key</td>
<td>When enabled, Tenable Vulnerability Management uses private key-based authentication for SSH connections instead of password authentication. If it fails, the password is requested.</td>
<td>no</td>
</tr>
<tr>
<td>Use privilege escalation</td>
<td>When enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, it will use it for the scan.</td>
<td>no</td>
</tr>
<tr>
<td>Custom password prompt</td>
<td>The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Vulnerability Management receiving an unrecognized password prompt on the target host's interactive SSH shell.</td>
<td>no</td>
</tr>
<tr>
<td>Targets to prioritize</td>
<td>(missing or bad snippet)</td>
<td>no</td>
</tr>
</tbody>
</table>

**What to do next:**

To verify the integration is working:
1. On the **My Scans** page, click the **Launch** button to initiate an on-demand scan.

![My Scans page screenshot](image)

2. Once the scan completes, click the scan.

The scan details appear.

Look for the following message - *OS Identification and Installed Software Enumeration over SSH: 97993*. This validates that authentication was successful.
API Configuration

API Keys Setup

Enable API Access
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

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

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 Vulnerability Management. The customized report defines the information needed for Tenable Vulnerability Management uploads.

To build the report:

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

Note: This report can be run on any of your previous discovery scans, exported as a .csv file, and uploaded as a scan target in Tenable Vulnerability Management.
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 Vulnerability Management and leaders in continuous monitoring, by visiting tenable.com.