Password Safe

Tenable.io Integration Guide

Table of Contents

Tenable.io and Password Safe Integration Guide

Use Password Safe as an External Credential Provider for Tenable.io Asset Scans

This guide provides information and steps for integrating Tenable.io with BeyondTrust Password Safe.

Security administrators know that conducting network vulnerability assessments means getting access to, and navigating, an ever-changing sea of usernames, passwords, and privileges.

Tenable.io is a cloud-based vulnerability management platform that is designed to help organizations identify and manage security risks across their entire IT infrastructure. By integrating Tenable applications with BeyondTrust Password Safe, customers have more choice and flexibility.

The benefits of integrating Tenable with Password Safe 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.

Configure Password Safe

To use the integration, the following items must be configured in Password Safe:

- API registration.
- API account and group with correct permissions.
- Asset must exist in Password Safe with the same asset name as in Tenable.io (case sensitive).
- Managed asset must exist in Password Safe with the same asset name as in Tenable.io (case sensitive).
- Managed account used for Tenable scan. This account must be API enabled and be linked to the managed asset.

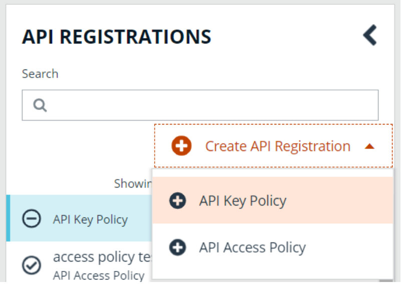
> ***Note:*** *The managed account must be a shared account and not a dedicated account.*

- Access policy that allows the API group or user to request the managed account.

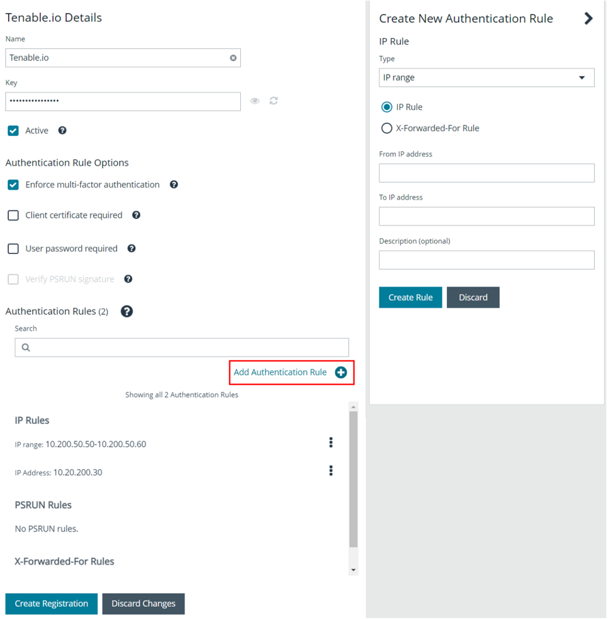
Create an API Registration

In Password Safe, all APIs must be registered. To register a new API:

1. In the BeyondInsight console, go to **Configuration > General > API Registrations**.
2. Click **Create API Registration**.
3. Select **API Key Policy**.



4. Provide a name for the API registration.
5. You must add an IP authentication rule for the address of your Tenable.io instance:
   - Click **Add Authentication Rule**.
   - From the **Type** dropdown, select **Single IP Address**.
   - Leave the **IP Rule** option selected.
   - Provide the **IP Address**.
   - Click **Create Rule**.
6. You must also add the IP range of the managed assets to be scanned.
   - Click **Add Authentication Rule**.
   - From the **Type** dropdown, select **IP Range**.
   - Leave the **IP Rule** option selected.
   - Provide **From** and **To** IP addresses.
   - Click **Create Rule**.
7. Click **Create Registration**.


Tenable.io Details

Name: Tenable.io

Key: ••••••••••••••••

☑ Active

Authentication Rule Options

☑ Enforce multi-factor authentication

□ Client certificate required

□ User password required

□ Verify PSRUN signature

Authentication Rules (2)

Showing all 2 Authentication Rules

IP Rules

IP range: 10.200.50.50-10.200.50.60

IP Address: 10.20.200.30

PSRUN Rules

No PSRUN rules.

X-Forwarded-For Rules

Create New Authentication Rule

IP Rule

Type: IP range

● IP Rule

○ X-Forwarded-For Rule

From IP address

To IP address

Description (optional)

> ***Note:** The **API Key** is required for the Tenable.io configuration.*

Create an Access Policy

Before you can configure an API group, you must have an access policy for the group that allows managed accounts to be requested and allows for API callers to override the automatic password changes after they are released. Create the access policy as follows:

1. In the BeyondInsight console, go to **Configuration > Privileged Access Management Policies > Access Policies**.
2. Select an existing access policy or create a new one.
3. In the access policy, click **Create Schedule** and select the appropriate options.
4. Under **Policy Types**, toggle **View Password** to enable it.
5. Check the **Allow API Rotation Override** option. This allows API callers to override the *Change Password After Any Release* managed account setting for view-type requests.
6. Once the new schedule information is completed, click **Create Schedule**.

Configure API Account and Group

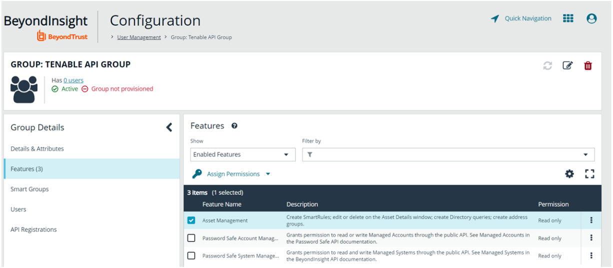
An API account and group must be configured for use by Tenable.io. You can use an existing local account and group, or create new ones.

To create a new user:

1. In the BeyondInsight console, go to **Configuration > Role Based Access > User Management**
2. Click the **Users** tab.
3. Click **Create New User** and select **Create a New User**.
4. Provide user details, such as identification and credentials, and click **Create User**.

To create a new group and enable features and Smart Groups for that group:

5. In the BeyondInsight console, go to **Configuration > Role Based Access > User Management**.
6. Click the **Groups** tab.
7. Click **Create New Group** and select **Create a New Group**.
8. Provide group name and description, and then click **Create Group**.
9. You are taken to the details for the group, where **Features** is selected by default.
10. In the **Features** grid, locate the following features, select them, and then click **Assign Permissions > Assign Permissions Read Only** above the grid:
    - Asset Management
    - Password Safe Account Management
    - Password Safe System Management



Show: Enabled Features

Filter by:

3 items (1 selected)

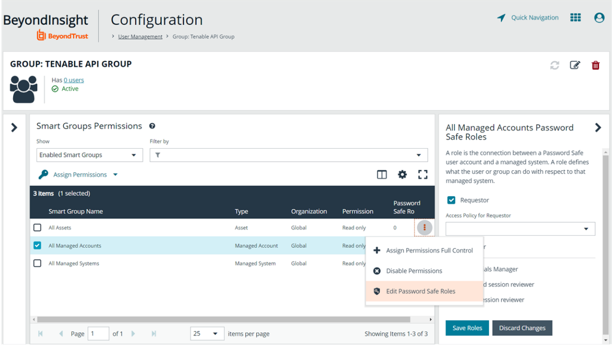
	Feature Name	Description	Permission
☑	Asset Management	Create SmartRules; edit or delete on the Asset Details window; create Directory queries; create address groups.	Read only
□	Password Safe Account Manag...	Grants permission to read or write Managed Accounts through the public API. See Managed Accounts in the Password Safe API documentation.	Read only
□	Password Safe System Manage...	Grants permission to read and write Managed Systems through the public API. See Managed Systems in the BeyondInsight API documentation.	Read only

***Tip:** Use the filters above the grids to easily locate the features by their names.*

11. Under **Group Details**,select **Smart Groups**.
12. In the **Smart Groups Permissions** grid, locate the following Smart Groups, select them, and then click **Assign Permissions > Assign Permissions Read Only** above the grid:
    - All Assets
    - All Managed Accounts
    - All Managed Systems

***Tip:** Use the filters above the grids to easily locate the Smart Groups by their names.*

13. The **All Managed Accounts** Smart Group must have **Requestor** selected as a Password Safe role.
    - Click the vertical ellipsis to the right of the **Smart Group**, and then select **Edit Password Safe Roles**.
    - Check the **Requestor** box, and then select a policy from the **Access Policy for Requestor** dropdown. This policy is applied to the managed account that is used for the scan.
    - Click **Save Roles**.

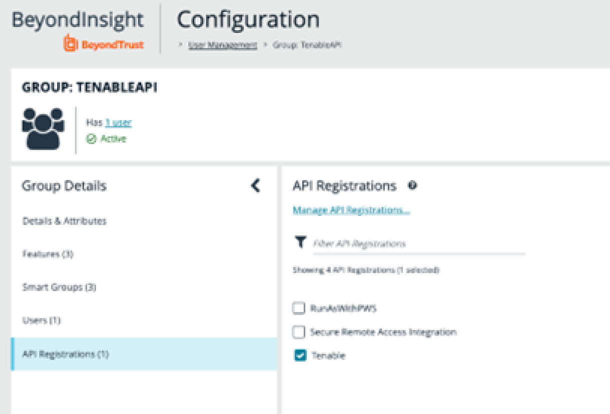


	Smart Group Name	Type	Organization	Permission	Password Safe Ro
□	All Assets	Asset	Global	Read only	0
☑	All Managed Accounts	Managed Account	Global	Read only	
□	All Managed Systems	Managed System	Global	Read only	

A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system.

☑ Requestor

14. To add the API user created above to the group:
    - Under **Group Details**, select **Users**.
    - Select **Users Not Assigned** from the **Show** dropdown list.
    - From the **Filter by** dropdown , select **Username**. Type the user name in the **Username** field.
    - Select the user, and then click **Assign User** above the grid.
15. Finally, assign the API that was registered for the integration to this group:
    - Under **Group Details**, select **API Registrations**. A list of API registrations is displayed.
    - Check the box beside the API registration created above.



□ RunAsWithPWS
□ Secure Remote Access Integration
☑ Tenable

Verify the Asset and Managed System in Password Safe

The asset scanned by Tenable.io must exist in the **Assets** and **Managed Systems** grids in BeyondInsight.

To verify that the asset exists in BeyondInsight:

1. In the BeyondInsight console, select **Assets**.
2. From the **Smart Group filter** dropdown on the **Assets** page, select **All Assets**. Verify that the asset to be scanned is displayed in the list of available assets.

To verify that the asset exists in as a managed system:

1. In the BeyondInsight console, select **Managed Systems**.
2. From the **Smart Group filter** dropdown on the **Managed Systems** page, select **All Managed Systems**. Verify that the asset to be scanned is displayed in the list of available managed systems.

Verify the Managed Account Used by Tenable.io Scan in Password Safe

The managed asset scanned by Tenable.io must be linked to an existing managed account in Password Safe. This managed account:

- Can be either a local or domain account
- Must be shared, not dedicated
- Must be a local admin on the asset being scanned
- Must be enabled for use with API

To confirm the account is enabled for use with API:

1. In the BeyondInsight console, go to **Managed Accounts**.
2. In the **Filter by** dropdown, select **Account**. Enter the account name in the **Account** field.
3. Click the vertical ellipsis to the right of the new group, and then select **Edit Account**.
4. Under **Account Settings**, make sure the **API Enabled** toggle button is enabled.

To confirm the account is linked to the system to be scanned:

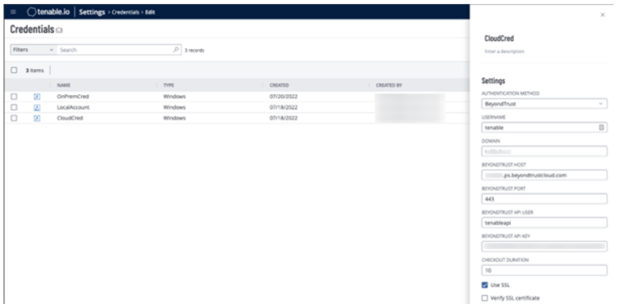
1. In the BeyondInsight console, go to **Managed Accounts**.
2. From the **Filter by** dropdown, select **Account**. Enter the account name in the **Account** field.
3. Click the vertical ellipsis to the right of the new group, and then select **Go to Advanced Details**. Under **Account Details**, select **Linked Systems**.
4. Select **Linked** under the **Show** dropdown. Verify that the linked system is listed.

Configure Tenable Integration

Within Tenable.io, the BeyondTrust Password Safe integration can be configured using either Windows or SSH.

Windows Integration

To integrate Tenable.io with BeyondTrust in Windows:



NAME	TYPE	CREATED	CREATED BY
OnPremCred	Windows	07/20/2022	[redacted]
LocalAccount	Windows	07/18/2022	
CloudCred	Windows	07/18/2022	

CloudCred

Enter a description

Settings

AUTHENTICATION METHOD: BeyondTrust

USERNAME: tenable

DOMAIN: [redacted]

BEYONDTRUST HOST: [redacted].ps.beyondtrustcloud.com

BEYONDTRUST PORT: 443

BEYONDTRUST API USER: tenableapi

BEYONDTRUST API KEY: [redacted]

CHECKOUT DURATION: 10

☑ Use SSL

□ Verify SSL certificate

1. Log in to Tenable.io.
2. In the upper-left corner, click the **Menu** icon. This displays the left navigation pane.
3. From the menu, click **Settings**.
4. On the **Settings** page, click **Credentials**. This displays the credentials table, which lists managed credentials that you have permission to view.
5. Click the **Can Edit** button next to the credentials title to open the credential form.
6. In the **Host** section, click **Windows**. Selected credential options are displayed.
7. Select **BeyondTrust** from the **Authentication Method** dropdown.
8. Configure the BeyondTrust credentials:

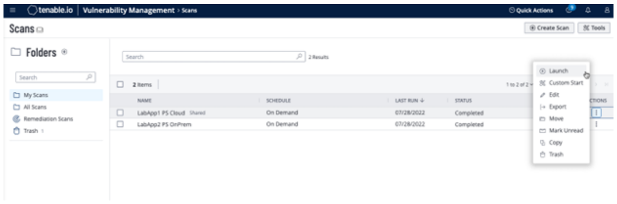
Option	Description	Required
Username	The username to log in to the hosts you want to scan.	Yes
Domain	The domain of the username, if required by BeyondTrust.	No
BeyondTrust Host	The BeyondTrust IP address or DNS address.	Yes
BeyondTrust Port	The port on which BeyondTrust listens.	Yes
BeyondTrust API 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 Tenable.io 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.io scans. If BeyondTrust changes a password during a scan, the scan fails.*	Yes
Use SSL	When enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.	No
Verify SSL Certificate	When enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.	No

9. To create a scan that uses these credentials:
   - Click the **Menu** icon in the upper-left corner.
   - From the menu, under **Vulnerability Management**, select **Scans**.
   - In the upper-right corner, click **Create Scan**. Select the appropriate scan template and update settings as required.
   - Select **Credentials** from the left menu, and then click **Add Credentials**. Select the BeyondTrust Password Safe credentials created in the previous step.
   - Click **Save**.

Verify Windows Integration

To verify that the Windows integration is working:

1. Click the **Menu** icon in the upper-left corner.
2. From the menu, under **Vulnerability Management**, select **Scans**.
3. Under **Folders**, select **My Scans**.
4. Select the ellipsis next to the scan you want to test. Click **Launch** to initiate an on-demand scan, and then click the completed scan to view scan details. The message *Microsoft Windows SMB Log In Possible: 10394* displays when authentication is successful.



NAME	SCHEDULE	LAST RUN	STATUS
LabApp1 PS Cloud Shared	On Demand	07/28/2022	Completed
LabApp2 PS OnPrem	On Demand	07/28/2022	Completed

SSH Integration

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

Requirements:

- Tenable.io account
- BeyondTrust account
- Required User Role - Standard, Scan Manager, or Administrator

To configure Tenable.io for BeyondTrust SSH:

1. Log in to Tenable.io.
2. Click the **Menu** icon in the upper-left corner.
3. From the menu, select **Settings**.
4. Under **Scanning**, click **Credentials**. The credentials table lists managed credentials that you have permission to view.
5. Click the **Can Edit** button next to the credentials title to open the credential form.
6. In the **Host** section, click **SSH**. Selected credential options are displayed.
7. Select **BeyondTrust** from the **Authentication Method** dropdown.
8. Configure the BeyondTrust credentials:

Option	Description	Required
Username	The username to log in to the hosts you want to scan.	Yes
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.io 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.io scans. If BeyondTrust changes a password during a scan, the scan fails.*	Yes
Use SSL	When enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.	No
Verify SSL Certificate	When enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.	No
Use Private Key	When enabled, Tenable.io uses private key-based authentication for SSH connections instead of password authentication. If it fails, the password is requested.	No

Option	Description	Required
Use Privilege Escalation	When enabled, BeyondTrustuses the configured privilege escalation command. If it returns a value, it will use it for the scan.	No
Custom Password Prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable.io receiving an unrecognized password prompt on the target host's interactive SSH shell.	No

Verify SSH Integration

To verify that the SSH integration is working:

1. Click the **Menu** icon in the upper-left corner.
2. From the menu, under **Vulnerability Management**, select **Scans**.
3. Under **Folders**, select **My Scans**.
4. Click the ellipsis next to the scan you want to test. Click **Launch** to initiate an on-demand scan, and then click the completed scan to view scan details. The message *OS Identification and Installed Software Enumeration over SSH: 97993* displays when authentication is successful.

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. Elevation can be enforced in BeyondInsight at system level or account level.

> *For more information, please see Add a Managed System Manually at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cloud/admin/add-assets/add-managed-systems.htm.*

Customized Report

You can build a customized report in BeyondInsight to import hosts from a CSV to scan in Tenable.io. The customized report defines the information needed for Tenable.io uploads.

To build the report:

1. In the BeyondInsight console, go to **Analytics & Reporting**.
2. Under **All Reports**, select **Assets**, and then select the report you want to view.
3. Select parameters to configure the report, and then click **View Report**.

> ***Note:*** *This report can be run on any previous discovery scan, exported as a CSV, and uploaded as a scan target in Tenable.io.*