Tenable and BeyondTrust Password Safe Integration Guide

Last Revised: April 01, 2026

Table of Contents

Welcome to BeyondTrust for Tenable

Security administrators know that conducting network vulnerability assessments means getting access to and navigating an ever-changing sea of user names, passwords, and privileges. By integrating Tenable applications with BeyondTrust, customers have more choice and flexibility. This document provides information and steps for integrating Tenable with BeyondTrust Password Safe and BeyondTrust Password Safe Cloud.

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.

Integration with Tenable Nessus

The BeyondTrust Password Safe integration with Tenable Nessus can be configured using either Database, Windows, or SSH.

Tenable Nessus Database Integration

Tenable provides full database support for BeyondTrust.

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

To configure Tenable for BeyondTrust database:

1. Log in to your Tenable user interface.
2. In the left navigation, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click the **Create Scan** button.

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

   The scan configuration 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 **Settings** 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 **BeyondTrust**.

    The 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 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 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 scans. If BeyondTrust changes a password during a scan, the scan fails.	yes
Use SSL	When enabled, the integration uses SSL through IIS for secure communications. Configure SSL through IIS in BeyondTrust	no

	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	When enabled, the intergation validates the SSL certificate. Configure SSL through IIS in BeyondTrust before enabling this option.	no

13. Do one of the following:
    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

    Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Tenable Nessus 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 your Tenable user interface.
2. In the left navigation, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click the **Create Scan** button.

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

   The scan configuration 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. In the **Select a Credential** menu, select the **Host** drop-down.
10. Select **SSH**.

    The **Settings** pane appears.
11. In the **Auth Type** drop-down box, click **BeyondTrust**.

    The BeyondTrust options appear.
12. Configure each option for the **SSH** authentication.

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 Nessus scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.	yes

	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.	
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target.	yes
Use SSL	When enabled, Tenable Nessus uses SSL through IIS for secure communications. You must 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.	no
Verify SSL certificate	When enabled, Tenable Nessus validates the SSL certificate. You must configure SSL through IIS in	no

	BeyondTrust before enabling this option.	
Use private key	When enabled, Tenable Nessus uses private key-based authentication for SSH connections instead of password authentication. If it fails, the password is requested.	no
Use privilege escalation	When enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, 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 Nessus receiving an unrecognized password prompt on the target host's interactive SSH shell.	no
Targets to prioritize credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	no

13. Do one of the following:

    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

> **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Tenable Nessus Windows Integration

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 your Tenable user interface.
2. In the left navigation, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click the **Create Scan** button.

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

   The scan configuration 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. In the **Select a Credential** menu, select the **Host** drop-down.
10. Select **Windows**.

    The **Settings** pane appears.
11. In the **Auth Type** drop-down box, click **BeyondTrust**.

The BeyondTrust options appear.

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

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
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Windows target.	no
Key Distribution	(Required if Kerberos Target Authentication is	yes

Center (KDC)	enabled) This host supplies the session tickets for the user.	
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Domain	(Required if Kerberos Target Authentication is enabled) The Kerberos Domain is the authentication domain, usually noted as the domain name of the target.	yes
Use SSL	When enabled, Tenable Nessus uses SSL through IIS for secure communications. You must 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.	no
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. Do one of the following:

    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

      Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Integration with Tenable Security Center

The BeyondTrust Password Safe integration with Tenable Security Center can be configured using either Windows or SSH.

Tenable Security Center SSH Integration

Tenable Security Center provides an option forBeyondTrust SSH integration. Complete the following steps to configure Tenable Security Center with BeyondTrust in SSH.

Requirements

- Tenable Security Center account
- BeyondTrust account

To configure Tenable Security Center for BeyondTrust SSH:

1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scanning**.

   A drop-down box appears.
3. Click **Credentials**.

   The **Credentials** window opens.
4. In the upper-right corner, click the **+ Add** button.

   The **Add Credential** window opens.
5. In the SSH section, click **BeyondTrust**.

   The **Add Credential** configuration page appears.
6. In the **General** section, enter a descriptive **Name**.
7. (Optional) Add a **Description** and select a **Tag**.
8. In the **BeyondTrust Credential** section, configure each field for **SSH** authentication.
9. Click **Save**.
10. Next, follow the steps for adding the credential to a scan.

Tenable Security Center Windows Integration

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

1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scanning**.

   A drop-down box appears.
3. Click **Credentials**.

   The **Credentials** window opens.
4. In the upper-right corner, click the **+ Add** button.

   The **Add Credential** window opens.
5. In the **Windows** section, click **BeyondTrust**.

   The **Add Credential** configuration page appears.
6. In the **General** section, enter a descriptive **Name**.
7. (Optional) Add a **Description** and select a **Tag**.
8. In the **BeyondTrust Credential** section, configure each field for **Windows** authentication.

   See the Tenable Security Center User Guide to get detailed descriptions for each option.
9. Click **Save**.
10. Next, follow the steps for adding the credential to a scan.

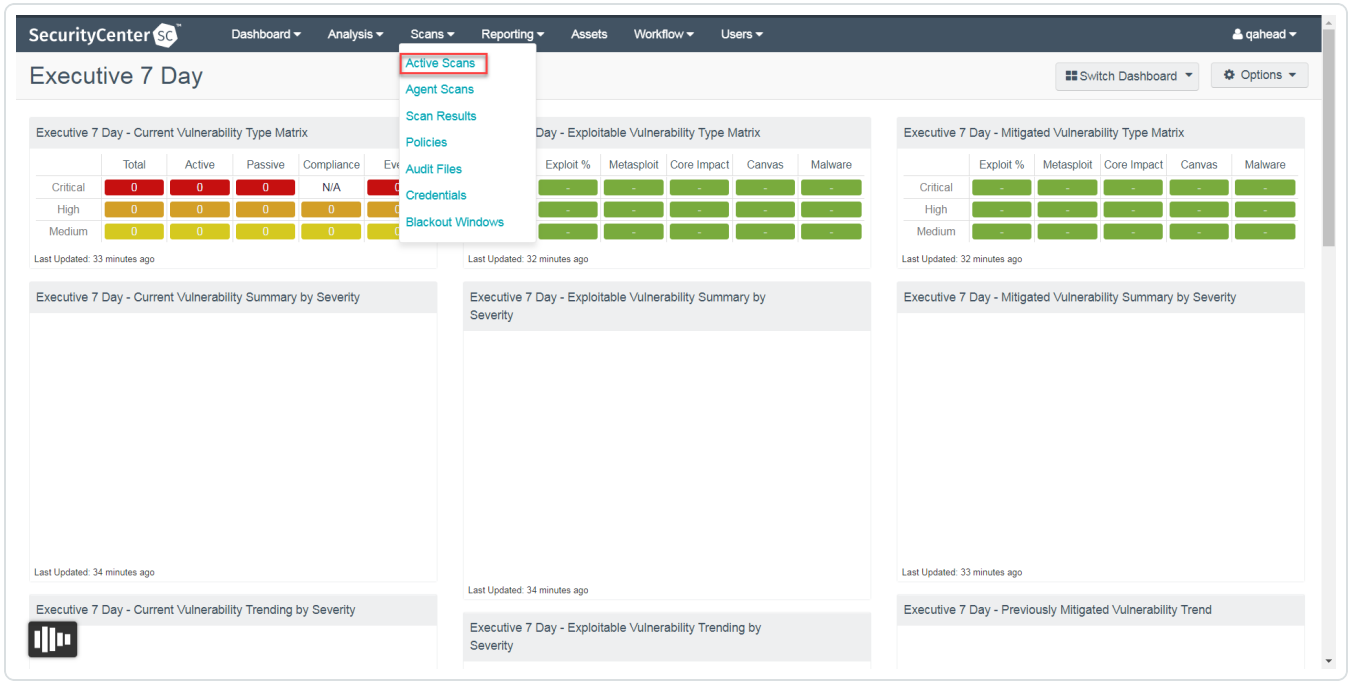
Add the BeyondTrust Credential to a Scan

To add the BeyondTrust credential to the scan:

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

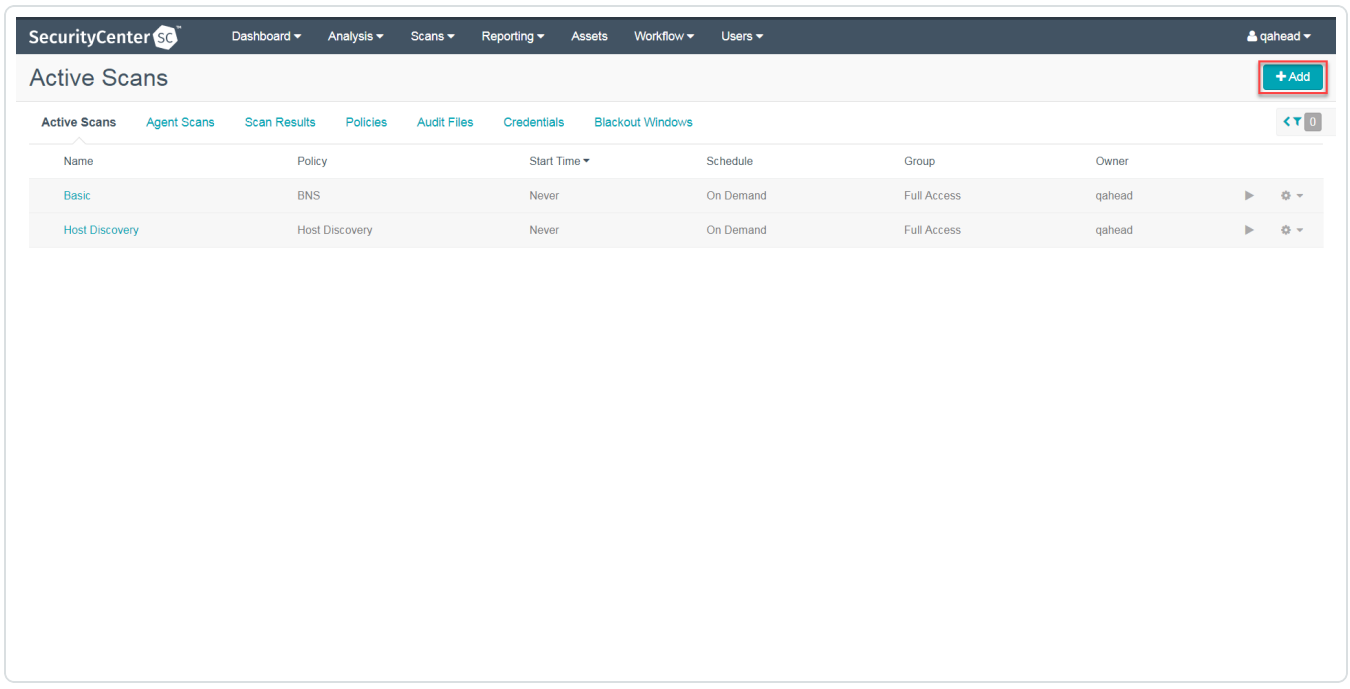
   A drop-down appears.

2. Select **Active Scans**.



The **Active Scans** window appears.

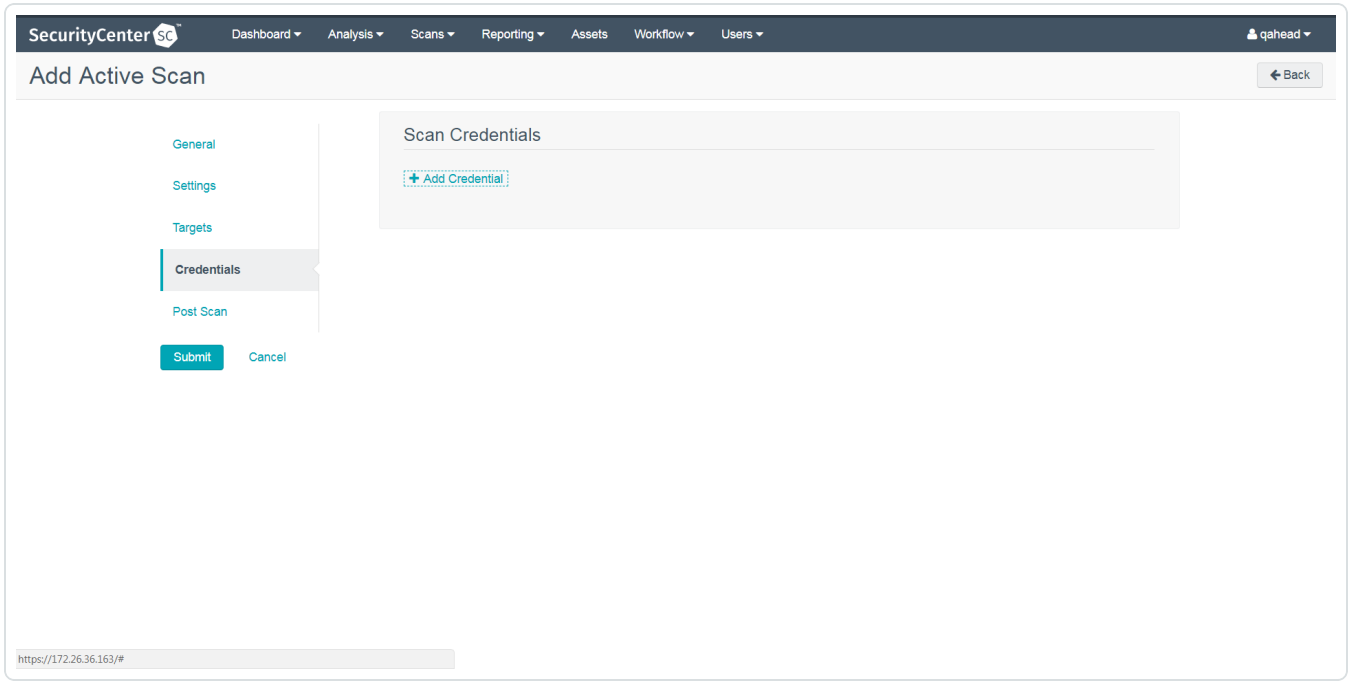
3. In the top-right corner, click **+Add**.



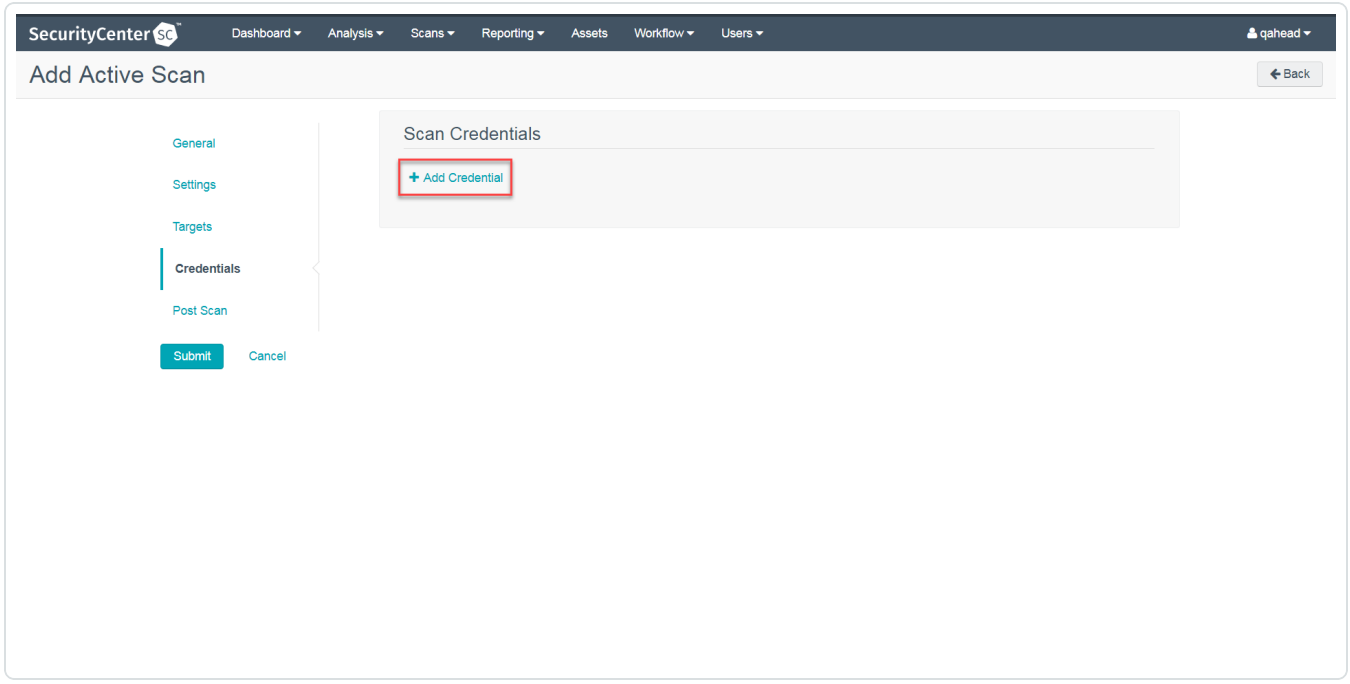
The **Add Active Scan** window appears.

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

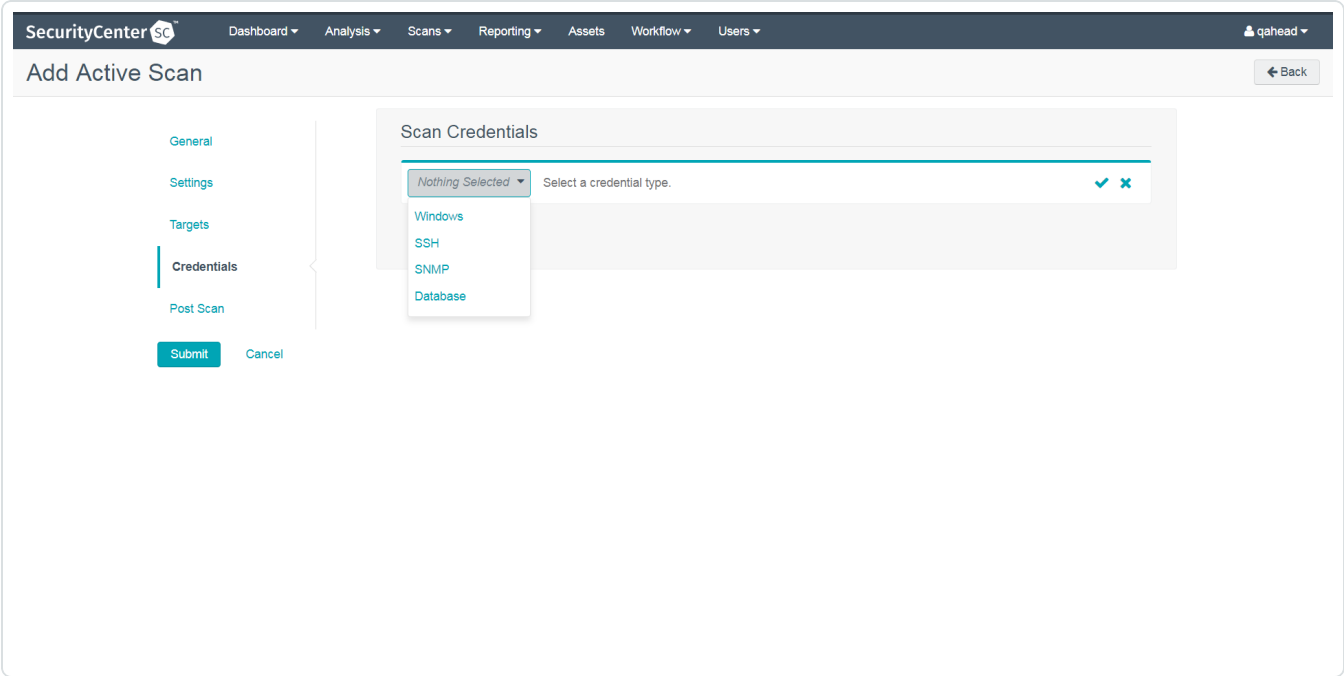
   The **Scan Credentials** section appears.



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



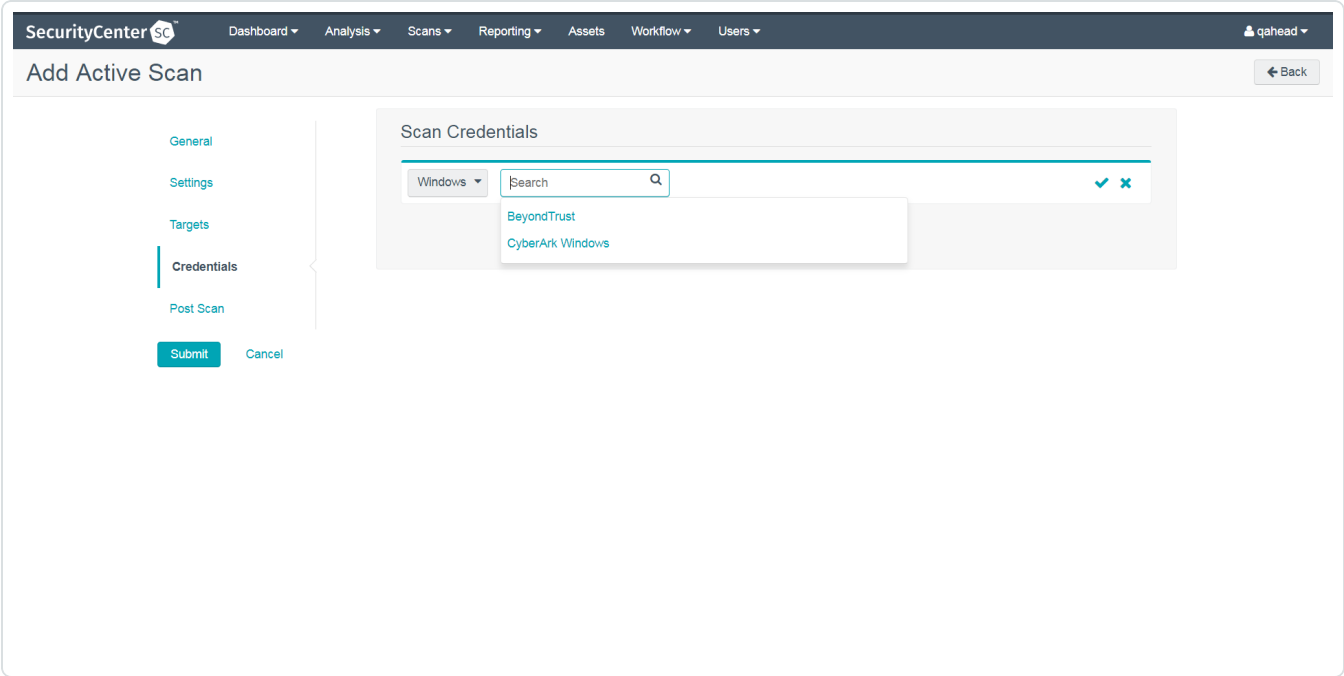
   A drop-down appears.



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**.

Integration with Tenable Vulnerability Management

The BeyondTrust Password Safe integration with Tenable Vulnerability Management can be configured using either Database, Windows, or SSH.

Database Integration

Tenable Vulnerability Management provides full database support for BeyondTrust.

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

To configure Tenable for BeyondTrust database:

1. Log in to your Tenable user interface.
2. In the left navigation, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click the **Create Scan** button.

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

   The scan configuration 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 **Settings** 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 **BeyondTrust**.

    The 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 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 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 scans. If BeyondTrust changes a password during a scan, the scan fails.	yes
Use SSL	When enabled, the integration uses SSL through IIS for secure communications. Configure SSL through IIS in BeyondTrust	no

	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	When enabled, the intergation validates the SSL certificate. Configure SSL through IIS in BeyondTrust before enabling this option.	no

13. Do one of the following:
    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

    Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

SSH Integration

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

Required User Role: Standard, Scan Manager, or Administrator

To configure Tenable Vulnerability Management for BeyondTrust SSH:

1. Log in to your Tenable user interface.
2. In the left navigation, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click the **Create Scan** button.

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

   The scan configuration 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. In the **Select a Credential** menu, select the **Host** drop-down.
10. Select **SSH**.

    The **Settings** pane appears.
11. In the **Auth Type** drop-down box, click **BeyondTrust**.

    The BeyondTrust options appear.
12. Configure each option for the **SSH** authentication.

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 Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins,	yes

	the new scan fails. **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.	
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target.	yes
Use SSL	When enabled, Tenable Vulnerability Management uses SSL through IIS for secure communications. You must 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.	no

Verify SSL certificate	When enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.	no
Use private key	When enabled, Tenable Vulnerability Management uses private key-based authentication for SSH connections instead of password authentication. If it fails, the password is requested.	no
Use privilege escalation	When enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, 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 Vulnerability Management receiving an unrecognized password prompt on the target host's interactive SSH shell.	no
Targets to prioritize credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	no

13. Do one of the following:

- If you want to save without launching the scan, click **Save**.
- If you want to save and launch the scan immediately, click **Save & Launch**.

> **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

What to do next:

To verify the integration is working:

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

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 your Tenable user interface.
2. In the left navigation, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click the **Create Scan** button.

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

   The scan configuration 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. In the **Select a Credential** menu, select the **Host** drop-down.
10. Select **Windows**.

    The **Settings** pane appears.
11. In the **Auth Type** drop-down box, click **BeyondTrust**.

    The BeyondTrust options appear.
12. Configure each option for the **Windows** authentication.

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 Vulnerability	yes

	Management 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 Vulnerability Management scans. If BeyondTrust changes a password during a scan, the scan fails.	
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Windows target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Domain	(Required if Kerberos Target Authentication is enabled) The Kerberos Domain is the authentication domain, usually noted as the domain name of the target.	yes
Use SSL	When enabled, Tenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.	no

	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	When enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.	no

13. Do one of the following:
    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

      Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

What to do next:

Verify the integration is working.

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

BeyondTrust Auto-Discovery

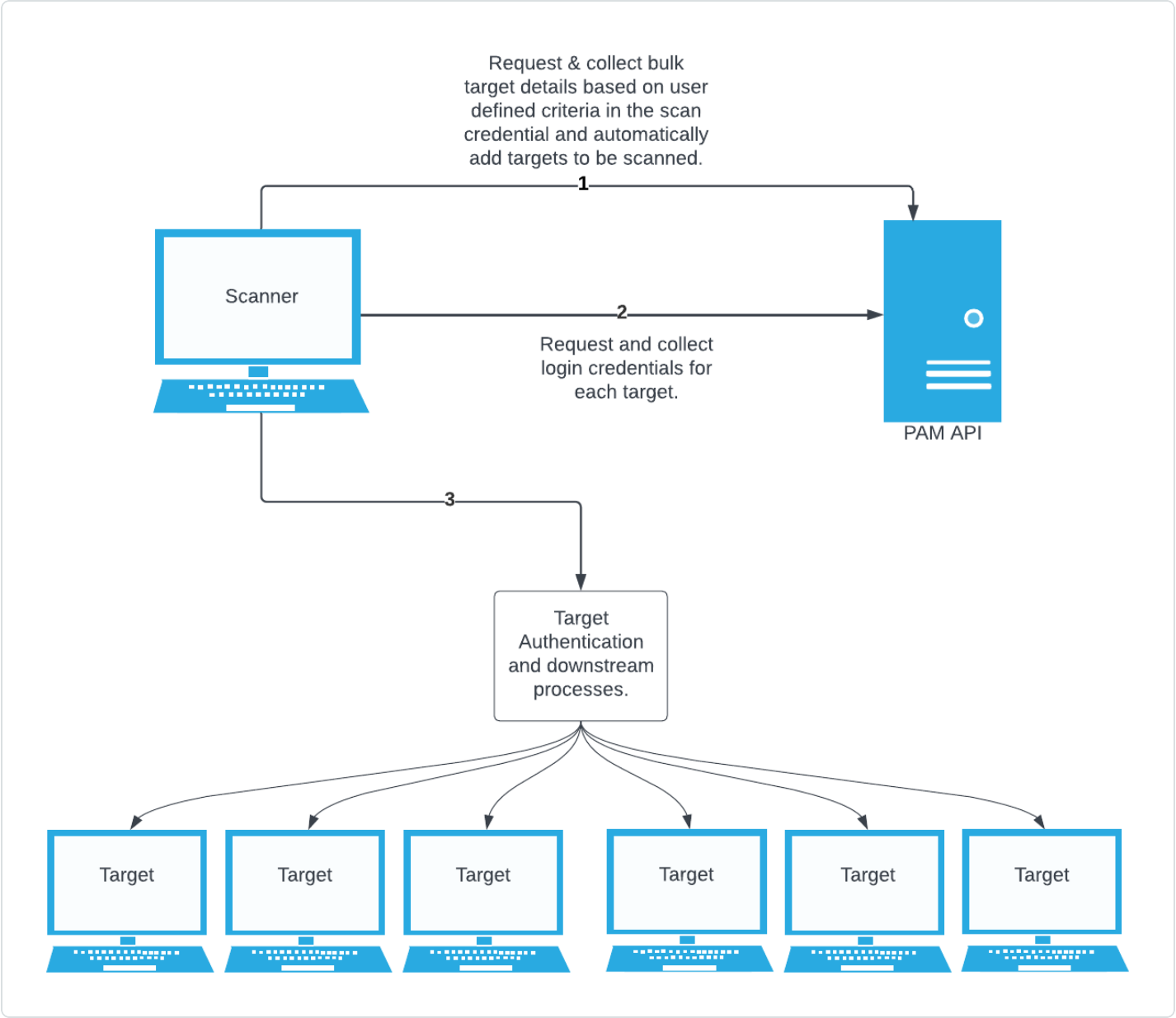
Tenable's BeyondTrust integration provides the Auto-Discovery feature with significant advantages. When using BeyondTrust Auto-Discovery, the scan automatically adds discovered hosts as scan targets with their respective credentials. With the Auto-Discovery feature, there is no need to enter these scan targets in the target list.

Enter one target in the target list. This target can be any pingable IP address or hostname, such as the IP address of the scanner, 127.0.0.1, or the address of one of the intended targets. This initial target kicks off the collection process. You can configure up to five BeyondTrust Auto-Discovery credentials.

The standard BeyondTrust integration requires configuring a scan credential with the name of a specific secret. This secret then functions as the authentication credentials for each of the hosts in the target list. You must enter the target list when you begin configuring the scan. You may also need to configure several different credentials in the scan if the various scan targets use different accounts to authenticate.

In contrast, BeyondTrust Auto-Discovery allows you to enter a search query to collect multiple accounts. It automatically configures these accounts and their respective machines as scan targets with credentials. It associates the scan targets individually with their respective accounts. It is critical that you understand the use of these parameters as they are described in the following sections.

> **Note:** Tenable relies on the presence of an IP address related to a System identified in the collection process. If a system does not have an IP address, Tenable is not be able to perform the Auto-Discovery process on that particular system related account.



Collection

Collect targets and accounts by Systems Pathway

This method gathers targets and accounts associated with multiple Systems in BeyondTrust. The application of this is more for Linux-based systems, as these are typically paired 1:1 between a system and an account. However, this is also an option for Windows and Database types. This is achieved by finding systems of a particular Platform and not of a specific Username.

> **Note:** In order to use the Systems Pathway method, users should never configure a credential with a Username value.

By default, Tenable integrations use the following Platform types when configuring BeyondTrust Auto-Discovery, so you do not need to enter a value. However, if you have configured a custom Platform within BeyondTrust, you can enter the name of the Platform in this field.

- SSH BeyondTrust Auto-Discovery: “linux”
- Windows BeyondTrust Auto-Discovery: “windows”
- Database BeyondTrust Auto-Discovery:
    - Oracle: “oracle”
    - PostgreSQL: “postgresql”
    - MySQL: “mysql”
    - SQL Server: “ms sql server”
    - MongoDB: “mongodb”
    - Sybase ASE: “sybase ase”
    - Cassandra: NOT SUPPORTED!
    - DB2: NOT SUPPORTED!

Cassandra and DB2 do not have supported Platforms in BeyondTrust. However, Tenable does give the user available credentials for the two database types for BeyondTrust Auto-Discovery. BeyondTrust supports the creation of custom Platform plugins, so a user can follow BeyondTrust’s guide to accomplish this. Consult with BeyondTrust and their documentation on this method.

In addition, Tenable has given you the ability to refine their search of System related accounts with the optional Workgroup Name field. Users may choose to organize systems and accounts within their BeyondTrust environment with specific Workgroup Names in order to take better advantage of this refined collection option.

Collect targets and accounts by Account Pathway

In contrast to the Systems Pathway, the Account Pathway relies on the entry of a specific Username in the credential. This method is perfect for multiple systems and accounts that have the same account Username, mostly seen in Windows configurations. This is achieved by you providing a specific account Username. Tenable finds the accounts associated with this username and all related Systems. In addition, Tenable automatically filters accounts by Platform type with the default

options listed above in the Systems Pathway method and we give the user the ability to refine their collection with a Workgroup Name option.

> **Note:** In order to use the Account Pathway method, you must configure a credential with a Username value

Debugging

The initial collection of accounts (except the password and/or ssh private key) is done once and on the arbitrary target/host entered in the target settings of the scan policy mentioned in the beginning of each section (SSH, Windows, and Database). Logs for the collection can be found in the **Debugging Log Reporting** on this particular host in the following logs:

- Database = `pam_database_auto_collect.nbin~BeyondTrust`
- SSH = `pam_ssh_auto_collect.nbin~BeyondTrust`
- Windows = `pam_smb_auto_collect.nbin~BeyondTrust`

Adding targets to the scan automatically

After the initial collection, the integration automatically adds the hosts and necessary knowledge base (KB) entries for an authenticated scan.

Logs from this stage are located in the Debugging Log Report plugin output on this host in the following logs:

- Database = `pam_database_auto_collect.log`
- SSH = `pam_ssh_auto_collect.log`
- Windows = `pam_smb_auto_collect.log`

To automatically add a target to the scan, the integration must collect an account that includes an IPAddress field containing either an IP address or a resolvable hostname. If the account does not have a valid IP address or resolvable hostname, the integration does not add the host to the scan. In this case errors from the function `fqdn_resolv()` trigger the creation of separate detailed logs:

- Database = `pam_database_auto_collect_resolv_func.log`
- SSH = `pam_ssh_auto_collect_resolv_func.log`
- Windows = `pam_smb_auto_collect_resolv_func.log`

Credential collection

After the collection and addition of host and KBs is complete, the authentication process kicks off on each of the hosts. For each host, the integration requests the following target credentials: username, password, SSH private key, private key passphrase, and, if applicable, the elevation command. If requesting an SSH Private Key for a target, simply check the box in the credential for "Use Private Key" and Tenable attempts to gather the ssh key in the same credential enumeration along with the other credential attributes of the host.This is no different (on the host level) than "normal."

- Database = `database_settings.nasl~BeyondTrust`
- SSH = `ssh_settings.nasl~BeyondTrust`
- Windows = `logins.nasl~BeyondTrust`

Privilege Escalation

As with the standard BeyondTrust Integration, the BeyondTrust Auto-Discovery integration supports privilege escalation. Refer to the **Elevation** section of this documentation for more information.

Limitations

It is only possible to use one account per host. If the search collects multiple accounts with the same machine, the first account that the search returns is used. Additionally, the **Debugging Log Report** includes a warning in the collection phase logs. Generally, Tenable recommends configuring scans to collect only a single account per machine to reduce the number of unnecessary requests.

A credential is limited to a single target authentication protocol. BeyondTrust Auto-Discovery is an authentication method of the SSH, Windows, or Database credential, so it is not possible to configure a single credential that collects both SSH and Windows accounts or targets.

Database Auto-Discovery

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

To configure Database auto-discovery for Tenable Vulnerability Management:

1. Log into your Tenable user interface.
2. In the left navigation, click **Scans**.

   The **Scans** page appears.

3. In the upper-right corner of the page, click the ⊕ **Create Scan** button.

   The **Select a Scan Template** page appears.

4. Select a scan template.

   The scan configuration 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 **Settings** 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 **BeyondTrust** Secret Server.

    The BeyondTrust Secret Server options appear.

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

Option	Description	Required
BeyondTrust Host	The IP or domain name of the BeyondTrust Web Server.	Yes
BeyondTrust Port	The port for the BeyondTrust Web Server. For example, 443.	Yes
BeyondTrust API user	The API user name associated with the API Key used for API authentication.	Yes
BeyondTrust API key	The API Key associated with the API user name used for API authentication.	Yes

Option	Description	Required
Use SSL	Enable if BeyondTrust is configured to support SSL.	No
Verify SSL Certificate	If enabled, verifies the SSL Certificate on the BeyondTrust server.	No
Username	The username for the target account.	No
Domain	The domain name of the target account.	No
Platform	Platform Name or Platform ID. Defaults to the following if left blank: • Oracle: “oracle” • PostgreSQL: “postgresql” • MySQL: “mysql” • SQL Server: “ms sql server” • MongoDB: “mongodb” • Sybase ASE: “sybase ase” • Cassandra: NOT SUPPORTED! • DB2: NOT SUPPORTED! **Note:** Cassandra and DB2 do not have supported Platforms in BeyondTrust. However, Tenable does give the user available credentials for the two database types for BeyondTrust Auto-Discovery. BeyondTrust supports the creation of custom Platform plugins, so a user can follow BeyondTrust’s guide to accomplish this. Consult with BeyondTrust and their documentation on this method.	No
Workgroup Name	Name of Workgroup in BeyondTrust. Used to isolate groups of managed systems and accounts.	No
Database Port	The port the database instance is listening on.	Yes

13. Do one of the following:

- If you want to save without launching the scan, click **Save**.
- If you want to save and launch the scan immediately, click **Save & Launch**.

  > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

SSH Auto-Discovery

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

To configure SSH auto-discovery for Tenable Vulnerability Management or Tenable Nessus:

1. Log in to your Tenable user interface.
2. In the left navigation, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click the **Create Scan** button.

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

   The scan configuration 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. In the **Select a Credential** menu, select the **Host** drop-down.

   The **Host** options appears.
10. Select **SSH**.

    The **Settings** pane appears.

11. In the **Auth Type** drop-down box, click **Tenable for Delinea Secret Server**.

    The **Tenable for Delinea Secret Server** options appear.

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

Option	Description	Required
BeyondTrust Host	The IP or domain name of the BeyondTrust Web Server.	Yes
BeyondTrust Port	The port for the BeyondTrust Web Server. For example, 443.	Yes
BeyondTrust API user	The API user name associated with the API Key used for API authentication.	Yes
BeyondTrust API key	The API Key associated with the API user name used for API authentication.	Yes
Use SSL	Enable if BeyondTrust is configured to support SSL.	No
Verify SSL Certificate	If enabled, verifies the SSL Certificate on the BeyondTrust server.	No
Username	The username for the target account.	No
Domain	The domain name of the target account.	No
Platform	Platform Name or Platform ID. Defaults to **Linux** if left blank.	No
Workgroup Name	Name of Workgroup in BeyondTrust. Used to isolate groups of managed systems and accounts.	No
Use Private Key	Select this to retrieve the SSH key for target authentication.	Yes
Use privilege escalation	Enable to use BeyondTrust privilege escalation. If enabled, Tenable uses the elevation command configured for the account in BeyondTrust.	Yes

13. Do one of the following:

- If you want to save without launching the scan, click **Save**.
- If you want to save and launch the scan immediately, click **Save & Launch**.

> **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Windows Auto-Discovery

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

To configure Windows auto-discovery for Tenable Vulnerability Management or Tenable Nessus:

1. Log in to your Tenable user interface.
2. In the left navigation, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click the **Create Scan** button.

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

   The scan configuration page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, enter an initial target in the target list. (This is arbitrary and only used to start the initial collection.) Valid options include the IP address of the scanner or the address of just one of the intended targets.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   The **Credentials** pane appears.
9. In the **Select a Credential** menu, select the **Host** drop-down.
10. Select **Windows**.

The **Settings** pane appears.

11. In the **Auth Type** drop-down box, click **BeyondTrust** Secret Server.

    The BeyondTrust Secret Server options appear.

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

Option	Description	Required
BeyondTrust Host	The IP or domain name of the BeyondTrust Web Server.	Yes
BeyondTrust Port	The port for the BeyondTrust Web Server. For example, 443.	Yes
BeyondTrust API user	The API user name associated with the API Key used for API authentication.	Yes
BeyondTrust API key	The API Key associated with the API user name used for API authentication.	Yes
Use SSL	Enable if BeyondTrust is configured to support SSL.	No
Verify SSL Certificate	If enabled, verifies the SSL Certificate on the BeyondTrust server.	No
Username	The username for the target account.	No
Domain	The domain name of the target account.	No
Platform	Platform Name or Platform ID. Defaults to **Windows** if left blank.	No
Workgroup Name	Name of Workgroup in BeyondTrust. Used to isolate groups of managed systems and accounts.	No

13. Do one of the following:

    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

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**.

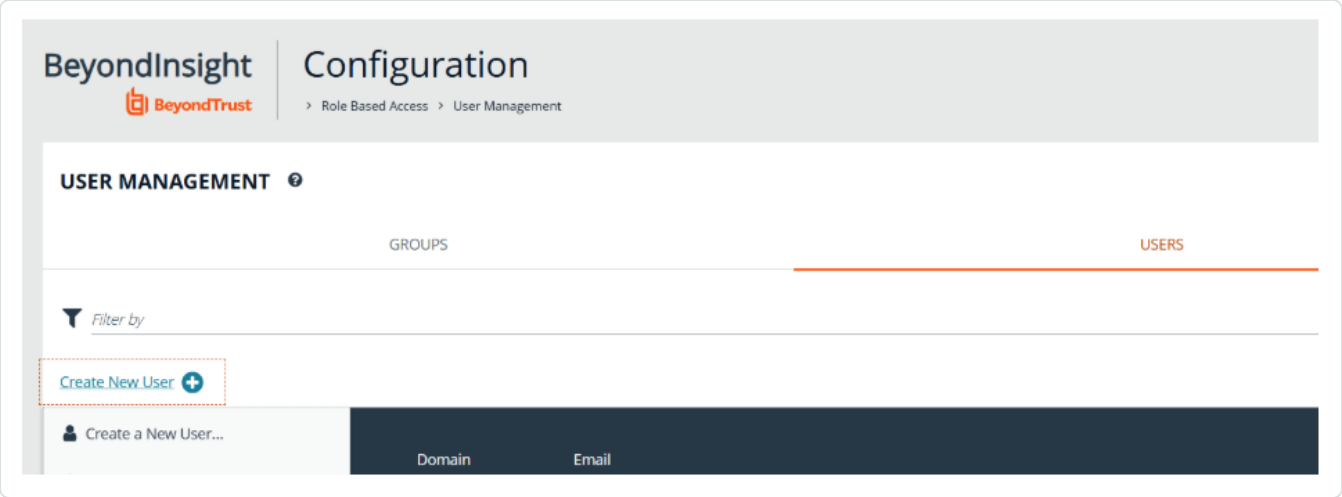
Once saved, the API Key is available for future requests.

API Account and Group

The following steps help you to configure an API account and group.

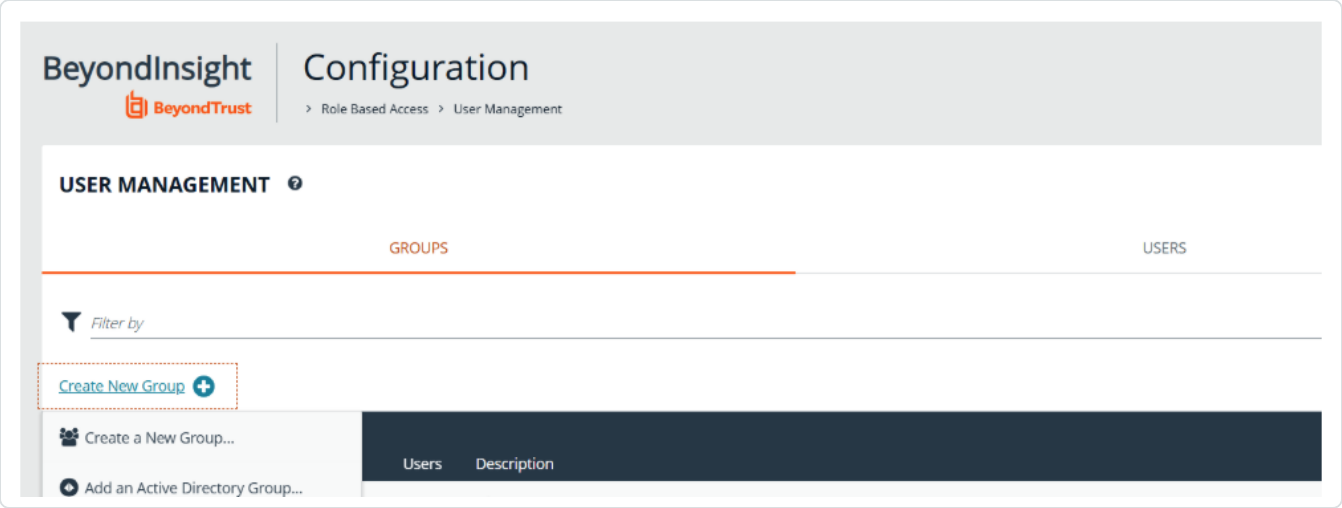
To create a new **local account**, or use an existing one:

1. Navigate to **Configuration > User Management**.
2. Click the **Users** tab.
3. Click **Create New User**.

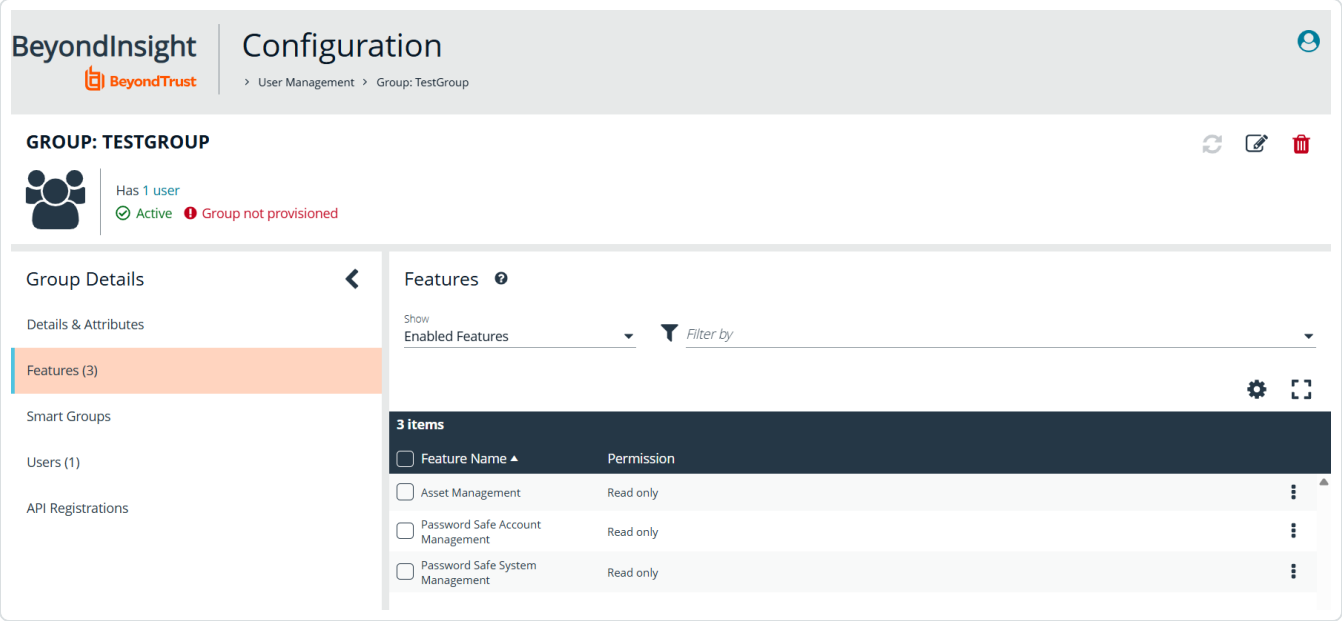


To create a new **group**, or use an existing one:

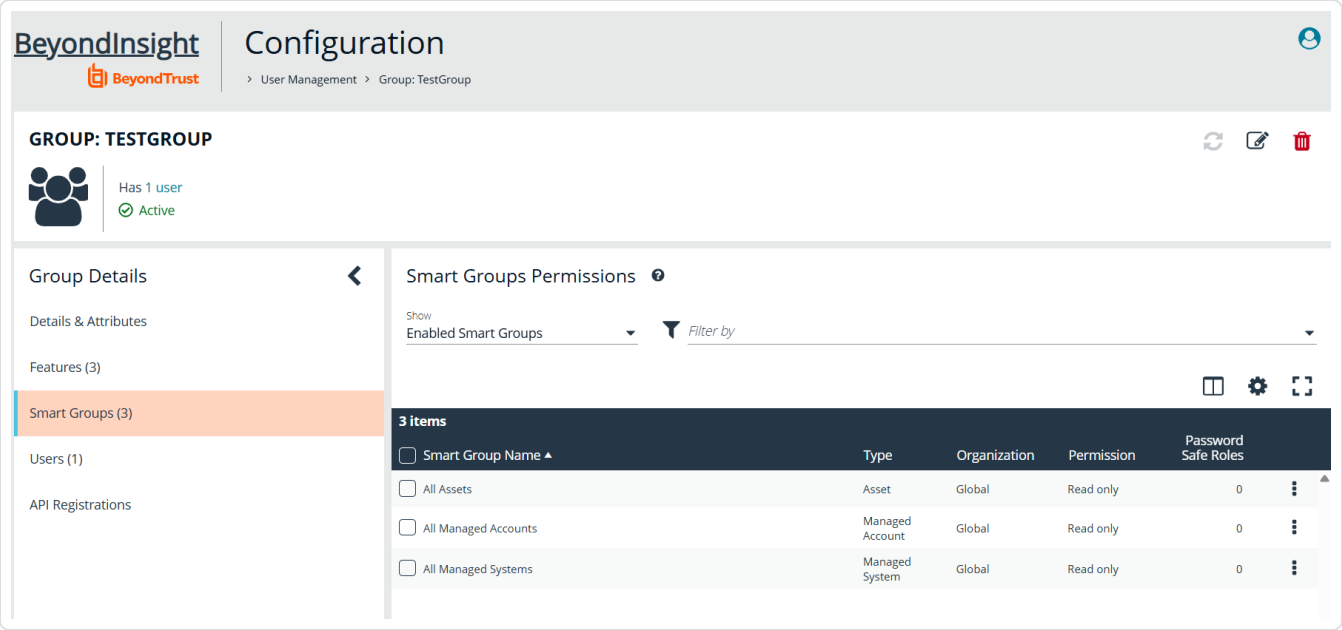
1. Navigate to **Configuration > User Management**.
2. Click the **Group** tab.
3. Click **Groups**.
4. Select **Create New Group**.



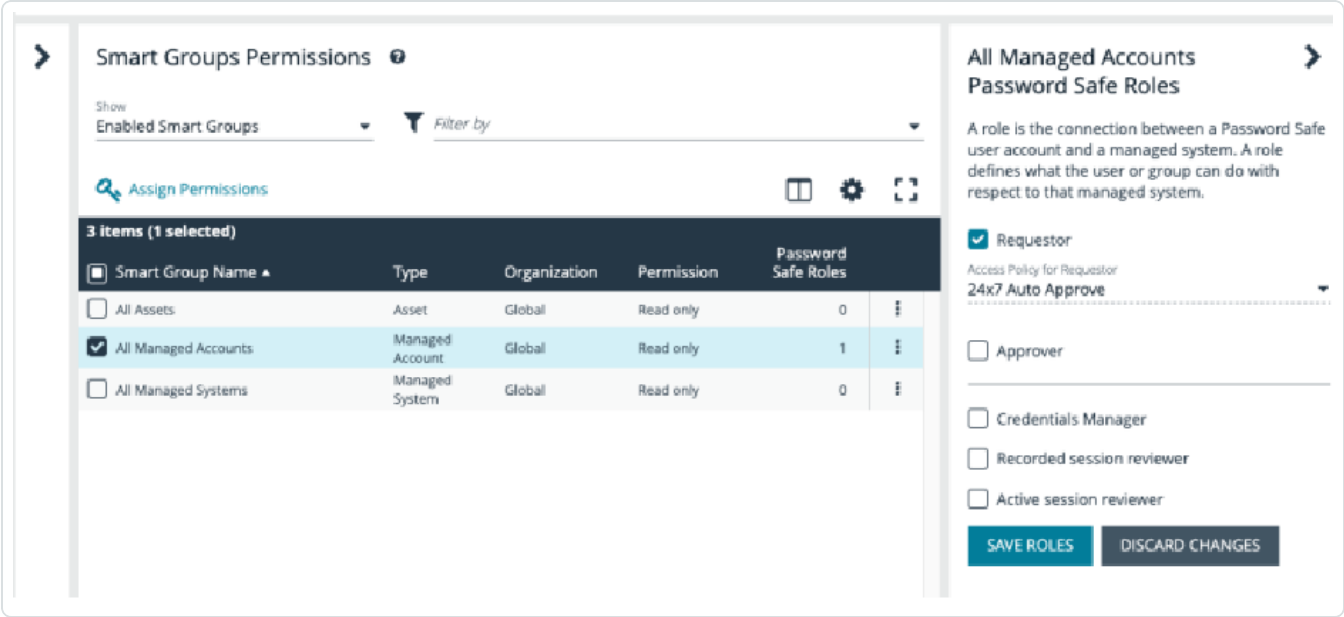
5. Provide the group name, and ensure the following features are enabled as read only:



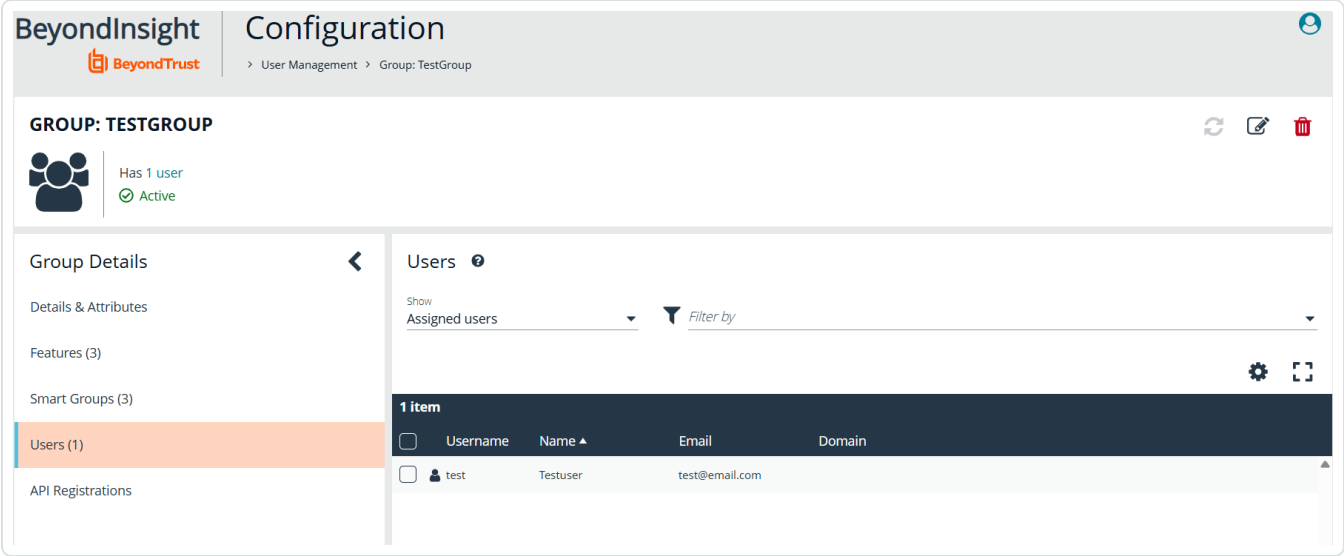
6. For Smart Groups, ensure the following are enabled with read only permission:



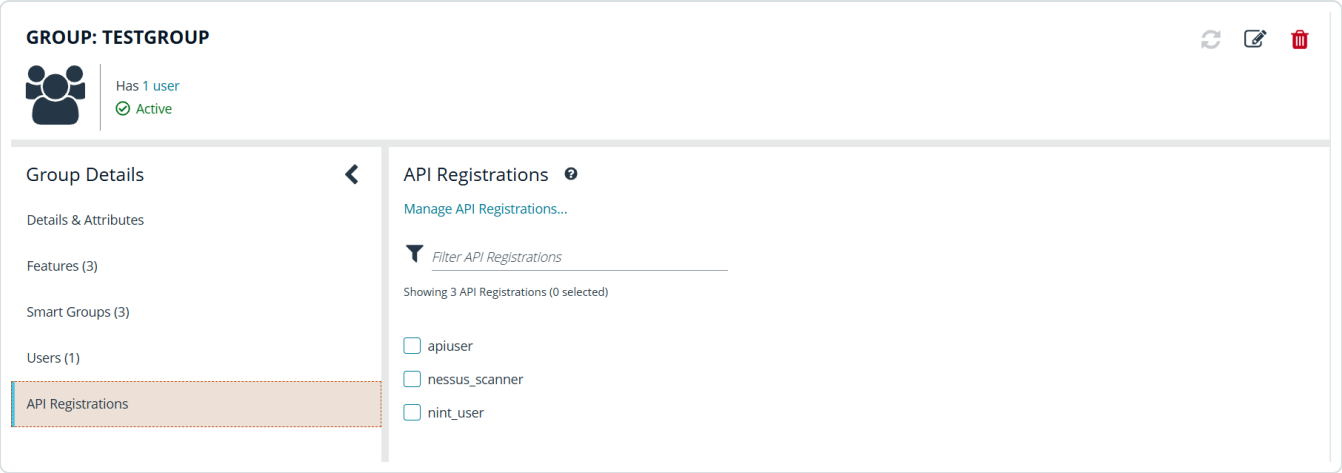
7. For **All Managed Accounts**, click on the ellipses to the right and select **Edit Password Safe Roles**.
8. Select **Requestor** and select an Access Policy that applies to the managed account that is used for the scan.



9. Ensure the API user you created in the previous step is added to the group.



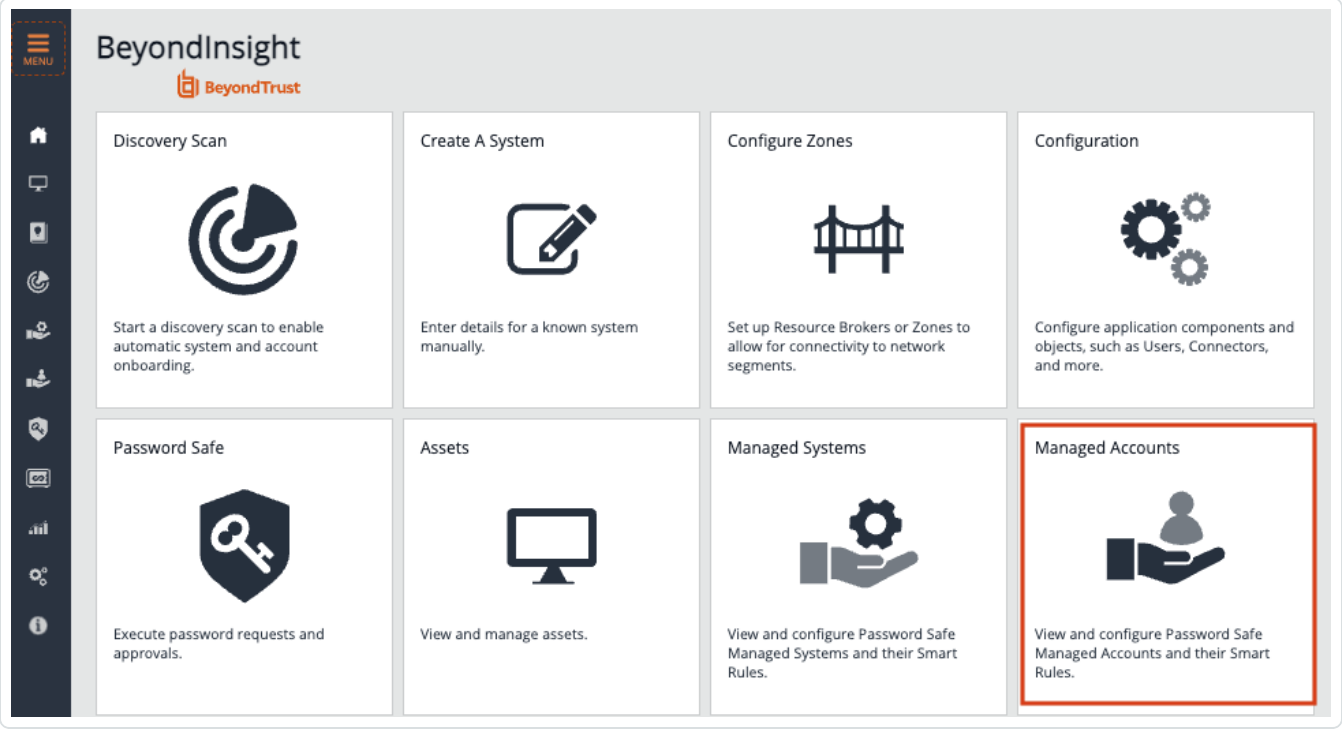
10. Finally, assign the API that was registered for this integration to this group.



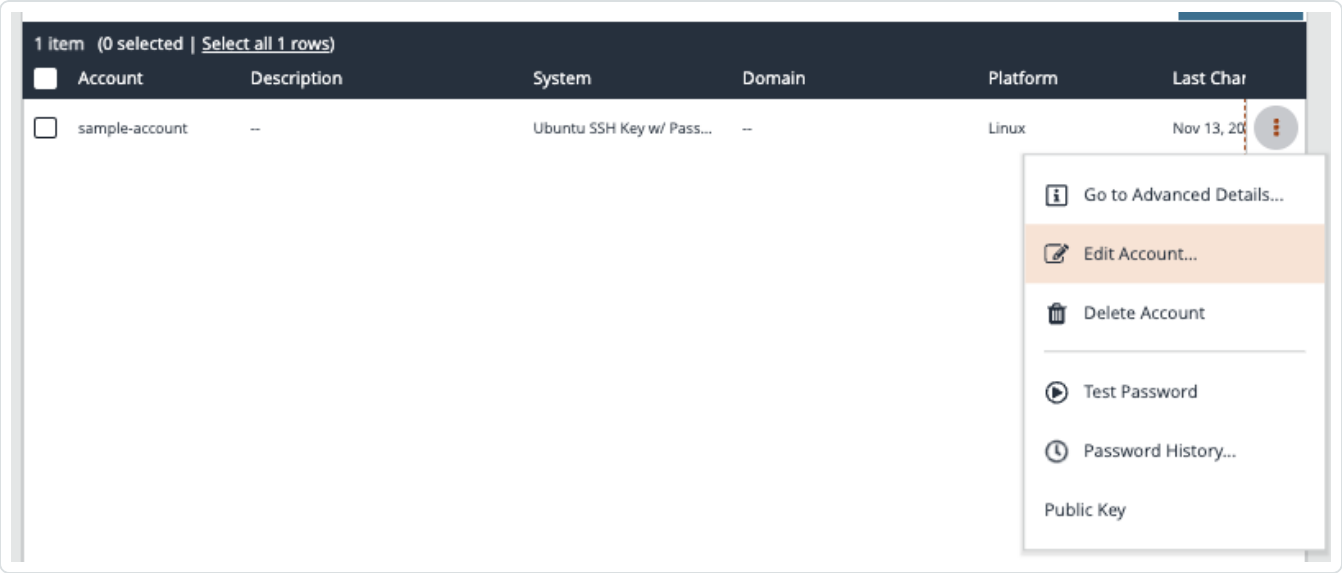
Enable API Access

To enable API access:

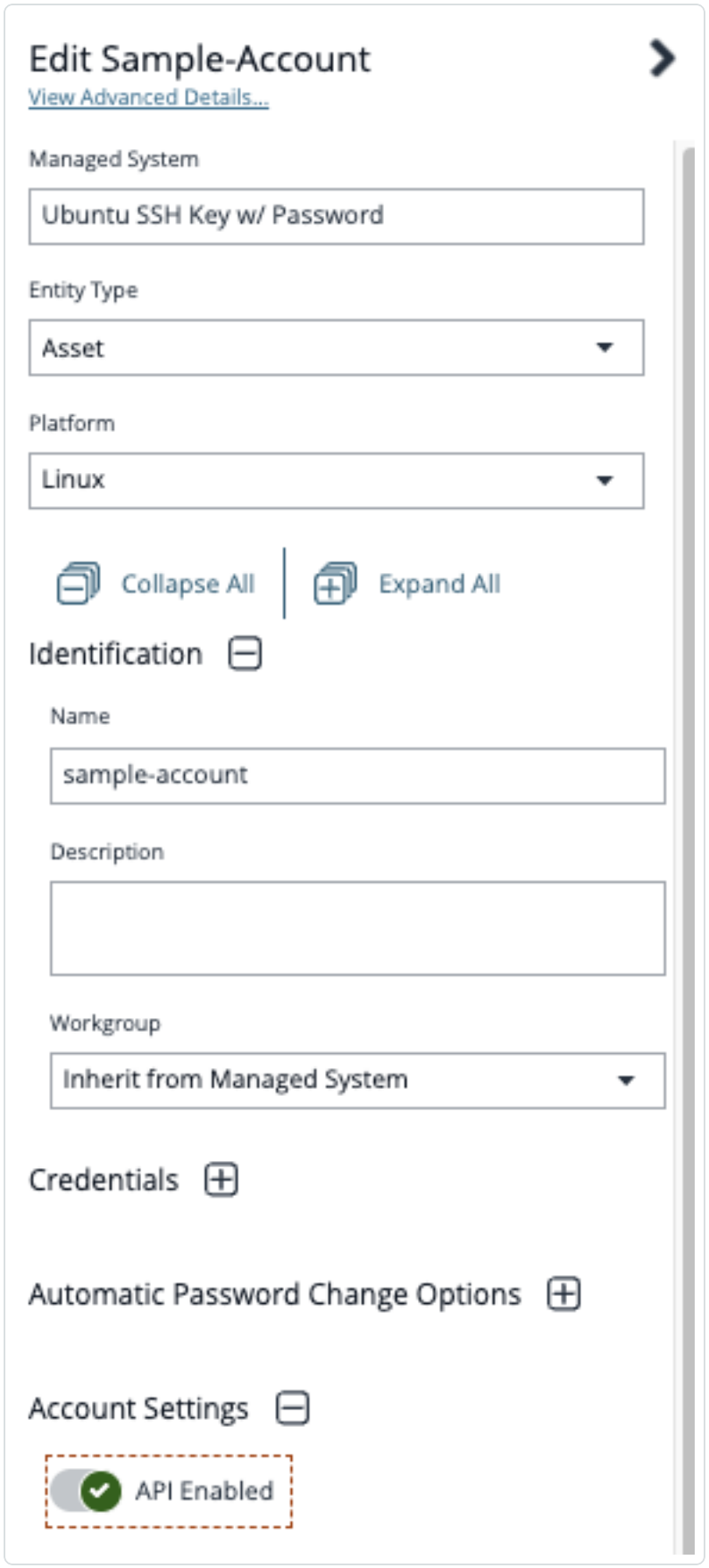
1. Log in to BeyondInsight.
2. Go to **Managed Accounts**.



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 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**.
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 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.